1. Úvod: logika, matematika, množiny

Vědci a inženýři se již několik set let obracejí na matematiku kvůli její spolehlivosti. Například vzorec pro kořeny kvadratické rovnice funguje zcela univerzálně, není rovnice, pro kterou by dal špatnou odpověď (pokud chybu neuděláme my při výpočtu). Tato spolehlivost závisí na dvou věcech.

Jedna z nich je přesnost ve vyjadřování. Matematický jazyk je speciálně navržen tak, aby nám umožňoval se jednoznačně vyjádřit. Výraznou složkou tohoto jazyka je používání množinového zápisu. Pro správné používání matematického jazyka je také zásadní znát dobře praktickou logiku. V první části si připomeneme její základy, které již mnozí čtenáři jistě znají. Podíváme se také na praktické dopady logických pravidel (1a.3) a představíme predikátovou logiku (1a.4).

V druhé části 1b této kapitoly se zaměříme na matematiku jako jazyk, jeho čtení a porozumění a také jak jej psát.

Druhým zdrojem spolehlivosti matematiky je to, že všechna svá tvrzení dokazuje. To je proces, který kombinováním již známých faktů ověří, že se nové tvrzení opravdu nemůže nikdy pokazit. Toto kombinování je potřeba dělat způsobem, který je hodnověrný a zaručí, že naše úvahy nepovedou od pravdivého k nepravdivému. Pokud se chce student věnovat matematice hlouběji, musí umět takovéto argumenty číst a chápat, později i psát.

Na tento klíčový proces se podíváme v třetí části 1c. Protože jde o věc, která bývá pro studenta pronikajícího do tajů matematiky jako vědy to nejtěžší, rozpovídáme se víc, než bývá v knihách obvyklé. Je pravděpodobné, že student mnohé při prvním čtení zcela nedocení, takže není špatný nápad se k této části (a k části 1b) vracet poté, co se v následujících kapitolách trochu více osmělí v matematice. Čtenář, který se jen snaží naučit postupy diskrétní matematiky a nečeká se od něj psaní důkazů, tuto část nebude potřebovat, ale jistě mu nezaškodí, když se tam ze zvědavosti podívá.

Nově nabyté zkušenosti si pak čtenář může procvičit v části poslední, kde si projdeme základní znalosti o množinách pořádným matematickým způsobem, tedy s formálními tvrzeními a důkazy.

Teď si jen stručně zopakujme základní množinové pojmy, které potřebujeme pro práci v knize.

Množiny tradičně značíme velkými písmeny anglické abecedy a jejich prvky malými, pokud je to rozumně možné. Značení $a \in A$ znamená, že objekt a je prvkem množiny A, naopak $a \notin A$ znamená, že objekt a není prvkem množiny A. Značení $A = B$ znamená, že jde o shodné množiny.

→ První drobná poučná poznámka: Proč jsme tam napsali „pokud je to rozumně možné“? Může se stát, že toto pravidlo dodržet nejde. Když například máme množiny $A = \{1, 2\}$ a $B = \{13, 23\}$, tak z nich můžeme vytvořit další množinu: $M = \big\{\{1, 2\}, \{13, 23\}\big\}$. Množina M má tedy dva prvky, A a B, což jsou také množiny, takže ← ať už je označíme malými či velkými písmeny, tak se proviníme proti oné citované zásadě.

Čtenář jistě zná prázdnou množinu čili množinu bez prvků, $\emptyset = \{\}$, ale obvykle spíše pracujeme s těmi neprázdnými. Množiny je možné zadat různými způsoby. Jeden populární způsob je výčtem prvků, třeba $M = \{1, 13, a, \diamond\}$. Druhý způsob se anglicky jmenuje „set builder“ a funguje tak, že se nejprve odvoláme na nějakou větší známou množinu (universum) a pak uvedeme, které prvky z tohoto universa patří do naší množiny. Například množina všech sudých přirozených čísel se zapíše $M = \{x \in \mathbb{N} : x \text{ sudé}\}$.

Čímž se dostáváme k nejznámějším universům, což jsou

- přirozená čísla $\mathbb{N} = \{1, 2, 3, \dots\}$; (natural numbers)
- celá čísla $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, \dots\}$; (integers)
- racionální čísla $\mathbb{Q} = \big\{\frac{p}{q} : p \in \mathbb{Z} \wedge q \in \mathbb{N}\big\}$; (rational numbers)
- reálná čísla $\mathbb{R}$. (real numbers)

V diskrétní matematice nás budou zajímat zejména přirozená a celá čísla.

Používají se i různé modifikátory:

- malé plus či mínus omezuje znaménko, třeba $\mathbb{Z}^+ = \{n \in \mathbb{Z} : n > 0\} = \mathbb{N}$ či $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$ nebo naopak $\mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}$;
- malá nula přidá nulu, třeba $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ nebo $\mathbb{R}_0^+ = \{x \in \mathbb{R} : x \geq 0\}$.

Zde je třeba varovat, že tato modifikační značení nejsou přijímaná úplně všemi, jsou i značení konkurenční, takže se zejména těm plusům a mínusům budeme snažit vyhýbat, množina $\mathbb{N}_0$ nám ovšem přijde často vhod.

Budeme také předpokládat, že čtenář zná základní množinové operace, tedy sjednocení, průnik, rozdíl a Kartézský součin. Zájemci o bližší pohled na množiny si mohou přečíst část 1d.

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. Zde je přiblížíme pro ty, kteří se s formální logikou ještě nesetkali, ale hlouběji nepůjdeme. Na této základní úrovni nejde o nic těžkého, je to vlastně selský rozum destilovaný do formulek.

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. 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), 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 (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, od výroků požadujeme, aby tam, kde je používáme (třeba v našem světě), měly jasně dánu pravdivostní hodnotu.

Toto pro změnu výroky nejsou: „ahoj“, „31“, „pavlač“, „beze mne“, „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.

→ Popravdě řečeno, ani teď to ještě není výrok, musíme se ještě domluvit, čím vlastně začíná déšť. Je jediná kapka déšť? To je trochu problém s aplikací logiky na skutečný život, kde je často mezi bílou a černou ještě „šedá zóna“. Chceme-li logiku aplikovat, musíme se vždy rozhodnout, kde přesně je hranice mezi ano a ne. V ← rámci přehlednosti zde do toho nebudeme moc rýpat, příklady „ze života“ jsou tu stejně jen jako ilustrace.

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) 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, 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, jak vlastně výroky spojujeme.

1a.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 a logickými spojkami, čímž vznikají výroky nové. 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.

• **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. „$p \to q$“ 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.

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, 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.

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. Formální zdůvodnění uvidíme níže (1a.3).

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 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 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 s výrokem $\neg p \vee q$. Všimněte si, že má v tabulce přesně stejné pravdivostní hodnoty jako implikace $p \Longrightarrow q$. To znamená, že z pohledu logiky jsou tyto dva výrazy naprosto rovnocenné a můžeme je

zaměňovat dle libosti, třeba „jestliže je pátek, tak je třináctého“ má stejnou pravdivost jako „není pátek nebo je třináctého“. V praxi je většinou forma $p \implies q$ 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.

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.

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 $\models\!\!\!\models$. Naše pozorování by se tedy zapsala takto:

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

Mnozí lidé, kteří logiku jen používají jako nástroj, namísto $\equiv$ píšou prostě rovnítko. Je to do značné míry přirozené (jde o logickou rovnost významů) a navíc se tento vztah silně podobá rovnosti algebraické, například je možné upravovat logické výrazy pomocí logických ekvivalencí postupně více navazujícími kroky úplně stejně, jako když upravujeme algebraické výrazy pomocí algebraických pravidel. My se zde ale budeme držet správného značení, jednak abychom byli přesní a taky proto, že budeme logiku používat v matematice a míchat v jednom výrazu „rovnítko“ logické a rovnítko algebraické není nejlepší nápad.

Jedno zjednodušení ale přijmeme, abychom ušetřili závorky, budeme automaticky předpokládat, že značka $\equiv$ ukončuje a začíná závorku.

1a.2 Pravidla

Začneme tím nejjednodušším.

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

Většina se dá rozmyslet selským rozumem. Vztahy v prvním sloupci ukazují, že zdvojováním výroků ani zdvojením negace nic nezískáme. Druhý sloupec jsme již potkali (prší a/nebo neprší). Další dva sloupce 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 jejich konjunkce závisí čistě na pravdivosti p. Takovéto identity se občas hodí při úvahách.

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 je v takovém rozmýšlení trénovaný. Podívejme se na další vlastnosti logických spojek:

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

Odborně řečeno, první odrážka ukazuje komutativitu spojek, druhá zase asociativitu a třetí ukazuje distributivní zákon. Tím prvním sloupcem 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 (a vyhodnotit) dle libosti.

Asociativní je i ekvivalence, takže má smysl psát výrazy jako $p \iff q \iff r$.

Distributivní zákon student také dobře zná. Pokud si představí místo $\wedge$ násobení a místo $\vee$ sčítání (což tak mimochodem opravdu funguje z pohledu binárního kódu), tak první rovnost třetí odrážky je vlastně jen roznásobením závorky. Druhá rovnost pak ukazuje, že u logiky se dá roznásobovat i v opačném umístění operací, což pro sčítání a násobení rozhodně neplatí.

Při této příležitosti stojí za zmínku, že implikace v seznamu chybí, není totiž ani komutativní (zásadní dopad uvidíme níže), ani asociativní, výraz typu $p \implies q \implies r$ tedy nemá smysl. 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 $16 : (4 : 2) = 8$. Na problém řetězení implikací ještě narazíme při důkazech.

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. Úplně stejnou věc lze říct o 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** 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 výraz ze vzorce.

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:

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

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.

1a.3 Logika v aplikacích

Logika se rozvíjela zároveň s rozvojem filosofie coby zárodku všech věd již u antických Řeků a prvního výrazného vrcholu dosáhla za středověku. V té době šlo o pravidla správného vedení úvah (a varování, že některé pokusy správné nejsou), která se předávala ve formě vzorových příkladů. O pár set let později pak formální logika nabídla jazyk k zachycení tohoto „rozmýšlení o přemýšlení“. Abychom si ukázali praktické dopady jejích závěrů, vrátíme se ke středověké myšlence příkladů.

Rozebereme si, co se dá (a nedá) dělat s implikací, což je pro matematiku (a logiku) spojka klíčová. Použijeme výrok V: „jestliže je dnes 29. února, pak je rok dělitelný čtyřmi“. Tvrdíme, že v rámci našeho světa je pravdivý. A opravdu, pokud dnes 29. února není, pak je celá implikace pravdivá (viz řádky v tabulce začínající nulou), a pokud 29. února je, pak už z pravidel pro tvorbu kalendáře vyplývá, že rok je dělitelný čtyřkou. Jinak řečeno, onen řádek z pravdivostní tabulky, ve které má implikace nulu, nemůže v našem světě reálně nastat.

Krásně tady mimochodem vidíme, že pravdivost výroků je vždy myšlena vzhledem ke konkrétnímu světu pravidel, v jiných kulturních okruzích už tato implikace pravdivá být nemusí. Nás v této knize bude zajímat pravivost výroků (nejčastěji implikací) ve světě matematiky. Podrobněji o tomto pojednáme v části 4c.15 o axiomech.

Stojí za zmínku, že i když teď víme, že výrok V je vždy pravdivý, tak vlastně nevíme nic konkrétního o dnech a rocích. To u implikace není cílem, ona nemá říct něco určitého o jednotlivých složkách, ale vyjadřuje se k jejich vzájemnému vztahu. Použít se to pak dá třeba takto:

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

Ve středověku tomu říkali „modus ponens“ a je to asi nejpřirozenější typ úvahy.

V praxi se to používá zejména v situacích, kdy nás zajímá pravdivost tvrzení q, ale do jeho zkoumání se nám nechce. Implikace $p \implies q$ nám umožňuje potvrdit pravdivost q tím, že ukážeme pravdivost p, což je doufejme příjemnější.

Tento vztah se často vyjadřuje slovy, že „p je **postačující podmínka** pro q“. Toto je z pohledu logiky stejné, jako říct, že implikace $p \implies q$ je pravdivá, jde o ekvivalentní vyjádření.

Než se posuneme dále, zmíníme se o zápisu. Tento typ úvahy zjevně funguje se všemi implikacemi a logika to bude chtít nějak vyjádřit. Středověká logika to svým studentům sdělovala příkladem, tak jako my výše, a v diskusi se pak na to odvolávali jménem: Podle modus ponens platí, že ...

Po zavedení symbolů je možné platnost této úvahy vyjádřit například slovy, že výrok

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

je vždy pravdivý. To se snadno ověří pravdivostní tabulkou. Tato forma ale stírá rozdíl mezi vstupními daty (ta první implikace) a procesem (ta hlavní implikace). V logice existuje speciální téma zvané odvozování, které dělá přesně to, co jméno napovídá: Studuje procesy, kterými lze z určité dané množiny faktů dospět zaručeně správně k jiné. Mají na to speciální značku a modus ponens se tam zapíše následovně:

$$\{p \implies q, p\} \models q$$

Zde se tím nebudeme zabývat, je to jen upozornění pro čtenáře, že by se na to mohl podívat (pokud jej to zaujalo). Pro doplnění dodejme, že zejména v anglosaské literatuře bývá obvyklé jakési „sčítací“ schéma

$$\begin{array}{l} p \Longrightarrow q \\ \underline{\quad p \quad} \\ \therefore\ q \end{array}$$

Vraťme se k situaci, že chceme znát něco o q, ale místo toho raději zkoumáme p. Co když se ukáže, že p není pravdivé? Pak máme smůlu a o q nevíme nic. Krásně to ukazuje náš příklad.

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

Je zjevné, že v dané situaci rok dělitelný čtyřkou být může i nemusí. To je typický a podstatný rys implikace. Dalo by se říct, že posouvá informaci od p ke q, ale jen informaci jednoho typu, jmenovitě pravdivost. Je to tedy nástroj nedokonalý a tato nespolehlivost dokáže někdy docela potrápit.

S tím blízce souvisí to, že pravdivost spolehlivě přechází jen jedním směrem, nedá se to obrátit.

- Platí: Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi.
- 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).

Z pravdivosti závěru tedy nevyplývá nutně pravdivost předpokladu, směr v implikaci nelze obecně obracet.

Formálně vzato, pravdivost implikace $p \Longrightarrow q$ nám nedovoluje automaticky získat informaci o pravdivosti implikace $q \Longrightarrow p$, obecně to jsou dvě nezávislá tvrzení.

Viděli jsme, že ten 29. únor neumíme pomocí roku vynutit, ale jistá souvislost tam přeci jen je.

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

Za středověku tomuto typu úvahy říkali „modus tollens“. Dá se na to dívat dvěma užitečnými způsoby.

Jednak vidíme, že pokud máme implikaci $p \Longrightarrow q$ a zajímá nás p, tak nám sice q nedovolí p potvrdit (tedy q není postačující podmínkou pro p, to už jsme viděli výše), ale dokáže pravdivost p vyloučit. Jinými slovy, pokud chceme, aby p platilo, tak je nutné mít q pravdivé, bez toho to nejde.

Vyjadřujeme to slovy „q je **nutná podmínka** pro p“ a opět jde o rovnocenné vyjádření faktu, že implikace $p \Longrightarrow q$ platí.

Za druhé vidíme, že pravdivá implikace $p \Longrightarrow q$ nám přeci jen umožňuje přesouvat informaci zprava doleva, jmenovitě informaci o nepravdě. 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 $p \Longrightarrow q$, pak se definuje její **obměna** jako $\neg q \Longrightarrow \neg p$. 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.

Příklad 1a.a: 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“ neboli „být přes 18 je nutné k tomu, aby mi bylo přes 21“. 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. Nabízí se tedy alternativní vyjádření „jestliže mohu pít, tak mohu i řídit“, což zní podezřele, raději si další úvahy v tomto směru odpustíme.
△

Vraťme se k otázce, zda lze pravdivou implikaci otočit. Viděli jsme, že obecně ne, ale v některých konkrétních případech i otočením získáme pravdivou implikaci. Máme pak dva pravdivé výroky $p \Longrightarrow q$ a $q \Longrightarrow p$, tedy pravdivost přechází v obou směrech. Pokud u obou implikací přejdeme k obměnám, tak opět dostáváme pravdivé výroky, jmenovitě $\neg q \Longrightarrow \neg p$ a $\neg p \Longrightarrow \neg q$, takže i informace o nepravdivosti přechází oběma směry.

Situace s pravdivou oboustrannou implikací tedy znamená, že výroky p a q nutně mají stejnou pravdivost, jinými slovy vlastně máme vztah ekvivalence $p \Longleftrightarrow q$.

To znamená, že v případě pravdivé ekvivalence je p nutnou i postačující podmínkou pro q a naopak, ekvivalence je již z podstaty symetrická. Ekvivalence máme v matematice velmi rádi, jsou ale vzácné.

1a.4 Predikátová logika

Většina výroků zkoumaných v praxi má v sobě zabudovány parametry. Třeba 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 $x = 23$ platí $x > 13$“ je pravdivý, výrok „pro $x = 3$ platí $x > 13$“ 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. Některé výroky platí 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“. Tento zápis (kterého se v této knize budeme držet) bohužel není standardní, není to jednotné. 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, viz třeba Fakt 1d.2), 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 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 1a.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 $y = -\frac{1}{2}x$, takže máme na výběr, pro platnost výroku je důležité mít alespoň jedno. 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. Příklad pravdivého výroku tohoto typu: $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon\ (|x|+1)^y = 1$. 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:

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

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 1a.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:

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

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 1a.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: $x = 3 \wedge \big[\exists y \in \mathbb{R}\colon\ y > x\big]$.

1a.5 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, vůbec se v tomto čísle i 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 $\forall h \in \mathbb{R}\colon\ h \geq 0$. 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. Uvidíme to hned v prvním pořádném důkazu části 1c

△

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.

Na to, jak se logika v matematice opravdu používá, se blíže podíváme ve zbytku kapitoly, 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) $\forall x \in \mathbb{R}$: $[x \geq 3 \vee x < 5]$;
(ii) $\exists x \in \mathbb{R}$: $[x \geq 3 \wedge x < 0]$;
(iii) $\forall x \in \mathbb{Z}$: $[x > 3 \wedge x < 7]$;
(iv) $\exists x \in \mathbb{Z}$: $[x \geq 3 \wedge x < 5]$;
(v) $\forall x \in \mathbb{R}$: $[x > 3 \implies x^2 > 9]$;
(vi) $\forall x \in \mathbb{R}$: $[x^2 > 9 \implies x > 3]$;
(vii) $\forall x \in \mathbb{R}$: $[x^2 < 0 \implies x = 13]$;
(viii) $\exists x \in \mathbb{R}$: $[x \geq 5 \implies x^2 = 40]$;
(ix) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}$: $x + y = 0$;
(x) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}$: $x + y = 0$;
(xi) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}$: $x \cdot y = 0$;
(xii) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}$: $x \cdot y = 0$;
(xiii) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}$: $\frac{x}{y} = 1$;
(xiv) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}$: $\frac{x}{y} = 1$;
(xv) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}$: $x < 3y$;
(xvi) $\exists y \in \mathbb{Z}\, \exists x \in \mathbb{Z}$: $x^2 - y^2 = 3$.

Cvičení 1a.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.
(i) Matematici nejsou normální.
(ii) Matematici jsou větší borci než nematematici.
(iii) Pokud Lojza není normální, tak už nikdo.
(iv) Je jen jeden matematik.
(v) Nikdy není jen jeden matematik.
(vi) Jsou dva matematici.
(vii) Lojza je největší borec.
(viii) I matematik může být normální.
(ix) Jedině matematici můžou být normální.
(x) Lojza s Pepou jsou buď oba normální, nebo oba nenormální.

Cvičení 1a.3: 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) $x < 13 \wedge [x^2 < 4 \vee x > 14]$;
(iii) $[\sin(x) < x^3 \wedge x < 3] \vee [\sin(x) < x^3 \wedge x > 1]$.

Cvičení 1a.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.
(i) $\forall x \in M$: $[p(x) \wedge q(x)] \equiv [\forall x \in M$: $p(x)] \wedge [\forall x \in M$: $q(x)]$;
(ii) $\forall x \in M$: $[p(x) \vee q(x)] \equiv [\forall x \in M$: $p(x)] \vee [\forall x \in M$: $q(x)]$;
(iii) $\exists x \in M$: $[p(x) \wedge q(x)] \equiv [\exists x \in M$: $p(x)] \wedge [\exists x \in M$: $q(x)]$;
(iv) $\exists x \in M$: $[p(x) \vee q(x)] \equiv [\exists x \in M$: $p(x)] \vee [\exists x \in M$: $q(x)]$;
(v) $p \wedge [\forall x \in M$: $q(x)] \equiv \forall x \in M$: $[p \wedge q(x)]$;
(vi) $p \vee [\forall x \in M$: $q(x)] \equiv \forall x \in M$: $[p \vee q(x)]$;
(vii) $p \wedge [\exists x \in M$: $q(x)] \equiv \exists x \in M$: $[p \wedge q(x)]$;
(viii) $p \vee [\exists x \in M$: $q(x)] \equiv \exists x \in M$: $[p \vee q(x)]$.

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

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): Dvě možnosti, jak se omezit pouze na matematiky. Implikace: $\forall x \in L$: $[m(x) \implies \neg n(x)]$.

Vytvořením množiny: $\forall x \in \{z \in L : m(z)\}$: $\neg n(x)$.
(ii): $\forall x, y \in L$: $\big[[m(x) \wedge \neg m(y)] \implies b(x,y)\big]$.
Šlo by i pomocí vhodných množin: Nechť $M = \{z \in L : m(x)\}$. Pak výrok zní $\forall x \in M\, \forall y \in L \setminus M$: $b(x,y)$.
(iii): $\neg n(\text{Lojza}) \implies [\forall x \in L$: $\neg n(x)]$.
(iv): Jsou to dva výroky, že existuje a že jich není víc. To druhé se dá vyjádřit více způsoby.
$\exists x \in L$: $\big[m(x) \wedge \forall y \in L \setminus \{x\}$: $\neg m(y)\big]$.
nebo $\exists x \in L$: $\big[m(x) \wedge \forall y \in L$: $[y \neq x \implies \neg m(y)]\big]$. nebo $\exists x \in L$: $\big[m(x) \wedge \forall y \in L$: $[m(y) \implies x = y]\big]$.
Poznámka: Tento poslední trik je u matematiků obzvláště oblíbený.
Poznámka: Výrok $[\exists x \in L$: $m(x)] \wedge [\forall y \in L \setminus \{x\}$: $\neg m(y)]$ není správný, protože se vymezení x nevztahuje na druhý výrok, tam je x neurčeno, což by nemělo být.
(v): $\neg[\exists! x \in L$: $m(x)]$. Ale $\exists!$ se snažíme vyhýbat, chce to alternativu: Vždy jsou alespoň dva, nebo taky žádný.
$\big[\exists x, y \in L$: $[x \neq y \wedge m(x) \wedge m(y)]\big] \vee [\forall x \in L$: $\neg m(x)]$.
(vi): Tohle je kombinace „jsou alespoň dva“ a „není víc“.
$\exists x, y \in L$: $\big[x \neq y \wedge m(x) \wedge m(y) \wedge \forall z \in L \setminus \{x, y\}$: $\neg m(z)\big]$.
(vii): $\forall x \in L$: $[x \neq \text{Lojza} \implies b(\text{Lojza}, x)]$. Pokud bychom napsali jen $\forall x \in L$: $b(\text{Lojza}, x)$, tak by to znamenalo, že Lojza je větší borec než on sám, což je nesmysl.
(viii): Tady není úplně jasné, co se tím míní. Jedna možnost je brát to jako popření výroku „matematici nejsou normální“: $\neg\big[\forall x \in L$: $[m(x) \implies \neg n(x)]\big]$.
Je možné to také brát jako závěr z objevení normálního matematika: $\exists x \in L$: $[m(x) \wedge n(x)]$.
Pokud aplikujeme pravidla pro negaci a operace, zjistíme, že nakonec oba výroky říkají totéž.
(ix): To je opět trochu tricky. 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: $\forall x \in L$: $[\neg m(x) \implies \neg n(x)]$.
Jinak řečeno, když už vidíme někoho normálního, tak jedině matematika: $\forall x \in L$: $[n(x) \implies m(x)]$.
Ty implikace jsou samozřejmě totéž, jde o obměnu.
(x): 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: $n(\text{Lojza}) \iff n(\text{Pepa})$.

1a.3: (i): $\equiv [x > 3 \wedge e^x = x^5\,] \vee [x > 3 \wedge x = 4\,] \equiv [x > 3 \wedge e^x = x^5\,] \vee x = 4$.
(ii): $\equiv [x < 13 \wedge x^2 < 4\,] \vee [x < 13 \wedge x > 14\,] \equiv [x^2 < 4\,] \vee F \equiv x^2 < 4$.
(iii): $\equiv \sin(x) < x^3 \wedge [x < 3 \vee x > 1\,] \equiv \sin(x) < x^3 \wedge T \equiv \sin(x) < x^3$.

1a.4: (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.5: (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. Jazyk matematiky

Jedním z cílů celé knihy je naučit čtenáře překládat mezi matematičtinou, logičtinou a lidštinou. Tyto znalosti obvykle student získává jaksi bokem při studiu rozličných matematických oborů, mnohým studentům dělá problémy se do toho nového světa vpravit a tato část je koncipovaná jako první seznámení, které by mělo čtenáři pomoci na další cestě. Protože se v této části věnujeme nejen čtení, ale i psaní matematičtinou (1b.1), není špatný nápad se sem občas vrátit ve chvíli, kdy už student sám začíná psát matematiku.

Aby mohla matematika o něčem získat spolehlivé informace, musí nejprve zcela přesně vymezit, co to vlastně je. Jinak by nastal problém, například není úplně jasné, co to vlastně je normální člověk, a tudíž ani nelze v mnoha případech rozhodnout, zda je ta či ona osoba normální. Na druhou stranu každý pozná, co je to sudé číslo, a proto je možné o nich s jistotou tvrdit spoustu věcí.

Specifikaci nových pojmů se v matematice říká **definice**. Většinou je nový pojem charakterizován vlastností, podle které se dá jednoznačně poznat. Lidé například tuší, že číslo je sudé, pokud jej lze vydělit dvojkou. To je samozřejmě třeba vyjádřit přesným jazykem, například tak, že když nám dá někdo číslo x, tak se ptáme, zda je číslo $\frac{x}{2}$ celé, tedy matematičtinou zapsáno $\frac{x}{2} \in \mathbb{Z}$. Protože dělení není matematicky zrovna nejlepší operace (není asociativní, občas selže, viz dělení nulou), dávají matematici přednost alternativnímu vyjádření, kdy si výsledek dělení označí písmenkem $\frac{x}{2} = k$, aby o něm mohli mluvit, a pak mají $x = 2k$. Dostávají tak typickou definici.

Definice.
Nechť x je reálné číslo. Řekneme, že je **sudé**, jestliže existuje $k \in \mathbb{Z}$ takové, že $x = 2k$.

Rozeberme si to. 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 sudé, podle toho, jak dopadne (či nedopadne) 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 sudé.

Všimněte si jedné podstatné věci. Protože podmínka přesně určuje, zda číslo je či není sudé, musí být mezi sudostí a podmínkou logický vztah, který umožňuje přenášet pravdivost i nepravdivost, jinými slovy ekvivalence. Formálně,

$$\forall x \in \mathbb{R}\colon \big[x \text{ sudé} \iff \exists k \in \mathbb{Z}\colon x = 2k\big].$$

Správně by tedy v definici mělo být napsáno „Řekneme, že x je sudé, právě tehdy když existuje . . . “. Z jazykových důvodů je ale zvykem psát tam „jestliže“, což značí implikaci: „$[x = 2k \wedge k \in \mathbb{Z}] \implies x$ sudé“.

Jinými slovy, je to vlastně napsáno špatně! Jenže je to zvyk, dělá se to tak už nejméně sto let a snad ve všech jazycích. Proto se s tím matematici smířili a prostě vědí, že definice je speciální útvar, ve kterém se „jestliže“ bere jako ekvivalence. Je to součástí zasvěcení do oboru, teď už to tajemství znáte, vítejte v tajné lóži matematiků (pro krvavý iniciační obřad si počkejte na první drsnější důkaz).

→ Poznámka stranou: Co když si někdo zavede jinou definici sudosti? 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 sudosti zavedl, namísto toho prohlásil, že sudá 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, byly vymyšleny tak, aby nám pomáhaly při práci, přičemž to, že se dožily současnosti, ukazuje, že se jejich autoři dobře trefili. U některých pojmů (zejména těch základních, třeba funkce) to trvalo desítky let, než se přišlo na „správnou“ definici.

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

Občas se stane, že je více užitečných možností, jak něco definovat, a lidé se nedokázali shodnout. Například v této knize máme $\mathbb{N} = \{1, 2, 3, \dots\}$, ale někteří autoři mají $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. Pak je třeba se mít na pozoru ← a vždy se dohodnout, s jakou definicí pojmu se zrovna pracuje.

Existují také definice, u kterých se testovat nemusí (takže nevzniká problém s implikací a ekvivalencí), ony prostě přímo řeknou, co se určitým pojmem myslí.

Definice.
Nechť x je reálné číslo. Symbolem x^2 značíme číslo $x \cdot x$.

Stojí za to poznamenat, že aby naše definice fungovaly, tak ještě předtím musíme mít definice udávající, co je to rovnost a co jsou reálná čísla a co je násobení, 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, kde to je všechno důsledně uděláno, v ostatních oborech už určité věci považujeme za známé (rovnost, rovnice, základní algebra atd.) a nevrtáme se v nich.

Máme tedy pojmy. 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 5a.12 a Věta 5c.11). Tato klasifikace je samozřejmě subjektivní a co je u jednoho autora důsledek, může mít jiný jako větu a podobně.

Základním předpokladem k ovládnutí matematiky je schopnost číst taková tvrzení ve smyslu rozumět tomu, co říkají. Jako příklad si rozebereme jedno snadné matematického tvrzení.

Fakt.
Nechť $n \in \mathbb{Z}$. Jestliže je n sudé, pak je i n^2 sudé.

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

- Pro každé $n \in \mathbb{Z}$ platí: Jestliže je n sudé, pak je n^2 sudé.

Teď už to snadno přeložíme do formálního jazyka:

- $\forall n \in \mathbb{Z}$: [n sudé $\implies$ n^2 sudé].

Jde o implikaci, nejoblíbenější matematickou strukturu. Neexistuje standardní matematické značení pro sudá čísla, takže nám tam nějaká lidská slova zůstala, to se občas stane. Pokud bychom se jich chtěli zbavit, museli bychom si nejprve takové značení zavést. Lze to udělat například formou množiny $S = \{n \in \mathbb{Z} : n \text{ sudé}\}$ čísel, se kterými chceme pracovat. Naše tvrzení pak lze zapsat takto:

- $\forall n \in \mathbb{Z}$: [$n \in S \implies n^2 \in S$].

Je to elegantní a stručné, což mají matematici rádi. Nutíme tím ale čtenáře, aby si to zase překládal do známějších pojmů, takže zrovna v tomto případě to asi nebude nejlepší verze. V části o logice jsme si také říkali, že tento zápis je totéž jako jiný zápis:

- $\forall n \in S$: $n^2 \in S$.

Je zajímavé, že v tomto značení se ztratila značka implikace, ale tento vztah je tam samozřejmě stále schován. Někdy se nabízí více variant, jakou logickou strukturu použít k zachycení české matematické věty, formálně to samozřejmě musí vyjít nastejno, ale může být rozdíl v praktickém používání.

Je také možné jít opačným směrem, k menší formálnosti. Můžeme třeba říct:

- Pro každé sudé $n \in \mathbb{Z}$ platí, že n^2 je sudé.
- Pro všechna sudá n platí, že n^2 je sudé.
- Všechna sudá čísla mají sudou druhou mocninu.
- Čtverce sudých čísel jsou sudé.

První přepis je jen zkomprimovaná původní verze, kdy jsme informaci z preambule přesunuli do hlavní věty. Druhý přepis je také stejně dobrý jako původní verze, jen zní méně „oficiálně“, což může být dokonce výhodou, čtenáře to tolik nezastraší. Třetí verze ukazuje, že se dokážeme obejít bez proměnné, aniž by to ubralo na srozumitelnosti. Přidělováme tím práci čtenáři, který by s tímto tvrzením chtěl dále pracovat a nějakou proměnnou by si zavést musel, na druhou stranu pokud chceme jen předat myšlenku, tak je výhodnější to čtenáři nekomplikovat symboly, tahle věta jde přímo na komoru. Podobně jako v literatuře, i v matematice bývá diskutována otázka dobrého stylu, která samozřejmě také záleží na osobním vkusu a preferencích, nicméně většina matematiků by se asi shodla, že je dobré nezavádět do tvrzení proměnné tam, kde to není nezbytně nutné. Poslední verze je pak mile starobylá a krásně kompaktní, ale do knihy bych ji asi nedal.

Někdy chceme o určitém objektu říci více věcí najednou, matematici pak tradičně číslují pomocí malých římských číslic.

Fakt.
Nechť $a \in \mathbb{R}$. Jestliže je $a > 0$, pak platí následující:
(i) $a^3 > 0$.
(ii) Pro všechna $x, y \in \mathbb{R}$ splňující $x < y$ platí $ax < ay$.

Bylo by také možné nepoužívat v uvozovacím řádku implikaci a místo toho napsat:
• Nechť $a \in \mathbb{R}$ splňuje $a > 0$. Pak platí ...
Dokonce by to šlo zkrátit ještě více:
• Pro $a > 0$ platí: ...
Tato verze je opět pěkně kompaktní a nezatěžuje čtenáře, ale má problém z formálního hlediska, protože není vůbec jasné, jaká a se berou. Libovolná celá čísla? Nebo snad reálná? Není to tedy úplně dobře. Pokud jsme ale v kapitole, která pojednává čistě o reálných číslech, pak je autor v pokušení to brát jako jasné a předpoklad vynechat, aby se tvrzení lépe četlo. Je to na hranici.

Co se týče formálního zápisu, (i) už je hotovo a (ii) je implikace:
• $\forall x, y \in \mathbb{R}$: $[x < y \implies ax < ay]$.

Poslední významný typ matematického tvrzení, který se občas objevuje, je hromadná ekvivalence.

Fakt.
Nechť $x, y \in \mathbb{R}$ splňují $x, y > 0$. Pak jsou následující tvrzení ekvivalentní:
(i) $x < y$.
(ii) $\frac{1}{y} < \frac{1}{x}$.
(iii) $x^2 < y^2$.

Formálně vzato to znamená, že libovolné dva výroky ze seznamu jsou navzájem ekvivalentní, ve Faktu jsou tedy schovány tři ekvivalence nebo také šest implikací. Lidově řečeno, všechna tři tvrzení podávají stejnou informaci.

Je důležité umět matematické texty nejen přečíst, ale také si rozmyslet, co vlastně říkají, například z pohledu praktického.

Příklad 1b.a: Jednou z populárních úloh matematické analýzy je najít pro zadanou funkci všechny body, ve kterých má lokální extrémy (pokud čtenář neví, co to je, tak by mu to nemělo vadit). Co nám o nich teorie říká?

Samozřejmě existuje definice lokálního extrému, takže je v principu možné pro určitý konkrétní bod rozhodnout, zda je lokálním extrémem, ale má to zásadní háček. Toto zkoumání nelze dělat hromadně, musí se dělat pro každý bod zvlášť, a těch bodů je na reálné ose docela dost (dokonce nekonečně mnoho), určitě bychom je nestihli projít všechny.

Je tedy třeba hledat jiný přístup. Na první pohled vypadá vysoce nadějně věta typu postačující podmínky:
• Jestliže má funkce f v bodě a vlastnost V, pak je tam lokální extrém.

Pokud je nutno vlastnost V zkoumat individuálně, pak máme zase problém. Zajímavější by bylo, kdyby šlo hromadně najít všechny body s vlastností V. Taková věc opravdu existuje, ale kupodivu nám to nepomůže splnit úkol. My totiž tímto postupem dokážeme (při troše štěstí) najít nějaké lokální extrémy, ale toto tvrzení je implikace. To znamená, že klidně mohou být body, které sice vlastnost V nemají, ale lokálními extrémy přesto jsou. Nenajdeme tak všechny žádané body.

V praxi se proto obvykle vychází z věty, která jde jakoby špatným směrem:
• Jestliže má funkce f v bodě a lokální extrém, pak je a kritickým bodem.

(Kritický bod je bod, ve kterém se derivace funkce chová určitým způsobem, ale to nás teď nezajímá. Je užitečné vědět, že kritické body se hledají relativně snadno.)

Tato věta nevypadá moc perspektivně, protože lokální extrémy teprve chceme hledat, takže nevíme, kdy je splněn předpoklad. Jenže má velice zajímavou obměnu:
• Jestliže funkce f nemá v bodě a kritický bod, pak tam také není lokální extrém.

Jinými slovy, pokud určíme množinu všech kritických bodů (což jde často relativně snadno), tak máme zaručeno, že nikde jinde už lokální extrémy nejsou. Řečeno formálně, býti kritickým bodem je nutná podmínka pro lokální extrém. Tato věta proto funguje jako efektivní „omezovač“. Díky ní se původní problém hledání extrémů na celé reálné ose redukuje na (doufejme) malou množinu kritických bodů. Tyto kandidáty pak už nějak protřídíme, například podmínkou z definice, pro pár bodů se to už vyplatí.

U některých nám může ušetřit práci ta postačující podmínka s vlastností V, ale u ní pořád zůstává problém spolehlivosti. Je tu možnost, že některý kritický bod vlastnost V nemá, ale lokální extrém je.

Z těchto úvah pak už vyplyne standardní algoritmus pro hledání extrémů, který se studenti učí v prvním semestru analýzy. Ideální by samozřejmě bylo kritérium ve tvaru ekvivalence, které zastane obě role najednou a přímo najde všechny lokální extrémy zkoumáním nějaké relativně jednoduché podmínky, bohužel jej nemáme.

Shrnuto, pokud hledáme nějaký objekt a stačí nám najít jeden, pak je dobré mít postačující podmínku typu „pokud něco funguje, tak už mám hledaný bod.“ Je ovšem třeba brát v úvahu případnou nespolehlivost. Pokud naopak chceme mít jistotu, že jsme našli všechny žádané body, pak je velmi užitečné mít nutnou podmínku. Je samozřejmě zbytečné se tohle učit nazpaměť. Cílem je porozumět logice (v tomto případě významu implikace) a matematice natolik, aby si to člověk v případě potřeby dokázal sám rozmyslet.

△

1b.1 Matematičtina jako jazyk komunikace

Matematici si neříkají jen definice a výsledky, ale vyprávějí si také o tom, jak nad věcmi přemýšleli (postupy, odvození). I čtenář bude patrně potřebovat tento způsob komunikace zvládnout, takže se na používání matematičtiny podíváme blíže. Je to jazyk jako každý jiný, takže má své ustálené postupy, ale také různé podoby podle toho, zda jde o neformální rozhovor nebo oficiální text, například v učebnici. Liší se také míra používání logických značek (což mimo jiné ovlivňuje čitelnost pro čtenáře), jedna věc ale zůstává: matematický text by měl dávat smysl a být logicky správný.

Příklad 1b.b: Student se pokusil řešit rovnici takto:

$$\begin{aligned} \frac{\sqrt{x}}{2} &= 3 \\ \sqrt{x} &= 6 \\ x &= 36 \end{aligned}$$

Co to vlastně znamená?

1. Nejprve se na to podíváme z hlediska „jazyka“. Jaký má matematický význam, když pod sebe napíšeme několik rovností či nerovností? Obvykle se to chápe jako soubor implikací, tedy z prvního řádku vyplývá druhý, z druhého třetí a tak dále. Náš úryvek tedy představuje dvě implikace. Jedna říká „jestliže $\frac{\sqrt{x}}{2} = 3$, pak $\sqrt{x} = 6$“ a druhá říká „jestliže $\sqrt{x} = 6$, pak $x = 36$“. Obě jsou pravdivé a dohromady proto dávají pravdivou implikaci „jestliže $\frac{\sqrt{x}}{2} = 3$, pak $x = 36$“.

Využíváme zde obecného „teleskopického“ principu (viz 1a.2), tedy že řetězec pravdivých implikací $p \implies r_1$, $r_1 \implies r_2$, … , $r_n \implies q$ se „sklapne“ do pravdivé implikace $p \implies q$. Z praktického pohledu to znamená, že když korektními kroky opakovaně přecházíme od rovnosti k rovnosti (či od nerovnosti k nerovnosti), tak pravdivost prvního řádku implikuje pravdivost posledního řádku.

2. Teď se zamyslíme nad zápisem. Řetízky implikací jsou patrně nejčastějším typem matematické úvahy a ne vždy stačí zapsat pod sebe několik rovnic, zejména proto, že třeba ty úvahy s rovnicemi vůbec nepracují. Jak to pak zapsat? Nabízí se stručný a výstižný obrázek:

$$\frac{\sqrt{x}}{2} = 3 \implies \sqrt{x} = 6 \implies x = 36.$$

Bohužel to nejde, protože implikace není asociativní operace, takže z pohledu logiky tento zápis nemá smysl. Bylo by pěkné mít úmluvu, že když napíšeme $p \implies r_1 \implies r_2 \implies \cdots \implies q$, tak to vlastně znamená řetězec implikací $[p \implies r_1] \wedge [r_1 \implies r_2] \wedge \cdots \wedge [r_m \implies q]$. Kupodivu ji ale matematici neudělali, ačkoliv je to nejčastější typ úvah a rozhodně by se to vyplatilo. Máme samozřejmě k dispozici korektní zápis

$$\Big(\frac{\sqrt{x}}{2} = 3 \implies \sqrt{x} = 6\Big) \wedge \big(\sqrt{x} = 6 \implies x = 36\big),$$

ale neznám nikoho, komu by se chtělo.

Situace je tedy takové, že se nabízí přehledný zápis, který ale nemůžeme oficiálně použít (třeba v knize), protože není korektní. Nicméně je tak přirozený, jej matematici běžně používají, když si mezi sebou povídají. Jsou si přitom vědomi, že nejde o implikaci jako takovou, ale o pohodlnou značku pro „z toho, co jsem právě řekl, vyplývá zase tohle“. Bylo by moc pěkné mít pro tento typ úvah oficiální symbol, jakousi zkratku na pomezí matematiky a češtiny. Nemáme. Mimochodem, v anglosaském světě na to mají znak $\therefore$ (viděli jste film Predator?) čtený „therefore“, který je velice užitečný pro neformální zápis, ale v oficiálním styku nebývá doporučován.

→ Je tu ještě jeden faktor. Čtenář asi správně cítí, že mezi větami „implikace $p \implies q$ je pravdivá“ a „z pravdivosti faktu p vyplývá fakt q“ je úzký vztah, ale logici-specialisti by nám vysvětlili, že to není úplně totéž. Některé logiky přímo irituje, když matematici nelogici v úvahách „zneužívají“ značku implikace. Jsou o
← tom zajímavé články na webu.

Když to tedy shrneme, jakkoliv je silné pokušení šetřit čas a zachycovat své úvahy pomocí značky $\Longrightarrow$, při oficiálních příležitostech (třeba v knize) je lepší se obětovat a jednotlivé zastávky v úvaze spojovat slovy vystihujícími, jak jsme se od jedné ke druhé dostali („proto“, „tudíž“, „odtud“). V našem konkrétním příkladě třeba takto: Když $\frac{\sqrt{x}}{2} = 3$, tak $\sqrt{x} = 6$ a proto $x = 36$. V neoficiálním hovoru pak přimhuřujeme očko.

V kapitolách této knihy používám v úvahách české věty, nicméně řešení ke cvičením musejí být stručná a váhal jsem, jakou značku použít. Anglické $\therefore$ ani logické $\models$ nejsou příliš známé a nechtělo se mi provokovat se značkou implikace, tak jsem nakonec použil $\longrightarrow$.

Mnohem důkladněji se o psaní matematiky rozepíšeme v následující části.

3. Nakonec se na to podíváme z hlediska obsahu. Už víme, že jde o dvě implikace, ale jakou informaci nám vlastně onen výpočet poskytnul? Studenti si často myslí, že našli řešení rovnice, ale není tomu tak. Tento postup korektními kroky dokázal, že pro libovolné (reálné?) číslo x platí implikace „pokud x řeší rovnici, pak $x = 36$“. My ovšem tuto implikaci na žádné x aplikovat neumíme, protože v této chvíli nevíme, která x vlastně rovnici řeší, tedy nevíme, zda je či není splněn předpoklad implikace. Tato implikace nám zatím nikterak nepomohla.

Nějaké informace nám ovšem náš výpočet přinesl, uvidíme je, když přejdeme k obměně „jestliže $x \neq 36$, tak x neřeší danou rovnici“. Jak jsme již diskutovali, tato slouží jako omezovač. Hledáme-li řešení, stačí vyšetřit bod $x = 36$. To snadno uděláme dosazením a teprve teď zjistíme, že máme řešení. Naše omezovací implikace pak zaručuje, že jiné není.

Pro srovnání se podívejme na podobný příklad:

$$\begin{aligned} \sqrt{3x-5} &= 1-x \\ 3x-5 &= x^2-2x+1 \\ 0 &= x^2-5x+6 \\ 0 &= (x-2)(x-3) \end{aligned}$$

Máme zde pravdivou implikaci „jestliže x řeší rovnici, tak $x = 2$ nebo $x = 3$“, která poskytuje dva kandidáty. Čtenář se ovšem hravě přesvědčí, že 2 ani 3 rovnici vlastně neřeší. Díky obměně „jestliže $x \neq 2$ a $x \neq 3$, tak x neřeší $\sqrt{3x-5} = 1-x$“ už víme, že žádná další čísla zkoušet nemá smysl, takže s jistotou víme, že dotyčná rovnice nemá (v $\mathbb{R}$) řešení.

Je zajímavé porovnat to ještě s dalším příkladem:

$$\begin{aligned} 2x+1 &= 13 \\ 2x &= 12 \\ x &= 6 \end{aligned}$$

Máme implikaci „pokud x řeší rovnici, pak $x = 6$“, která omezuje, ale tentokráte byly všechny provedené úpravy ekvivalentní, takže výpočet je platný i v opačném směru a máme implikaci „pokud $x = 6$, tak x řeší rovnici“. V jednom postupu jsme tedy udělali dvě věci, potvrdili $x = 6$ jako řešení a zároveň vyloučili ostatní čísla. Toto je případ, se kterým se studenti na základní a střední škole setkávají nejčastěji, proto také často netuší, co se vlastně v tomto upravovacím postupu všechno skrývá.

△

1b.2 Poznámka Jak mluvit matematicky: I toto bývá pro začátečníka občas problém. Stává se například, že student má u zkoušky napsat znění určité věty či definici. Je nesmysl učit se definice a věty doslova, takže student většinou napíše něco, co mu přijde podobné, a občas se diví, že to zkoušející neuzná.

Samozřejmě není vůbec špatně, když student řekne něco svými slovy (naopak často v průběhu učení studentovi pomůže pochopit význam nějakého textu, pokud si jej přeloží do svého jazyka). Zejména u zkoušky, když je student nervózní, obvykle zkoušející odpustí i stylistické nedostatky (pokud zásadně neovlivňují srozumitelnost textu). Tím klíčovým je logický význam.

Představme si studenta, který řekne/napíše následující: „Neutrální prvek znamená, že když kdykoliv je x tak je n aby $x + n = 0$.“

Omluvme neobratnost textu, podívejme se na význam. V zásadě jsou tam všechny klíčové složky definice, ale není to ono. Problém je v logické struktuře: Nejprve přijde x, pak n. Zapsáno formálně:

- $\forall x\, \exists n$: $x + n = 0$.

A tohle je špatně, správná definice totiž zní

- $\exists n\, \forall x$: $x + n = 0$.

V první části jsme si vysvětlovali, že na pořadí kvantifikátorů záleží, tyto dva výroky tedy nejsou totožné.

Naopak tohle bych asi u zkoušky uznal (s přihouřením oka), jakkoliv to stylisticky není nejlepší: „Neutrální prvek je n že všechna $x \in X$ mají $x + n = x$.“ Určitě by to šlo říct lépe, asi bych vytkl, že není určeno, odkud se

n bere, ale vidím tam důležité rysy: Správné pořadí určení prvků n a x (tedy že n je jedno univerzální), a že se x uvažuje libovolné (tedy n funguje pro úplně všechna x).

Nelíbilo by se mi toto: „Neutrální prvek je takové $n \in X$, že pro $x \in X$ platí $x + n = x$." Stylisticky je to přímo vzorové, logické pořadí jednotlivých částí správné, ale zase tam chybí klíčové slovo „pro všechna" u toho x, aby to šlo uznat.

Kontroverzní je následující verze: „Neutrální prvek je takové $n \in X$, že $x+n = x$ pro všechna $x \in X$." Došlo zde k prohození pořadí, namísto $\forall x$: $p(x)$ zde máme $p(x)\forall x$. V zásadě jde o anglicismus, v anglicky psané literatuře bývá tento způsob vyjádření běžný. Je pravda, že takto ta věta lépe plyne, z jazykového hlediska je příjemnější. Existuje také neoficiální úmluva, co to vlastně znamená, to prokaždítko z konce věty se má přesunout o jedno doleva, tedy před vlastnost, ke které se vztahuje. Oficiální pravidla nicméně nejsou a jistě se dají vymyslet nejednoznačné situace, takže za sebe bych radil si na tohle nezvykat.

Abychom to uzavřeli, pokud má student něco napsat slovy, měl by se zamyslet, zda jsou tam vyjádřeny všechny důležité logické náležitosti a zda svými slovy správně vystihl strukturu odpovídajícího logického výroku.
△

Důkladněji se o psaní matematiky rozepíšeme v následující části.

Cvičení

Cvičení 1b.1: Vymyslíme si následující definici:
Řekneme, že přirozené číslo n má „vlastnost V", pokud existují přirozená čísla k, l splňující $n = k^2 - l^2$.
Rozhodněte, která z čísel 5, 6, 7, 8 mají vlastnost V.

Cvičení 1b.2: Vymyslíme si následující definici:
Řekneme, že přirozené číslo n má „vlastnost W", pokud pro všechna $k \in \mathbb{N}$ platí, že $k^2 + 2k + n$ je druhá mocnina přirozeného čísla.
Rozhodněte, která z čísel 1, 2, 6 mají vlastnost W.

Cvičení 1b.3: Vymyslíme si následující definici:
Řekneme, že přirozená čísla a, b jsou „p-spojena", pokud $a - b$ nebo $b - a$ je prvočíslo.
Rozhodněte, která z dvojic čísel 7 a 2, 12 a 25, 3 a 13 jsou p-spojena.

Cvičení 1b.4: Uvažujme následující neformální zápisy úvah.
(i) n prvočíslo $\longrightarrow [n$ liché $\vee\ n = 2]$.
(ii) $[a > 0 \wedge a^2 - a - 2 = 0] \longrightarrow a = 2$.
Přeložte je do češtiny.

Cvičení 1b.5: Diskutujte logický význam následujících úprav:

$$\begin{aligned} \sqrt{2x-1} &= 2 - x \\ 2x - 1 &= 4 - 4x + x^2 \\ 0 &= x^2 - 6x + 5 \\ (x-1)(x-5) &= 0 \end{aligned}$$

Diskutujte řešitelnost dané rovnice.

Cvičení 1b.6: Diskutujte logický význam následujících úprav:

$$\begin{aligned} \sqrt{x^2-3} &= 1 - x \\ x^2 - 3 &= 1 - 2x + x^2 \\ 2x &= 4 \\ x &= 2 \end{aligned}$$

Diskutujte řešitelnost dané rovnice.

Řešení:
1b.1: 5 má vlastnost V, protože $5 = 3^2 - 2^2$.
6 nemá vlastnost V. Když si píšeme druhé mocniny čísel, zjistíme, že se brzy rozestupy stanou většími než 6. Jediní kandidáti na k, l jsou proto čísla $1, 2, 3$ a snadno nahlédneme, že žádné dvě z nich nedají šestku coby $k^2 - l^2$.
7 má vlastnost V, protože $7 = 4^2 - 3^2$. 8 má vlastnost V, protože $8 = 3^2 - 1^2$.
1b.2: 1 má vlastnost W, protože pro libovolné $k \in \mathbb{N}$ máme $k^2 + 2k + 1 = (k+1)^2$.
2 nemá vlastnost W, například volba $k = 1$ dává $k^2 + 2k + 2 = 5$, což není druhá mocnina přirozeného čísla.

6 nemá vlastnost W. Pro číslo $k = 1$ sice podmínka platí, $k^2+2k+6 = 9 = 3^2$, ale pro $k = 2$ už ne, $k^2+2k+6 = 14$ není čtvercem přirozeného čísla. Protože je v definici prokaždítko, tento případ stačí k popření.

1b.3: Dvojice 7 a 2 je p-spojena, neboť $7 - 2 = 5$ je prvočíslo.

Dvojice 12 a 25 je p-spojena, neboť $25 - 12 = 13$ je prvočíslo.

Dvojice 3 a 13 není p-spojena, neboť ani $13 - 3 = 10$, ani $3 - 13 = -10$ nejsou prvočísla.

1b.4: (i): Pokud je n prvočíslo, pak je liché nebo rovno 2.

(ii): Jestliže je a kladné a řeší rovnici $x^2 - x - 2 = 0$, pak je rovno 2.

1b.5: Úpravy dokazují implikaci „jestliže x řeší rovnici, pak $x = 1$ nebo $x = 5$“. Znamená to, že v množině $\mathbb{R} \setminus \{1, 5\}$ určitě nejsou kořeny. Jedna z úprav (jmenovitě umocnění na druhou) není ekvivalentní, proto postup nelze otočit.

Zkouška ukáže, že $x = 5$ rovnici neřeší, zato $x = 1$ ano, je to jediné reálné řešení.

1b.6: Úpravy dokazují implikaci „jestliže x řeší rovnici, pak $x = 2$“. Jedna z úprav (jmenovitě umocnění na druhou) není ekvivalentní, proto postup nelze otočit.

Zkouška ukáže, že $x = 2$ rovnici neřeší, ta proto díky oné implikaci žádné reálné řešení nemá.

1c. Důkazy

Většina matematických tvrzení začíná kvantifikátorem, což představuje první rozcestí při rozhodování, kudy se má důkaz ubírat. Není třeba se něco učit, je to opět jen selský rozum.

• $\exists x \in M$: $p(x)$.

Pokud tvrzení začíná existítkem, pak je (přirozeně) třeba ukázat, že existuje nějaké x žádané vlastnosti. Občas se přímo povede takový prvek konkrétně najít či zkonstruovat. 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. V knize se několik (málo) existenčních výroků najde a vždy jsme tam schopni žádaný prvek přímo dohledat, zde jeden velmi snadný příklad.

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

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

Takže to bylo opravdu snadné. Jak se dokazuje, že takový 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. Tím se ovšem dostáváme k druhému kvantifikátoru.

• $\forall x \in M$: $p(x)$.

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.

To ovšem není typický případ, množina M bývá spíš větší, třeba nekonečná. Pak je třeba dokazovat hromadně, pro všechny prvky najednou. To se dělá tak, že si vezmeme typického zástupce, který ale nebude konkrétní. Vezmeme si tedy prvek x, který je vybrán zcela libovolně z množiny M, ale nikoliv námi, takže my vlastně nevíme, co je to přesně za objekt. Víme o něm čistě ty věci, které vyplývají z jeho původu v množině M. Pomocí těchto informací pak dokážeme platnost tvrzení $p(x)$. Zase uvedeme jeden směšně jednoduchý příklad.

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. Příklady uvidíme vzápětí.

Je také nutné vědět, jak se dokazuje nepravdivost tvrzení. U obecného kvantifikátoru stačí najít jediné $x \in M$, pro které $p(x)$ neplatí, tzv. **protipříklad**, a celé tvrzení už je nepravdivé. 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 1c.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 dále $1 > 0$, 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. Ještě se k tomu vrátíme, zde jen konstatujme, že základní algebru (třeba práci s nerovnostmi) v této knize řešit nechceme.

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: $\forall x \in \mathbb{R}$: $[x < 5 \vee x \geq 0]$.

S **Rozbor:** Důkaz začne slovy „vezměme libovolné $x \in \mathbb{R}$“, ale není jasné, jak dál. O tomto čísle víme jen to, že je reálné, a máme ukázat pravdivost složitějšího výroku. Ten má dvě části spojené nebotítkem, takže aby byla ukázána jeho pravdivost, stačí potvrdit jednu ze složek. My ovšem nevíme, na kterou s naším x mířit, protože o něm nic nevíme.

Zde se právě nabízí trik, kdy si informaci dodáme sami rozdělením množiny $\mathbb{R}$ na části. Třeba na dvě (ať nemusíme moc pracovat), a aby se to hodilo k důkazu, rozřízneme $\mathbb{R}$ v nule.

Důkaz: Mějme libovolné $x \in \mathbb{R}$. Uvažujme dvě možnosti.

1) $x \geq 0$. Pak je automaticky splněn výrok $x < 5 \vee x \geq 0$.

2) $x < 0$. Protože $0 < 5$, platí pak i $x < 5$ a výrok $x < 5 \vee x \geq 0$ je pravdivý.

Obě možnosti potvrdily platnost dokazovaného výroku, čímž je důkaz hotov.

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 $n \leq n^2$.

Protože žádanou nerovnost umíme dokázat jen pro část $\mathbb{Z}$, budeme zase dělit na případy. Co s ostatními čísly? Nula se také snadno potvrdí a u záporných dokonce ani není třeba nic počítat, jak hned uvidíme.

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, uvidíme to níže).

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“. Potkáváme to například v diskusi u Faktu 1d.3.

V předchozích částech jsme také naráželi na situace s více kvantifikátory.

Příklad 1c.b: Tvrzení: $\forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}$: $x + y = 1$.

V části 1a.4 jsme si rozmysleli, co toto vlastně znamená (ke každému x hledáme individuální y) a v příkladě 1a.1 jsme si u téměř totožného příkladu rozmysleli, že něco takového platí. Teď to dokážeme. Jak bude důkaz vypadat? Začneme prvním kvantifikátorem. Ten říká, že důkaz bude 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.

△

S kvantifikátory si tedy umíme poradit a je čas zaměřit se na to, jak vypadá dokazované tvrzení, protože to samozřejmě také výrazně ovlivní podobu důkazu. 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. Stojí tedy za to se implikací pořádně zabývat. Existuje několik základních přístupů, začneme tím nejpřirozenějším.

1c.1 Přímý důkaz

Funguje přesně tak, jak to zní, prostě dokážeme přímo, co se po nás chce. Zní to samozřejmě, ale níže uvidíme, že to kupodivu jde i jinak. Lehký příklad nám odhalí to podstatné.

Příklad 1c.c: Dokážeme výrok $\forall x \in \mathbb{R}$: $[x > 5 \implies x^2 > 25]$.

S Rozbor: Protože máme dokázat něco o výroku začínajícím prokaždítkem, víme, jak náš důkaz začne: vezmeme si obecného zástupce, tedy libovolné $x \in \mathbb{R}$. O tomto neznámém čísle pak je třeba odvodit, že splňuje danou implikaci. To je ovšem problém vzhledem k tomu, že o něm víme jen to, že je to reálné číslo. Nabízí se oblíbaný trik, rozdělíme si situaci na případy. Určitě by nám pomohlo vědět, zda $x > 5$ platí či ne, to je dobrá nápověda. Struktura důkazu by tedy měla vypadat takto:

Nechť $x \in \mathbb{R}$ je libovolné.
1) Jestliže $x > 5$, pak ... a proto $[x > 5 \implies x^2 > 25]$ platí.
2) Jestliže $x \leq 5$, pak ... a proto $[x > 5 \implies x^2 > 25]$ platí.

Pokud se nám podaří zaplnit prázdná místa, tak máme důkaz hotov.

Varianta $x \leq 5$ je zajímavá, protože v tomto případě má dotyčná implikace nesplněný předpoklad a tudíž automaticky platí, bez ohledu na to, co dělá x^2. Čili odrážka 2) je zcela triviální.

Vidíme, že to podstatné se děje v části 1), kde se rozhodne o osudu naší implikace. U této varianty je splněn předpoklad implikace, pro její pravdivost je tedy nutné ukázat, že platí i závěr $x^2 > 25$. Stručně řečeno, v této variantě je třeba pomocí předpokladu $x > 5$ odvodit závěr $x^2 > 25$.

Tím bychom tento příklad v zásadě mohli skončit, protože není naším cílem honit nerovnice, ale učit se, jak vytvářet správně strukturované důkazy. Takže jen pro úplnost:

Důkaz:
Nechť $x \in \mathbb{R}$ je libovolné.
1) Jestliže $x > 5$, pak je mimo jiné x kladné. Můžeme tedy nerovnici $x > 5$ vynásobit kladnými čísly x, popřípadě 5, a dostáváme dvě nerovnosti, $x^2 > 5x$ a $5x > 25$. Jejich spojením získáme $x^2 > 25$. Proto implikace $[x > 5 \implies x^2 > 25]$ platí.
2) Jestliže $x \leq 5$, pak implikace $[x > 5 \implies x^2 > 25]$ automaticky platí díky nepravdivému předpokladu.

△

Tento příklad je vysoce poučný. Uvažujme situaci, kdy dokazujeme tvrzení ve tvaru
$\forall x \in M$: $p(x) \implies q(x)$.
V takové situaci si vždycky můžeme rozdělit M na variantu, kdy $p(x)$ platí, a zbývající případ, kdy $p(x)$ neplatí. V tomto druhém případě pak implikace $p(x) \implies q(x)$ platí automaticky.

Závěr: Při dokazování implikace $p(x) \implies q(x)$ nás vůbec nezajímá situace, kdy $p(x)$ neplatí, o osudu implikace rozhodne čistě případ, kdy je $p(x)$ splněno. Z toho důvodu je zvykem tu snadnou variantu zcela ignorovat a rovnou začít důkaz tím, že uvažujeme nějaké libovolné x splňující $p(x)$. Pro ně pak potřebujeme ukázat platnost závěru $q(x)$.

Tento přístup lze odůvodnit i jinak. Opusťme speciální případ kvantifikátoru a podívejme se na obecnou situaci, kdy prostě potřebujeme dokázat implikci $p \implies q$. To znamená, že musíme vyloučit možnost, že by v rámci matematického světa mohly nastat ty řádky pravdivostní tabulky, kde má implikace nulu. Takový řádak je ovšem jen jeden, a je to právě situace, kdy je p splněno. To znamená, že je zbytečné se zabývat řádky začínajícími nulou, z těch se pravdivost implikace poznat nedá. Rozhoduje případ, kdy je p splněno, čili stačí se na tento případ zaměřit, předpoklad p se pak stává něčím, co lze v důkazu využít.

Vlastně to znamená, že se pak ocitáme v určitém světě (máme k dispozici jisté informace) a chceme dokázat, že v něm platí i q. Všimněte si, že tím neříkáme, že je to p opravdu splněno, jen si představujeme, k čemu by vedlo, kdyby splněno bylo.

Ukážeme si tento postup na několika příkladech, Protože je zároveň naším cílem naučit se dobře matematičtinu, budeme si představovat, že už děláme normální matematiku a narazili jsme na regulérní, vážně míněné tvrzení. Může vypadat třeba takto.

Fakt.
Pro všechna celá čísla n platí, že když je n sudé, tak je i n^2 je sudé.

Začneme tím, že si tento fakt přeložíme do logického jazyka.

• $\forall n \in \mathbb{Z}$: [n sudé $\implies$ n^2 sudé].

Už víme, že důkaz budeme muset začít tím, že si vezmeme libovolné celé číslo n. Pro toto (neznámé) celé číslo pak musíme ukázat platnost dotyčné implikace. Uděláme to přímo, takže budeme navíc předpokládat, že číslo n je sudé. Tím dostáváme určitou informaci, kterou můžeme používat, kdykoliv nám to přijde vhodné. Potřebujeme ukázat, že číslo n^2 je sudé. Máme tedy kostru důkazu:

Důkaz: Zvolme libovolné $n \in \mathbb{N}$, které je sudé. Pak ... a proto je n^2 sudé.

Zbývá doplnit prázdné místo, tedy překlenout mezeru mezi tím, co máme (n je sudé), a tím, co chceme mít (n^2 je sudé). Obvykle bývá dobré si rozmyslet, co vlastně ta daná informace říká. Zde se odvoláme k definici sudosti, která nám nabídne charakterizaci pomocí algebraického vzorce. Situace pak vypadá následovně.

• Známo: n je celé číslo
$n = 2k$ pro nějaké $k \in \mathbb{Z}$

• Chceme: $n^2 = 2l$ pro nějaké $l \in \mathbb{Z}$.

Zde upozorníme na jeden častý začátečnický omyl. Definice sudosti po nás chce vyjádření $n^2 = 2k$, ale to nelze použít, protože k už má svůj význam v levé části. Jinak řečeno, kdybychom použili i napravo k, tak bychom nutili obě čísla n a n^2, aby po vydělení dvojkou dávala stejný výsledek. To je ovšem něco, co téměř jistě pro naše n fungovat nebude. Volbou jiného písmene jsme číslu n^2 dali svobodu volby, jak má po vydělení dvěma vypadat, naštěstí je to v pořádku (viz 1a.5).

Zpět k důkazu. Jsme v klíčovém okamžiku, máme dobrou představu o tom, co chceme, i jaké nástroje máme. Potřebujeme najít nějaké spojení mezi levým a pravým sloupcem. Jak jej najdeme? Sloupeček vpravo nám říká, že potřebujeme vědět něco o n^2. Sloupeček vlevo nám nedává moc na výběr, použijeme to, co víme o n:

$$n^2 = (2k)^2 = 4k^2.$$

My chceme ukázat, že toto číslo je dvojnásobek celého čísla, což by mělo jít jednoduchou úpravou: $n^2 = 2 \cdot (2k^2)$. Protože je k celé, je i číslo $2k^2$ celé, můžeme mu říkat l a máme hotovo.

To co jsme předvedli, není důkaz, ale sled myšlenek, které nás k němu přivedly. Důkaz vznikne, když naše úvahy srozumitelně a logicky správně napíšeme:

Důkaz: Nechť n je libovolné celé číslo, předpokládejme, že je sudé. Pak existuje $k \in \mathbb{Z}$ takové, že $n = 2k$, proto také $n^2 = 4k^2 = 2 \cdot 2k^2$. Označíme-li $l = 2k^2$, pak je $l \in \mathbb{Z}$ a $n^2 = 2l$, proto podle definice je n^2 sudé. □

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 vyplněný čtvereček (já šetřím toner) či zkratka Q.E.D. z latinského „quod erat demonstrandum“ neboli „což bylo dokázati“. Vlastenci dávají CBD.

Všimněte si klíčových momentů. Důkaz začíná věcmi, které jsou pravdivé buď opravdu, nebo to alespoň předpokládáme (máme celé číslo, sudost n předpokládáme, tedy je to vlastně také daná věc). Odtud pak jednotlivými

kroky dojdeme k cíli, přičemž každý krok je odůvodněn něčím, co je rovněž známé: definice sudosti nám dá k, pravidla algebry nám dají vzorec pro n^2, vlastnosti množiny celých čísel zaručí, že i číslo l je celé. Obecně se lze odvolávat na věci, které nám dává tvrzení (preambule, předpoklad implikace), na obecně známá fakta a již dříve dokázaná tvrzení.

Takto tedy vypadá správný přímý důkaz: Začne tím, co známe, a pomocí kroků, které jsme schopni odůvodnit, dojde k tomu, co potřebujeme.

Viděli jsme, že tvorba důkazu zahrnuje dvě etapy. Nejprve je třeba najít ty správné argumenty – cihličky, ze kterých je důkaz sestaven, a vytvořit mezi nimi spojení. Pak je nutno tyto kroky správně seřadit, vytvořit koherentní text, který čtenáře přesvědčí, že opravdu čte důkaz. Tyto dvě etapy se mnohdy významně liší, dokonce i profesionální matematici často ke správnému důkazu dojdou úvahami, které jsou velmi vzdáleny konečné podobě v knize. Jednoduché důkazy lze obvykle napsat zpatra, ale pro začátečníka bývá lepší, když si nejprve přehledně shrne situaci, najde správné kroky a pak znovu a načisto napíše důkaz, přičemž si hlídá logickou návaznost a další věci, o kterých píšeme v radách 1c.8.

Jedním z důvodů, proč bývá pro studenty obtížné ovládnout umění důkazu, je právě to, že v knihách nacházejí důkazy vyčištěné k dokonalosti a zbavené všech zbytečných slov, což zamrzí zejména u těch, které by čtenáři napověděly, jak na ten důkaz autor vůbec přišel. Budeme proto zejména v této části (ale částečně i v dalších kapitolách) výrazně ukecanější, než bývá v knihách zvykem, ať podhrneme oponu a umožníme studentovi nakouknout do zákulisí.

Další nebezpečí spočívá v tom, že když student čte vyleštěný důkaz, tak má pocit, že krásně vidí, jak to do sebe zapadá, že tomu rozumí, že to vlastně umí. Tento pocit pak trvá do chvíle, kdy má sám podobný důkaz vytvořit. Doporučujeme tedy hodně cvičit.

Vrátíme se k našemu důkazu a popovídáme si o různých aspektech dokazování, přičemž využijeme dlouholeté zkušenosti s tím, co studenti na písemkách vydávají za důkaz. Své komentáře rozdělíme do tématických poznámek.

1c.2 Poznámka: Když dávám podobné věci do písemek, relativně často tam najdu něco jako tohle:

$n \in \mathbb{Z}$ sudé
$n = 2k,\ k \in \mathbb{Z}$ $\qquad n^2 = 2l$
$(2k)^2 = 2l$
$4k^2 = 2l$
$\underline{l = 2k^2}$

Toto není důkaz, jakkoliv ten zápis docela dobře zachycuje úvahy, kterými jsme výše k důkazu dospěli. Problém je, že pokud bychom to vzali jako logický text, tak se sudost n^2 stává východiskem, nikoliv závěrem. V zásadě se tu říká, že z předpokladu „n sudé a n^2 sudé“ vyplývá, že $l = 2k^2$. To první ovšem předpokládat nemůžeme, protože sudost n^2 není východiskem, ale závěrem, a fakt $l = 2k^2$ určitě nebyl tím, co jsme chtěli dokázat.

Častou chybou začátečníka je právě to, že „důkaz“ jde logicky špatným směrem. Má to svůj důvod. Když začínáme důkaz vymýšlet, tak je důležité, aby něco navádělo naše myšlenky správným směrem, a tím něčím je logicky právě to, co chceme dokázat. Často je to něco abstraktního, takže si to překládáme, zjednodušujeme, abychom se do toho uměli lépe trefit. Jinými slovy, jakoby si „jdeme naproti“.

$$p \longrightarrow \longrightarrow \longrightarrow\ r \qquad\qquad s \longleftarrow \longleftarrow q.$$

Namísto do q se pak trefujeme do s, což se často dobře podaří.

$$p \longrightarrow \longrightarrow \longrightarrow\ r \longrightarrow s \longleftarrow \longleftarrow q.$$

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

$$p \longrightarrow \longrightarrow \longrightarrow r \longrightarrow s \longleftrightarrow \longleftrightarrow q.$$

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

$$p \longrightarrow \longrightarrow \longrightarrow r \longrightarrow s \longrightarrow \longrightarrow q.$$

S tím, že obvykle ještě míváme vstupy pravdivých užitečných faktíků uprostřed důkazu, takže typický sled úvah je možná lépe vyjádřen obrázkem

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

Problémy se správným směrováním se objevují i v důkazech psaných slovy, kde bývá dalším zdrojem problémů volba slov. Následující odstavec opisuji prakticky doslova z jedné písemky.

Nechť je n sudé, pak $n = 2k$ pro $k \in \mathbb{Z}$. Pokud je $-n$ sudé, tak $-n = 2l$ pro $l \in \mathbb{Z}$. Z rovnosti $n = 2k$ dostáváme $-n = 2(-k)$ a $-k \in \mathbb{Z}$, proto je $-n$ sudé.

V tomto „důkazu“ je špatně druhá věta. Symbolicky zapsáno jde o implikaci, jmenovitě „$-n$ sudé $\implies$ $-n = 2l$ pro $l \in \mathbb{Z}$“. Problém zase je, že předpoklad této implikace není v dané chvíli znám, takže tato implikace má nulovou informační hodnotu. Pokud bychom druhou větu vynechali, dostáváme tento text:

Nechť je n sudé, pak $n = 2k$ pro $k \in \mathbb{Z}$. Odtud dostáváme $-n = 2(-k)$ a $-k \in \mathbb{Z}$, proto je $-n$ sudé.

Toto je vlastně korektní důkaz. V jeho posledním kroku mimochodem používáme fakt, že existuje vztah mezi sudostí čísla $-n$ a vyjádřením ve tvaru $-n = 2l$, takže pro autora důkazu bylo jistě užitečné, že si tento vztah během vymýšlení důkazu připomněl. Měl si ho ale připomenout někde bokem, ne jej napsat do důkazu v místě, kde se nehodil. Navíc v důkazu o chvíli později potřebujeme vztah přesně opačný, tedy že z $-n = 2l$ vyplývá sudost $-n$ (naštěstí i to platí, ve skutečnosti je tam ekvivalence). Takže nejen že dotyčný student zařadil do důkazu větu, která tam nepatřila, navíc šlo o opačný směr implikace, než bylo později potřeba, čímž student zkoušejícímu ukázal, že se s logikou ještě nesžil. Byla to ale teprve první malá semestrální písemka, takže student měl ještě šanci ze své chyby poučit.

K tomuto zásadnímu tématu se ještě vrátíme níže.

△

Poznámka: Náš důkaz vycházel z formalizace, která zní $\forall x \in \mathbb{Z}$: n sudé $\implies$ n^2 sudé.

My jsme si ovšem v části o jazyce ukázali, že ono tvrzení lze také formálně zapsat jinak. Nejprve se zavede značení $S = \{n \in \mathbb{Z} : n \text{ sudé}\}$ pro množinu čísel, která nás zajímají, a pak už píšeme $\forall x \in S$: $n^2 \in S$.

Jak by se toto dokazovalo, když tam žádná implikace není? Snadno. Každý prvek z S má něco splňovat, tak to ukážeme. Vezmeme si libovolné $n \in S$. Co tedy o něm víme? Že je to celé číslo a že je sudé. Vidíme, že vlastně vycházíme ze stejných faktů, jako když jsme dokazovali implikaci.

O tomto čísle máme dokázat, že je u něj n^2 z S neboli že n^2 je celé číslo a že je sudé. To první je ovšem snadné a to druhé je přesně totéž, co jsme dělali už předtím, takže z praktického hlediska obě logické formulace skončí u stejné práce.

Není to žádná náhoda, výrok „$\forall x \in M$: $p(x)$“ se obecně dá přepsat do tvaru „$(\forall x)\ [x \in M \mapsto p(x)]$“, proto by i důkazy obou měly být v podstatě stejné.

△

Poznámka: Důkaz je na to, jak je snadný, docela dlouhý. Člověk se většinou snaží ušetřit čas i papír, zejména když dojde na neformální rozhovor, ale třeba také na písemce. Pak to svádí třeba k tomuto:

$\forall n \in \mathbb{Z}$: n sudé $\longrightarrow n = 2k \longrightarrow n^2 = 2 \cdot 2k^2 \longrightarrow n^2$ sudé.

Tento „důkaz“ není správný, protože neukázal, že je n^2 sudé. Jak to? Tento text nikde neukázal splnění podmínky z definice. Je to poznat už z toho, že tak, jak je napsán, by poslední krok prošel i s číslem $n = \sqrt{\pi}$. Opravdu, $\pi = 2 \cdot 2k^2$, kde $k = \sqrt{\frac{\pi}{4}}$, odtud nás důkaz vede k tvrzení „$n^2 = \pi$ je sudé“. Vidíme, že v té definici sudosti není poznámka o $k \in \mathbb{Z}$ podružná, naopak je zcela klíčová, a my jsme to v našem „důkazu“ neuvedli, takže jsme nebyli oprávněni udělat ten poslední krok.

Správně odůvodněný poslední krok tedy vypadá takto: „$[n^2 = 2 \cdot (2k^2) \wedge 2k^2 \in \mathbb{Z}] \implies n^2$ sudé“. Jenže to $2k^2 \in \mathbb{Z}$ se musí něčím odůvodnit, nejlépe tím, že vlastně $k \in \mathbb{Z}$. Odkud to víme? Z definice sudosti aplikované na n, čili to je další věc, kterou jsme zapomněli. Druhý pokus o krátký důkaz:

$\forall n \in \mathbb{Z}$: n sudé $\implies n = 2k$, $k \in \mathbb{Z} \implies n^2 = 2 \cdot 2k^2$ a $2k^2 \in \mathbb{Z}$, proto n^2 sudé.

Tohle by možná prošlo načmárané na ubrousku v baru (vznikl tak nejeden významný výsledek), ale v knize určitě ne. V minulé sekci jsme si vysvětlili, že při zápise úvahy bychom neměli zneužívat znaménko pro implikaci. Je tu navíc problém s logickou strukturou. Podívejme se na krok „$[n = 2k \wedge k \in \mathbb{Z}] \implies n^2 = 2 \cdot 2k^2$“. Opravdu to $n^2 = 2 \cdot 2k^2$ vyplývá z faktu, že $k \in \mathbb{Z}$? My vlastně čtenáře pokusem o logický zápis mateme, protože $n^2 = 2 \cdot 2k^2$ vyplývá čistě z faktu $n = 2k$.

Naše potíže se symbolickým zápisem vyplývají z toho, že důkaz je ve skutečnosti jakoby dvojkolejný, což bychom na onom ubrousku našemu kolegovi velice výstižně znázornili obrázkem

$$n \text{ sudé} \longrightarrow \left\{ \begin{array}{l} n = 2k \longrightarrow n^2 = 2(2k^2) \\ k \in \mathbb{Z} \longrightarrow 2k^2 \in \mathbb{Z} \end{array} \right\} \longrightarrow n^2 \text{ sudé.}$$

Toto je mimochodem časté, typický důkaz se nepohybuje jednou logickou linkou, je spíše jako řeka, která přibírá přítoky, občas se rozdvojí, pak zase spojí. V neformálním styku je možné toto vystihnout jakýmsi grafovým obrázkem, podobně jak jsme to před teď udělali. Bývá to velice efektivní při předávání představy, jak takový důkaz plyne, ale v knihách to nenajdeme. Jednak to není považováno za dostatečně správné, ale i kdybychom se rozhodli být nekonformní, tak je tu problém technický, sázení textu nám zajímavější situace nedovolí znázornit.

Při oficiálních příležitostech je tedy lepší se vyhýbat značkám (zejména $\implies$) a spíše používat k popisu plynutí důkazu slova. Mimo jiné si tak otevřeme snadná dvířka pro občasný přísun informací zvenčí slovy „obecně platí“. △

Abychom toto téma uzavřeli, správnou kompozici důkazů včetně úrovně detailů se člověk naučí praxí. Takže další příklad.

Fakt.
Nechť $x \in \mathbb{R}$. Jestliže $x > 0$, pak $x(x^2 + 1) > 0$.

Neboli všechna kladná čísla splňují $x(x^2+1) > 0$. Pokud použijeme formalizaci doslovně tak, jak je věta napsána, dostáváme

• $\forall x \in \mathbb{R}$: $[x > 0 \implies x(x^2 + 1) > 0]$.

Nebo můžeme schovat předpoklady do množiny, což jde snadno, protože značení pro kladná reálná čísla už existuje.

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

Není ale až tak známé, čtenáři asi ocení spíš první verzi.

S **Rozbor:** Protože jde o obecný výrok, začneme tím, že si vezmeme univerzálního zástupce x. Pro něj chceme dokázat platnost implikace, proto si přibereme předpoklad, že $x > 0$. Potřebujeme pak odvodit (bez znalosti, o které číslo jde), že $x(x^2 + 1) > 0$, přičemž kromě předpokladů $x \in \mathbb{R}$ a $x > 0$ můžeme použít i další věci, které s jistotou víme o reálných číslech. Symbolicky:

• Známo: x je reálné číslo
$x > 0$

• Chceme: $x(x^2 + 1) > 0$.

Je třeba najít nějaké propojení. Nabízí se pravidlo, že součin dvou kladných čísel je kladný. O x to už víme z předpokladu, výraz $x^2 + 1$ je také vždy kladný, to by mělo jít.

Je potřeba nějak dokazovat, že $x^2 + 1 > 0$? To je dobrá otázka, osobně bych to asi v této knize nedělal, bral bych to jako samozřejmou znalost. Naštěstí to nemusíme řešit, protože se můžeme odkázat na již odvedenou práci, jmenovitě tvrzení v příkladu 1c.a. Recyklace výsledků je v matematice oblíbená, tak si to alespoň vyzkoušíme v praxi.

Tím už máme jasno, jak se to dokáže, ještě potřebujeme vymyslet, jak to napsat. Fakta, jak je máme seřazena, mají podobu soutoku dvou řek:

$$\left.\begin{array}{l}\text{předpoklad } x > 0\\ \text{vždy platí } x^2 + 1 > 0\end{array}\right\} \implies x(x^2 + 1) > 0.$$

Je potřeba to napsat do jednoho proudu, takže si vybereme, kde začneme, a druhý proud se nám v polovině přidá, třeba takto.

Důkaz: Nechť $x \in \mathbb{R}$ je libovolné. Každé reálné číslo splňuje $x^2 + 1 > 0$ (viz příklad 1c.a), z předpokladu také $x > 0$ a víme, že součin dvou kladných čísel je kladný. Proto $x(x^2 + 1) > 0$.

□

Pro úplnost ještě ukážeme, jak by tento důkaz vypadal v běžné kapitole nevěnované dokazování. Rovnou jich ukážeme několik.

Důkaz je zřejmý.

Důkaz je triviální.

Důkaz je snadný a přenecháme jej čtenáři jako cvičení.

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 a dokáže se hravě, ani se nemusím snažit u zkoušek.

Vraťme se ještě k důkazu vyčerpáním neboli rozdělováním na případy. Ne vždy je k úspěchu nutné dojít u každé cesty ke stejnému cíli.

Fakt 1c.3.
Nechť $x \in \mathbb{R}$ splňuje $(x + 2)(x - 3) < 0$. Pak $x^2 < 9$.

S **Rozbor:** Logický zápis nabízí dvě přirozené možnosti. Přímý přepis dává implikaci:

- $\forall x \in \mathbb{R}$: $[(x+2)(x-3) < 0 \implies x^2 < 9]$.

Nabízí se také možnost zavést speciální množinu $M = \{x \in \mathbb{R} : (x+2)(x-3) < 0\}$ a pak použít vyjádření

- $\forall x \in M$: $x^2 < 9$.

Když si začneme rozebírat, jak se tyto dvě verze dokazují, tak v úplně prvním kroku bude rozdíl. Verze implikační říká, že máme vzít libovolné $x \in \mathbb{R}$ a předpokládat o něm, že $(x+2)(x-3) < 0$. Druhá verze říká, že máme vzít libovolný prvek $x \in M$. Jenže to při bližším pohledu dává přesně stejnou informaci jako u první verze, takže oba přepisy nakonec vedou na stejný důkaz.

Důkaz: Uvažujme libovolné reálné x splňující $(x+2)(x-3) < 0$. Pak jsou dvě možnosti:
a) $x+2 > 0$ a $x-3 < 0$ neboli $x > -2$ a $x < 3$. Pak $-2 < x < 3$, tedy $|x| < 3$ a proto $x^2 < 9$.
b) $x+2 < 0$ a $x-3 > 0$ neboli $x < -2$ a $x > 3$. Toto nemůže nastat.

□

Pokud druhá možnost nemůže nastat, tak tam nejsou x, které by dokazovanou implikaci učinily neplatnou, tudíž tato varianta neovlivní platnost dokazovaného tvrzení. Možnosti sice nevedly ke stejnému závěru, ale platný důkaz to je.

1c.4 Nepřímý důkaz

I ten slouží k dokazování implikace, finta spočívá v tom, že se namísto té dané dokazuje její obměna (viz část 1a), což je z logického pohledu totéž. Proč bychom to chtěli dělat? Obvykle tak činíme v případě, že nám p nedává vhodný startovní materiál.

Fakt.
Nechť $x \in \mathbb{R}$. 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 dále, že $x = 0$. Pak $x^2 = x \cdot x = 0 \cdot 0 = 0$.

□

To byl samozřejmě triviální příklad, ale pěkně ukázal podstatu nepřímého důkazu. Setkáme se s ním také v příkladě 1c.d či například u Faktu 1d.3.

1c.5 Důkaz sporem

Důkaz sporem je jedním z nejmocnějších nástrojů. Bývá také nadužíván a často použit špatně, dokonce je špatně učí některé středoškolské učebnice. Jak tedy skutečný důkaz sporem funguje?

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. Oblíbenou situací je, když chceme dokázat, že něco neexistuje. To se přímo dokazuje špatně (dokažte, že kolem nás nelítají neviditelní a nenahmatatelní Marťani 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. Ukážeme si to.

Čtenáře patrně nepřekvapí tvrzení, že existuje záhadné číslo $z \in \mathbb{R}$ s vlastností, že pro libovolné $x \in \mathbb{R}$ platí $x \cdot z = 0$. Formálně a s upozorněním na význam pořadí kvantifikátorů:

- $\exists z \in \mathbb{R}\, \forall x \in \mathbb{R}$: $x \cdot z = 0$.

Důkaz je snadný, představíme číslo $z = 0$, to splňuje požadovanou vlastnost, protože opravdu pro libovolné $x \in \mathbb{R}$ platí $x \cdot 0 = 0$. A co sčítání?

Fakt 1c.6.
Neexistuje číslo $z \in \mathbb{R}$ takové, že pro všechna $x \in \mathbb{R}$ platí $x + z = 0$.

Důkaz: Tvrzení dokážeme 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.

Jako příklad znovu dokážeme (tentokráte sporem), že pro všechna reálná čísla platí $x > 0 \implies x(x^2 + 1) > 0$.

Důkaz: Mějme libovolné reálné číslo x a předpokládejme, že platí $x > 0$ a také $x(x^2 + 1) \leq 0$ (negace závěru). Nerovnost můžeme vydělit kladným číslem x na obou stranách a ona pořád zůstane platná, máme tedy $x^2 + 1 \leq 0$. Takže $x^2 \leq -1$, zároveň $x^2 \geq 0$, spojením dostáváme $0 \leq x^2 \leq -1$ neboli $0 \leq -1$, což je spor.

□

Je vidět, že v tomto případě byl přímý důkaz výhodnější. Poznat, kdy je lepší dokazovat implikaci sporem, se člověk naučí praxí.

Řadě středoškoláků namluvili, že implikace $p \implies q$ se sporem dokazuje takto: Vyjdeme z toho, že q neplatí, a dojdeme k tomu, že také p neplatí, což je ve sporu s předpokladem p. Tento postup má několik problémů. Z logického pohledu nejde o důkaz sporem, protože nevycházíme z negace implikace. Z metodického postupu je to nevhodný přístup, protože jestliže jsme z neplatnosti q odvodili neplatnost p, tak jsme už vlastně udělali nepřímý důkaz, máme hotovo a je zcela zbytečné ještě na konec naroubovat jako ocásek zcela uměle nějaký spor.

Někdy se to vykládá tak, že se vyjde z předpokladu, že p platí a q neplatí, což je negace implikace, tedy správný začátek důkazu sporem. Pak se ale řekne, že se máme zkusit dostat k tomu, že p neplatí, čímž vznikne hledaný spor. Formálně je to už pravda, ale je to zbytečně omezující, ten spor je totiž možné vyrobit klidně i jinak, nemusíme se nutit dojít k negaci p.

Tím jsme probrali hlavní metody důkazu. Obecně se dá říci, že obvykle jako první zkoušíme důkaz přímý, protože svou strukturou kopíruje dané tvrzení, což pomáhá při jeho vytváření i pochopení u čtenáře. Důkaz nepřímý či sporem volíme v případech, kdy nám zkušenost napoví, že by to tak bylo lepší (popřípadě když se nám přímý důkaz ne a ne podařit, tak se rozhodneme zkusit něco jiného). Obvykle je lepší zkusit nejprve důkaz nepřímý, protože případů, kdy je důkaz sporem tím nejvhodnějším, zase tolik není.

Dosavadní zkušenosti zkusíme vydestilovat do několika (doufejme užitečných) rad.

S 1c.7 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. Rozmyslete si základní kostru důkazu, ta je dána strukturou dokazovaného výroku: Jaký je tam kvantifikátor, jaká logická spojka v tvrzení – nejspíše implikace. Měl by tak vzniknout hlavní plán: Kde začneme, odkud kam chceme dojít. Případný rozklad na případy lze také často vidět již v této fázi.

2. Udělejte si pořádek v situaci. Rozmyslete si, co máte k dispozici ze zadání (tedy co „víte“), a k čemu máte dojít. V obou kategoriích mohou dále přibýt alternativní přepisy, obvykle se totiž vyplácí podívat se na to, co známe, a vyjádřit si to jiným způsobem (pokud to jde), totéž platí o cílových tvrzeních.

Pokud se vám během vytváření důkazu vyskytnou další faktíky, přidávejte si je do správných kategorií („mám“ versus „chci k tomu dojít“). Dá se říct, že vymýšlení důkazu je proces, jak faktíky převést z kategorie „chci tam“ do kategorie „už mám“.

Je opravdu důležité mít v tomto pořádek. Když pak budete psát načisto korektní důkaz, je kritické se při každém použití nějakého faktíku ujistit, že je opravdu v kategorii „mám“ neboli mohu to použít. Další výhodou takového přehledu je, že když se zadrhnete, tak je možné se podívat na seznam věcí, které jsou k dispozici. Použili jste už všechno nebo je tam ještě něco, co je k dispozici? Tato jednoduchá věc často výrazně napoví. Pokud napíšete důkaz a nepoužijete v něm všechny předpoklady, tak je to většinou znamení, že je někde chyba.

3. Vyplatí se zamyslet nad pojmy, se kterými se v dokazovaném tvrzení pracuje, ujasnit si, co umožňují, jaký jazyk se s nimi pojí. Například relace je ve skutečnosti množina dvojic, je tedy možné používat množinové nástroje (sjednocení a podobně). Dělitelnost čísel je zase vlastnost (pravdivý či nepravdivý výrok), takže ji není možné třeba

„násobit“ jako rovnici, nelze prostě jen tvrdit, že vztah $a \mid b$ „rozšíříme“ číslem c na $(ca) \mid (cb)$. Když pracujeme s řešením rovnice, tak se vyplatí myslet na to, jak se vlastně pozná, že je něco řešením rovnice: Prostě dosadíme.

V mnoha případech také pomůže, když se nějaký pojem přeloží do jiného jazyka. Nejčastěji takto používáme přepis podle definice, ale jsou i další možnosti. Někdy tak dostaneme nápovědu, kudy vést důkaz. Například mezi pojmy spojitosti a derivovatelnosti na první pohled nějaká vazba není. Když se ale podíváme na jejich definice, zjistíme, že obě definice používají pojem limity, což je klíčem k nalezení jejich vzájemného vztahu.

Někdy nás přechod k alternativě prostě jen psychologicky nakopne. Například to, že objekt a není v jisté množině A, lze zapsat $a \notin A$, $\neg(a \in A)$ či dokonce $a \in \overline{A}$. Může se stát, že jedno z těch vyjádření vyloženě zapadne do situace, zatímco ostatní by případný důkaz jen komplikovaly.

4. Všechno si pište. Typická situace: Student potřebuje pomoci s důkazem. Přijdu a vidím, že má na papíře pěkně srovnáno, co ví a kam se chce dostat. Začal si v hlavě sumírovat postup, ale zadrhnul se a neví, jak dál. Vypráví mi, kam zatím došel, a já mu řeknu, ať to napíše. Student to udělá, podívá se na to a najednou ví, co dál. Kdybych dostal stovku pokaždé, co tohle zažiju, mohl bych svůj plat dávat na charitu.

Mozek pracuje lépe s tím, co vnímá očima, než s tím, co má v sobě (zjednodušeně řečeno, sám do sebe nevidí). Zkušený dokazovač si dokáže ledacos v hlavě srovnat, ale pro začátečníka může být rozdíl mezi napsaným a jen v hlavě představovaným rozhodující. Pokud máte nějaký nápad, napište si jej a pak se na něj podívejte.

Když tohle děláte nějakou chvíli, máte před sebou stránku či dvě popsané matematickými výrazy, v mnoha případech jde o již zavržené slepé uličky, prostě zmatek. Udělejte si novou stránku, kam si přehledně vypište, co máte k dispozici (a k čemu se už umíte korektně dostat) a co chcete mít na konci. Pak se na to zkuste znovu podívat.

Když nevíte, kudy kam, tak si projděte, zda jste už zkusili použít vše, co máte k dispozici. Znovu se podívejte, kam se chcete dostat. Je to nějaké tvrzení, ve kterém se nejspíš objevují nějaké matematické objekty. Zkuste se o každém z nich zamyslet, co o něm víte a které z daných faktíků o něm něco vypovídají.

5. Když máte pocit, že už máte důkaz, tak zkuste zresetovat mozek a pak ten důkaz načisto napsat. Když začátečník vymýšlí drobet komplikovanější odvození, tak jsou jeho poznámky zřídka využitelné jako důkaz, je nutné je nejprve „učesat“. Při tom přepisování si hlídejte, zda fungují podstatné náležitosti. Jsou jednotlivé „proto“ správně odůvodněny? Je to, co v důkazu používáte, opravdu již v dané chvíli známo jako pravdivé?

6. Napsaný důkaz si znovu projděte, tentokráte „z nadhledu“, kdy ignorujete jednotlivé technické detaily (výpočty a tak). Je správná jeho celková struktura? Plynou myšlenky správným směrem, navazují na sebe? Použili jste předpoklady, které vám byly k dispozici? Dojde důkaz opravdu na konci k tomu, co potřebujete? Pokud po půl stránce výpočtu vítězoslavně podtrhnete $1 = 1$, tak je to skoro určitě špatně, protože toto jste asi dokazovat nechtěli.

△

Náš důkaz je také třeba rozumně napsat. Následující rady se ovšem vztahují na psaní matematiky všeobecně.

S 1c.8 Poradní koutek: Jak psát (a číst) matematičtinu.

Zachycovat úvahy pomocí matematicko-logického zápisu vyžaduje praxi. Existují typické chyby, které se u začátečníků objevují, a mnohé se dají odchytit jednoduchými triky.

1. To, co napíšeme, by mělo po nahrazení symbolů českými slovy tvořit věty. Podmět, přísudek a tak podobně a dohromady by to mělo dávat smysl. Jestliže náš zápis končí symboly „$\implies 13$“, tak po překladu do češtiny dostáváme „a proto 13“. Člověk ani nemusí moc rozumět matematice, aby poznal, že tohle zní podezřele. Co třináct? Kde? Nebo možná kdy? Zato zápis „$\implies x = 13$“ už smysl dává (což ještě neznamená, že je to dobře, ale je to dobrý začátek).

Naopak věty psané slovy by to překladu do logičtiny měly říkat to, co chceme vyjádřit.

2. V logických tvrzeních by měly sedět **typy** jednotlivých součástí. Uvažujme zápis „$3 + 5 = 7 \implies x > 5$“. Nevíme, oč tam jde, takže nebudeme řešit pravdivost, ale všimneme si, že spojka $\implies$ spojuje výroky. Na levé straně vidíme „$3 + 5 = 7$“, to je výrok, stejně jako věc „$x > 5$“ napravo. Z tohoto pohledu tedy celé tvrzení není nesmyslné, pracuje se správnými pojmy.

Na druhou stranu úvaha „$1 + 2 \implies x > 5$“ už špatně je, a to na základní úrovni. Část „$1 + 2$“ totiž není výrok (s hodnotou True či False), ale algebraická operace, jejímž výstupem je číslo. Logická spojka $\implies$, ať už použitá v logickém světě či jako neformální zkratka pro slova „z toho vyplývá“, ale musí pracovat s hodnotami True/False, už z principu neumí pracovat s čísly. Programátoři v tomto jistě vidí chybu špatného typu dat.

Podobně nelze úvahu „$6 \mid a \implies 4 \mid a$“ neboli „jestliže 6 dělí a, pak také 4 dělí a“ (viz kapitola 2, opět nás teď nezajímá, zda je fakticky správná) zapsat ve formě „$\frac{a}{6} \implies \frac{a}{4}$“. Slovní spojení „$6 \mid a$“ je výrok, proto jej lze nahradit hodnotami True či False, což jsou pro logické odvozování ty správné hodnoty. Na druhou stranu „$\frac{a}{6}$“ je

matematická operace, jejímž výstupem je číslo. Z čísla jako takového nelze logicky odvodit nic. Pokud bychom ovšem napsali „$\frac{a}{6} \in \mathbb{Z} \implies \frac{a}{4} \in \mathbb{Z}$“, tak už to zase smysl má, protože „$\frac{a}{6} \in \mathbb{Z}$“ je výrok (pravdivý či nepravdivý).

Na závěr pár skutečných perel odchycených u zkoušek:

• $\forall x \implies x > 2$.

Česky například „pro každé x, z toho vyplývá, že $x > 2$“. Asi to mělo být $\forall x$: $x > 2$.

• Protože $A \cap B$, musí být $A \subseteq B$.

Protože „$A \cap B$“ není ani pravdivé, ani nepravdivé, ale množina, jen těžko z toho budeme něco odvozovat.

3. Každá proměnná, kterou v úvahách použijeme, musí odněkud přijít. Některá „písmenka“ přijdou již ze zadání. Pokud máme diskutovat pravdivost tvrzení „je-li funkce f spojitá v bodě a, pak je tam i diferencovatelná“, tak v našich úvahách očekáváme výskyt písmen f a a a jejich význam je zjevný, to jsou dané objekty (funkce a bod, z kontextu usuzujeme na nevyslovené prokaždítko, tedy jsou libovolně vybrané).

Pokud se pak v našich úvahách objeví třeba x, pak nemůže spadnou jen tak odnikud. Obvykle si nová písmenka zavádíme sami, pak musíme říct, jak jsou vybírána. Typicky bychom mohli říct „vezměme libovolné reálné x“, takže by se v zápisu našich úvah mělo objevit $\forall x \in \mathbb{R}$. Často také vybíráme nějaké speciální, třeba „uvažujme x takové, že $f(x) = f(a)$“. Pak očekáváme, že se v zápise objeví značka existítka. V takovém případě ovšem musíme doložit, že vůbec nějaký objekt tohoto typu existuje. Jednoduchý příklad takovéto úvahy (kde n je již dáno):

„Je-li n sudé, pak podle definice existuje $k \in \mathbb{Z}$ takové, že $n = 2k$“.

Shrnuto, pokud se v našem zápise objeví neznámé písmenko, tak by mělo být doprovázeno kvantifikátorem a vymezením, odkud a jak přišlo.

Tato jednoduchá zásada může odhalit mnohé chyby ještě dříve, než se stanou akutními. Typický příklad: Zatímco správný zápis matematické indukce je

$$\forall n \in \mathbb{N}: \ [V(n) \implies V(n+1)],$$

studenti někdy napíší: „Předpokládejme, že pro každé n platí $V(n)$. Tvrdíme, že pak platí i $V(n+1)$“. Toto se symbolicky zapíše jako

$$[\forall n \in \mathbb{N}: \ V(n)] \implies V(n+1).$$

Je to jistě špatně, a to ani nemusíme nic vědět o indukci. Zatímco n v levé části je kvantifikováno prokaždítkem a tudíž víme, odkud se bere (uživatel si jej vybírá dle libosti), to n napravo od implikace spadlo z nebe, vůbec nevíme, co je zač. Je také libovolné? Nebo nějaké speciální? Mohla by to být moje šťastná třináctka?

Shrnuto, pokud něco matematického vymyslíme a zkusíme to zapsat, je pak dobré si to po sobě znovu přečíst a hlídat si ony tři formální aspekty: Má to být češtinářsky čitelné, pojmy mají být správně používány a neznámé musí být nějak uvedeny. Pokud náš text tímto testem projde, tak ještě nemusí jít o korektní matematickou úvahu, ale alespoň v něm nebudou elementární chyby a zkoušející se nám nebude posmívat.

△

Na závěr se ještě podíváme na dva poučné příklady.

Příklad 1c.d: Dokážeme následující tvrzení:

• Každé prvočíslo větší než 2 je liché.

Nejprve si toto tvrzení formalizujeme. Nabízí se několik možností. První využívá kombinovaného předpokladu.

• $\forall n \in \mathbb{N}$: $\big[[n \text{ prvočíslo a } n > 2] \implies n \text{ liché}\big]$.

Druhá možnost využívá množinu $N_2 = \{n \in \mathbb{N} : n > 2\}$ a zní

• $\forall n \in N_2$: $[n \text{ prvočíslo} \implies n \text{ liché}]$.

Pak je také možnost zavést $P_2 = \{n \in \mathbb{N} : n \text{ prvočíslo} \wedge n > 2\}$ a psát

• $\forall n \in P_2$: n liché.

V této chvíli není jasné, zda některá verze není lepší. Normálně bychom preferovali tu úplně první, protože čtenáře nezatěžuje novým značením.

Jak by vypadal přímý důkaz? Rozmyslete si, že ve všech formalizacích bychom začali stejně: Vzali bychom libovolné přirozené číslo n, o kterém bychom navíc předpokládali, že je to prvočíslo a splňuje $n > 2$. Měli bychom o něm dokázat, že je liché.

Podle rad o vytváření důkazů je teď čas si rozmyslet, co máme k dispozici. Co to vlastně znamená, že je n prvočíslo? Podle definice to znamená, že jej není možné rozložit jako součin dvou přirozených čísel větších než 1. To je ovšem nepříjemný typ informace, říká, že něco není možné. Není jasné, jak bychom se z toho mohli někam dostat, když nemáme v ruce něco konkrétního.

Nabízí se inspirace, že bychom raději pracovali s informací opačnou, tedy že n není prvočíslo, pak bychom totiž získali něco konkrétního, jmenovitě rozklad. Jak se dostaneme k negaci? Nepřímým důkazem. Zkusíme tedy tento přístup.

Abychom mohli dělat nepřímý důkaz, potřebujeme přejít k obměně implikace, což nás vrací k oněm třem verzím výše. Hned vidíme, že třetí není vhodná. U prvních dvou by obměny dopadly následovně (viz pravidla pro negování):

- $\forall n \in \mathbb{N}$: $\big[n$ sudé $\implies [n$ není prvočíslo nebo $n \leq 2]\big]$.
- $\forall n \in N_2$: $[n$ sudé $\implies n$ není prvočíslo $]$.

První formulaci bychom dokazovali tak, že bychom vzali sudé přirozené číslo a pokoušeli se s ním trefit do závěru. Ten je ovšem složitější, neboť má dvě části, ne že by to nešlo, ale vypadá to na mírnou komplikaci. Raději se podíváme dál.

Druhou verzi bychom dokazovali tak, že vezmeme sudé přirozené číslo větší než 2 a zkusíme o něm ukázat, že není prvočíslo. To vypadá jako něco, co by mělo jít. Tato verze tedy vypadá nejnadějněji. Protože jde o jednoduchý příklad, zkusíme rovnou napsat důkaz, konec konců, máme již praxi.

Důkaz: Nechť n je sudé přirozené číslo větší než 2. Pak jej lze zapsat jako $n = 2k$ pro $k \in \mathbb{Z}$. Co víme o čísle k? Protože $n > 2$, tak nutně musí platit $k > 1$. Ukázali jsme, že číslo n lze napsat jako součin dvou přirozených čísel (dvojky a k), která jsou větší než 1, proto podle definice n není prvočíslo.

□

V tomto příkladě jsme viděli, že nemusí být úplně jedno, jakým způsobem formálně vyjádříme text tvrzení. Nestává se to často. Pro úplnost ukážeme, jak by vypadal důkaz, pokud bychom pracovali s prvním vyjádřením.

Nechť n je sudé přirozené číslo. Pak jej lze zapsat jako $n = 2k$ pro $k \in \mathbb{Z}$. Rozebereme dva případy. Pokud $n \leq 2$, pak je pravdivý výrok „n není prvočíslo nebo $n \leq 2$“ a důkaz je hotov.

Pokud by platilo $n > 2$, tak by také nutně platilo $k > 1$. V tomto případě bychom tedy měli rozklad n jako součin dvou přirozených čísel větších než 1, proto podle definice n není prvočíslo. Opět jsme potvrdili platnost závěru. Jiná možnost pro n není, důkaz je tedy hotov.

△

Příklad 1c.e: Dokážeme, že pro všechna $x \in \mathbb{R}$, která nejsou rovna ± 1, platí

$$\frac{x+1}{x-1} + \frac{x-1}{x+1} = 2\frac{x^2+1}{x^2-1} \qquad (*)$$

Mnoho lidí by zkusilo rovnost upravovat, přičemž v prvním kroku by se zbavili zlomků pomocí násobení faktorem $(x-1)(x+1)$. To je povoleno, protože pracujeme s čísly x, pro která tento výraz není nulový.

$$\begin{aligned} \frac{x+1}{x-1} + \frac{x-1}{x+1} &= 2\frac{x^2+1}{x^2-1} \\ (x+1)^2 + (x-1)^2 &= 2(x^2+1) \\ x^2 + 2x + 1 + x^2 - 2x + 1 &= 2x^2 + 2 \\ 0 &= 0 \end{aligned}$$

Co tento výpočet ukázal? Dokázali jsme platnost implikace „pokud platí rovnost $(*)$, tak $0 = 0$“. My jsme ovšem rovnost $0 = 0$ dokazovat nechtěli, takže rozhodně není čas výpočet podtrhnout a skončit.

Praktický význam tohoto postupu je, že jsme nalezli úpravy, které by mohly vést k důkazu. Klíčová otázka zní, zda byly tyto úpravy (kromě toho, že jsou korektní) také ekvivalentní, tedy zda by fungovaly i při čtení opačným směrem. V tomto případě to je pravda, čímž dostáváme platný důkaz (úpravy značíme za šikmou čárou napravo):

$$\begin{aligned} 0 &= 0 && \big/ + 2x^2 + 2 \\ 2x^2 + 2 &= 2x^2 + 2 && \big/ \text{algebra} \\ x^2 + 2x + 1 + x^2 - 2x + 1 &= 2x^2 + 2 && \big/ \text{algebra} \\ (x+1)^2 + (x-1)^2 &= 2(x^2+1) && \big/ \div (x+1)(x-1) \\ \frac{x+1}{x-1} + \frac{x-1}{x+1} &= 2\frac{x^2+1}{x^2-1} \end{aligned}$$

Pokud se nám to nechce přepisovat, je možné pod onen předchozí postup přidat následující magickou větu: „Protože byly všechny úpravy ekvivalentní, je možné výpočet provést v opačném směru, čímž dostaneme důkaz.“ Samozřejmě musíme nejdřív zkontrolovat, že máme pravdu.

Další zajímavá možnost se nabízí, když si všimneme, že (s výjimkou řádku se zlomkem) se vlastně výraz na levé straně vůbec fakticky neliší, jen jen upravujeme, totéž platí pro pravou stranu. Náš první (nesprávný) postup tedy

nabízí další zajímavou myšlenku, a to sjet po jedné straně až k rovnosti, která je zjevná, a pak druhou stranou zase vyjet nahoru. Dostáváme tak řetěz rovností

$$(x+1)^2+(x-1)^2 = x^2+2x+1+x^2-2x+1 = 2x^2+2 = 2(x^2+1).$$

Toto je vysoce perspektivní postup, protože neupravujeme rovnice, tudíž nás nemusí zajímat nějaká ekvivalence kroků, my prostě používáme známé algebraické identity. Někdy je tento přístup dokonce i kratší, protože občas se stane, že při postupném upravování rovnice musíme na jedné straně ještě pracovat, zatímco ta druhá je již hotová a jen ji pořád opisujeme.

V některých situacích je rozdíl mezi přístupy dokonce zásadní. To se týká zejména situací, kdy dokazujeme nerovnosti, pak je totiž často přístup ekvivalentními úpravami nemožný, zatímco postup postupnými kroky realizovat lze. Tento rozdíl se ukáže jako klíčový v některých příkladech v kapitole 8 o indukci.

V tomto příkladě nicméně máme drobnou komplikace, ještě tam nějak potřebujeme doplnit ten zlomek. Dá se to udělat například vytvořením potřebného faktoru přechodem na společný jmenovatel.

$$\begin{aligned}\frac{x+1}{x-1}+\frac{x-1}{x+1} &= \frac{(x+1)^2+(x-1)^2}{(x-1)(x+1)} = \frac{x^2+2x+1+x^2-2x+1}{(x-1)(x+1)}\\ &= \frac{2x^2+2}{(x-1)(x+1)} = 2\frac{x^2+1}{x^2-1}.\end{aligned}$$

Tento důkaz je z mnoha hledisek nejlepší.

△

Cvičení

Cvičení 1c.1: Použijte následující úpravy

$$\begin{aligned}\left(\sqrt{18}+\sqrt{8}\right)^2-\left(\sqrt{18}-\sqrt{8}\right)^2 &= \left(4\sqrt{3}\right)^2\\ 18+2\sqrt{18}\sqrt{8}+8-18+2\sqrt{18}\sqrt{8}-8 &= 4^2\cdot 3\\ 4\sqrt{18}\sqrt{8} &= 48\\ 4\sqrt{18\cdot 8} &= 48\\ 4\sqrt{144} &= 48\\ 4\cdot 12 &= 48\end{aligned}$$

jako inspiraci k důkazu rovnosti z prvního řádku pomocí řetězu rovností a algebraických úprav.

Cvičení 1c.2 (*dobré)**:** V každém následujícím zadání dostanete tři či dva jednoduché výroky. Uspořádejte je tak, aby vznikla korektní matematická úvaha, a napište ji správně slovy.

(i) $x>0$, $x>1$, $x^2>1$;
(ii) $x^2>2$, $x>2$, $x<-2$;
(iii) $x=3$, $x^2-2x-3=0$;
(iv) 2 dělí a, 6 dělí a;
(v) 3 dělí a, 2 dělí a, 6 dělí a;
(vi)* $x-y=3$, $3x+y=1$, $5x+2y=1$.

Cvičení 1c.3: Dokažte či vyvraťte následující tvrzení.

(i) $\forall x\in\mathbb{R}$: $[x<5\vee x^2>4]$;
(ii) $\forall n\in\mathbb{Z}$: [n je sudé $\vee n>4$];
(iii) $\forall x\in\mathbb{R}\,\exists y\in\mathbb{R}$: $x+y=2$;
(iv) $\forall x\in\mathbb{R}\,\exists y\in\mathbb{R}$: $x\cdot y=1$;
(v) $\forall m\in\mathbb{N}\,\exists n\in\mathbb{N}$: $m-n=2$;
(vi) $\exists m\in\mathbb{Z}\,\forall n\in\mathbb{N}$: $\frac{m}{n}=0$;
(vii) $\exists m\in\mathbb{Z}\,\forall n\in\mathbb{Z}$: $m+n=n$;
(viii) $\exists m\in\mathbb{Z}\,\forall n\in\mathbb{Z}$: $m+n=2m$;
(ix) $\forall n\in\mathbb{Z}\,\exists m\in\mathbb{N}$: $m=|n|$;
(x) $\forall n\in\mathbb{Z}\,\exists m\in\mathbb{N}_0$: $m=|n|$;
(xi) $\forall n\in\mathbb{Z}\,\exists m\in\mathbb{Z}$: $[|m|=|n|\wedge m\neq n]$;
(xii) $\forall n\in\mathbb{N}\,\exists m\in\mathbb{N}$: $n=m^2$.

Cvičení 1c.4: Představme si, že existuje definice, která popisuje, kdy jsou čísla „pěkná“. Konkrétní obsah tohoto pojmu nás nebude zajímat, podstatné je, že podle této definice každé číslo x buď je pěkné, což značíme $p(x)$, nebo pěkné není, což přirozeně značíme $\neg p(x)$. Uvažujme následující tvrzení:

• Jestliže jsou všechna celá čísla pěkná, pak jsou všechna sudá čísla pěkná.

a) Zapište toto tvrzení formálním jazykem. Můžete použít symbol S pro množinu všech sudých čísel.
b) Dokažte toto tvrzení.
c) Napište obměnu tohoto tvrzení.
d) Dokažte tuto obměnu; jde vlastně o nepřímý důkaz původního tvrzení.
e) Dokažte původní tvrzení sporem.

Řešení:
1c.1: $\left(\sqrt{18}+\sqrt{8}\right)^2-\left(\sqrt{18}-\sqrt{8}\right)^2=18+2\sqrt{18}\sqrt{8}+8-18+2\sqrt{18}\sqrt{8}-8=4\sqrt{18}\sqrt{8}=4\sqrt{144}=4\cdot 12$ $=16\cdot 3=\left(4\sqrt{3}\right)^2$. Tento postup je kratší.
1c.2: (i): Pro libovolné $x\in\mathbb{R}$ platí: Jestliže $x^2>1$ a $x>0$, pak $x>1$.
Alternativa: Nechť $x\in\mathbb{R}$. Jestliže $x^2>1$ a $x>0$, pak $x>1$.
Alternativa: Pro libovolné $x\in\mathbb{R}$ splňující $x>0$ platí: Jestliže $x^2>1$, pak $x>1$.
Poznámky: Je možné použít i jinou množinu než $\mathbb{R}$, například celá čísla.
Nabízí se ještě jeden výrok: Jestliže $x>0$ a $x>1$, pak $x^2>1$. Toto je sice pravdivé tvrzení, ale není to korektní úvaha, protože mate čtenáře: Onen předpoklad $x>0$ je v ní zbytečný, platí $x>1\implies x^2>1$.
(ii): Pro všechna $x\in\mathbb{R}$ platí: Jestliže $x^2>2$, pak $x>2$ nebo $x<-2$.
Alternativa: Pro všechna $x\in\mathbb{R}$ platí: Jestliže $x>2$ nebo $x<-2$, pak $x^2>2$.
(iii): Pro všechna $x\in\mathbb{R}$ platí: Jestliže $x=3$, pak $x^2-2x-3=0$.
Poznámka: Neplatí „Jestliže $x^2-2x-3=0$, pak $x=3$.“
(iv): Pro každé $a\in\mathbb{Z}$ platí: Jestliže 6 dělí a, pak 2 dělí a.
(v): Pro každé $a\in\mathbb{Z}$ platí: Jestliže 6 dělí a, pak 2 dělí a a 3 dělí a.
Alternativa: Pro každé $a\in\mathbb{Z}$ platí: Jestliže 3 dělí a a 2 dělí a, pak 6 dělí a.
(vi): Zde je třeba si rozmyslet, že jde o tři nezávislé rovnice a kdykoliv si dvě vybereme, dostáváme pokaždé řešení $x=1$, $y=-2$, takže pak je splněna automaticky i třetí rovnice. Nabízí se proto tři možné úvahy, toto je jedna z nich:
Pro každé $x,y\in\mathbb{R}$ platí: Jestliže $x-y=3$ a $3x+y=1$, pak $5x+2y=1$.
1c.3: (i): Platí. D: Libov. $x\in\mathbb{R}$. 1) Pokud $x<5$, pak $[x<5\vee x^2>4]$ je T. 2) Pokud $x\geq 5$, pak $x^2\geq 25>4$, proto $[x<5\vee x^2>4]$ je T.
(ii): Neplatí. D: $n=3$.
(iii): Platí. D: Libov. $x\in\mathbb{R}$, pak $y=2-x$ splňuje.
(iv): Neplatí. D: Pro $x=0$ je pro libovolné y vždy $x\cdot y=0$, ne 1.
(v): Neplatí. Pokus o D platnosti: Dáno $m\in\mathbb{N}$, volíme $n=m-2$. Pak sice $m-n=2$, ale neplatí vždy $n\in\mathbb{N}$. D neplatnosti: Když $m=1$, tak pro všechna $n\in\mathbb{N}$ platí $m-n=1-n\leq 0$, tedy nelze splnit $=2$.
(vi): Platí. D: Zvolíme $m=0$, pak $\forall n\in\mathbb{N}$: $\frac{0}{n}=0$.
(vii): Platí. D: Zvolíme $m=0$, pak $\forall n\in\mathbb{Z}$: $0+n=n$.
(viii): Neplatí. D: Sporem. Kdyby existovalo takové m, tak mimo jiné $m+1=2m$ a $m+2=2m$. Odečtením rovnic $1=0$, spor.
(ix): Nabízí se volit přímo $m=|n|$, ale nakonec neplatí. D: Pro $n=0$ bychom museli vzít $m=0$, ale $0\notin\mathbb{N}$.
(x): Platí. D: Dáno libov. $n\in\mathbb{Z}$. Zvolme $m=|n|$, pak platí vzorec a $m\in\mathbb{N}_0$.
(xi): Nabízí se volit $m=-n$, ale zas ta nula. Neplatí. D: Pokud $n=0$, tak neexistuje číslo m splňující $|m|=0$ a $m\neq 0$.
(xii): Neplatí. D: Pro $n=2$ neexistuje $m\in\mathbb{N}$ splňující $m^2=2$. Proč? $1^2<2$ a když $m\geq 2$, tak $m^2\geq 4>2$.
1c.4: a) $[\forall n\in\mathbb{Z}\colon p(n)]\implies[\forall m\in S\colon p(m)]$. Všimněte si, jak závorky vymezují platnost kvantifikátorů.
b) Předpokládejme, že platí $[\forall n\in\mathbb{Z}\colon p(n)]$. Dokážeme závěr implikace. Vezměme libovolné $m\in S$. Pak také $m\in\mathbb{Z}$, proto podle předpokladu $p(m)$.
c) Formálně: $\neg[\forall m\in S\colon p(m)]\implies\neg[\forall n\in\mathbb{Z}\colon p(n)]$.
Pravidla pro negaci dají $[\exists m\in S\colon\neg p(m)]\implies[\exists n\in\mathbb{Z}\colon\neg p(n)]$.
d) Předpokládejme, že existuje $m\in S$ takové, že $\neg p(m)$. Pak ovšem také $m\in\mathbb{Z}$ a $\neg p(m)$, což ukazuje pravdivost závěru.
e) Předpokládejme, že platí $[\forall n\in\mathbb{Z}\colon p(n)]$, ale neplatí $[\forall m\in S\colon p(m)]$. Pak musí existovat $m\in S$ takové, že $\neg p(m)$. Ovšem $m\in\mathbb{Z}$, proto podle předpokladu $p(m)$. Pro toto číslo tedy zároveň platí $p(m)$ a $\neg p(m)$, což není možné, je to spor.
Přečtěte si tyto důkazy lidštinou, třeba: Předpokládejme, že všechna celá čísla jsou pěkná, ale neplatí už to o všech sudých. Pak existuje sudé číslo, které není pěkné. Atd. Dávají ty důkazy smysl?

1d. Množiny

Množiny jsou jedním ze základních pojmů matematického jazyka, umožňují nám vyjádřit, že něco máme (či nemáme). Pomocí množin se ale také dokazují základy, na kterých matematika stojí (čísla, základní operace, rovnosti a nerovnosti atd). Není divu, že teorie množin je samostatným oborem, o kterém jsou napsány hromady tlustých knih. My se teorii množin jako takové věnovat nebudeme (trochu se o problematiku matematických základů otřeme například zde 4c.15).

V této části se zaměříme na věci, které jsou pracovními nástroji každého matematika, tedy na to, co se dá s množinami běžně dělat (zejména operace). Nebude to nejspíš pro čtenáře nic nového, a právě toho chceme využít.

Na již známém materiálu si ukážeme, jak matematika staví teorie, a procvičíme si dokazování. To je také hlavní smysl této části. Pokud budou čtenáři při prvním čtení dělat potíže abstraktní argumenty, může mu pomoci začít s důkazy v kapitolách, kde se pracuje s konkrétními objekty, třeba s čísly v kapitole o dělitelnosti, a k této části se později vrátit.

Matematika obvykle začíná definicí základních pojmů, se kterými dále budeme pracovat, ale na to, abychom uměli správně matematicky zavést množinu, bychom se museli ponořit výrazně hlouběji do teorie množin. Proto se proviníme proti dobrým mravům a jen naznačíme.

Množina je neuspořádaný soubor objektů, které jsou jednoznačně specifikovány. Tyto objekty se nazývají **prvky** dané množiny. Množina je těmito objekty jednoznačně dána, jinými slovy, pokud mají dvě množiny stejné prvky, pak je to tatáž množina.

By a **set** we mean an arbitrary collection of objects (called its **elements**).

Připomeňme, že značení $a \in A$ znamená, že objekt a je prvkem množiny A, naopak $a \notin A$ znamená, že objekt a není prvkem množiny A. Značení $A = B$ znamená, že jde o shodné množiny, naopak $A \neq B$ znamená, že množiny shodné nejsou, tedy nemají stejné prvky.

Rozeberme si, co naše „skorodefinice“ množiny vlastně říká. To o jednoznačné specifikaci znamená, že musíme u libovolného objektu být schopni rozhodnout, zda do dotyčné množiny patří či ne. Protože jde o soubory neuspořádané, nezáleží na pořadí. Množiny $\{a, b\}$ a $\{b, a\}$ jsou proto shodné. Vyplývá to ostatně i z poslední věty výše: Obě tyto množiny mají shodné prvky, jmenovitě a a b, tudíž musí být podle naší „skorodefinice“ shodné. Tato věta má ovšem ještě jeden zásadní dopad. I množina $\{a, b, b\}$ má prvky a a b, takže musí platit $\{a, b\} = \{a, b, b\}$. Jestliže se vás tedy někdo zeptá, kolik prvků má množina s pěti červenými kolečky, pak odpověď zní, že jeden (červené kolečko), leda že by každé to kolečko bylo nějak jiné. Jakkoliv to při prvním setkání může působit zvláštně, je to přesně to pravé pro praktickou práci s množinami.

Množiny je možno zadat různými způsoby. Jeden populární je výčtem prvků, třeba $M = \{1, 13, a, \diamond\}$. Jde o způsob názorný, nicméně není perspektivní pro větší množiny, například specifikace $\{3, 5, 7, \dots\}$ nedává množinu, protože nevíme, zda do ní číslo 9 patří či ne. Mimochodem, nepatří, další číslo je 11, já jsem totiž chtěl množinu lichých prvočísel. Jenže jsem vám to neřekl matematicky správně.

Jak vidíte, je lepší se zápisu s tečkami vyhýbat, a to zejména při definování množiny, nicméně když pak dále s korektně definovanou množinou pracujeme, tak je zápis s ukázkou prvků pro svou názornost výhodný a běžně používaný. Pak je tu ještě speciální případ, zápis $\{1, 2 \dots, n\}$ je v matematické literatuře běžný dokonce i v definicích, rozumí se, že se tím míní množina zapsaná korektně $\{k \in \mathbb{N} : k \leq n\}$.

Další populární metoda je novou množinu popsat pomocí podmínky, která rozhoduje, kdo do ní patří a kdo ne. Například onu množinu výše jsem vám měl správně zadat takto: $M = \{n \in \mathbb{N} : n \text{ je liché prvočíslo}\}$. To už je správná definice, protože umíme s jistotou rozhodnout, která čísla do ní patří a která ne (třeba ona devítka ne). Tento způsob zápisu se anglicky nazývá „set builder“ a není tak samozřejmý, jak na první pohled vypadá. Souvisí to s tím, proč jsme nebyli schopni napsat jednoduchou definici pojmu množiny, a také s tím, proč je teorie množin tak hluboká a zásadní pro celou matematiku. Dovolíme si proto první odbočku pro pokročilé a zvědavé.

Poznámka: Intuitivní představa množin bývá taková, že si vymyslíme nějakou vlastnost s predikátem $p(x)$ a ptáme se, pro které objekty je splněna. Když shromáždíme všechny objekty, které ji splňují, dostaneme množinu, zapsalo by se to $\{x : p(x)\}$. Takto se na množiny díval například otec teorie množin Cantor, když ji v polovině 19. století představil světu, a docela dlouho vydržela.

Není to ale tak jednoduché, jak to vypadá. Uvažujme množinu $\{x : x \text{ kladné}\}$. Do ní by mělo patřit vše, co je kladné. Leží v ní tedy i laskavost? Evidentně je třeba začít přemýšlet o tom, na čem všem budeme podmínku $p(x)$ testovat. Ale i kdybychom se omezili čistě na matematické objekty, problémům se nevyhneme. To se ukázalo na přelomu 19. a 20. století, populárním se stal zejména Russelův paradox z roku cca 1901.

Začneme tímto: Existují množiny, které jsou svými vlastními prvky. Pro člověka, který se ještě kolem množin moc nemotal, je to asi překvapením, a popravdě řečeno i zkušený matematik by si jen těžko vybavil, kdy takovou podivnost potkal naposledy, ale jde to. Třeba takto: Uvažujme vlastnost mít nekonečně mnoho prvků (přesná definice nekonečnosti přijde, ale snad máme nějakou představu už teď). Pokud bychom přijali onen intuitivní způsob vytváření množin, tak nám vznikne množina A všech nekonečných množin. Prázdná nebude, třeba $\mathbb{N} \in A$ nebo $\mathbb{R} \in A$. A teď to přijde: Toto A samotné má nekonečně mnoho prvků, protože určitě vymyslíme nekonečně mnoho nekonečně velkých množin, stačí třeba vzít $\mathbb{N}$ a postupně odebírat $1, 2, 3, \dots$, vznikají tak různé nekonečné množiny a všechny jsou v A. Proto podle definice $A \in A$, množina je svým vlastním prvkem. Takže stát se to může. Teď jsme připraveni na to hlavní.

Definujme množinu B jako množinu všech množin, které nejsou svými vlastními prvky, naším zápisem tedy $B = \{M : M \notin M\}$. Díky předchozímu odstavci již vnímáme, že tato vlastnost není automatická, a také oceňujeme,

že snad každá množina, kterou si člověk normálně představí, patří zrovna sem do B. Třeba množina $\{13, 14\}$ určitě není svým prvkem a tudíž leží v B. Protože každá množina buď je nebo není svým vlastním prvkem, tak leží buď v A nebo v B.

Kde tedy leží množina B? Kdyby byla svým vlastním prvkem, tedy $B \in B$, pak by nesplňovala podmínku z definice, proto by muselo platit $B \notin B$. Pak ale podmínku z definice splní, proto $B \in B$, pak ale ... Není tedy možné rozhodnout, zda B patří do B, což je pro teorii množin smrtící. Je to tzv. paradox, je z podobné líhně jako ten o pánovi, co prohlásí „Já teď lžu".

Bylo tedy nutno přepracovat teorii množin, jmenovitě změnit způsob, kterým se množiny tvoří, aby se tím zakázaly určité nepříjemnosti. To se povedlo a už nějakých sto let máme uznávanou teorii množin, která těmito problémy netrpí.

Z pohledu praktického se problémům vyhneme tak, že si na začátku zvolíme již existující množinu jako tzv. universum U, ve kterém budeme dále pracovat (v této knize většinou $\mathbb{Z}$). Pak už si můžeme vytvářet nové množiny tak, že si vezmeme nějakou podmínku $p(x)$, která se vztahuje k prvkům z U, a můžeme definovat množinu $M = \{x \in U : P(x)\}$. Dá se ukázat, že když tvoříme množiny takto, tak už paradoxy nelze vyrobit.

Těch zajímavých okamžiků je v teorii množin více, ale při běžné „spotřební" práci se na problémy nenarazí. Spousta lidí si proto vystačí s intuitivní představou, říká se tomu naivní teorie množin a my se s ní spokojíme také.

△

Je čas představit si první definici. Připomínáme, že tradičně se definice píší jako implikace, ale míní se ekvivalence (viz část 1b).

Definice.
Nechť A, B jsou množiny. Řekneme, že A je **podmnožina** B, značeno $A \subseteq B$, jestliže jsou všechny prvky A také prvky B.
Řekneme, že A je **vlastní podmnožina** B, jestliže $A \subseteq B$, ale $A \neq B$.
Vztahu býti podmnožinou říkáme **inkluze**.

We say that a set A is a **subset** of a set B, denoted $A \subseteq B$, if all elements of A are also elements of B.
We say that A is a **proper subset** of B if $A \subseteq B$ but $A \neq B$.

Definice inkluze formálně: $A \subseteq B \iff [\forall a \in A\colon a \in B]$.

Na tento způsob zápisu byste si měli pomalu začít zvykat. Pokud si ještě nerozumíte s kvantifikátory, koukněte se do sekce 1a.4.

Někteří autoři značí vlastnost býti vlastní podmnožinou jako $A \subset B$. Má to ale problém, protože jiní autoři používají z lenosti $A \subset B$ pro běžnou vlastnost inkluze (dokonce někdy i já, ale ne v této knize, na to jsem si dal pozor). Ve významu značení $\subset$ je tedy zmatek, proto jej tady zavádět nebudeme a spokojíme se se značením $A \subseteq B$, kterému rozumí všichni stejně.

Když matematici zavedou nový pojem či vlastnost, tak hned začnou přemýšlet, jak funguje a jak se chová. Čím více se o něm dozví, tím snáze se s ním pak bude pracovat, podobně jako nám znalost rozličných identit (roznásobování závorky, krácení ve zlomcích atd.) usnadňují zacházení s algebraickými výrazy. V jistém smyslu se dá říci, že toto je jednou z hlavních náplní matematiky: Dozvídat se co nejvíce o různých pojmech (a své objevy dokazovat).

Podíváme se tedy na rozličná užitečná pravidla a vyzkoušíme si důkazy. Začneme něčím snadným.

Fakt 1d.1.
Nechť A, B, C jsou množiny. Jestliže $A \subseteq B$ a $B \subseteq C$, pak $A \subseteq C$.

Neprve si to rozebereme. Výrok má platit pro všechny trojice množin, proto si vezmeme libovolné množiny A, B, C a chceme pro ně ukázat pravdivost implikace

$$[A \subseteq B \wedge B \subseteq C] \implies A \subseteq C.$$

Dokazujeme implikaci, proto její předpoklad budeme brát jako něco daného, co je pravda. K dispozici tedy máme tvrzení $A \subseteq B$ a $B \subseteq C$. Je dobré si rozmyslet, co to říká. Podle definice jsou všechny prvky z A také v B a všechny prvky z B také v C.

Pomocí těchto daných faktů máme dojít k tomu, že $A \subseteq C$. Zde je přímo klíčové si to zase přeložit do podrobnějšího popisu. Chce se po nás ukázat, že každý prvek z A je také v C. Tím máme dáno základní schéma důkazu, je třeba vzít nějaký (libovolný) prvek $a \in A$ a pomocí daných faktů jej dovést až do C. To se zdá být snadné, a proto přistoupíme k důkazu. Dáme si pozor, abychom kroky správně logicky seřadili a všechny je dobře odůvodnili.

Důkaz (rutinní, poučný)**:**
Uvažujme libovolné množiny A, B, C. Předpokládejme, že $A \subseteq B$ a $B \subseteq C$. Ukážeme, že pak $A \subseteq C$.
Nechť $a \in A$ je libovolné. Podle předpokladu $A \subseteq B$ pak také $a \in B$. Z toho podle předpokladu $B \subseteq C$ zase dostaneme $a \in C$ a důkaz je hotov.

□

Poznámka: Tento důkaz by se v „normální“ knize odbyl slovem „triviální“, my jsme si na něm připomněli několik důležitých věcí: Že je dobré udělat si pořádek v tom, co máme k použití a kam se máme dostat, že je dobré si důkaz nejprve rozmyslet, než jej napíšeme načisto, a že hotový důkaz má mít správnou logickou strukturu: Vyjít z toho, co je dáno, dospět tam, kam se máme dostat, a každý krok umět zdůvodnit. V důkazech určených pokročilejšímu čtenáři se odůvodnění, která jsou dost jasná, vynechávají, pozornost se věnuje klíčových krokům. My zde budeme zejména ze začátku psát důkazy podrobněji, ať se to pořádně naučíme.
△

Zkušenost naznačuje, že nejlépe jdou studentům důkazy střední či středně lehčí. Že je trápí důkazy těžší, není žádný překvapovák, ale paradoxně hodně potrápí i důkazy velmi snadné, zejména když jde o věci, které vypadají jako naprosto jasné. Mnohdy pak začátečník nevidí, co k tomu ještě říct. Pak často velmi pomůže, když se vrátíme k základům, k definicím pojmů a logickým pravidlům. Hned si to předvedeme.

Fakt 1d.2.
Nechť A je libovolná množina. Pak platí následující:
(i) $A \subseteq A$;
(ii) $\emptyset \subseteq A$.

S **Rozbor:** U vlastnosti (i) nám definice říká, že vlastně chceme dokázat toto: $\forall x \in A$: $x \in A$. To zjevně platí a není třeba k tomu dál nic dodávat. Pokud tedy čtenáři ukážeme tento překlad, měli bychom jej již přesvědčit o pravdivosti prvního tvrzení.
(ii) je tvrdší oříšek. Podle definice máme ukázat, že $\forall x \in \emptyset$: $x \in A$. Normálně bychom si vzali typického zástupce, tedy libovolné x z množiny, a pro něj bychom ukázali, že leží v A. Jenže v prázdné množině žádný zástupce není, takže vlastně nemáme co dělat. Jak tuto situaci interpretujeme z pohledu logiky? Jedna možnost je si říct, že se tím pádem daný výrok nemůže pokazit, v prázdné množině určitě nenajdeme protipříklad na tvrzení $x \in A$. Takže tím by celé tvrzení mělo být pravdivé. Formálnější přístup se nabízí, když kvantifikátor s vymezením množiny převedeme do alternativního logického tvaru.

Důkaz (poučný)**:** (i): Vezměme libovolnou množinu A. Chceme ukázat, že $\forall a \in A$: $a \in A$, což zjevně platí.
(ii): Nechť A je libovolná množina. Chceme ukázat pravdivost tvrzení $\forall x \in \emptyset$: $x \in A$, což ve formální logice přepisujeme do tvaru $\forall x$: $[x \in \emptyset \implies x \in A]$. Protože je výrok $x \in \emptyset$ vždy nepravdivý, je celá implikace automaticky pravdivá.

□

Poznámka: Onen přepis do tvaru implikace lze použít i v tvrzení (i). To, co od A chceme, se dá přepsat do tvaru

$$\text{Pro libovolný objekt } x \text{ platí: } x \in A \implies x \in A.$$

Tato implikace je samozřejmě pravdivá. Obecně se dá dokázat (třeba pravdivostní tabulkou, viz kapitola 1a), že implikace $p \implies p$ je vždy pravdivá.
△

Nebyly to typické důkazy, protože vlastně ani nevycházely z vlastností množin, ale pravidel logiky.
Ještě těžší by bylo napsat důkaz následujícího tvrzení.

Fakt 1d.3.
Nechť A, B jsou množiny. Pak $A = B$ právě tehdy, když $A \subseteq B$ a $B \subseteq A$.

Toto je zrovna jedna z věcí, které asi čtenáři přijdou naprosto jasné, co by k tomu ještě dodával? Začněme malým rozborem, kde krásně uvidíme, jak nám návrat k principům poradí. Na začátku si budeme muset vzít libovolné množiny A, B. Pro ně máme ukázat ekvivalenci, takže vlastně budeme dokazovat dvě implikace:
1) $A = B \implies [A \subseteq B \wedge B \subseteq A]$,
2) $[A \subseteq B \wedge B \subseteq A] \implies A = B$.

Určitě budeme muset použít definici, jak u inkluze, tak u rovnosti množin. Obě tyto definice pracují se stejnými pojmy, jmenovitě s tím, kde leží či neleží prvky, což vypadá velmi nadějně. Strukturu důkazu již vidíme, tak si naznačíme, jak by to vypadalo.

1) Předpokládejme, že $A = B$, což dle definice znamená, že tyto dvě množiny mají stejné prvky.

Nejprve ukážeme, že pak $A \subseteq B$. Podle definice tedy máme ukázat, že $\forall a \in A$: $a \in B$. Nechť je $a \in A$ libovolné. Protože A a B mají stejné prvky, tak $a \in A$ znamená také $a \in B$ a je to hotovo.

Dále by bylo třeba ukázat, že i $B \subseteq A$. Vzhledem k symetrii situace půjde vlastně o stejný důkaz, jen se prohodí písmenka. Obvykle pak píšeme frázi „důkaz $B \subseteq A$ je obdobný“ nebo třeba „platnost $B \subseteq A$ plyne ze symetrie situace“.

Pokud je čtenář trochu nejistý, nakolik povídání o „stejných prvcích“ představuje korektní matematický důkaz, tak má k tomu dobrý důvod. Tento Fakt se totiž dotýká samotných základů množin, nepříznivě se teď projevuje, že vlastně nemáme pořádnou matematickou definici množiny a chybí nám i vhodný formální jazyk. To je také důvod, proč jsme nezačali psát oficiální důkaz a jen si o tom povídáme. Je to povídání užitečné, protože si opakujeme dobré návyky pro vytváření důkazů.

Jestli důkaz první implikace vypadal místy spíš jako přemlouvání čtenáře, aby moc neprotestoval, u důkazu druhé implikace je situace snad ještě horší. A protože si zde hlavně chceme procvičovat logiku a dokazovací nástroje, tak na opačný směr použijeme nepřímý důkaz (viz kapitola 1c), kde kupodivu argumenty vypadají poněkud věrohodněji.

Namísto implikace $[A \subseteq B \wedge B \subseteq A] \implies A = B$ tedy budeme dokazovat její obměnu

$$\neg(A = B) \implies \neg(A \subseteq B \wedge B \subseteq A),$$

což se přepíše pomocí de Morganových zákonů (viz kapitola 1a) jako

$$A \neq B \implies [\neg(A \subseteq B) \vee \neg(B \subseteq A)]. \qquad (*)$$

Teď tuto implikaci dokážeme.

Předpokládejme tedy, že $A \neq B$. Rovnost množin je definována přes obecný kvantifikátor (všechny jejich prvky jsou sdíleny). Její negací je tedy tvrzení, že existuje prvek, který není sdílen (viz negace kvantifikátorů v kapitole 1a). Náš předpoklad $A \neq B$ tedy říká, že existuje nějaký prvek x, který je v jedné z těchto množin ale ne v druhé. Jsou dvě možnosti:

a) Jedna možnost je, že existuje nějaké $x \in A$ takové, že $x \notin B$. To znamená, že ne každý prvek z A je v B, jinými slovy našli jsme protipříklad proti tvrzení $A \subseteq B$. Je zajímavé, že tento myšlenkový přechod lze realizovat i pomocí pravidla o negaci kvantifikátoru:

$$\exists x \in A\colon \neg(x \in B) \equiv \neg[\forall x \in A\colon x \in B] \equiv \neg[A \subseteq B].$$

Protože platí $\neg(A \subseteq B)$, platí i disjunkce $\neg(A \subseteq B) \vee \neg(B \subseteq A)$ (pro její pravdivost stačí, aby byla splněna některá ze složek). Pokud tedy nastane situace $x \in A$ ale $x \notin B$, pak je kýžená implikace $(*)$ dokázána.

b) Druhá možnost je, že $x \in B$, ale $x \notin A$. Stejným argumentem jako v a) pak ukážeme, že neplatí $B \subseteq A$ a tudíž i v tomto případě je ona implikace $(*)$ pravdivá.

Žádný jiný případ už není možný, takže dokazovaná implikace (obměna) platí.

Končíme s opakováním důkazů, začneme trochu rozvíjet poznatky o množinách. Obvykle pracujeme s více množinami a všechny jsou schovány uprostřed jedné velké množiny, universa U, ze kterého při své práci nevyskočíme. V rámci tohoto universa pak množiny všelijak kombinujeme či vytváříme nové. Asi každý čtenář se již potkal se sjednocením množin (sesypeme všechny jejich prvky do jednoho pytlíčku), průnikem (to, co je množinám společné) a doplňkem (všechny prvky mimo). Teď si ukážeme formální definice, čtenář už by je měl být schopen plynule číst a překládat do srozumitelné představy.

Definice.
Nechť A, B jsou množiny v nějakém universu U. Definujeme jejich
sjednocení: $A \cup B = \{x \in U : x \in A \vee x \in B\}$;
průnik: $A \cap B = \{x \in U : x \in A \wedge x \in B\}$;
rozdíl či **doplněk** B **v** A**:** $A \setminus B = \{x \in U : x \in A \wedge x \notin B\}$;
kartézský součin: $A \times B = \{(a, b) : a \in A \wedge b \in B\}$, zde (a, b) značí uspořádanou dvojici.

Anglickou verzi uděláme méně formální, ať si čtenář zvyká na jazyk.

Let A, B be sets in some universe U. We define their
union $A \cup B$ as the set of all elements that are in A or in B;
intersection $A \cap B$ as the set of all elements that are both in A and B;
difference $A \setminus B$ as the set of all elements that are in A but not in B;

Cartesian product as the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

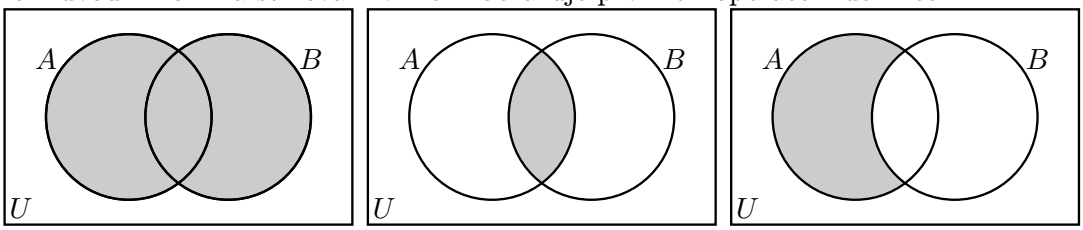
Množinový rozdíl se také někdy značí $A - B$, ale silně se doporučuje to nedělat, protože se to v některých situacích plete s úplně jinou operací. Tomuto rozdílu se také říká „relativní doplněk B a A“ (relative complement of B in A, relative complement of B with respect to A). Máme ještě jednu populární operaci.

Definice.
Nechť A je množina v nějakém universu U. Definujem její **doplněk** vzhledem k U jako
$$A^c = \overline{A} = \{x \in U : x \notin A\}.$$

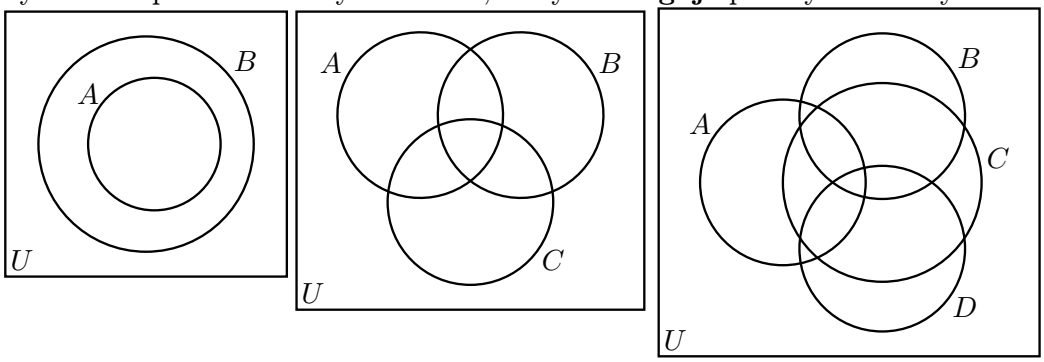
Let A be a set in a universe U. We define its **complement** (with respect to U) as the set $A^c = \overline{A}$ of all elements of U that are not in A.

Spíš z povinnosti uděláme příklad: Když třeba $A = \{1, 2, 13\}$ a $B = \{13, 23\}$, pak $A \cup B = \{1, 2, 13, 23\}$, $A \cap B = \{13\}$, $A \setminus B = \{1, 2\}$ a $A \times B = \{(1, 13), (1, 23), (2, 13), (2, 23), (13, 13), (13, 23)\}$.
Co je doplněk A? To není jasné, protože jsme neřekli, v jakém universu pracujeme. Nabízí se třeba universum $\mathbb{N}$, pak je $\overline{A} = \{3, 4, \dots, 11, 12, 14, 15, 16, \dots\}$. Jenže můžeme vzít jiné U a pak bude $\overline{A}$ jiné. Dá se říct, že pokud nějaká situace vyžaduje, aby se dělal doplněk, tak už bývá z kontextu jasné i U, a pokud doplňky nepotřebujeme, tak nám v zásadě U nijak nechybí. Spousta lidí ani neví, že jsou nějaká universa, i my jsme teď v pohodě vytvořili třeba $A \cup B$, aniž bychom znali U.

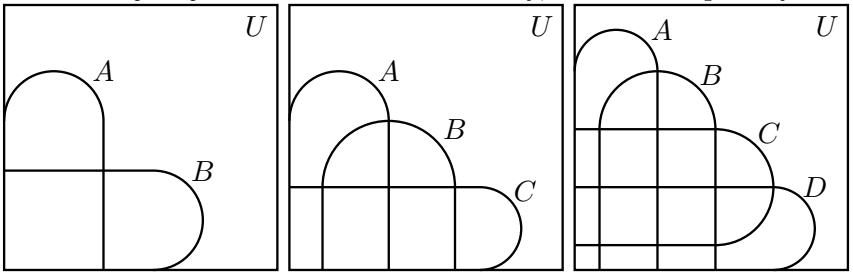
Dobrým znázorněním vztahu mezi množinami jsou tzv. **Vennovy diagramy**. Následující obrázky ukazují standardní znázornění dvou množin a stínování v nich zobrazuje první tři operace z definice.



Někdy chceme obrázkem vyjádřit přímo určitou situaci. Následující obrázek ukazuje situaci, kdy $A \subseteq B$. Připojili jsme také klasický obrázek pro tři množiny a obrázek, který **nefunguje** pro čtyři množiny.



Proč nefunguje? Protože na něm není místo pro prvky, které jsou v A, B a D, ale nejsou v C, tedy chybí tam místo na vyznačení množiny $(A \cap B \cap D) \setminus C$. Dá se dokázat, že nelze vytvořit obrázek ze čtyř kružnic, který by vyhovoval (jinými slovy, ať už nakreslíte čtyři kružnice jakkoliv, vždycky bude existovat určitý typ prvků, pro které ten obrázek nebude mít chlíveček). Co s tím? Jedna možnost je namísto jedné z kružnic použít klobásoid, což ale není moc estetické. Existují zajímavé alternativní obrázky, které už to pro čtyři množiny dokážou:



Tyhle obrázky zase neumí pět množin, ale ještě mi to nikdy nechybělo.

Následující vlastnosti množinových operací by měly být samozřejmé.

Fakt 1d.4.
Nechť A, B jsou množiny. Pak platí:
(i) $A \subseteq A \cup B$, $B \subseteq A \cup B$;
(ii) $A \cap B \subseteq A$, $A \cap B \subseteq B$;
(iii) $A \setminus B \subseteq A$.

S Rozbor: Všechny vlastnosti dokážeme tak, že inkluze převedeme podle definice, tedy budeme pracovat s prvky. Ukáže se, že ani nemusíme dělat nějakou množinovou matematiku, tvrzení vyplývají z obecných pravidel pro výroky p, q:

- Jestliže platí p, pak platí i výrok $p \vee q$;
- Jestliže platí výrok $p \wedge q$, prak platí i p.

Důkaz (rutinní)**:** (i): Dokážeme, že $A \subseteq A \cup B$. Nechť $x \in A$ je libovolné. Z pravdivosti výroku $x \in A$ vyplývá i pravdivost výroku $x \in A \vee x \in B$ a tedy $x \in A \cup B$. Důkaz hotov.

Důkaz $B \subseteq A \cup B$ je obdobný.

(ii): $A \cap B \subseteq A$: Nechť $x \in A \cap B$. Pak $x \in A \wedge x \in B$, proto tedy $x \in A$. Důkaz je hotov, druhé tvrzení plyne ze symetrie.

(iii): Nechť $x \in A \setminus B$. Pak platí $x \in A \wedge x \notin B$, proto $x \in A$.

□

Všimněte si, že při důkazu (ii) jsme napsali jen „nechť $x \in A \cap B$“. Pokládá se za samozřejmé, že se v takové situaci bere x libovolné, tudíž se šetří místem a časem a to slovo se vynechává, i zde to budeme dělat. Pokud student předvádí důkaz u zkoušky, tak ať raději to „libovolné“ napíše, ať ukáže zkoušejícímu, že ví, co se děje.

Mimochodem, mohlo by se stát, že namísto inkluzí budou v těch vztazích rovnosti? A pokud ano, tak za jakých okolností? Matematici si pořád kladou takové zvědavé otázky, odpovědi na tyto dvě najdete ve cvičení 1d.1.

Vlastností (pravidel), které by šlo pro množinové operace vymyslet, je spousta, jako nejdůležitější se obvykle uvádí následující desítka.

Věta 1d.5. (zákony pro počítání s množinami)
Nechť A, B, C jsou libovolné množiny z universa U. Pak platí následující:
(i) $A \cup \emptyset = A$, $A \cap U = A$; (zákony identity)
(ii) $A \cap \emptyset = \emptyset$, $A \cup U = U$; (zákony dominance)
(iii) $A \cup A = A$, $A \cap A = A$; (idempotence)
(iv) $\overline{\overline{A}} = A$; (zákon komplementu)
(v) $A \cup B = B \cup A$, $A \cap B = B \cap A$; (komutativní zákon)
(vi) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$; (asociativní zákon)
(vii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; (distributivní zákon)
(viii) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$; (De Morganovy zákony)
(ix) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$; (zákony absorbce)
(x) $A \cup \overline{A} = U$, $A \cap \overline{A} = \emptyset$. (zákony doplňku)

Doporučujeme, aby si čtenář postupně všechna pravidla prošel a pokaždé si začal kreslit Vennovy diagramy dané situace, aby sám pro sebe zjistil, co se v jednotlivých případech děje. Není totiž cílem naučit se tato pravidla nazpamět (s možnou výjimkou De Morganových zákonů), ale porozumět jim, aby vám platnost těch pravidel přišla stejně přirozená jako platnost $7 + 5 = 5 + 7$. Když je pak člověk v situaci, kdy by nějaké to pravidlo potřeboval, tak se mu samo nabídne, jako se člověku nabízí třeba krácení ve zlomcích, aniž by o tom znal nějakou větu. Pro matematika je většina těchto tvrzení „jasná“, v jeho světě to tak prostě fungovat musí, stejně jako když v našem světě pustíme kámen, tak všichni víme, co se pak stane, nemusíme si na to pamatovat nějaké věty.

Připomněli jsme si algebru a není to náhoda. Když si čtenář ve vzorečcích výše nahradí $\overline{A}$ symbolem $-a$, $A \cap B$ symbolem $a \cdot b$ a $A \cup B$ symbolem $a + b$, tak zjistí, že mnohé z pravidel jsou stejná jako pravidla, která zná pro algebraické operace. Platí to i pro (i) a (ii), pokud nahradí $\emptyset$ číslem 0 a U „číslem“ ∞ (pak je třeba brát a kladné). Zajímavé je, že v bodě (vi) dokonce dostáváme distributivní zákon („roznásobení závorky“) i pro prohozenou pozici násobení a sčítání. Tato analogie ovšem nefunguje úplně dokonale, některá pravidla – třeba (iii) – takto převést nejdou.

Při práci s čísly a výrazy také velmi pomáhá, když člověk předem ví, že určité věci dělat nesmí, třeba že nelze napsat $\frac{1}{2+3}$ jako $\frac{1}{2} + \frac{1}{3}$. Podobně mnoho věci selhává pro množinové operace a o nejsvůdnějších by měl člověk vědět, asi nejzrádnější uvidíte za chvíli a ve cvičení 1d.2.

Pokud si čtenář vlastnosti prošel, tak jistě zjistil, že hlavně těch prvních pět je opravdu jasných, dokazují se stejně snadno jako vlastnosti v předchozím tvrzení. Ukážeme proto jen pár důkazů pro zajímavost a zbytek těch lehkých necháme čtenáři. Zaměříme se hlavně na distributivní zákon a De Morganovy zákony.

Důkaz (rutinní, poučný)**:** (iv): Napíšeme si množinu vlevo a budeme upravovat její podmínku. Je asi zřejmé, že když v definici množiny podmínku příslušnosti nahradíme jinou, která je ekvivalentní (říká totéž), tak se dotyčná množina nezmění.

$$\overline{\overline{A}} = \{x \in U : x \notin \overline{A}\} = \{x \in U : \neg[x \in \overline{A}]\} = \{x \in U : \neg[\neg[x \in A]]\} = \{x \in U : x \in A\} = A.$$

(vi): Abychom ušetřili místo a čas, tak si pomocí ekvivalence $\iff$ mezi sebou popovídáme o tom, kdy leží prvky v obou množinách, a zjistíme, že za těchtýž podmínek, tedy množiny jsou stejné. Pro libovolné $x \in U$ totiž platí

$$x \in A \cup (B \cup C) \iff x \in A \vee [x \in (B \cup C)] \iff x \in A \vee [x \in B \vee x \in C] \iff [x \in A \vee x \in B] \vee x \in C$$
$$\iff [x \in (A \cup B)] \vee x \in C \iff x \in (A \cup B) \cup C.$$

Použili jsme definici sjednocení, nejprve jsme výchozí výraz „rozbalili“, dokud to ještě šlo, a ve chvíli, kdy jsme se dostali k základním pojmům, jsme to zase „zabalili“ do žádaného tvaru. Poznamenejme, že jsme si mohli dovolit ekvivalence takto „řetězit“, protože pro ně platí asociativita. S implikacemi už by to nešlo.

(vii): Dokážeme první vztah, druhý je obdobný. V tomto případě přímý důkaz jako výše nebude tak snadný. Když si nejsme jisti, obvykle pomůže vrátit se k základům, tedy standardnímu způsobu. Rovnost proto dokážeme přes dvě inkluze, ty se pak dokazují podle definice, tedy implikace pro náležení prvků.

1) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$: Nechť $x \in A \cap (B \cup C)$. Pak $x \in A$ a $x \in B \cup C$. Druhý fakt nabízí dvě možnosti.

Jestliže $x \in B$, pak spolu s $x \in A$ dostaneme $x \in A \cap B$, proto $x \in (A \cap B) \cup (A \cap C)$.

Jestliže $x \in C$, pak symetricky dostaneme $x \in A \cap C$, proto $x \in (A \cap B) \cup (A \cap C)$.

Pokryli jsme všechny (obě) možnosti, důkaz je úplný.

V části 2) tento rozbor možností, které jsou v podstatě stejné, nahradíme odvolávkou na symetrii.

2) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$: Nechť $x \in (A \cap B) \cup (A \cap C)$. Pak x leží alespoň v jednom z těch průniků, díky symetrii můžeme předpokládat, že $x \in A \cap B$. Pak $x \in A$ a také $x \in B$. To druhé ale dává $x \in B \cup C$, tedy $x \in A \cap (B \cup C)$ a důkaz je hotov.

(viii): Nechť A, B, C jsou množiny.

a) Dokážeme, že $\overline{A \cup B} = \overline{A} \cap \overline{B}$, zase přes dvě inkluze.

a1) Nechť x je libovolný prvek z $\overline{A \cup B}$. To znamená, že $x \notin A \cup B$. Prvky $x \in A \cup B$ splňují $x \in A \vee x \in B$, prvky mimo tedy splňují negaci této vlastnosti, což je podle de Morganových zákonů pro formální logiku rovno

$$\neg(x \in A \vee x \in B) \equiv \neg(x \in A) \wedge \neg(x \in B) \equiv x \notin A \wedge x \notin B.$$

To znamená, že $x \in \overline{A} \wedge x \in \overline{B}$, tedy $x \in \overline{A} \cap \overline{B}$. Právě jsme dokázali, že $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

a2) Nechť naopak $x \in \overline{A} \cap \overline{B}$. Podíváme-li se na předchozí řádky, tak uvidíme, že všechny kroky byly vratné neboli obousměrné, takže zpětným chodem dospějeme k tomu, že $x \in \overline{A \cup B}$.

Takže oba směry šlo ukázat najednou. Ukážeme si to vzápětí.

b) Teď dokážeme, že $\overline{A \cap B} = \overline{A} \cup \overline{B}$, a to oba směry najednou. Aby to bylo formálně správně, budeme upravovat podmínky v množinách.

$$\begin{aligned}\overline{A \cap B} &= \{x \in U : x \notin A \cap B\} = \{x \in U : \neg(x \in A \cap B)\} = \{x \in U : \neg(x \in A \wedge x \in B)\} \\ &= \{x \in U : \neg(x \in A) \vee \neg(x \in B)\} = \{x \in U : x \notin A \vee x \notin B)\} = \{x \in U : x \in \overline{A} \vee x \in \overline{B}\} \\ &= \overline{A} \cup \overline{B}.\end{aligned}$$

□

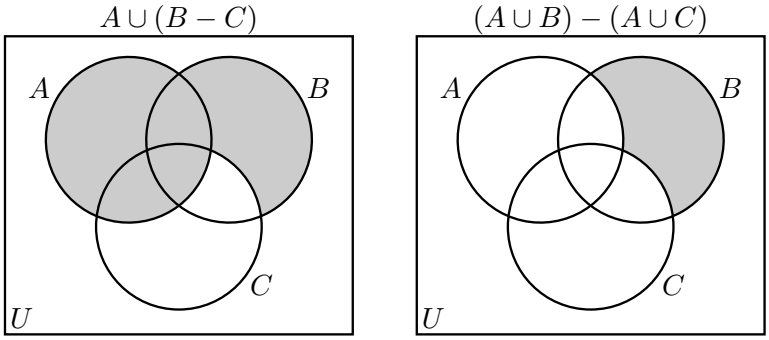
Všechna právě probraná pravidla z Věty mají své prakticky stejně vypadající bratříčky ve formální logice, stačí namísto $\cap$ psát $\wedge$, místo $\cup$ se píše $\vee$, doplněk se nahradí negací, $\emptyset$ je F a podobně. Mezi množinovými a logickými operacemi je úzká souvislost, v důkazu výše to bylo také vidět, například de Morganovo pravidlo pro množiny jsme dokazovali pomocí de Morganova pravidla pro logické výrazy.

Poznámka: Zatím jsme jen dokazovali, že něco platí. Může se ale stát, že nám někdo předhodí tvrzení, které není dobře, třeba toto:

Pro libovolné množiny A, B, C platí $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$.

(Je to pokus o distributivní zákon, zkusili jsme „roznásobit“ tu závorku.)

Jak zjistíme, zda má cenu to dokazovat? Jedna možnost je zakreslit si obě množiny ve Vennově diagramu.



Vidíme, že nejde o stejné objekty. Jak se tedy dokáže, že je dané tvrzení nepravdivé? Toto tvrzení je uvedeno obecným kvantifikátorem „pro všechny množiny“. K vyvrácení tedy stačí najít jediný protipříklad, kdy dané tvrzení selže (viz kapitola 1c). Obrázek nás inspiruje, stačí zvolit množiny tak, aby na nich byl vidět ten rozdíl v obrázku, neboli chceme mít prvek v místě, kde se obrázky liší. Zvolme tedy třeba $A = \{13\}$ a $B = C = \emptyset$, pak

$$A \cup (B \setminus C) = \{13\} \cup \emptyset = \{13\}, \text{ zatímco } (A \cup B) \setminus (A \cup C) = \{13\} \setminus \{13\} = \emptyset.$$

Tento protipříklad tedy dokázal, že dané tvrzení neplatí.

Mimochodem, obrázek naznačuje, že by první množina měla vždy obsahovat tu druhou. A to je pravda, viz cvičení 1d.1 (ix).

△

Když mají matematici operace pro dva objekty, tak se většinou nezastaví a chtějí je pro víc objektů. Ukážeme si standardní cestu, kterou k tomu dospívají. Začneme třemi množinami: Jak bychom vymysleli $A \cap B \cap C$? Protože dvě množiny pronikat umíme, nabízí se dělat tři postupně. Nejprve pronikneme $A \cap B$ a ten výsledek pak s C, formálně zapsáno to je $(A \cap B) \cap C$. To je zajímavý nápad, ale má zádrhel: Proč zrovna takto, proč nezačít třeba $B \cap C$, celkem pak $A \cap (B \cap C)$? V takové chvíli člověka zachrání hlavně asociativní zákon (což je moment, který se vyskytne opakovaně i v dalších kapitolách). Ten říká, že je jedno, které závorkování použijeme, takže nápad, který jsme měli, funguje docela dobře.

Jakmile umíme proniknout tři množiny, není důvod se zastavit a nepřidat množinu čtvrtou, můžeme třeba definovat $A \cap B \cap C \cap D$ jako $(A \cap B \cap C) \cap D$ a díky asociativitě zase víme, že to vyjde nastejno jako třeba $(A \cap B) \cap (C \cap D)$, což je také zajímavá možnost, protože používá jen průniky dvou množin.

Podobně pak uděláme průnik pěti, šesti, 50 atd. množin. Jak to pak ale zapsat pořádně? Nejjednodušší způsob je rekurzí či indukcí, což v zásadě znamená, že se na tu definici díváme od konce (viz ten příklad se čtyřmi množinami):

$$\bigcap_{i=1}^{n+1} A_i = \left(\bigcap_{i=1}^{n} A_i\right) \cap A_{n+1}.$$

Toto je typ definice, který se používá často a zde na to máme speciální kapitolu 8a o indukci a rekurzi (berte to jako první vlaštovku či reklamu). Například chceme-li průnik pěti množin A_1 až A_5, tak vzorec s $n = 4$ říká, že nejprve musíme umět proniknout 4 množiny,

$$A_1 \cap \ldots \cap A_5 = (A_1 \cap \ldots \cap A_4) \cap A_5.$$

Na spočítání $A_1 \cap \ldots \cap A_4$ podle stejného vzorce, ale s $n = 3$, zase potřebujeme umět proniknout tři množiny $A_1 \cap A_2 \cap A_3$, odtud už se další iterací konečně dopracujeme k průniku dvou množin $A_1 \cap A_2$, který umíme, tak ho uděláme. Načež následuje „zpětný chod“ naším rozkladem: Výsledek $A_1 \cap A_2$ pronikneme s A_3 (průnik dvou množin umíme), tento výsledek s A_4, ten pak s A_5.

Tento způsob je klasický, spolehlivě zobecňuje asociativní operace na více objektů. Často se povede, že operace, která tak vnikne, má dokonce nějaký rozumný význam. Když si například člověk rozmyslí, které prvky jsou v množině $(A \cap B) \cap C$, tak zjistí, že to jsou přesně ty, které jsou zároveň ve všech třech množinách, podobně se to dá rozmyslet i pro více množin. Naše definice rekurzí tak zachovala hlavní smysl, průnik se ptá na to, co je společné. Podobně bychom mohli rekurzí definovat sjednocení pro více množin a zjistilo by se, že i tato operace funguje stejně jako ta pro dvě, sesypává prvky z množin do jedné společné. Nabízí se tak možnost definovat operace pro mnoho množin najednou pomocí velice čitelné podmínky.

Definice.
Nechť $A_1, A_2, \dots, A_n$ jsou množiny ve stejném universu U. Definujeme

$$\bigcup_{k=1}^{n} A_k = \{x \in U : \exists k \in \{1,2,\dots,n\}\colon x \in A_k\},$$

$$\bigcap_{k=1}^{n} A_k = \{x \in U : \forall k \in \{1,2,\dots,n\}\colon x \in A_k\},$$

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \dots \wedge a_n \in A_n\}.$$

Jestliže jde o stejné množiny, tedy $A_i = A$ pro všechna i, pak značíme $A_1 \times A_2 \times \cdots \times A_n = A^n$.

V praxi se často místo „$k \in \{1,2,\dots,n\}$“ píše $k = 1, 2, \dots, n$.

Brzy uvidíme, že definice, kterou jsme nakonec zvolili, je výrazně vhodnější pro důkazy. Pokud bychom totiž operace zobecňovali na více objektů rekurzí, musely by všechny důkazy probíhat matematickou indukcí.

Další výhodou je, že se v definici vlastně nikde nepoužívá fakt, že k bereme zrovna z přirozených čísel. Máme tedy možnost zvolit pro indexování i jinou množinu než $\{1,2,\dots,n$, hlavní myšlenka (spojování, hledání společných prvků) se pak zachová. Zase přidáme i kartézský součin, ať to máme při jednom.

Definice.
Nechť I je nějaká množina indexů. Nechť A_i pro $i \in I$ jsou množiny ve stejném universu U. Definujeme

$$\bigcup_{i \in I} A_i = \{x \in U : \exists i \in I\colon x \in A_i\},$$

$$\bigcap_{i \in I} A_i = \{x \in U : \forall i \in I\colon x \in A_i\}.$$

Příklad 1d.a: Uvažujme $A_i = \{i, i+1\}$ pro $i \in \mathbb{N}$. Máme tedy nekonečný soubor dvouprvkových množin, například $A_{13} = \{13, 14\}$, $A_{42} = \{42, 43\}$ atd. Nejprve se zamyslíme nad konečnými sjednoceními a průniky.

1) Jako inspiraci si všimneme, že $A_1 \cup A_2 = \{1,2,3\}$ a $A_1 \cup A_2 \cup A_3 = \{1,2,3,4\}$, takže si tipneme, že pro $n \in \mathbb{N}$ je $\bigcup_{i=1}^{n} A_i = \{1,2,3,\dots,n,n+1\}$. Důkaz:

$n+1 \in A_n$ a pro $i = 1,\dots,n$ platí $i \in A_i$, proto $\{1,2,3,\dots,n,n+1\} \subseteq \bigcup_{i=1}^{n} A_i$. Naopak pokud $j \in A_i$ pro nějaké $i = 1,\dots,n$, tak určitě $i \le j \le i+1$, tedy $1 \le j \le n+1$. Proto $\bigcup_{i=1}^{n} A_i \subseteq \{1,2,3,\dots,n,n+1\}$.

2) Podobně si vyzkoušíme $A_1 \cap A_2$, $A_1 \cap A_2 \cap A_3$ (zkoušíte to?), pak se zdá jasné, že

$$\bigcap_{i=1}^{n} A_i = \begin{cases} \{1,2\}, & n = 1; \\ \{2\}, & n = 2; \\ \emptyset, & n \ge 3. \end{cases}$$

Důkaz: Pokud $n \ge 3$, pak ten průnik obsahuje prvky společné mimo jiné množinám A_1 a A_3, tedy prvky z množiny $\{1,2\} \cap \{3,4\} = \emptyset$.

3) Teď se podíváme na nekonečné případy.

Protože každé $i \in \mathbb{N}$ leží alespoň v nějaké ze zúčastněných množin (konkrétně $i \in A_i$), dostáváme $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N}$. Naopak každé číslo z $\mathbb{N}$ se s většinou našich množin míjí (určitě $i \notin A_j$ pro $j > i$), proto $\bigcap_{i=1}^{\infty} A_i = \emptyset$.

△

V příkladu jsme použili dva způsoby specifikace indexů, $\bigcap_{i \in \mathbb{N}}$ a $\bigcap_{i=1}^{\infty}$, jsou rovnocenné a můžete si vybrat. Pokud je I jasné z kontextu, tak jeho specifikaci někdy vynecháváme a píšeme jen $\bigcup A_i$ či $\bigcap A_i$.

Příklad 1d.b: Množina indexů může být opravdu veliká. Nechť $I = \mathbb{R}$. Pro libovolné reálné číslo r definujeme C_r jako množinu všech číslic, které se při zápisu r (v desítkové soustavě) použily (v případech, kdy jsou možné zápisy dva, volíme ten neperiodický). Například $C_{1.07} = \{0,1,7\}$, sice platí, že $1.07 = 1.069999999\dots$, ale dohodli jsme se, že preferujeme neperiodický zápis, pokud to jde. Také víme, že $17/6 = 2.83333...$, proto $C_{17/6} = \{2,3,8\}$,

a třeba $C_\pi = \{0,1,2,3,4,5,6,7,8,9\}$. Dostáváme opravdu velký soubor množin $\{C_r\}$, ještě uvidíme, že je mnohem větší než ten z předchozího příkladu.

Protože je každá číslice použita v nějakém reálném čísle, je $\bigcup_{r\in\mathbb{R}} C_r = \{0,1,2,3,4,5,6,7,8,9\}$. Žádná cifra ale není ve všech číslech, proto $\bigcap_{r\in\mathbb{R}} C_r = \emptyset$.

△

Příklad 1d.c: Nechť $I = \mathbb{R}$. Pro $x \in I$ nechť L_x je množina všech lidí, která považuje x za své šťastné číslo. Pak $\bigcup L_x$ je množina všech číselně pověrčivých lidí a $\bigcap L_x$ je množina všech lidí, pro které je šťastné každé číslo.
△

Všechny vlastnosti, které známe o průniku a sjednocení dvou množin, budou pravdivé i v případě, kdy se je podaří rozumně zobecnit pro více množin. Platí to pro distributivní zákon (viz cvičení 1d.8), pravidlo pro doplněk, zejména ovšem máme následující tvrzení.

Věta 1d.6. (De Morganovy zákony)
Nechť A_i pro $i \in I$ jsou množiny ve stejném universu U, kde I je nějaká množina indexů. Pak

$$\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A}_i \qquad \text{a} \qquad \overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A}_i.$$

Důkaz (rutinní, poučný)**:** Nejprve dokážeme první vztah, a to dlouze a komentovaně:

Prvek x leží v $\overline{\bigcup A_i}$ právě tehdy (podle definice doplňku), když neleží v $\bigcup A_i$, což je (podle definice sjednocení) právě tehdy, když není pravda, že existuje i, aby $x \in A_i$. Výraz $\neg(\exists i \in I\colon x \in A_i)$ je podle pravidel logiky totéž jako $\forall i \in I\colon \neg(x \in A_i)$, tedy x neleží v žádném A_i, což je (podle definice doplňku) právě tehdy, když leží ve všech $\overline{A}_i$, což je (podle definice průniku) právě tehdy, když leží v $\bigcap \overline{A}_i$.

Ukázali jsme, že $x \in \overline{\bigcup A_i} \iff x \in \bigcap \overline{A}_i$, čímž je rovnost těchto dvou množin dokázána.

Druhý vztah dokážeme v zásadě stejným důkazem, teď jej ale zapíšeme čistě symbolicky, abyste si procvičili překlad do lidštiny.

$$\begin{aligned} x \in \overline{\bigcap A_i} &\iff x \notin \bigcap A_i \iff \neg\big(x \in \bigcap A_i\big) \iff \neg(\forall i \in I\colon x \in A_i) \\ &\iff \exists i \in I\colon \neg(x \in A_i) \iff \exists i \in I\colon x \notin A_i \iff \exists i \in I\colon x \in \overline{A}_i \iff x \in \bigcup \overline{A}_i. \end{aligned}$$

□

Ten druhý důkaz byl tedy opravdu úsporný, kdyby se tak psaly matematické knihy, tak by vážily čtvrtinu. Nevýhoda by byla, že by je nikdo nedokázal rozumně číst, ani matematici ne, protože i je by zdržoval překlad z matematičtiny do lidštiny, pro začátečníka by pak byly zcela nesrozumitelné. Klasické důkazy v knihách jsou tedy obvykle jakýmsi kompromisem mezi tím ukecaným a tím stručným výše.

Poznámka: Všimněte si, že jsme nedefinovali množinový rozdíl pro více množin. Důvod je jednoduchý, odečítání není asociativní, tudíž nevíme, jak vlastně dělat $A \setminus B \setminus C$ (viz cvičení 1d.2 (ix)). Obdobně to ostatně funguje s čísly, umíme počítat $3+7+13$, ale co je $7-3-2$? Problém je právě v nedostatku asociativity u odčítání, výrazy $(7-3)-2$ a $7-(3-2)$ nejsou stejné.
△

Někdy bývá důležité, zda spolu dvě množiny mají či nemají něco společného, dokonce si to zasloužilo speciální jméno.

Definice.
Množiny A, B se nazývají **disjunktní**, jestliže $A \cap B = \emptyset$.

To je velice užitečný pojem, až budeme dělat kombinatoriku, tak se bez něj neobejdeme.

Příklad 1d.d:
Zajímavá otázka: Jak bychom tento pojem rozšířili pro více množin? Mohli bychom zkusit udělat definici, že množiny A_i jsou disjunktní, pokud platí $\bigcap A_i = \emptyset$. Tato definice by byla korektní, určitě už někoho napadla, ale v knihách ji nepotkáme. Z pohledu praktického je totiž k ničemu. Stačí si představit případ tří množin. Pokud

platí $A_1 \cap A_2 = \emptyset$, pak už také nutně $A_1 \cap A_2 \cap A_3 = \emptyset$, ať už je A_3 jakákoliv. Takto zavedený pojem by tedy o dotyčných množinách mnoho neřekl.

Pokud chceme vyjádřit, že nějaké množiny spolu nemají nic společného, pak většinou potřebujeme jinou frázi: Chce se, aby množiny A_i byly **po dvou disjunktní**, což znamená, že $A_i \cap A_j = \emptyset$ pro libovolné $i \neq j$. Tato podmínka odpovídá situaci, kterou si ve Vennově diagramu představíme jako zcela oddělené kroužky.
△

Na závěr ještě doplníme jeden pojem.

Definice.
Nechť A je množina. Definujeme **potenční množinu** A, značeno $P(A)$, jako množinu všech podmnožin A.

Příklad 1d.e: Jestliže $A = \{a, b\}$, pak $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
△

Jako rozcvičku si ukážeme jednu vlastnost, která je z matematického hlediska triviální, ale důkaz může být pro začátečníka poněkud drsný.

Fakt 1d.7.
Nechť A, B jsou množiny. Jestliže $A \subseteq B$, pak $P(A) \subseteq P(B)$.

S Rozbor: V důkazu si vezmeme množiny A, B splňující $A \subseteq B$ a budeme muset ukázat, že $P(A) \subseteq P(B)$. Zde se často začátečník zadrhne, protože $P(A)$ je objekt, který je pro něj nový, je to cosi komplikovaného a záhadného. Zachrání nás návrat ke kořenům. Nejprve se odvoláme na definici inkluze, která poradí, ať dokážeme vlastnost $\forall m \in P(A)$: $m \in P(B)$.

Zde je dobré se na chvíli zamyslet, s jakými objekty vlastně pracujeme. Co jsou to ty m? $P(A)$ je množina všech podmnožin A, takže $m \in P(A)$ je vlastně nějaká podmnožina A. S tímto objektem tedy někdy pracujeme jako s prvkem (když mluvíme o $P(A)$ a $P(B)$) a jindy jako s množinou (když se budeme pohybovat v A, B). Tahle dvojakost bývá pro začátečníka dalším problémem bránícím v úspěchu. Opravdu se vyplatí se zamyslet. Teď už to máme, je čas na důkaz, opět trochu ukecanější.

Důkaz (rutinní)**:** Předpokládejme, že máme libovolné množiny A, B splňující $A \subseteq B$. Ukážeme, že $P(A) \subseteq P(B)$.

Vezměme tedy libovolný prvek m z $P(A)$. Podle definice $P(A)$ je m podmnožinou A, ale máme také předpoklad $A \subseteq B$, tudíž podle Faktu 1d.3 je $m \subseteq B$. Proto podle definice $P(B)$ platí $m \in P(B)$ a důkaz je hotov. □

1d.8 Reprezentace množin v počítačích

Nekonečně mnoho dat počítač nespolkne, takže už z principu budeme v počítačích pracovat s množinami konečnými. Existuje pak jednoduchý způsob, jak si je reprezentovat. Začneme tím, že vezmeme konečné universum a jeho prvky si očíslujeme, $U = \{u_1, \ldots, u_n\}$. Každá podmnožina A tohoto universa se pak dá jednoduše zakódovat jako binární řetězec (číslo) délky n tak, že i-tá cifra je 1, pokud $u_i \in A$, jinak je to nula.

Například v universu $U = \{u_1 = 1, u_2 = 13, u_3 = a, u_4 = \diamond, u_5 = 23\}$ se množina $A = \{13, 23\}$ zakóduje jako 01001, popřípadě 10010, podle toho, jestli jsme si vybrali kódování (čtení řetězce) zprava doleva nebo naopak. V zásadě je to jedno, jen se pak toho kódování musíme už pořád držet `:-)`.

Jednou z velkých výhod této reprezentace je, že se pak krásně dělají množinové operace pomocí logických operací na bitech odpovídajících kódovacích řetězců. Sjednocení množin odpovídá logická disjunkce jednotlivých bitů, naopak průnik je přesně konjunkce neboli obyčejné binární násobení bitů. To jsou operace, které má počítač rád, takže je všechno v pohodě.

Teď přijdou cvičení a jejich řešení jsou často psána vysoce kondenzovaně. Čtenář si tak může procvičit překlad těchto úvah do češtiny, mělo by to vždy rozumně jít.

Cvičení

Cvičení 1d.1 (*dobré, +poučné)**:** Pravidel pro množinové operace je mnohem víc, než jsme uvedli v textu. Dokažte následující:
Nechť A, B, C jsou množiny v univerzu U. Pak platí:
(i) $\overline{A} = U \setminus A$;
(ii)$^+$ $A \setminus B = A \cap \overline{B}$;
(iii) $\overline{A \setminus B} = \overline{A} \cup B$;
(iv) $A \cap (B \setminus A) = \emptyset$;
(v) $(A \setminus B) \cap (B \setminus C) = \emptyset$;
(vi) $(A \setminus B) \setminus C \subseteq A \setminus C$;
(vii)$^{*+}$ $A \cup (B \setminus A) = A \cup B$;
(viii)$^+$ $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$;
(ix)$^+$ $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(x)$^+$ $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
(xi)$^{**+}$ $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$;
(xii)$^{*+}$ $A \subseteq B$ právě tehdy, když $\overline{B} \subseteq \overline{A}$;
(xiii)$^{*+}$ $A \subseteq B$ právě tehdy, když $A \cap B = A$;
(xiv)$^{*+}$ $A \subseteq B$ právě tehdy, když $A \cup B = B$;
(xv) $P(A) \subseteq P(B) \implies A \subseteq B$.
Poznámka: Všimněte si, že ve třech případech se jedná o distributivní zákon. Bod (viii) ukazuje, že $-$ umí roznásobit závorku se sjednocením zprava, ale v (ix) vidíme, že zleva už to nejde, tam je třeba vzorec upravit. Bod (x) ukazuje, že $\cap$ umí roznásobit závorku s odčítáním, pro další kombinace operací se podívejte do následujícího cvičení.

Cvičení 1d.2 (poučné, *dobré)**:** Rozhodněte, zda pro libovolné množiny A, B, C platí následující vztahy. Pak buď příslušný vztah dokažte, nebo dokažte, že neplatí.
V případě, že rovnost neplatí, rozmyslete si, jestli nebude platit alespoň nějaká inkluze, a tu dokažte.
Poznámka: Některé důkazy jsou dosti trikové, ale u všech příkladů byste měli být schopni určit, zda uvedená rovnost platí, popřípadě která inkluze platí. Dobré důkazy klidně vynechte. Mimochodem, v bodech (viii)-(xii) zkoumáme platnost různých verzí distributivního zákona.
(i) $(A \setminus B) \cup B = A$;
(ii) $(A \cap B) \cup (A \cap \overline{B}) = A$;
(iii) $(A \setminus B) \setminus C = (A \setminus C) \setminus B$.
(iv)** $(A \setminus B) \setminus C = A \setminus (B \setminus C)$;
(v) $(A \setminus B) \cup (B \setminus C) = A \setminus C$;
(vi) $P(A \cap B) = P(A) \cap P(B)$;
(vii) $P(A \cup B) = P(A) \cup P(B)$;
(viii)* $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$;
(ix)* $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$;
(x)* $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$;
(xi): $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$;
(xii): $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$;
(xiii)* $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Cvičení 1d.3 (rutinní)**:** Nechť A, B, C, D jsou množiny. Platí $(A \setminus B) \setminus (C \setminus D) = (A \setminus C) \setminus (B \setminus D)$? Svou odpověď zdůvodněte.

Cvičení 1d.4 (poučné)**:** Uvažujme množinu indexů $I = \mathbb{N}$ a množiny M_i pro $i \in I$. Najděte výsledky operací $\bigcup_{i=1}^{n} M_i$, $\bigcup_{i=1}^{\infty} M_i$, $\bigcap_{i=1}^{n} M_i$ a $\bigcap_{i=1}^{\infty} M_i$, jestliže
(i) $M_i = \{1, 2, 3, ..., i\} = \{k \in \mathbb{N} : k \leq i\}$ pro $i \in \mathbb{N}$;
(ii) $M_i = \{i, i+1, i+2, \dots\} = \{k \in \mathbb{N} : k \geq i\}$ pro $i \in \mathbb{N}$.
Poznámka: První zápis množinu výstižně popisuje, druhý je matematicky správný.

Cvičení 1d.5 (poučné)**:** Uvažujme množinu indexů $I = \mathbb{R}^+ = (0, \infty)$ a množiny M_r pro $r \in I$. Najděte $\bigcup_{r \in I} M_r$ a $\bigcap_{r \in I} M_r$, jestliže
(i) $M_r = (-r, 13 + r)$;
(ii) $M_r = \langle -r, 13 + r \rangle$;
(iii) $M_r = (-r, r)$.

Cvičení 1d.6 (poučné)**:** Uvažujme množiny indexů $I = (0, 1)$ a $J = \langle 0, 1 \rangle$. Najděte $\bigcup_{r \in I} M_r$ a $\bigcap_{r \in I} M_r$, $\bigcup_{r \in J} M_r$ a $\bigcap_{r \in J} M_r$, jestliže
(i) $M_r = (-r, 13 + r)$;
(ii) $M_r = \langle -r, 13 + r \rangle$.

Cvičení 1d.7 (poučné)**:** Nechť A_i pro $i \in I$ jsou množiny v universu U. Dokažte, že pro libovolnou podmnožinu indexů $J \subseteq I$ pak platí následující:
(i) $\bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i$;
(ii) $\bigcap_{i \in I} A_i \subseteq \bigcap_{i \in I} A_i$.

Cvičení 1d.8 (poučné)**:** Nechť A a A_i pro $i \in I$ jsou množiny v universu U. Dokažte, že pak platí následující:
(i) $A \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} (A \cap A_i)$;

(ii) $A \cup \bigcap\limits_{i\in I} A_i = \bigcap\limits_{i\in I}(A \cup A_i)$.

Řešení:

Připomeňme, že značka $\longrightarrow$ znamená „z toho nalevo vyplývá to napravo“. Zavedeme i $\longleftrightarrow$ pro odvození, které je platné v obou směrech a používáme je při důkazu ekvivalence. Rovnou se také dohodneme, že tyto značky automaticky ukončují předchozí a otevírají následující logický výraz, to nám ušetří spoustu závorek.

1d.1: (i): Zkusíme oba směry najednou, připoměňme, že pracujeme jen s prvky z universa, tedy $x \in U$.
$\forall x \in \overline{A} \longleftrightarrow x \notin A \wedge x \in U \longleftrightarrow x \in U \setminus A$.
(ii): Zkusíme oba směry najednou: $x \in A \setminus B \longleftrightarrow x \in A \wedge x \notin B \longleftrightarrow x \in A \wedge x \in \overline{B} \longleftrightarrow A \cap \overline{B}$.
(iii): $x \in \overline{A \setminus B} \longleftrightarrow \neg[x \in A \setminus B] \longleftrightarrow \neg[x \in A \wedge x \notin B] \longleftrightarrow x \notin A \vee x \in B \longleftrightarrow x \in \overline{A} \cup B$.
(iv): Sporem, existuje $x \in A \cap (B \setminus A)$, pak $x \in A \wedge x \in (B \setminus A) \longrightarrow x \in A \wedge (x \in B \wedge x \notin A) \longrightarrow x \in A \wedge x \notin A$, spor.
(v): Sporem, existuje $x \in (A \setminus B) \cap (B \setminus C)$, pak $x \in (A \setminus B) \wedge x \in (B \setminus C) \longrightarrow$
$(x \in A \wedge x \notin B) \wedge (x \in B \wedge x \notin C) \longrightarrow x \in B \wedge x \notin B$, spor.
Nebo pomocí (ii): $(A \setminus B) \cap (B \setminus C) = (A \cap \overline{B}) \cap (B \cap \overline{C}) = A \cap (\overline{B} \cap B) \cap \overline{C} = A \cap \emptyset \cap \overline{C} = \emptyset$.
(vi): $x \in (A \setminus B) \setminus C \longrightarrow (x \in A \wedge x \notin B) \wedge x \notin C \longrightarrow x \in A \wedge x \notin C \longrightarrow x \in A \setminus C$.
Nebo pomocí (ii): $(A \setminus B) \setminus C = (A \cap \overline{B}) \cap \overline{C} = (A \cap \overline{C}) \cap \overline{B} \subseteq A \cap \overline{C} = A \setminus C$.
(vii): Dokázat dvě inkluze. 1) $A \cup (B \setminus A) \subseteq A \cup B$: $\forall x \in A \cup (B \setminus A)$: $x \in A \vee x \in (B \setminus A)$
$\longrightarrow x \in A \vee (x \in B \wedge x \notin A) \longrightarrow x \in A \vee x \in B \longrightarrow x \in A \cup B$.
2) $A \cup B \subseteq A \cup (B \setminus A)$: $\forall x \in A \cup B$: $x \in A \vee x \in B$. Rozdělíme na případy. Pokud $x \in A$, pak $x \in A \cup (B \setminus A)$. Pokud $x \in B$, tak zase dva případy. Jestliže $x \in B \wedge x \in A$, pak $x \in A$ a přejdeme na předchozí. Jestliže $x \in B \wedge x \notin A$, pak $x \in B \setminus A \longrightarrow x \in A \cup (B \setminus A)$.
Nebo pomocí (ii): $A \cup (B \setminus A) = A \cup (B \cap \overline{A}) = (A \cup B) \cap (A \cup \overline{A}) = (A \cup B) \cap U = A \cup B$.
(viii): Zkusíme oba směry najednou pomocí distributivního zákona pro formální logiku: $x \in (A \cup B) \setminus C \longleftrightarrow$
$(x \in A \vee x \in B) \wedge x \notin C \longleftrightarrow (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C) \longleftrightarrow x \in (A \setminus C) \vee x \in (B \setminus C) \longleftrightarrow$
$x \in (A \setminus C) \cup (B \setminus C)$.
Snažší varianta pomocí (ii): $(A \cup B) \setminus C = (A \cup B) \cap \overline{C} = (A \cap \overline{C}) \cup (B \cap \overline{C}) = (A \setminus C) \cup (B \setminus C)$.
(ix): Zkusíme oba směry najednou pomocí distributivního zákona a De Morganova zákona pro formální logiku:
$A \setminus (B \cup C) \longleftrightarrow x \in A \wedge \neg(x \in B \cup C) \longleftrightarrow x \in A \wedge \neg(x \in B \vee x \in C) \longleftrightarrow$
$x \in A \wedge \neg(x \in B) \wedge \neg(x \in C) \longleftrightarrow x \in A \wedge x \in A \wedge \neg(x \in B) \wedge \neg(x \in C) \longleftrightarrow$
$(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \longleftrightarrow x \in (A \setminus B) \wedge x \in (A \setminus C) \longleftrightarrow x \in (A \setminus B) \cap (A \setminus C)$.
Snažší varianta pomocí (ii) a De Morgana pro množiny:
$A \setminus (B \cup C) = A \cap \overline{B \cup C} = A \cap \overline{B} \cap \overline{C} = A \cap A \cap \overline{B} \cap \overline{C} = (A \cap \overline{B}) \cap (A \cap \overline{C}) = (A \setminus B) \cap (A \setminus C)$.
(x): Zkusíme oba směry najednou pomocí distributivního zákona a De Morganova zákona pro formální logiku:
$A \setminus (B \cap C) \longleftrightarrow x \in A \wedge \neg(x \in B \cap C) \longleftrightarrow x \in A \wedge \neg(x \in B \wedge x \in C) \longleftrightarrow$
$x \in A \wedge (\neg(x \in B) \vee \neg(x \in C)) \longleftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \longleftrightarrow x \in (A \setminus B) \vee x \in (A \setminus C) \longleftrightarrow$
$(A \setminus B) \cup (A \setminus C)$.
Snažší varianta pomocí (ii) a De Morgana pro množiny:
$A \setminus (B \cap C) = A \cap \overline{B \cap C} = A \cap (\overline{B} \cup \overline{C}) = (A \cap \overline{B}) \cup (A \cap \overline{C}) = (A \setminus B) \cup (A \setminus C)$.
(xi): Tento důkaz je jedním směrem relativně snadný a používá distributivní zákon, těžší je najít směr opačný. Ukáže se, že ten snadný směr je vlastně ekvivalentní a funguje i naopak (rozmyslete si).
$x \in (A \cap B) \setminus (A \cap C) \longleftrightarrow x \in A \cap B \wedge \neg(x \in A \cap C) \longleftrightarrow x \in A \cap B \wedge \neg(x \in A \wedge x \in C) \longleftrightarrow$
$(x \in A \wedge x \in B) \wedge (x \notin A \vee x \notin C) \longleftrightarrow [(x \in A \wedge x \in B) \wedge x \notin A] \vee [(x \in A \wedge x \in B) \wedge x \notin C] \longleftrightarrow$
$[x \in A \wedge x \notin A \wedge x \in B] \vee [x \in A \wedge (x \in B \wedge x \notin C)] \longleftrightarrow [F \wedge x \in B] \vee [x \in A \wedge x \in (B \setminus C)] \longleftrightarrow$
$F \vee [x \in A \cap (B \setminus C)] \longleftrightarrow x \in A \cap (B \setminus C)$.
(xii): 1) Předpoklad $A \subseteq B$, chceme $\forall b \in \overline{B}$: $b \in \overline{A}$. Jedna možnost sporem: Nechť existuje $b \in \overline{B}$ takové, že $b \notin \overline{A}$. Pak $b \in A$, podle předpokladu $b \in B$. Takže $b \in \overline{B} \wedge b \in B$, spor.
Alternativa: Předpoklad říká $\forall x$: $x \in A \longrightarrow x \in B$. Přejdeme k ekvivalentní obměně: $\forall x$: $x \notin B \longrightarrow x \notin A$ neboli $\forall x$: $x \in \overline{B} \longrightarrow x \in \overline{A}$, přesně jak potřebujeme.
2) Předpoklad $\overline{B} \subseteq \overline{A}$, chceme $A \subseteq B$. Podle 1) plyne z předpokladu $\overline{\overline{A}} \subseteq \overline{\overline{B}}$, což je právě $A \subseteq B$.
(xiii): 1) Předpoklad $A \subseteq B$, chceme $A \cap B = A$. Ukážeme dvě inkluze.
Důkaz $A \cap B \subseteq A$: $\forall x \in A \cap B$: $x \in A \wedge x \in B \longrightarrow x \in A$.
Důkaz $A \subseteq A \cap B$: $\forall a \in A$: $a \in B$ dle předpokladu. Proto $a \in A \wedge a \in B \longrightarrow a \in A \cap B$.
2) Předpoklad $A \cap B = A$, chceme $A \subseteq B$. Důkaz:
$\forall a \in A$: $a \in A \cap B$ dle předpokladu, proto $a \in A \wedge a \in B \longrightarrow a \in B$.
(xiv): 1) Předpoklad $A \subseteq B$, chceme $A \cup B = B$. Ukážeme dvě inkluze. Důkaz $A \cup B \subseteq B$:

$\forall x \in A \cup B$: $x \in A \vee x \in B$, ale předpoklad dává, že i v případě $a \in A$ je $a \in B$, proto každopádně $x \in B$.
Důkaz $B \subseteq A \cup B$: $\forall b \in B$: $a \in B \longrightarrow a \in A \wedge a \in B \longrightarrow a \in A \cup B$.
2) Předpoklad $A \cup B = B$, chceme $A \subseteq B$. Důkaz: $\forall a \in A$: $a \in A \cup B = B$ dle předpokladu, proto $a \in B$.
(xv): Předpoklad říká, že prvky $P(A)$ jsou i prvky $P(B)$, zde je zásadní si uvědomit, že množina $P(A)$ má jako prvky podmnožiny A. Chceme ukázat, že prvky z A jsou v B:
$a \in A \longrightarrow \{a\} \subseteq A \longrightarrow \{a\} \in P(A) \longrightarrow \{a\} \in P(B) \longrightarrow \{a\} \subseteq B \longrightarrow a \in B$.
1d.2: (i): Protipříklad: třeba $A = \emptyset$, $B = \{13\}$. Platí ale $A \subseteq (A \setminus B) \cup B$: Nechť $a \in A$ libovolné. Dvě možnosti: $x \in B$, pak $x \in (A \setminus B) \cup B$, nebo $x \notin B$, pak $x \in A \wedge x \notin B \longrightarrow x \in (A \setminus B) \longrightarrow x \in (A \setminus B) \cup B$.
Formální důkaz: $x \in A \longleftrightarrow x \in A \wedge T \longleftrightarrow x \in A \wedge (x \notin B \vee x \in B) \longleftrightarrow$
$(x \in A \wedge x \notin B) \vee (x \in A \wedge x \in B) \longrightarrow x \in (A \setminus B) \vee x \in B \longrightarrow x \in (A \setminus B) \cup B$.
(ii): Platí. Dvě inkluze. $(A \cap B) \cup (A \cap \overline{B}) \subseteq A$: $x \in (A \cap B) \cup (A \cap \overline{B}) \longrightarrow x \in (A \cap B) \vee x \in (A \cap \overline{B}) \longrightarrow$
$x \in A \vee x \in A \longrightarrow x \in A$.
$A \subseteq (A \cap B) \cup (A \cap \overline{B})$: Nechť $x \in A$. Dvě možnosti. Pokud $x \in B$, pak $x \in A \wedge x \in B \longrightarrow x \in (A \cap B) \longrightarrow$
$x \in (A \cap B) \cup (A \cap \overline{B})$. Nebo $x \notin B$, pak $x \in A \wedge x \notin B \longrightarrow x \in (A \cap \overline{B}) \longrightarrow x \in (A \cap B) \cup (A \cap \overline{B})$.
(iii): Platí, důkaz obou směrů najednou: $x \in (A \setminus B) \setminus C \longleftrightarrow x \in (A \setminus B) \wedge x \notin C \longleftrightarrow$
$(x \in A \wedge x \notin B) \wedge x \notin C \longleftrightarrow (x \in A \wedge x \notin C) \wedge x \notin B \longleftrightarrow x \in (A \setminus C) \wedge x \notin B \longleftrightarrow x \in (A \setminus C) \setminus B$.
(iv) Protipříklad: $A = B = C = \{1\}$. Platí ale $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$ (důkaz dost trikový):
$x \in (A \setminus B) \setminus C \longrightarrow x \in (A \setminus B) \wedge x \notin C \longrightarrow x \in A \wedge x \notin B \wedge x \notin C \longrightarrow x \in A \wedge x \notin B$
$\longrightarrow x \in A \wedge x \notin B \vee x \in C \longrightarrow x \in A \wedge \neg(x \in B \wedge x \notin C) \longrightarrow x \in A \wedge \neg[x \in (B \setminus C)]$
$\longrightarrow x \in A \wedge x \notin (B \setminus C) \longrightarrow x \in A \setminus (B \setminus C)$.
(v): Protipříklad: třeba $A = C = \emptyset$, $B = \{13\}$. Platí ale $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$: $x \in A \setminus C \longrightarrow x \in A \wedge x \notin C$.
Dvě možnosti. Pokud $x \in B$, tak $x \in A \wedge x \in B \wedge x \notin C \longrightarrow x \in B \wedge x \notin C \longrightarrow x \in (B \setminus C) \longrightarrow$
$x \in (A \setminus B) \cup (B \setminus C)$.
Nebo $x \notin B$, pak $x \in A \wedge x \notin B \wedge x \notin C \longrightarrow x \in A \wedge x \notin B \longrightarrow x \in (A \setminus B) \longrightarrow x \in (A \setminus B) \cup (B \setminus C)$.
(vi): Platí, dokážeme dvě inkluze. 1) $P(A \cap B) \subseteq P(A) \cap P(B)$: Nechť $x \in P(A \cap B)$, pak x je vlastně podmnožina $A \cap B$. Proto $x \subseteq A \wedge x \subseteq B \longrightarrow x \in P(A) \wedge x \in P(B) \longrightarrow x \in P(A) \cap P(B)$.
2) $P(A) \cap P(B) \subseteq P(A \cap B)$: $x \in P(A) \cap P(B) \longrightarrow x \in P(A) \wedge x \in P(B) \longrightarrow x \subseteq A \wedge x \subseteq B \longrightarrow$
$x \subseteq A \cap B \longrightarrow x \in P(A \cap B)$.
(vii): Protipříklad: třeba $A = \{1, 2\}$, $B = \{3, 4\}$. Pak množina $M = \{2, 3\}$ leží v $P(A \cup B)$, ale není ani v $P(A)$, ani v $P(B)$, tedy není v jejich sjednocení. Platí ale $P(A) \cup P(B) \subseteq P(A \cup B)$:
$x \in P(A) \cup P(B) \longrightarrow x \in P(A) \vee x \in P(B) \longrightarrow x \subseteq A \vee x \subseteq B \longrightarrow x \subseteq A \cup B \longrightarrow x \in P(A \cup B)$.
(viii): Protipříklad: $A = \{13\}$, $B = C = \emptyset$. Platí ale $(A \cup B) \setminus (A \cup C) \subseteq A \cup (B \setminus C)$: $x \in (A \cup B) \setminus (A \cup C) \longleftrightarrow$
$(x \in A \vee x \in B) \wedge \neg(x \in A \vee x \in C) \longleftrightarrow (x \in A \vee x \in B) \wedge (x \notin A \wedge x \notin C) \longleftrightarrow$
$(x \in A \wedge x \notin A \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C) \longrightarrow F \vee (x \in (B \setminus C)) \longleftrightarrow x \in (B \setminus C) \longrightarrow$
$x \in A \cup (B \setminus C)$.
(ix): Protipříklad: $A = B = \{1\}$, $C = \emptyset$. Platí ale $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cap C)$: $x \in (A \setminus B) \cap (A \setminus C) \longleftrightarrow x \in$
$(A \setminus B) \wedge x \in (A \setminus C) \longleftrightarrow x \in A \wedge x \notin B \wedge x \in A \wedge x \notin C \longleftrightarrow x \in A \wedge (\neg x \in B \wedge \neg x \in C) \longrightarrow$
$x \in A \wedge (\neg x \in B \vee \neg x \in C) \longleftrightarrow x \in A \wedge \neg(x \in B \wedge x \in C) \longleftrightarrow$
$x \in A \wedge \neg(x \in B \cap C) \longleftrightarrow x \in A \wedge x \notin (B \cap C) \longleftrightarrow x \in A \setminus (B \cap C)$.
(x): Protipříklad: $A = B = \{1\}$, $C = \emptyset$. Platí ale $A \setminus (B \cup C) \subseteq (A \setminus B) \cup (A \setminus C)$: $x \in A \setminus (B \cup C) \longleftrightarrow$
$x \in A \wedge x \notin (B \cup C) \longleftrightarrow x \in A \wedge \neg(x \in B \cup C) \longleftrightarrow x \in A \wedge \neg(x \in B \vee x \in C) \longleftrightarrow$
$x \in A \wedge x \notin B \wedge x \notin C) \longleftrightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \longleftrightarrow x \in (A \setminus B) \wedge x \in (A \setminus C) \longrightarrow$
$x \in (A \setminus B) \vee x \in (A \setminus C) \longleftrightarrow x \in (A \setminus B) \cup (A \setminus C)$.
(xi): Platí, zkusíme oba směry najednou, začneme od složitějšího: $x \in (A \setminus C) \cap (B \setminus C) \longleftrightarrow$
$x \in (A \setminus C) \wedge x \in (B \setminus C) \longleftrightarrow (x \in A \wedge x \notin C) \wedge (x \in B \wedge x \notin C) \longleftrightarrow x \in A \wedge x \notin C \wedge x \in B \wedge x \notin C \longleftrightarrow$
$x \in A \wedge x \in B \wedge x \notin C \longleftrightarrow x \in (A \cap B) \wedge x \notin C \longleftrightarrow x \in (A \cap B) \setminus C$.
(xii): Platí, zkusíme oba směry najednou: $x \in (A \cup B) \setminus C \longleftrightarrow x \in (A \cup B) \wedge x \notin C \longleftrightarrow$
$(x \in A \vee x \in B) \wedge x \notin C \longleftrightarrow (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C) \longleftrightarrow x \in (A \setminus C) \vee x \in (B \setminus C) \longleftrightarrow$
$x \in (A \setminus C) \cup (B \setminus C)$.
(xiii): Platí, zkusíme oba směry najednou, začneme od složitějšího: $x \in (A \setminus C) \setminus (B \setminus C) \longleftrightarrow$
$x \in (A \setminus C) \wedge x \notin (B \setminus C) \longleftrightarrow (x \in A \wedge x \notin C) \wedge \neg(x \in B \wedge x \notin C) \longleftrightarrow (x \in A \wedge x \notin C) \wedge (x \notin B \vee x \in C) \longleftrightarrow$
$(x \in A \wedge x \notin C \wedge x \notin B) \vee (x \in A \wedge x \notin C \wedge x \in C) \longleftrightarrow (x \in A \wedge x \notin C \wedge x \notin B) \vee (x \in A \wedge F) \longleftrightarrow$
$(x \in A \wedge x \notin C \wedge x \notin B) \vee F \longleftrightarrow x \in A \wedge x \notin C \wedge x \notin B \longleftrightarrow (x \in A \wedge x \notin B) \wedge x \notin C \longleftrightarrow$
$(x \in (A \setminus B) \wedge x \notin C \longleftrightarrow x \in (A \setminus B) \setminus C$.
1d.3: Neplatí, intuitivně vidíme, že vpravo odebíráme celé C, zatímco vlevo jen zmenšené C, na tomto pocitu zkusíme založit protipříklad: $A = C = D = \{13\}$, $B = \emptyset$.
1d.4: (i): $\{1, 2, 3, \ldots, n\}$, $\mathbb{N}$, $\{1\}$, $\{1\}$.

(ii): $\mathbb{N}$, $\mathbb{N}$, $\{n, n+1, n+2, n+3, \dots\}$, $\emptyset$.
1d.5: (i): $\mathbb{R}$, $\langle 0, 13\rangle$; (ii): $\mathbb{R}$, $\langle 0, 13\rangle$; (iii): $\mathbb{R}$, $\{0\}$.
1d.6: (i): $(-1, 14)$, $\langle 0, 13\rangle$, $(-1, 14)$, $(0, 13)$; (ii): $(-1, 14)$, $\langle 0, 13\rangle$, $\langle -1, 14\rangle$, $\langle 0, 13\rangle$.

Cvičení 1d.7 (poučné)**:** (i): $\forall x \in \bigcup_{i\in J} A_i$: existuje $i \in J$ aby $x \in A_i$, ale $J \subseteq I$, proto také $i \in I$ a $x \in \bigcup_{i\in I} A_i$.
(i): $\forall x \in \bigcap_{i\in I} A_i$: Platí $\forall i \in I$: $x \in A_i$. Ale $\supset\subseteq I$, takže také $\forall i \in J$: $x \in A_i$. Ale $\supset\subseteq I$ neboli $x \in \bigcap_{i\in I} A_i$.
1d.8: (i): $x \in A \cap \bigcup_{i\in I} A_i \longleftrightarrow x \in A \wedge x \in \bigcup_{i\in I} A_i \longleftrightarrow x \in A \wedge \big(\exists i \in I\colon x \in A_i\big) \longleftrightarrow$
$\exists i \in I\colon (x \in A \wedge x \in A_i) \longleftrightarrow \exists i \in I\colon (x \in A \cap A_i) \longleftrightarrow x \in \bigcup_{i\in I}(A \cap A_i)$.
(ii): $x \in A \cup \bigcap_{i\in I} A_i \longleftrightarrow x \in A \vee x \in \bigcap_{i\in I} A_i \longleftrightarrow x \in A \vee \big(\forall i \in I\colon x \in A_i\big) \longleftrightarrow \forall i \in I\colon (x \in A \vee x \in A_i) \longleftrightarrow$
$\forall i \in I\colon (x \in A \cup A_i) \longleftrightarrow x \in \bigcap_{i\in I}(A \cup A_i)$.