1 Matematika jako část logiky

Matematika, kterou jste se učili na střední škole, byla spíše matematikou praktickou. To znamená, že obsahovala hlavně návody jak počítat s čísly, jak upravovat různé výrazy (např. algebraické nebo výrazy s goniometrickými funkcemi) nebo jak vyřešit nějakou konkrétní soustavu lineárních rovnic. Nicméně současná matematika není věda, která by se snažila řešit různé typy konkrétních úloh. Návody na řešení těchto úloh jsou obvykle jen důsledkem nějaké matematické teorie. Matematickou teorii dostaneme tak, že naše objekty zájmu, které chceme studovat (např. přímky a body v rovině), popíšeme množinou tzv. axiomů (tj. tvrzení o kterých víme, že je naše studované objekty splňují, např. každá dvojice ruzných bodů určuje právě jednu přímku). Hlavním úkolem matematika potom je hledat jiná tvrzení, která z těchto axiomů plynou (tzn. jsou pravdivá v dané teorii, protože o axiomech víme, že platí). Matematiku můžeme tedy obecně popsat, jako vědu, která se snaží nacházet pravdivá tvrzení v jednotlivých matematických teoriích. Je to tedy část logiky, protože logika je vědou, která popisuje pravidla správného usuzování (tzn. jak z nějakých pravdivých tvrzení vyvozovat jiná pravdivá tvrzení).

1.1 Logika

Naším úkolem v tomto kurzu bude objevovat pravdivá tvrzení v jedné konkrétní matematické teorii (v teorii lineárních prostorů). Co to tedy tvrzení je? Tvrzení je věta, která je buď pravdivá nebo nepravdivá. Příklady mohou být:

1. "Číslo 10 je dělitelné číslem 3."
2. "Existuje nekonečně mnoho prvočísel."
3. "Každý úhel může být roztřetěn pomocí pravítka a kružítka."

První tvrzení je evidentně nepravdivé. Druhé je pravdivé, jak ukázal slavný matematik Euclides. Poslední je příklad nepravdivého výroku, jehož nepravdivost dokázal Galois.

Samozřejmě v běžném jazyce máme spoustu vět, kterým nelze přiřadit žádnou pravdivostní hodnotu (tj. nejsou to tvrzení v našem smyslu) např:

1. Citoslovce: "Mlask."
2. Tázací věty: "Chceš mě kotě?"
3. Příkazy: "Chlastej!"

Složitější tvrzení se obvykle skládají z jednodušších tvrzeních pomocí logických spojek (např. číslo 5 je liché nebo sudé). Pravdivost takového tvrzení potom záleží na pravdivosti oněch jednodušších tvrzeních a na logických spojkách, které byly v daném případě použity. Ukažme si tedy jednotlivé logické spojky, se kterými se budeme v matematice stále potkávat.

Negace

Máme-li nějaké tvrzení T, můžeme z něho s pomocí negace vyrobit opačné tvrzení (symbolicky ho značíme $\neg T$), které platí, když neplatí T a neplatí, když T platí. Např. pokud T je tvrzení "5 je prvočíslo", pak $\neg T$ je tvrzení "5 není prvočíslo". Schematicky můžeme tuto skutečnost zapsat pomocí následující tabulky, kde 0 představuje fakt, že dané tvrzení není pravdivé a 1, že pravdivé je:

T	$\neg T$
0	1
1	0

Konjunkce

Mějme dvě tvrzení A, B. Konjunkce těchto tvrzení (symbolicky ji značíme $A \wedge B$) je tvrzení, které platí pouze v případě, kdy platí obě tvrzení A a B. Ve všech ostatních případech je nepravdivé. Tvrzení $A \wedge B$ obvykle čteme jako "A a B" nebo "A a také B" nebo "A a zároveň B". Např. tvrzení "7 je prvočíslo a také 3 je prvočíslo" je pravdivé a tvrzení "7 je prvočíslo a 4 je prvočíslo" je nepravdivé, protože 4 není prvočíslo. Způsob jakým konjunkce pracuje můžeme opět znázornit tabulkou:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Disjunkce

Mějme dvě tvrzení A, B. Disjunkce těchto tvrzení (symbolicky ji značíme $A \vee B$) je tvrzení, které neplatí pouze v případě, kdy neplatí obě tvrzení A a B. Ve všech ostatních případech je pravdivé. Tvrzení $A \vee B$ obvykle čteme jako "A nebo B". Např. tvrzení "7 je prvočíslo nebo 4 je prvočíslo" je pravdivé a tvrzení "6 je prvočíslo nebo 4 je prvočíslo" je nepravdivé, protože ani 6 ani 4 není prvočíslo. Způsob jakým disjunkce pracuje můžeme opět znázornit tabulkou:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Všimněte si, že matematika spojku "nebo" používá ve slučovací významu, tj. pravdivost jedné části disjukce stačí na pravdivost celé disjunkce (ale mohou platit klidně obě dvě). Kdežto v běžném jazyce používáme někdy spojku "nebo" i ve vylučovacím významu. Např. větou "K obědu si dám guláš nebo svíčkovou." obvykle míníme, že si dáme jen jedno z těchto dvou jídel a ne obě zároveň.

Implikace

Mějme opět dvě tvrzení A, B. Implikace těchto tvrzení (symbolicky ji značíme $A \Rightarrow B$) je tvrzení, které neplatí pouze v případě, kdy platí tvrzení A a neplatí B. Ve všech ostatních případech je pravdivé. Způsob jakým implikace pracuje můžeme opět znázornit tabulkou:

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Tvrzení $A \Rightarrow B$ obvykle čteme jako "Když A, pak B" nebo "Jestliže A, potom B" nebo "Z A plyne B" nebo "Nechť A. Pak B". Např. tvrzení "Když je číslo x sudé, pak je dělitelné 2" je pravdivé a tvrzení "Když je číslo x liché, pak je dělitelné 2" je nepravdivé.

Implikace je pro pochopení obvykle složitější, protože není jasné, proč $0 \Rightarrow 0$ a $0 \Rightarrow 1$ jsou pravdivá tvrzení. Důvod proč je implikace definována, tak jak je, pokusíme osvětlit na následujícím příkladě. Nechť A je tvrzení "Student Bořislav Nemrava mi dá milión korun českých" a B je tvrzení "Dám panu Bořislavu Nemravovi na konci semetru jedničku z algebry". Pokud tvrdím, že tvrzení $A \Rightarrow B$ (tj. "Když mi student Bořislav Nemrava dá milión korun českých, pak dám panu Bořislavu Nemravovi na konci semetru jedničku z algebry") je pravdivé, v kterých případech lžu? Zřejmě jen v případě, kdy dostanu peníze a jedničku na konci semestru nedám. V případech, kdy žádné

peníze nedostanu, můžu dát známku, jakou chci, protože nejsem vázán oním úplatkem a tudíž neporušuji platnost svého tvrzení $A \Rightarrow B$.

Důvod proč implikace $A \Rightarrow B$, kde tvrzení A je nepravdivé, je pravdivá, lze vysvětlit i na našem předchozím příkladu "Když je číslo x sudé, pak je dělitelné 2". Chceme totiž aby takovéto tvrzení platilo pro všechna celá čísla, tzn. musí platit jak pro $x = 2$, tak i pro $x = 3$.

Ekvivalence

Mějme opět dvě tvrzení A, B. Ekvivalence těchto tvrzení (symbolicky ji značíme $A \Leftrightarrow B$) je tvrzení, které platí pouze v případech, kdy buď platí obě tvrzení A, B zároveň nebo zároveň neplatí. Ve všech ostatních případech je nepravdivé. Způsob jakým ekvivalence pracuje můžeme opět znázornit tabulkou:

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Tvrzení $A \Leftrightarrow B$ obvykle čteme jako "A právě tehdy, když B". Příkladem ekvivalence je např. tvrzení: "Číslo x je dělitelné prvočíslem p právě tehdy, když x^2 je dělitelné p^2".

Kvantifikátory

Příklady tvrzení s implikací a ekvivalencí obsahovaly libovolné, ale pevné číslo x. Označme jako $A(x)$ tvrzení "Když je číslo x sudé, pak je dělitelné 2". Symbol "x" v závorkách za A naznačuje, že pravdivost tohoto tvrzení bude záviset na čísle, které za x dosadíme. Kdyby jsme nyní chtěli nějakým způsobem zapsat skutečnost, že $A(x)$ je pravdivé pro všechny celá čísla x, museli bychom s naším současným aparátem psát, tvrzení $A(0) \wedge A(1) \wedge A(2) \wedge \ldots$ je pravdivé, tj. tvrzení platí pro $x = 0$, $x = 1$, $x = 2$, atd. To samozřejmě není moc praktické, proto logika obsahuje další prvky, kterým se říká kvantifikátory. Kvantifikátory máme dva: první "pro všechny" (značí se symbolicky $\forall$) a druhý "existuje" (značí se symbolicky $\exists$). Jestliže tedy máme tvrzení $A(x)$, které je závislé na x, můžeme z něho vyrobit dvě tvrzení:

1. "Pro všechna x je $A(x)$ pravdivé". Symbolicky zapisujeme jako $(\forall x)A(x)$. Tvrzení $(\forall x)A(x)$ je pravdivé když $A(x)$ pravdivé pro libovolné x a nepravdivé když existuje takové x, že $A(x)$ pro něj není pravdivé. Např. "Pro všechna celá čísla x platí: když x je sudé, pak je dělitelné 2" je pravdivé tvrzení a "Pro všechna celá čísla x platí: když x je liché, pak je dělitelné 3" je nepravdivé, protože 5 je liché a není dělitelné 3.

2. "Existuje x takové, že $A(x)$ je pravdivé". Symbolicky zapisujeme jako $(\exists x)A(x)$. Tvrzení $(\exists x)A(x)$ je pravdivé, když existuje alespoň jedno x takové, že tvrzení $A(x)$ pro něj platí a nepravdivé, když takové x neexistuje. Např. "Existuje celé číslo větší než 100" je pravdivé tvrzení, protože např. 101 je celé číslo větší než 100. Naopak tvrzení "Existuje reálné číslo jehož druhá mocnina je záporná" je nepravdivé.

Pokud v symbolickém zápisu kvantifikátorů chceme přesně stanovit odkud x pochází, uděláme to následovně. Označme množinu reálných čísel $\mathbb{R}$ a množinu komplexních čísel $\mathbb{C}$. Poslední příklad můžeme potom zapisovat takto: $(\exists x \in \mathbb{R})(x^2 < 0)$. Toto tvrzení není pravdivé. Naopak $(\exists x \in \mathbb{C})(x^2 < 0)$ je příkladem pravdivého tvrzení, protože $i^2 = -1$. Obdobný zápis se používá i s kvantifikátorem $\forall$ např.: $(\forall x \in \mathbb{R})A(x)$.

1.2 Definice, věta, důkaz

Nyní máme vymezen zakladní jazyk (tj. logické spojky a kvantifikátory), který matematika používá. Zároveň jsme i stanovili, co jednotlivé prvky tohoto jazyka znamenají (tj. víme, jak určit pravdivost

složených tvrzení, když známe pravdivost jeho podčástí). Jak už bylo v úvodu řečeno, matematika se zabývá hledáním pravdivých tvrzení, které plynou axiomů (tj. tvrzení, která jsme prohlásili za pravdivá, protože víme, že naše studované objekty je určitě splňují). Bohužel žádný obecný postup, jak tyto pravdivá tvrzení hledat neexistuje, takže vždy záleží na schopnostech konkretního matematika, jaká tvrzení z axiomů odvodí. Nicméně, když už najde nějaké zajímavé tvrzení, které mu přijde pravdivé v dané teorii, musí dokázat, že to tak vskutku je. Pak teprve může prohlásit, že jeho nalezené tvrzení je pravdivé.

Metod, jak nějaké tvrzení dokázat máme několik. Protože většina matematických tvrzení je ve tvaru implikace nebo ekvivalence, zaměříme se na důkazy tvrzení typu $A \Rightarrow B$ a $A \Leftrightarrow B$. Ve skutečnosti se stačí zaměřit jenom na tvrzení typu $A \Rightarrow B$, protože důkaz tvrzení $A \Leftrightarrow B$ lze převést na důkaz dvou implikací. Můžeme se totiž snadno pomocí tabulky přesvědčit, že tvrzení $A \Leftrightarrow B$ je ekvivalentní s tvrzením $(A \Rightarrow B) \wedge (B \Rightarrow A)$, tj. když platí jedno, platí i druhé a naopak.

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
0	0	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	1	1	1

Oba sloupce $A \Leftrightarrow B$ a $(A \Rightarrow B) \wedge (B \Rightarrow A)$ jsou stejné, což znamená, že obě tvrzení jsou ekvivalentní. Pokud tedy chceme dokázat tvrzení ve tvaru $A \Leftrightarrow B$, stačí když dokážeme, že platí $A \Rightarrow B$ i $B \Rightarrow A$, protože potom musí být pravdivá i jejich konjunkce.

Než přistoupíme k diskuzi jednotlivých typů důkazů, je potřeba uvést, že není v silách tohoto psaného materiálu, vysvětlit úplně tuto problematiku. Koneckonců matematici začátečníci se učí dokazovat tak, že se snaží pochopit důkazy svých vyspělejších kolegů a pak jejich postupy používat ve své vlastní práci.

Předpokládejme, že chceme dokázat tvrzení $A \Rightarrow B$. Tvrzení A se obvykle nazývá předpoklad a tvrzení B závěr.

Přímý důkaz

První metoda důkazu je tzv. přímý důkaz. Protože jediný případ, kdy by implikace $A \Rightarrow B$ nebyla pravdivá, je případ, kdy A je pravdivé a B nikoli, stačí když ukážeme, že tento případ nenastává. Tzn. budeme předpokládat, že tvrzení A je pravdivé a pokusíme se ukázat, že i B musí už být pravdivé. K tomu aby jsme ukázali, že B už musí být pravdivé můžeme využít nejen náš předpoklad, že A platí, ale i pravdivost axiomů a jiných už dokázaných tvrzení v dané teorii. Samotný důkaz potom probíhá tak, že vícenásobnou aplikací korektních dedukčních pravidel[1] na A, axiomy a již dokázaná tvrzení, odvodíme nová tvrzení. Pokud mezi je i tvrzení B máme vyhráno.

Pokusíme se přímý důkaz ilustrovat na velmi jednoduchém příkladě. Předpokládejme, že objekty našeho zájmu jsou celá čísla. Konkrétně nás bude zajímat jaké vlastnosti má sčítání celých čísel. Dále předpokládejme, že následující tvrzení jsou buď naše axiomy nebo již dokázaná tvrzení:

1. Reflexivita rovnosti: $a = a$
2. Symetrie rovnosti: Když $a = b$, pak $b = a$. Symbolicky: $a = b \;\Rightarrow\; b = a$.
3. Transitivita rovnosti: Když $a = b$ a $b = c$, pak $a = c$. Symbolicky: $(a = b \;\wedge\; b = c) \;\Rightarrow\; a = c$.
4. Jednoznačnost sčítání: Když $a = a'$ a $b = b'$, pak $a + b = a' + b'$. Symbolicky:

$$(a = a' \;\wedge\; b = b') \;\Rightarrow\; a + b = a' + b' \,.$$

[1] Co jsou korektní dedukční pravidla nám říká logika. Uvedeme si jen některé příklady. Např. pokud víme, že tvrzení C a $C \Rightarrow D$ jsou pravdivá, můžeme usoudit, že i tvrzení D je pravdivé, protože kdyby nebylo, muselo by být C nebo $C \Rightarrow D$ nepravdivé. Tomuto dedukčnímu pravidlu se říká modus ponens. Jiným příkladem je např. dedukční pravidlo: z pravdivosti $C \Rightarrow D$ a $D \Rightarrow E$ odvoď $C \Rightarrow E$ (transitivita implikace). Jako poslední uvedeme dedukční pravidlo generalizace. Pokud ukážeme, že nějaké tvrzení $A(x)$ je pravdivé pro libovolné pevné x, můžeme odvodit pravdivost tvrzení $(\forall x)A(x)$.

5. Neutrální prvek: $0 + a = a$

U všech výše uvedených tvrzení představují a, b, c libovolná pevná celá čísla. Pomocí těchto tvrzení dokážeme následující tvrzení:

Tvrzení 1 *Když $a = 0$, pak $a + b = b$ (Symbolicky $a = 0 \;\Rightarrow\; a + b = b$).*

Důkaz: Rozdělíme důkaz na jednotlivé kroky a u každého z nich uvedeme z kterých tvrzení plyne.

a) Podle tvrzení 1 víme, že $b = b$ je pravdivé.

b) Protože dokazujeme implikaci, předpokládáme, že $a = 0$ je také pravdivé.

c) Z kroků a) a b) můžeme odvodit, že je pravdivá i konjunkce $a = 0 \wedge b = b$, protože konjunkce je pravdivá, když jsou pravdivé obě její části.

d) Podle tvrzení 4 víme, že $(a = 0 \;\wedge\; b = b) \;\Rightarrow\; a + b = 0 + b$ je pravdivé.

e) Aplikací modus ponens na c) a d) odvodíme pravdivost tvrzení $a + b = 0 + b$.

f) Podle tvrzení 5 víme, že $0 + b = b$ je pravdivé.

g) Z kroků e) a f) můžeme odvodit stejně jako jsme to udělali v kroku c), že je pravdivá i konjunkce $a + b = 0 + b \;\wedge\; 0 + b = b$.

h) Podle tvrzení 3 víme, že $(a + b = 0 + b \;\wedge\; 0 + b = b) \;\Rightarrow\; a + b = b$ je pravdivé.

i) Aplikací modus ponens na g) a h) odvodíme pravdivost tvrzení $a + b = b$. A tím je důkaz hotov.

□

Je celkem zřejmé, že takto detailně důkazy psát nejde, protože by nám brzo došel papír nebo pamět počítače. Proto se důkazy většinou zkracují s tím, že zkušený čtenář (pokud bude chtít) jednotlivé detaily zrekonstruuje sám. Tudíž předchozí důkaz by se zapisoval asi nějak takto: protože předpokládáme, že $a = 0$, dostaneme $a+b = 0+b = b$. Automaticky se tedy například předpokládá, že čtenář zná všechny vlastnosti rovnosti (reflexivita, symetrie, transitivita).

Nepřímý důkaz

Nepřímý důkaz tvrzení $A \Rightarrow B$ probíhá stejně jako přímý důkaz, jen s tím rozdílem, že se snažím místo tvrzení $A \Rightarrow B$ dokázat tvrzení $\neg B \Rightarrow \neg A$. Obě tvrzení jsou totiž ekvivalentní, jak se snadno přesvědčíme pomocí tabulky:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

Postup opět ilustrujeme na příkladě. Nechť objekty našeho zájmu jsou opět celá čísla. Tentokrát již nebudeme uvádět podrobný důkaz, ale jen jeho stručnou verzi.

Tvrzení 2 *Nechť a a b jsou celá čísla. Když $a \neq 0$, pak existuje nejvýše jedno celé číslo x takové, že $ax = b$. Symbolicky:*

$$\neg(a = 0) \;\Rightarrow\; ((\exists x_1, x_2)(ax_1 = b \;\wedge\; ax_2 = b) \;\Rightarrow\; x_1 = x_2)\,.$$

Důkaz: Všíměte si, že věta také připouští neexistenci x takového, že $ax = b$. To znamená, že buď existuje jedno nebo žádné, ale nikdy ne více. Např. pro $a = 2$ a $b = 3$ neexistuje celé číslo x tak, že $ax = b$. Všimněte si také druhé části symbolického zápisu, jak je vyjádřen fakt, že více než jedno x nemůže existovat. Implikace v této druhé části vlastně říká, že kdyby existovali dvě celá čísla x_1, x_2, pak už musí být stejná.

Důkaz budeme provádět nepřímo, to znamená, že budeme předpokládat že neplatí závěr tvrzení $(\exists x_1, x_2)(ax_1 = b \ \wedge \ ax_2 = b) \ \Rightarrow \ x_1 = x_2$ a ukážeme, že předpoklad $\neg(a = 0)$ neplatí také.

Co tedy znamená, že neplatí závěr $(\exists x_1, x_2)(ax_1 = b \wedge ax_2 = b) \ \Rightarrow \ x_1 = x_2$. Vidíme, že závěr má tvar implikace a ta neplatí jen tehdy, když platí její předpoklad tj. $(\exists x_1, x_2)(ax_1 = b \wedge ax_2 = b)$ a neplatí její závěr $x_1 = x_2$. Z platnosti $(\exists x_1, x_2)(ax_1 = b \ \wedge \ ax_2 = b)$ tedy víme, že existují dvě celá čísla x_1 a x_2 taková, že $ax_1 = b$ a $ax_2 = b$. Z neplatnosti $x_1 = x_2$ plyne, že $x_1 \neq x_2$. Nyní použijeme běžné vlastnosti celých čísel a rovnosti. Protože $ax_1 = b = ax_2$, dostaneme $0 = ax_1 - ax_2 = a(x_1 - x_2)$. Z nerovnosti $x_1 \neq x_2$ plyne $x_1 - x_2 \neq 0$. Jelikož ale $a(x_1 - x_2) = 0$, musí nutně platit $a = 0$ a $\neg(a = 0)$ tedy neplatí, což jsme měli dokázat. □

Důkaz indukcí

Důkaz indukcí je metoda, která nám umožňuje dokázat, že nějaké tvrzení platí pro všechna přirozená čísla větší než nějaké přirozené číslo n_0 (typicky $n_0 = 0$ nebo $n_0 = 1$). Těch je samozřejmě nekonečně mnoho a proto není možné tvrzení dokazovat pro každé přirozené číslo zvlášť. Předpokládejme, že chceme dokázat tvrzení $A(x)$ pro všechna přirozená čísla $x \geq n_0$. Důkaz indukcí probíhá ve dvou krocích:

1. Nejprve dokážeme, že tvrzení $A(n_0)$ je pravdivé.
2. Následně pro libovolné pevné přirozené číslo $n \geq n_0$ předpokládáme, že tvrzení $A(x)$ platí pro všechna x taková, že $n_0 \leq x \leq n$. Z tohoto předpokladu musíme ukázat, že i tvrzení $A(n + 1)$ je pravdivé[2].

Aplikaci důkazu indukcí si ukážeme na příkladě.

Tvrzení 3 *Nechť n je přirozené číslo větší nebo rovno 1. Pak*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}\,.$$

Důkaz: Důkaz budeme provádět indukcí pro $n_0 = 1$. V prvním kroku musíme ověřit, že tvrzení platí pro $n = 1$. To je ale zřejmé, protože $1 = \frac{1(1+1)}{2}$. V druhém kroku si vezmeme libovolné pevné $n \geq 1$ a z předpokladu platnosti tvrzení pro všechna přirozená čísla x splňující $1 \leq x \leq n$ dokážeme, že tvrzení platí i pro $n+1$. Nám konkrétně v tomto případě bude stačit jen předpoklad, že tvrzení platí pro $x = n$. Nyní ukážeme, že tvrzení je platné i pro $n + 1$:

$$1 + 2 + 3 + \cdots + n + (n + 1) = \frac{n(n+1)}{2} + (n + 1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\,.$$

V první rovnosti jsme použili fakt, že tvrzení je platné pro n. Pak jsme již jen upravili výsledný výraz tak, aby bylo patrné, že pravá strana rovnosti má tvar pravé strany tvrzení pro $n + 1$. □

Ukážeme si ještě jeden příklad.

Tvrzení 4 *Každé přirozené číslo $n \geq 2$ je buď prvočíslo nebo lze vyjádřit jako součin prvočísel.*

[2] Velmi často se jako druhý krok indukce uvádí toto: pro libovolné pevné $n \geq n_0$ dokažte z předpokladu platnosti $A(n)$ tvrzení $A(n + 1)$, tj. musíme dokázat platnost implikace $A(n) \Rightarrow A(n + 1)$. Obě formulace jsou ekvivalentní.

Důkaz: Důkaz budeme opět provádět indukcí, tentokrát ale pro $n_0 \geq 2$. První krok je jednoduchý. Musíme ověřit, že tvrzení platí pro $n = 2$. To je ale zřejmé, protože 2 je prvočíslo. Předpokládejme tedy nyní, že tvrzení platí pro všechna přirozená čísla x splňující $2 \leq x \leq n$. Ukážeme, že tvrzení platí i pro $n+1$. Pokud $n+1$ je prvočíslo, pak tvrzení platí. Takže zbývá akorát ukázat, že tvrzení platí i pro případ, kdy $n+1$ není prvočíslo. Jestliže ale $n+1$ není prvočíslo, je možno ho vyjádřit, jako součin dvou menších přirozených čísel p, q, tj. $n+1 = pq$ a $2 \leq p, q < n+1$. Z našeho předpokladu tedy plyne, že tvrzení platí pro p i q. Tudiž p i q lze vyjádřit jako součin prvočísel. Protože $n+1 = pq$, vidíme, že i $n+1$ lze vyjádřit jako součin prvočísel. □

K poslednímu tvrzení dodejme, že jsme dokázali část důležitého tvrzení z aritmetiky, které se nazývá Základní věta aritmetiky.

Tvrzení 5 (Základní věta aritmetiky) *Každé přirozené číslo $n \geq 2$ je buď prvočíslo nebo lze vyjádřit* jednoznačně *jako součin prvočísel.*

Důkaz tohoto tvrzení uvádět nebudeme. Všiměte si, že my jsme v předchozím důkazu ukázali, že rozklad na prvočísla je možno udělat, ale neukázali jsme, že to jde udělat jen jedním způsobem. To, že to jde právě jedním způsobem, je obsahem Základní věty aritmetiky. Tento fakt je v této větě vyjádřen slovem "jednoznačně".

Důkaz sporem

Dalším typickým důkazovým postupem je důkaz sporem. U důkazu sporem vždy předpokládáme, že námi dokazované tvzení neplatí a odvodíme z tohoto předpokladu spor (tj. nějaké nepravdivé tvrzení). Cheme-li tedy dokázat implikaci $A \Rightarrow B$, předpokládáme, že $A \Rightarrow B$ neplatí, což znamená, že platí předpoklad A a neplatí závěr B (tj. předpokládáme, že platí $A \wedge \neg B$). Pokud se nám podaří z tohoto předpokladu vyvodit spor je důkaz hotov. Tímto postupem tedy chceme ukázat, že nemůže nastat případ, kdy by platil předpoklad implikace a neplatil závěr.

Tvrzení 6 *Číslo $\sqrt{2}$ není racionální.*

Důkaz: Toto tvrzení na první pohled nevypadá jako implikace. Nicméně když si ho vyjádříme symbolicky nějakou tu implikaci objevíme. Tvrzení, že číslo $\sqrt{2}$ není racionální, vlastně říká, že ať už si vezmeme jakékoli racionální číslo x, tak určitě bude platit $x \neq \sqrt{2}$. Dokazované tvrzení tedy můžeme zapsat takto:

$$(\forall x)(x \in \mathbb{Q} \;\Rightarrow\; x \neq \sqrt{2})\,.$$

Tento výraz říká, že pro všechna čísla x, když x patří do množiny racionálních čísel $\mathbb{Q}$, tak už musí platit $x \neq \sqrt{2}$. Pokud tedy chceme toto tvrzení dokázat sporem, budeme předpokládat, že neplatí. To ale znamená, že musí existovat racionální číslo x takové, že $x = \sqrt{2}$.

Řekněme si nejprve, co znamená, že nějaké číslo x je racionální. Asi ze střední školy víte, že je možno ho vyjádřit jako podíl dvou celých čísel p, q, tj. $x = \frac{p}{q}$. Takže musí tedy platit $\frac{p}{q} = \sqrt{2}$. Upravou předchozí rovnosti dostaneme:

$$p^2 = 2q^2\,. \tag{1}$$

Číslo p lze podle Tvrzení 5 můžeme vyjádřit jako součin prvočísel. Vezmeme všechny dvojky, co se v tomto součinu nacházejí a vyjádříme p jako $p = 2^k p'$, kde k je počet oněch dvojek a p' už není dělitelné dvěmi. Podobně to uděláme s q, které vyjádříme jako $q = 2^n q'$, kde n je počet dvojek v q. Teď dosadíme za p, q do rovnice (1) a dostaneme:

$$(2^k p')^2 = 2(2^n q')^2\,.$$

Podle Základní věty aritmetiky (Tvrzení 5) musí být počet dvojek na obou stranách předchozí rovnosti stejný, protože ani p' ani q' není dělitelné dvěmi. Na levé straně máme $2k$ dvojek a na pravé straně máme $2n+1$ dvojek. Musí tedy platit $2k = 2n+1$, ale to není zřejmě možno, protože sudé číslo $2k$ se nemůže rovnat lichému $2n+1$. A to je onen kýžený spor. □

Matematický text

Nyní se zaměříme na to jak vypadá matematický text. Začneme terminologií. Matematická tvrzení obvykle pojmenováváme různými jmény podle jejich významu, složitosti důkazu, atd. Uveďme si několik jmen, se kterými se můžete v literatuře setkat. Hlavní tvrzení se nazývají *Věty*. Pomocná tvrzení, jejichž důkazy jsou obvykle technické, nazýváme *Lemmata*. Pokud nějaké tvrzení bezprostředně plyne z nějaké věty, je označováno jako *Důsledek*. Tvrzení, jejichž důkazy jsou velmi jednoduché, se nazývají *Pozorování*. U pozorování se většinou ani důkaz neuvádí.

Jak už jsme zmínili na začátku, ukolem matematiky je objevovat platná tvrzení v dané matematické teorii. To znamená, že matematický text se převážně skládá, z těchto tvrzení (tj. vět, lemmat, důsledků, pozorování) a jejich důkazů. Nicméně v matematické textu se objevuje ještě jeden důležitý prvek a to je *Definice*. V každé teorii máme nějaké základní pojmy (např. bod v geometrii nebo číslo v aritmetice), jejichž struktura nás už nezajímá, tzn. nezajímá nás například, co to je číslo, ale jaké vzájemné vztahy mezi sebou čísla splňují. Nicméně není možné s těmito základními pojmy vystačit, protože naše tvrzení by pak byli velmi dlouhá. Proto pomocí definic zavádíme pojmy nové. Ukažme si příklady.

Definice 1 *Celé číslo x nazýváme* kladné*, pokud platí $x > 0$.*

Definice 2 *Celé číslo x nazýváme* liché*, pokud lze vyjádřit jako dvojnásobek nějakého celého čísla n plus 1, tj. $x = 2n + 1$.*

V první definici jsme zavedli pojem kladného celého čísla a v druhé lichého. Po zavedení nových pojmů je možné tyto pojmy používat v dalším textu, v podstatě jako zkratky. Např. můžeme zformulovat tvrzení "pro všechna lichá celá čísla platí ...". To je samozřejmě úspornější než kdybychom psali "pro všechna celá čísla, která lze lze vyjádřit jako dvojnásobek nějakého celého čísla n plus 1, platí ...".

1.3 Teorie množin

Základní matematickou teorií, ve které pracuje dnes většina matematiků, je teorie množin. Základní pojem této teorie je pojem *množina*. Množina má představovat jakýsi soubor prvků. Pokud chceme mluvit o nějaké konkrétní množině, je potřeba ji nějak zapsat. To lze udělat několika způsoby. Konečné množiny lze zapsat výčtem, např. $\{1, 5, 3, 100\}$. I nekonečné množiny můžeme někdy zapsat výčtem, např. množina všech lichých kladných čísel lze vyjádřit jako $\{1, 3, 5, 7, 9, \ldots\}$, s tím, že čtenář z prvních několika prvků pochopí o jakou množinu jde. Pro některé důležité množiny máme obvykle vyhrazeny speciální symboly. Množinu přirozených čísel budeme značit $\mathbb{N}$, množinu celých čísel $\mathbb{Z}$, množinu racionálních čísel $\mathbb{Q}$, množinu reálných čísel $\mathbb{R}$ a množinu komplexních čísel $\mathbb{C}$. Další speciální symbol máme pro množinu, která neobsahuje žádné prvky (tzv. prázdná množina). Značí se obvykle $\emptyset$ nebo $\{\}$. Fakt, že nějaký prvek x náleží do množiny M, budeme značit $x \in M$. Opačné tvrzení budeme značit $x \notin M$. Tak např. $\sqrt{2} \in \mathbb{R}$ a $\sqrt{2} \notin \mathbb{Q}$.

Jiný způsob, jak zapsat množinu, je pomocí nějakého tvrzení $A(x)$, které platí pro ty prvky x, které do množiny mají patřit, a pro ostatní neplatí. Množinu pak zapíšeme $\{x \mid A(x)\}$ a čteme jako "množina všech x, která splňují $A(x)$". Např. $\{x \mid x \in \mathbb{R} \text{ a } x^2 - 2x + 1 \geq 0\}$ je množina všech reálných čísel x, která splňují nerovnici $x^2 - 2x + 1 \geq 0$. Někdy zkráceně píšeme nalevo od symbolu $\mid$ odkud se prvky x berou. Např. $\{x \in \mathbb{R} \mid x^2 + 1 = 0\}$ je množina všech reálných čísel x, které splňují rovnici $x^2 + 1 = 0$. Asi pro vás nebude překvapení, že tato množina je prázdná, protože žádné reálné číslo splňující rovnici $x^2 + 1 = 0$ neexistuje. Naopak množina $\{x \in \mathbb{C} \mid x^2 + 1 = 0\}$ není prázdná a obsahuje dvě komplexní čísla i a $-i$.

Jeden z axiomů teorie množin je tzv. axiom extensionality. Ten říká, že dvě množiny se rovnají právě tehdy, když mají stejné prvky. To znamená, že když chceme ukázat, že dvě množiny X,Y se rovnají, musíme pro libovolný prvek x ukázat, že když patří do množiny X, pak patří i do množiny Y a pokud patří do Y, pak patří také do X. Symbolicky zapsáno musíme ukázat platnost tohoto tvrzení:

$$(x \in X \;\Rightarrow\; x \in Y) \;\wedge\; (x \in Y \;\Rightarrow\; x \in X)\,.$$

To je možno přepsat pomocí ekvivalence takto: prvek x patří do množiny X právě tehdy, když patří do Y. Symbolicky:

$$x \in X \;\Leftrightarrow\; x \in Y\,.$$

Z axiomu extensionality plynou některá základní pozorování o množinách. Např. nezáleží na pořadí v jakém prvky ve výčtu uvádíme, tj. $\{1,3\} = \{3,1\}$. Nebo nemá smysl uvažovat, že by nějaká množina obsahovala nějaký prvek vícekrát, protože $\{7,7\} = \{7\}$.

Kromě rovnosti mezi množinami používá matematika ještě pojem inkluze. Chceme-li nějak vyjádřit, že všechny prvky množiny X patří i do množiny Y, zapisujeme tuto skutečnost $X \subseteq Y$ a čteme X je podmnožinou Y. Pokud tedy chceme pro nějaké dvě množiny X, Y, dokázat, že $X \subseteq Y$ platí, musíme ukázat, že pro libovoné $x \in X$, platí i $x \in Y$, tj. ukázat platnost implikace $x \in X \;\Rightarrow\; x \in Y$. Pomocí inkluze $\subseteq$ můžeme vyjádřit rovnost dvou množin takto: $X = Y$ právě tehdy, když $X \subseteq Y$ a zároveň $Y \subseteq X$.

S množinami můžeme také dělat různé operace. Základní operace jsou průnik a sjednocení. Mějme dvě množiny X a Y. Průnik X a Y značíme $X \cap Y$ a sjednocení X a Y značíme $X \cup Y$. Množiny $X \cap Y$ a $X \cup Y$ jsou potom definovány následovně:

$$\begin{aligned} X \cap Y &= \{x \mid x \in X \wedge x \in Y\}\,, \\ X \cup Y &= \{x \mid x \in X \vee x \in Y\}\,. \end{aligned}$$

Průnik $X \cap Y$ tedy obsahuje prvky, které patří do obou množin zároveň a sjednocení $X \cup Y$ obsahuje prvky, které patří alespoň do jedné z množin. Např. $\{0,1,3,\pi\} \cap \{0,\pi,4\} = \{0,\pi\}$ a $\{0,1,3,\pi\} \cup \{0,\pi,4\} = \{0,1,3,\pi,4\}$.

Poslední operací s množinami, o které se zmíníme, je operace kartézského součinu. Máme-li nějaké dva prvky x a y, symbolem (x,y) budeme značit tzv. uspořádanou dvojici. Slovem uspořádanou dáváme najevo, že na pořadí prvků v (x,y) záleží. Např. $(3,5) \neq (5,3)$. Kartézský součin dvou množin X a Y (značíme $X \times Y$) je potom množina:

$$X \times Y = \{(x,y) \mid x \in X \;\wedge\; y \in Y\}\,.$$

Kartézský součin $X \times Y$ je tedy množina všech uspořádaných dvojic (x,y), jejichž první složka je z množiny X a druhá z množiny Y. Pokud $X = Y$, píšeme místo $X \times X$ jen X^2.

Opakovaným použitím kartézského součinu můžeme vyrábět množiny uspořádaných n-tic. Např. $X \times X \times X \times X = \{(x_1,x_2,x_3,x_4) \mid x_1,x_2,x_3,x_4 \in X\}$ je množina všech uspořádaných čtveřic prvků z X. Tuto množinu značíme zkráceně X^4. Podobně X^n značí množinu uspořádaných n-tic prvků z X, kde $n \in \mathbb{N}$.

1.4 Zobrazení

Nyní přistoupíme k jednomu z nejzásadnějších pojmů celé matematiky a tím je pojem zobrazení. Tento pojem zavedeme v následující definici:

Definice 3 *Nechť X a Y jsou množiny. Podmnožinu f kartézského součinu $X \times Y$ (tj. $f \subseteq X \times Y$) nazveme* zobrazení z množiny X do množiny Y*, pokud ke každému $x \in X$ existuje právě jedna uspořádaná dvojice $(x,y) \in f$. Fakt, že f je zobrazení z množiny X do množiny Y značíme $f : X \to Y$. Množinu X nazýváme* definiční obor *a množinu Y* obor hodnot*. Zobrazení se také někdy říká* funkce*.*

Všimněte si, že pro různé prvky $y \neq y'$ z množiny Y nemůže nastat případ, kdy $(x,y) \in f$ a zároveň $(x,y') \in f$. Pokud tedy pro nějaké pevné $x \in X$ platí $(x,y) \in f$, je prvek y už jednoznačně určen, a můžeme si ho pojmenovat *hodnota f v bodě x* a označit symbolem $f(x)$. To znamená, že dvojice $(x,f(x))$ jsou právě ty dvojice, které patří do f. Jinými slovy množinu uspořádaných dvojic f můžeme vyjádřit také takto: $\{(x,f(x)) \in X \times Y \mid x \in X\}$. Příklady zobrazení mohou např. být:

$$g = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$$

nebo

$$h = \{(x, y) \in \mathbb{N} \times \mathbb{R} \mid y = \sqrt{x}\}\,.$$

Zobrazení g je zobrazení z množiny reálných čísel do množiny reálných čísel a zobrazení h je zobrazení z množiny přirozených čísel do množiny reálných čísel.

Pokud chceme nějaké zobrazení definovat musíme vlastně definovat jakousi množinu uspořádaných dvojic. Nicméně, protože každé zobrazení f má tu vlastnost, že ke každému prvku x definičního oboru existuje právě jedna hodnota y z oboru hodnot, taková, že (x, y) patří do f, nedefinujeme obvykle zobrazení jako množinu uspořádaných dvojic, ale jen předpisem, který každému prvku z definičního oboru přiřadí jeden prvek z oboru hodnot. Takže výše uvedené příklady zobrazení bychom tedy běžně definovali takto: $g : \mathbb{R} \to \mathbb{R}$ takové, že $g(x) = x^2$ a $h : \mathbb{N} \to \mathbb{R}$ takové, že $h(x) = \sqrt{x}$. Výrazy $g : \mathbb{R} \to \mathbb{R}$, $h : \mathbb{N} \to \mathbb{R}$ nám totiž přesně specifikují definiční obory a obory hodnot, a výrazy $g(x) = x^2$, $h(x) = \sqrt{x}$ zase přesně definují, které uspořádané dvojice do zobrazení patří.

S naší definicí zobrazení jako množiny můžeme lehce zodpovědět otázku, kdy se dvě zobrazení $f : X \to Y$, $g : X \to Y$ rovnají.

Věta 1 *Nechť $f : X \to Y$, $g : X \to Y$ jsou zobrazení. Pokud pro všechny $x \in X$ platí $f(x) = g(x)$, pak $f = g$.*

Důkaz: Chceme dokázat, že pokud pro všechny $x \in X$ platí $f(x) = g(x)$, pak f a g se rovnají. Protože f a g jsou množiny, stačí ukázat, že mají stejné prvky (viz axiom extensionality). Připomeňme, že každý prvek f lze vyjádřit, jako uspořádanou dvojici $(x, f(x)) \in X \times Y$. Vezmeme tedy libovolný prvek $(x, f(x))$ z f a ukážeme, že patří také do g. Z předpokladu $f(x) = g(x)$, dostaneme $(x, f(x)) = (x, g(x))$, protože dvě uspořádané dvojice se rovnají, když mají stejné odpovídající složky. Ale dvojice $(x, g(x))$ patří do g. Takže jsme ukázali, že $f \subseteq g$. Inkluzi $g \subseteq f$ lze dokázat obdobně. □

Pokud máme na oboru hodnot definovány nějaké operace (např. sčítání nebo násobení), můžeme tyto operace přenést i na zobrazení. Nechť $f : X \to \mathbb{R}$ a $g : X \to \mathbb{R}$ jsou zobrazení z množiny X do množiny reálných čísel. Reálná čísla jak známo umíme sčítat a násobit. Nyní budeme definovat pomocí sčítání a násobení reálných čísel nová zobrazení $f + g$ a fg představující součet a součin zobrazení f a g.

Definice 4 *Nechť $f : X \to \mathbb{R}$, $g : X \to \mathbb{R}$ jsou zobrazení a c je reálné číslo. Definujeme zobrazení $f + g : X \to \mathbb{R}$, $fg : X \to \mathbb{R}$ a $cf : X \to \mathbb{R}$ takto:*

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x) \\ (cf)(x) &= cf(x) \end{aligned}$$

Zobrazení $f + g$ tedy přiřazuje prvku x z množiny X součet reálných čísel $f(x)$ a $g(x)$. Zobrazení fg přiřazuje prvku x jejich součin. A zobrazení cf přiřazuje prvku x součin reálných čísel c a $f(x)$.

Protože sčítání a násobení reálných čísel splňuje různé vlastnosti (např. $a + b = b + a$ pro všechna $a, b \in \mathbb{R}$), zajímá nás, které z těchto vlastností se přenesou i na operace se zobrazeními. Konstantní zobrazení z množiny X do množiny reálných čísel $\mathbb{R}$, které každému $x \in X$ přiřadí 0, budeme značit $\bar{0}$, tj. $\bar{0} = \{(x, 0) \in X \times \mathbb{R} \mid x \in X\}$. Zřejmě $\bar{0} = cf$ pro libovolné zobrazení f a $c = 0$. Zobrazení cf pro $c = -1$ budeme značit $-f$.

Věta 2 *Nechť $f : X \to \mathbb{R}$, $g : X \to \mathbb{R}$ a $h : X \to \mathbb{R}$ jsou zobrazení. Potom platí následující tvrzení:*

1. *Sčítání zobrazení je komutativní: $f + g = g + f$.*
2. *Sčítání zobrazení je asociativní: $f + (g + h) = (f + g) + h$.*

3. *Zobrazení* $\bar{0}$ *je neutrální prvek:* $f + \bar{0} = f$.

4. $(f + (-g))(x) = f(x) - g(x)$ *pro všechna* $x \in X$.

Důkaz: U prvních třech tvrzení dokazované věty máme ukázat rovnost dvou zobrazení. Podle Věty 1 stačí ověřit, že pro libovolný prvek x z množiny X se hodnoty obou zobrazení v bodě x rovnají. Poslední tvrzení ukazuje, že zobrazení $f + (-g)$ funguje jako rozdíl dvou zobrazení.

1. $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$, druhá rovnost plyne z komutativity sčítání reálných čísel (tj. $a + b = b + a$ pro všechna $a, b \in \mathbb{R}$).

2. $(f + (g + h))(x) = f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) = ((f + g) + h)(x)$, druhá rovnost plyne z asociativity sčítání reálných čísel (tj. $a + (b + c) = (a + b) + c$ pro všechna $a, b, c \in \mathbb{R}$).

3. $(f + \bar{0})(x) = f(x) + 0 = f(x)$, druhá rovnost plyne z faktu, že $a + 0 = a$ pro všechna $a \in \mathbb{R}$.

4. $(f + (-g))(x) = f(x) + (-g)(x) = f(x) + (-1)g(x) = f(x) - g(x)$.

□

Zobrazení $f + (-g)$ budeme značit $f - g$. Díky poslednímu bodu předchozí věty, je toto značení rozumné, protože zobrazení $f - g$ se skutečně chová, jako kdybychom ho definovali přenesením operace rozdílu z reálných čísel na zobrazení podobně, jako jsme to udělali se sčítáním a násobením.

Podobné vlastnosti má i násobení, jak vypovídá následující věta. Konstantní zobrazení z množiny X do množiny reálných čísel $\mathbb{R}$, které každému $x \in X$ přiřadí 1, budeme značit $\bar{1}$, tj. $\bar{1} = \{(x, 1) \in X \times \mathbb{R} \mid x \in X\}$.

Věta 3 *Nechť* $f : X \to \mathbb{R}$, $g : X \to \mathbb{R}$ *a* $h : X \to \mathbb{R}$ *jsou zobrazení. Potom platí následující tvrzení:*

1. *Násobení zobrazení je komutativní:* $fg = gf$.

2. *Násobení zobrazení je asociativní:* $f(gh) = (fg)h$.

3. *Zobrazení* $\bar{1}$ *je neutrální prvek:* $f\,\bar{1} = f$.

4. *Násobení zobrazení je distributivní vzhledem ke sčítání:* $f(g + h) = fg + fh$.

Důkaz: U všech tvrzení dokazované věty máme ukázat rovnost dvou zobrazení. Podle Věty 1 stačí ověřit, že pro libovolný prvek x z množiny X se hodnoty obou zobrazení v bodě x rovnají.

1. $(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$, druhá rovnost plyne z komutativity násobení reálných čísel (tj. $ab = ba$ pro všechna $a, b \in \mathbb{R}$).

2. $(f(gh))(x) = f(x)(g(x)h(x)) = (f(x)g(x))h(x) = ((fg)h)(x)$, druhá rovnost plyne z asociativity násobení reálných čísel (tj. $a(bc) = (ab)c$ pro všechna $a, b, c \in \mathbb{R}$).

3. $(f\,\bar{1})(x) = f(x)\,1 = f(x)$, druhá rovnost plyne z faktu, že $a1 = a$ pro všechna $a \in \mathbb{R}$.

4. $(f(g + h))(x) = f(x)\,(g + h)(x) = f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x) = (fg)(x) + (fh)(x) = (fg+fh)(x)$, druhá rovnost plyne z distributivity násobení reálných čísel vzhledem ke sčítání (tj. $a(b + c) = ab + ac$ pro všechna $a, b, c \in \mathbb{R}$).

□

Nakonec si ukážeme některé vlastnosti funkce cf.

Věta 4 *Nechť* $f : X \to \mathbb{R}$, $g : X \to \mathbb{R}$ *jsou zobrazení a* a, b *reálná čísla. Potom platí následující tvrzení:*

1. $a(bf) = (ab)f$.
2. $(a+b)f = af + bf$.
3. $a(f+g) = af + ag$.
4. $1f = f$.

Důkaz: Všechna tvrzení jsou v podstatě zřejmá a asi byste je dokázali dokázat sami. □

2 Polynomy

V této části se budeme zabývat speciálními zobrazeními, které se nazývají polynomy nebo někdy také mnohočleny. Začneme tedy definicí polynomu.

Definice 5 *Zobrazení $f : \mathbb{R} \to \mathbb{R}$ se nazývá reálný polynom, pokud existují reálná čísla $a_0, a_1, \ldots, a_n$ taková, že $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ pro všechna $x \in \mathbb{R}$. Čísla $a_0, a_1, \ldots, a_n$ se nazývají* koeficienty polynomu. *Fakt, že $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ stručně také zapisujeme:*

$$f(x) = \sum_{i=0}^{n} a_i x^i \,. \tag{2}$$

Podobně zobrazení $g : \mathbb{C} \to \mathbb{C}$ se nazývá komplexní polynom, pokud existují komplexní čísla $b_0, b_1, \ldots, b_n$ taková, že $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ pro všechna $x \in \mathbb{C}$.

Množinu reálných (komplexních) polynomů značíme $P_{\mathbb{R}}$ ($P_{\mathbb{C}}$).

Protože polynomy jsou zobrazení do množiny reálných čísel máme pro ně definovány operace sčítání, násobení a násobení reálným číslem (viz Definice 4)[3]. Automaticky pro ně také platí všechny vlastnosti, které jsme dokázali ve Větách 2, 3 a 4. To, co ovšem nevíme je, jestli výsledky těchto operací budou opět polynomy (jestli jsou takzvaně *uzavřené* na operace sčítání, násobení a násobení reálným číslem). Např. pokud vynásobíme dva polynomy, víme, že výsledek bude zobrazení, ale nevíme, jestli to bude polynom.

Začneme nejdříve s jednoduchým pozorováním. Konstantní zobrazení $\bar{0}$ je zřejmě polynom, protože existuje reálné číslo (koneckonců i komplexní) $a_0 = 0$ takové, že $\bar{0}(x) = a_0$ pro všechna $x \in \mathbb{R}$. Zobrazení $\bar{0}$ budeme tedy nazývat *nulový polynom.*

Pozorování 1 *Nechť f je reálný (komplexní) polynom takový, že $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Potom zřejmě pro všechna x z definičního oboru platí*

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0 = \\ &= 0x^{n+1} + a_n x^n + \cdots + a_1 x + a_0 = \\ &= 0x^{n+2} + 0x^{n+1} + a_n x^n + \cdots + a_1 x + a_0 = \cdots \end{aligned}$$

Pokud tedy bude potřeba můžeme výraz počítající hodnotu polynomu f v bodě x protáhnout o libovolnou délku tak, že přidané koeficienty položíme rovny nule. To se hodí zejména v případě, kdy chceme, aby dva různé polynomy měly stejný počet koeficientů.

Nyní již můžeme dokázat, že polynomy jsou skutečně uzavřené na výše zmíněné operace.

Věta 5 *Nechť f, g jsou reálné (komplexní) polynomy a c je reálné (komplexní) číslo. Pak zobrazení $f+g$, fg a cf jsou opět reálné (komplexní) polynomy (jinými slovy množina polynomů je uzavřená na operace sčítání, násobení a násobení reálným číslem).*

[3] Podobně lze operace zavést i pro komplexní polynomy.

Důkaz: Věta tvrdí, že zobrazení $f+g$, fg a cf jsou polynomy. Podle definice polynomu musíme tedy ukázat ve všech třech případech existenci koeficientů. Protože f a g jsou polynomy můžeme jejich hodnoty v bodě x vyjádřit takto:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i\,, \qquad g(x) = b_n x^n + \cdots + b_1 x + b_0 = \sum_{i=0}^{n} b_i x^i\,. \tag{3}$$

Podle Pozorování 1 jsme si mohli dovolit vyjádřit hodnoty polynomů f i g v bodě x se stejným počtem koeficientů.

Nyní dokážeme postupně, že $f+g$, fg a cf jsou polynomy. Začneme zobrazením $f+g$.

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i\,.$$

Okomentujme předchozí rovnosti. První rovnost je akorát definice sčítání dvou zobrazení (viz Definice 4). Druhá rovnost je dosazení za $f(x)$ a $g(x)$ podle rovnice (3). Poslední rovnost plyne z vlastností reálných (komplexních) čísel. Vidíme tedy, že hodnotu zobrazení $f+g$ v bodě x jsme schopni vyjádřit v takovém tvaru, v jakém ho udává rovnice (2). Zobrazení $f+g$ je tedy polynom a reálná (komplexní) čísla $a_0+b_0, a_1+b_1, \ldots, a_n+b_n$ jsou jeho koeficienty.

Podobně ukážeme že zobrazení cf je polynom.

$$(cf)(x) = cf(x) = c\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (ca_i) x^i\,.$$

Koeficienty polynomu cf tedy jsou čísla $ca_0, ca_1, \ldots, ca_n$.

Nakonec ukážeme, že i zobrazení fg je polynom.

$$(fg)(x) = f(x)g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{2n} c_i x^i\,, \tag{4}$$

kde pro $k = 0, 1, 2, \ldots, 2n$ je

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i}\,.$$

Výraz na pravé straně rovnice (4) jsme dostali roznásobením závorek a sdružením členů se stejnou mocninou u x k sobě. Tzn. roznásobením tohoto výrazu $(a_n x^n + \cdots + a_1 x + a_0)(b_n x^n + \cdots + b_1 x + b_0)$. □

Jednou ze základních charakteristik polynomu je jeho stupeň. Napišme si jeho definici.

Definice 6 *Nechť f je reálný nebo komplexní polynom takový, že $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ pro všechna x z definičního oboru. Stupeň polynomu f (označujme* st f*) je největší $m \in \mathbb{N}$ takové, že $a_m \neq 0$. Stupeň nulového polynomu $\bar{0}$ definujeme z technických důvodů -1. Polynom stupně 0 budeme nazývat* konstantní.

Věta 6 *Nechť f, g jsou polynomy t.ž. $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. Pak $f = g$ p.t.k.* st $f =$ st g *a $a_i = b_i$ pro všechna $i \in \{0, \ldots,$ st $f\}$.*

Důkaz: Sporem: pokud $m \neq n$, pak prodloužíme f a g na stejný počet koeficientů. Máme

$$\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} b_i x^i$$

$$\sum_{i=0}^{n}(a_i - b_i)x^i = 0$$

Existuje polynom h t.ž. $h(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$ pro všechna $x \in \mathbb{R}(\mathbb{C})$. □

Věta 7 *Nechť f a g jsou polynomy. Pak platí:*

1. $\operatorname{st} f \pm g \leq \max\{\operatorname{st} f, \operatorname{st} g\}$.
2. $\operatorname{st} cf = \operatorname{st} f$ *pro* $c \neq 0$.
3. $\operatorname{st} fg = \operatorname{st} f + \operatorname{st} g$ *pokud* $f, g \neq \bar{0}$.

Věta 8 *Nechť f, g jsou polynomy a $g \neq \bar{0}$. Pak $\exists$ jednoznačně určené polynomy p a z t.ž. $f = gp + z$ a $\operatorname{st} z < \operatorname{st} g$.*

Důkaz: □
Existence plyne z algoritmu dělení polynomů. Jednoznačnost dokážeme sporem. Přepokladáme, že existují polynomy p_1, p_2, z_1, z_2 t.ž. $p_1 \neq p_2$ nebo $z_1 \neq z_2$ a

$$f = gp_1 + z_1\,,\ f = gp_2 + z_2\,,\ \operatorname{st} z_1 < \operatorname{st} g\,,\ \operatorname{st} z_2 < \operatorname{st} g\,.$$

$$gp_1 + z_1 = gp_2 + z_2$$
$$g(p_1 - p_2) = z_2 - z_1$$

Protože $p_1 - p_2 \neq \bar{0}$ a $g \neq \bar{0}$ máme:

$$\operatorname{st} g(p_1 - p_2) = \operatorname{st} g + \operatorname{st}(p_1 - p_2) = \operatorname{st}(z_2 - z_1) \leq \max\{\operatorname{st} z_2, \operatorname{st} z_1\} < \operatorname{st} g$$

Jedině když $\operatorname{st}(p_2 - p_1) = -1$, tj. $p_1 = p_2$. A tudíž

$$z_2 - z_1 = g(p_1 - p_2) = g\bar{0} = \bar{0}$$

□

Definice 7 *Nechť f, g jsou polynomy. Říkáme, že f je dělitelný g (g dělí f), pokud $z = \bar{0}$.*

Příklad na dělení.

$$(2x^5 - x^4 + 4x^3 + 3x^2 - x + 1) : (x^3 + x^2 - x + 1)$$

3 Hornerovo schema

$$\begin{aligned} f(x) &= a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ &= (a_4x + a_3)x^3 + a_2x^2 + a_1x + a_0 \\ &= ((a_4x + a_3)x + a_2)x^2 + a_1x + a_0 \\ &= (((a_4x + a_3)x + a_2)x + a_1)x + a_0 \end{aligned}$$

$$f(x_0) = (((a_4x_0 + a_3)x_0 + a_2)x_0 + a_1)x_0 + a_0$$

$$\begin{aligned} b_4 &= a_4 \\ b_3 &= b_4x_0 + a_3 \\ b_2 &= b_3x_0 + a_2 \\ b_1 &= b_2x_0 + a_1 \\ b_0 &= b_1x_0 + a_0 \end{aligned}$$

Pak

$$f(x_0) = b_0\,, \quad f(x) = (x - x_0)(b_4x^3 + b_3x^2 + b_2x + b_1) + b_0\,.$$

	a_4	a_3	a_2	a_1	a_0
x_0		b_4x_0	b_3x_0	b_2x_0	b_1x_0
	b_4	b_3	b_2	b_1	b_0

Příklad:

$$2x^4 - 3x^3 + 5x^2 - x + 6\,, \qquad x_0 = -2$$

4 Kořeny

Definice 8 *Nechť f je nenulový polynom. Reálné (komplexní) číslo c nazveme kořenem f, pokud $f(c) = 0$.*

Věta 9 *Komplexní číslo c je kořenem polynomu f p.t.k. f je dělitelný polynomem $x - c$.*

Důkaz:

($\Rightarrow$) Nechť $f(c) = 0$. $f = (x - c)p + z$ a $\operatorname{st} z < \operatorname{st}(x - c) = 1$. Takže $\operatorname{st} z = 0$ nebo $\operatorname{st} z = -1$. Polynom z je tedy konstatní, tj. $z(x) = b$ pro nějaké $b \in \mathbb{R}$. Máme tedy:

$$f(x) = (x - c)p(x) + b$$

Protože c je kořen, dostaneme:

$$0 = f(c) = (c - c)p(c) + b = 0p(c) + b = b$$

($\Leftarrow$) Nechť $f(x) = (x - c)p(x)$. Pak $f(c) = (c - c)p(c) = 0$. Takže c je kořen.

□

Definice 9 *Nechť f je polynom. Reálné (komplexní) číslo c nazveme k-násobným kořenem f, pokud k je největší přirozené číslo t.ž. $(x - c)^k$ dělí f. Číslo k se nazývá násobnost.*

Věta 10 (Základní věta algebry) *Každý $f \in P_{\mathbb{C}}$ t.ž. $\operatorname{st} f \geq 1$ má alespoň jeden kořen.*

Důsledek 1 *Nechť $f \in P_{\mathbb{C}}$ t.ž. $\operatorname{st} f = n \geq 1$ a $f(x) = \sum_{i=0}^{n} a_i x^i$. Pak*

$$f(x) = a_n(x - c_1)^{k_1}(x - c_2)^{k_2} \cdots (x - c_m)^{k_m}\,,$$

kde $c_1, \ldots, c_m \in \mathbb{C}$ jsou všechny kořeny f a $k_1, \ldots, k_m, m \in \mathbb{N}$ takové, že $n = k_1 + k_2 + \cdots + k_m$.

Důkaz: Inkukcí podle stupně.

1. Pro $n = 1$ platí, protože $a_1x + a_0 = a_1(x + \frac{a_0}{a_1})$.

2. Nechť $\operatorname{st} f = n$. Podle ZVA má f kořen, tj. $f = (x-c)^k p$. Zřejmě

$$n = \operatorname{st} f = \operatorname{st}(x-c)^k + \operatorname{st} p = k + \operatorname{st} p$$

$$\operatorname{st} p = n - k$$

Z indukčního předpokladu:

$$p = b(x-c_1)^{k_1}\cdots(x-c_m)^{k_m}\,, \qquad n-k = k_1+\cdots+k_m\,.$$

Dosazením:

$$f = (x-c)^k p = b(x-c)^k(x-c_1)^{k_1}\cdots(x-c_m)^{k_m}$$

Zřejmě $b = a_n$.

□

Věta 11 *Nechť $f \in P_{\mathbb{C}}$ s reálnými koeficienty a $c = a+bi$ je jeho k-násobný kořen. Pak $\overline{c} = a-bi$ je také k-násobný kořen f.*

Důkaz: Nechť $f(x) = a_n x^n + \cdots + a_0$. Pak

$$\overline{f(x)} = \overline{a_n x^n + \cdots + a_0} = \overline{a_n}(\overline{x})^n + \cdots + \overline{a_0} = a_n(\overline{x})^n + \cdots + a_0 = f(\overline{x})\,.$$

Protože $\overline{f(x)} = f(\overline{x})$ a $\overline{\overline{x}} = x$, máme $f(x) = \overline{f(\overline{x})}$.

$$\begin{aligned} f(x) &= \overline{f(\overline{x})} = \overline{(\overline{x}-c)^k(b_n(\overline{x})^n + \cdots + b_0)} \\ &= (\overline{\overline{x}}-\overline{c})^k(\overline{b}_n(\overline{\overline{x}})^n + \cdots + \overline{b}_0) \\ &= (x-\overline{c})^k(\overline{b}_n x^n + \cdots + \overline{b}_0) \end{aligned}$$

□

Důsledek 2 *Nechť $f \in P_{\mathbb{R}}$ a $\operatorname{st} f$ je lichý. Pak f má alespoň jeden reálný kořen.*

Věta 12 *Nechť $f \in P_{\mathbb{R}}$. Pak*

$$f(x) = a_n(x-c_1)^{k_1}\cdots(x-c_m)^{k_m}(x^2+b_1x+d_1)^{l_1}\cdots(x^2+b_rx+d_r)^{l_r}\,.$$

Důkaz:

$$f(x) = a_n(x-c_1)^{k_1}\cdots(x-c_m)^{k_m}$$

Když se $(x-c_i)^{k_i}$ vyskytuje v rci nahoře, pak se $(x-\overline{c_i})^{k_i}$ vyskytuje také. Můžeme je roznásobit:

$$(x-c_i)^{k_i}(x-\overline{c_i})^{k_i} = (x^2-(c_i+\overline{c_i})x + c_i\overline{c_i})^{k_i} = (x^2 - 2\mathrm{Re}(c_i)x + |c_i|^2)^{k_i}$$

□

Definice 10 *Nechť $f \in P_{\mathbb{R}}$. Řekneme, že f je ireducibilní nad tělesem $\mathbb{R}$, pokud neexistují $g, h \in P_{\mathbb{R}}$ t.ž. $f = gh$ a $\operatorname{st} g, \operatorname{st} h \geq 1$.*

Důsledek 3 *Nekonstatní polynom $f \in P_{\mathbb{R}}$ je ireducibilní p.t.k. $\operatorname{st} f = 1$ nebo $\operatorname{st} f = 2$ a f má pouze komplexní kořeny.*

Věta 13 *Nechť $f(x) = a_n x^n + \cdots + a_0$ je polynom stupně n a $a_i \in \mathbb{Z}$. Pokud $f(\frac{p}{q}) = 0$, kde $\frac{p}{q} \in \mathbb{Q}$ a p, q jsou nesoudělná, pak p dělí a_0 a q dělí a_n.*

Důkaz: Dosadíme $\frac{p}{q}$ do $f(x)$:

$$0 = f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0$$

Vynásobíme q^n:

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$$

Tudíž:

$$a_n p^n = -q(a_{n-1}p^{n-1} + \cdots + a_1 pq^{n-2} + a_0 q^{n-1})$$
$$a_0 q^n = -p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1})$$

Takže q dělí $a_n p^n$ a protože p, q jsou nesoudělná, dělí i a_n. Podobně p dělí a_0. □

Příklad:

$$3x^4 - 2x^3 + x^2 - 2x + 6$$
$$p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}, \qquad q \in \{\pm 1, \pm 3\}$$
$$\frac{p}{q} \in \{\pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{3}, \pm\frac{2}{3}\}$$