# Maturita Formalita

**aneb Jak zvládnout matematiku na jedničku?**

**15. března 2025**

Stížnosti a návrhy na vylepšení můžete zasílat na můj email:

**jonas.vybiral.jv@gmail.com**.

# Obsah

# Úvod

*Sine mathematica vita nulla est (Bez matematiky život nestojí za nic).*

autor neznámý

Tento text má být snaha o trochu pokročilejší nahled na elementární matematiku potřebnou k maturitě. Měl by být vhodný jak pro studenty, kteří se chtějí připravit na maturitu, tak pro ty, kteří chtějí získat hlubší porozumění matematice. Než se pustíme do vysvětlení jak tato kniha funguje, chci Vás odkázat opět na můj email, kam můžete zasílat veškeré dotazy, nejasnosti a připomínky:

**jonas.vybiral.jv@gmail.com**.

Bežné matematické knihy jsou psané ve formátu definice-věta-důkaz (co tyto věci znamenají se dozvíte brzy). Toto však v tomto textu naleznete pouze v omezené míře. Místo toho se budeme snažit vysvětlit matematické pojmy a věty tak, aby byly srozumitelné pro každého. Pokusím se avšak přidat nějaký nahled na to, jak by to mohlo vypadat, kdybychom se snažili být formální.

Formát knihy bude většinou následující: nejdříve se seznámíme s nějakým pojmem což bude většinou vyznačeno následujícím rámečkem:

> Důležitý pojem nebo pravidlo. Rámečkům věnujte extra pozornost.

Poté čtenáři představíme nějaký příklad, který by měl ilustrovat, jak daný pojem funguje. Příklady budou vyznačeny následovně:

**Příklad 0.0.1** Příklad na procvičení daného pojmu. Tento příklad bude i řešený.

**Cvičení 0.0.2** Cvičení na procvičení daného pojmu.

**Nápověda 0.0.2** Pokud bude cvičení náročnější budeme se snažit vždy poskytnout nápovědu aby čtenáři mohla být cesta k řešení usnadněna.

**Řešení 0.0.2** Řešení cvičení. Občas bude vynecháno, aby si čtenář mohl cvičení zkusit sám. Vynechávat řešení budeme většinou jen u problémů, které už byly dostatečně procvičeny.

# Kapitola 1

# Matematická logika a důkazy

*Only prove something that already seems to be obvious.*

Grant Sanderson

V této kapitole se seznámíme s některými základními pojmy a pravidly, které nám pomohou v matematickém uvažování. Základními bloky jsou pojem výrok a práce s nimi. Po zavedení těchto pojmů se seznámíme s důkazy, díky kterým můžeme ověřit správnost tvrzení.

## 1.1 Výroková logika

Zde se budeme pouze věnovat základní výrokové logice a na konci si lehce zmíníme něco o predikátové logice. Výroková logika je základním nástrojem matematiky, který nám umožňuje formulovat veškeré matematické tvrzení.

Výrok je tvrzení u kterého lze rozhodnout, zda je pravdivé nebo nepravdivé. Výroky budeme značit písmeny $p, q, r, \dots$. Pravdivost výroku budeme značit 1 a nepravdivost 0. Těmto číslům se říká pravdivostní hodnoty.

**Příklad 1.1.1** Uvedeme si zde několik příkladů výroků:

- $p$: Venku prší.
- $q$: $2 + 2 = 69$.
- $r$: Praha je hlavní město České republiky.
- $s$: 4 je prvočíslo.
- $t$: $x^2 + 1 = 0$ má reálná řešení.

**Cvičení 1.1.2** Koukněte se na příklad 1.1.1 a rozhodněte, zda jsou jednotlivé výroky pravdivé nebo nepravdivé.

**Řešení 1.1.2**

- $p$: Venku prší. — Špatně zapsaný výrok. Není určeno, kde se nacházíme.
- $q$: $2 + 2 = 69$. — Nepravda. 0.
- $r$: Praha je hlavní město České republiky. — Pravda. 1.
- $s$: 4 je prvočíslo. — Nepravda. 0.
- $t$: $x^2 + 1 = 0$ má reálná řešení. — Nepravda. 0.

**Příklad 1.1.3** Důležité je také uvést si, co výrok není.

- Jak se máš?
- Bum!
- Pozor na psa!
- Černá je nejlepší barva. (Toto je názor, nikoliv výrok. Redakce si však myslí, že to je pravda.)

Ještě než se vrhneme na logické spojky, představíme si co to znamená negace výroku.

**Negace** nebo-li NOT výroku $p$ je výrok, který tvrdí opak výroku $p$. Negaci výroku $p$ budeme značit $\neg p$.

**Příklad 1.1.4** Vezměme si výrok $p$: Voda v moři je slaná. Negací tohoto výroku je výrok $\neg p$: Voda v moři není slaná.

Upozorňujeme, že v příkladu 1.1.4 opravdu měníme jen slovo 'je' na 'není'. Nepoužíváme například 'Voda v moři je sladká'. Důvodem pro to je, že ne všechno je dichotomie pravda/nepravda. Některé výroky mohou být pravdivé, nepravdivé nebo něco mezi tím. Vezměme například výrok *Kámen je zelený*. Negace je *Kámen není zelený*. Ale nevíme, zda je kámen modrý, červený nebo třeba duhový.

**Cvičení 1.1.5** Opět se vraťte k příkladu 1.1.1 a určete negace jednotlivých výroků.

**Řešení 1.1.5**

- $\neg p$: Venku neprší.
- $\neg q$: $2 + 2 \neq 69$.
- $\neg r$: Praha není hlavní město České republiky.
- $\neg s$: 4 není prvočíslo.
- $\neg t$: $x^2 + 1 = 0$ nemá reálná řešení.

Výroky samotné jsou sice fajn ale co s nimi dělat? K tomu nám poslouží logické spojky. Je to způsob jakým můžeme spojovat výroky do složitějších celků. Proč? Dozvíte se za chvíli.

Rozlišujeme 4 základní logické spojky:
**Konjunkce ($\wedge$):** Konjunkce nebo-li AND výroků $p$ a $q$ je výrok, který je pravdivý právě tehdy, když jsou pravdivé oba výroky $p$ a $q$.
**Disjunkce ($\vee$):** Disjunkce nebo-li OR výroků $p$ a $q$ je výrok, který je pravdivý právě tehdy, když je pravdivý alespoň jeden z výroků $p$ a $q$.
**Implikace ($\Rightarrow$):** Implikace nebo-li IF-THEN výroků $p$ a $q$ je výrok, který je nepravdivý právě tehdy, když je výrok $p$ pravdivý a $q$ nepravdivý. V tomto případě lze nad tím přemýšlet jako nad slibem. Když mi někdo něco slíbí, tak to musí splnit, ale pokud to neslíbí, tak je jedno co udělá.
**Ekvivalence ($\Leftrightarrow$):** Ekvivalence nebo-li IF-AND-ONLY-IF výroků $p$ a $q$ je výrok, který je pravdivý právě tehdy, když jsou oba výroky $p$ a $q$ pravdivé nebo oba nepravdivé.

Pro větší přehlednost si můžete vytvořit tabulku pravdivostních hodnot pro jednotlivé logické spojky.

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $p \Rightarrow q$ | $p \Leftrightarrow q$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |

**Příklad 1.1.6** Uveďme si několik příkladů na logické spojky:

- Konjunkce: $p \wedge q$: Venku prší a je teplo.
- Disjunkce: $p \vee q$: Venku prší nebo je teplo.
- Implikace: $p \Rightarrow q$: Když prší, tak je mokro.
- Ekvivalence: $p \Leftrightarrow q$: Venku prší právě tehdy, když je mokro.

**Cvičení 1.1.7** Vraťte se k příkladu 1.1.1 a zkuste si spojit výroky pomocí logických spojek.

## 1.2 Odbočka — Predikátová logika

Predikátová logika staví na výrokové logice a rozšiřuje ji o kvantifikátory. Pracuje se zde také s množinami výroků. Ty nám umožňují mluvit o všech prvcích nějaké množiny. Základními kvantifikátory jsou:

- Univerzální kvantifikátor $\forall$: Výrok $\forall x \in M : P(x)$ znamená, že výrok $P(x)$ platí pro všechny prvky množiny $M$.
- Existenciální kvantifikátor $\exists$: Výrok $\exists x \in M : P(x)$ znamená, že existuje prvek množiny $M$, pro který platí výrok $P(x)$.

Toto se nám bude hodit při důkazech, kde budeme chtít mluvit o všech prvcích nějaké množiny (co je množina se také dozvíte). Negace a spojování kvantifikátorů také funguje, ale je to lehce složitější.

**Příklad 1.2.1** V predikátové logice se pracuje v takzvaném univerzu. To si vždy zvolíme. Může to být například množina všech reálných čísel, množina všech lidí, množina všech zvířat, atd. Většinou se značí písmenem $U$. Ukažme si nyní dva příklady. Pokud si za naše univerzum zvolíme množinu všech reálných čísel, můžeme napsat:

- $\forall x \in \mathbb{R} : x^2 \geq 0$. Tento výrok je pravdivý, protože druhá mocnina reálného čísla je vždy nezáporná.
- $\exists x \in \mathbb{R} : x^2 = -1$. Tento výrok je nepravdivý, protože druhá mocnina reálného čísla je vždy nezáporná.

Nyní zvolme univerzum všech lidí. Zvolme si takzvané predikáty $M(x)$ a $G(x)$, které budou respektive znamenat, že $x$ zvládnul maturitu a $x$ je génius. Nyní můžeme napsat:

- $\forall x \in \text{Lidé} : M(x) \Rightarrow G(x)$. Tento výrok říká, že každý, kdo zvládl maturitu, je génius. O pravdivosti se zde raději nebudeme bavit.
- $\exists x \in \text{Lidé} : M(x) \wedge G(x)$. Tento výrok říká, že existuje někdo, kdo zvládl maturitu a je génius.

Všimněte si, že v prvním příkladě jsme mluvili o všech reálných číslech a v druhém o všech lidech. To je důležité, protože výrok může být pravdivý v jednom univerzu a nepravdivý v jiném.

Nyní si ukážeme, jak se neguje kvantifikátor. Negace univerzálního kvantifikátoru je existenciální kvantifikátor a naopak.

$$\begin{aligned} \neg(\forall x \in M : P(x)) &\Leftrightarrow \exists x \in M : \neg P(x) \\ \neg(\exists x \in M : P(x)) &\Leftrightarrow \forall x \in M : \neg P(x) \end{aligned} \tag{1.1}$$

Je to celkem intuitivní. Pokud něco platí pro všechny, stačí nám najít jedno, kde to neplatí. Pokud neexistuje ani jedno, kde to platí, tak to neplatí pro všechny.

## 1.3 Odbočka — Přirozená dedukce

Jeden z formálních dokazovacích systémů je přirozená dedukce. Tento systém je založen na pravidlech, které nám umožňují odvodit nové výroky z již známých.[1] Většina pravidel je intuitivních a vychází z toho, jak my lidé přirozeně uvažujeme. Tato sekce je uvedena opět jako odbočka, ale doporučuji si ji projít abyste v dalších kapitolách chápali jak se dělají důkazy.

Je zde pár pravidel, ale ty si uvádět nebudeme. Koukneme se na příklady a vysvětlíme si to u nich.

Většinou našim cílem bude odvodit nějaký výrok $q$ z předpokladů $p_1, p_2, \ldots, p_n$. To značíme jako $p_1, p_2, \ldots, p_n \vdash q$. Předpoklad je výrok, který považujeme za pravdivý. Nutno ještě zmínit co znamená pomocný předpoklad. Pro větší přehlednost si kreslíme box kolem našeho ‘světa’ ve kterém se pohybujeme. Pokud si vytvoříme nový box, tak to znamená, že v něm a jen v něm platí ty předpoklady, které jsme si tam napsali. Pokud z něj odejdeme, tak už ty předpoklady neplatí. Může se to zdát zbytečné, ale většinou nám to pomůže důkaz dokončit viz příklad 1.3.2.

**Příklad 1.3.1** Ukažme si nyní, jak bychom mohli dokázat, že $p \wedge q \vdash q \wedge p$. Budeme postupovat pomocí přirozené dedukce. Začneme tedy předpokladem $p \wedge q$ a budeme chtít dokázat $q \wedge p$.

1. $p \wedge q$ (předpoklad)
2. $p$ (eliminace konjunkce z 1)
3. $q$ (eliminace konjunkce z 1)
4. $q \wedge p$ (zavedení konjunkce z 3 a 2)

Tímto jsme dokázali, že $p \wedge q \vdash q \wedge p$. Zde jsme použili pravidla eliminace konjunkce a zavedení konjunkce. Tyto pravidla vychází z toho, že pokud víme, že platí $p \wedge q$, tak víme, že platí $p$ a $q$ samostatně a naopak. U ostatních pravidel to tak jednoduché nebude.

Provedeme si nyní nějakou přípravu, která bude působit zbytečně, ale v dalších kapitolách se nám to bude hodit.

**Příklad 1.3.2** Ukažme si, jak bychom mohli dokázat, že $p \Rightarrow q \vdash \neg q \Rightarrow \neg p$. Budeme postupovat pomocí přirozené dedukce. Začneme tedy předpokladem $p \Rightarrow q$ a budeme chtít dokázat $\neg q \Rightarrow \neg p$.

1. $p \Rightarrow q$ (předpoklad)

    2. $\neg q$ (pomocný předpoklad)
    3. $\neg p$ (modus tollens z 1 a 2)

4. $\neg q \Rightarrow \neg p$ (zavedení implikace z 2 a 3)

Tímto jsme dokázali, že $p \Rightarrow q \vdash \neg q \Rightarrow \neg p$. Zde jsme použili pravidlo modus tollens. To říká, že pokud víme, že platí $p \Rightarrow q$ a $\neg q$, tak můžeme odvodit $\neg p$. To vychází přímo z definice implikace. Pokud někdo něco nesplnil, ale slib ‘vyšel’ pozitivně, tak to znamená, že to ani neslíbil. Zde je krásně vidět, jak nám pomocný předpoklad pomohl. Protože jsme viděli, že když budeme předpokládat $\neg q$, tak můžeme odvodit $\neg p$ a z toho jsme zavedli chtěnou implikaci.

Pozorného čtenáře jistě napadlo, že místo tohoto postupu si můžeme napsat pravdivostní tabulku a zjistit, že tvrzení platí. To bychom se připravili o všechnu zábavu a pro složitější tvrzení by tabulka rostla exponenciálně. Uvedeme si zde pro představu jak by vypadala tabulka pro příklad 1.3.2

| $p$ | $q$ | $p \Rightarrow q$ | $\neg q$ | $\neg p$ | $\neg q \Rightarrow \neg p$ |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 |

[1] Přirozený důsledek lze zavést i pro predikátovou logika, ale to je nad rámec tohoto textu.

**Příklad 1.3.3** Podívejme si nyní na důležitý příklad $p \Rightarrow q \dashv\vdash \neg p \vee q$.

1. $p \Rightarrow q$ (předpoklad)
2. $p \vee \neg p$ (tertium non datur)

    3. $p$ (pomocný předpoklad)
    4. $q$ (modus ponens z 1 a 3)
    5. $\neg p \vee q$ (zavedení disjunkce z 4)

    6. $\neg p$ (pomocný předpoklad)
    7. $\neg p \vee q$ (zavedení disjunkce z 6)

8. $\neg p \vee q$ (elimiace disjunkce z 2, 3–5 a 6–7)

---

1. $\neg p \vee q$ (předpoklad)

    2. $p$ (pomocný předpoklad)
    3. $q$ (eliminace disjunkce z 1 a 2)

4. $p \Rightarrow q$ (zavedení implikace z 2 a 3)

Využili jsme zde pravidla *tertium non datur* nebo-li pravidlo vyloučeného třetího. To říká, že v našem logickém systému platí, že platí buď $p$ nebo $\neg p$.

**Poznámka 1.3.4** Pro zajímavost existují další běžné logické spojky, které se dají odvodit z těchto základních. Máme zde například XOR (exclusive OR) $\oplus$, který říká, že platí buď $p$ nebo $q$, ale ne oba zároveň. Dalšími jsou NAND $|$ a NOR $\downarrow$, které jsou negacemi AND a OR.

**Cvičení 1.3.5** Napište si, jak by vypadali výše zmíněné spojky pomocí základních spojek.

**Příklad 1.3.6** Pojďme si nyní odpočinout od úplně formálních příkladů a podívat na trochu méně formální příklad. Mějme následující tvrzení:

- Na výlet pojede Petr nebo Quido.
- Jestliže pojede Quido, pojede Simona a nepojede Renata.
- Jestliže pojede Tomáš, pojede i Renata.
- Jestliže pojede Simona, pojede Tomáš.

Chceme zjistit, zda je pravda trvzení ‘Petr pojede na výlet’.[2] Budeme postupovat pomocí přirozené dedukce. Začneme tedy předpoklady, které máme a budeme chtít dokázat, že Petr pojede na výlet. Pojmenujeme si výroky $p$: Petr pojede na výlet, $q$: Quido pojede na výlet, $s$: Simona pojede na výlet, $t$: Tomáš pojede na výlet, $r$: Renata pojede na výlet.

[2]Toto lze také převést na problém sématického důsledku a řešit resoluční metodou. Tímto spojením se zabýva věta o úplnosti, která je též nad rámec této středoškolské knihy.

1. $p \vee q$ (předpoklad)
2. $q \Rightarrow (s \wedge \neg r)$ (předpoklad)
3. $t \Rightarrow r$ (předpoklad)
4. $s \Rightarrow t$ (předpoklad)

> 5. $\neg p$ (pomocný předpoklad)
> 6. $q$ (eliminace disjunkce z 1)
> 7. $s \wedge \neg r$ (modus ponens z 2 a 6)
> 8. $s$ (eliminace konjunkce z 7)
> 9. $t$ (modus ponens z 4 a 8)
> 10. $r$ (modus ponens z 3 a 9)
> 11. $\neg r$ (elimace konjunkce z 7)
> 12. $\perp$ (eliminace negace z 10 a 11)

13. $\neg\neg p$ (reductio ad absurdum z 5–12)
14. $p$ (eliminace dvojí negace z 13)

Tímto jsme dokázali, že Petr pojede na výlet. Zde jsme použili pravidla eliminace disjunkce, modus ponens a reductio ad absurdum. Pojďme si spolu pravidla vysvětlit.

- Eliminace disjunkce: Pokud víme, že platí $p \vee q$ a víme, že jedno z nich neplatí, tak můžeme odvodit to druhé.
- Modus ponens: Pokud víme, že platí $p \Rightarrow q$ a $p$, tak můžeme odvodit $q$. Někdo mi něco slíbil a já vím, že slib byl úspešný, takže to i splnil.
- Reductio ad absurdum: Pokud předpokládáme něco a dokážeme, že z toho vyplývá spor, tak můžeme odvodit, že to, že platí negace našeho předpokladu.

**Cvičení 1.3.7** Ať si taky něco procvičíte, zkuste si dokázat, že $p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r$.[3]

**Řešení 1.3.7**

1. $p \Rightarrow q$ (předpoklad)
2. $q \Rightarrow r$ (předpoklad)

> 3. $p$ (pomocný předpoklad)
> 4. $q$ (modus ponens z 1 a 3)
> 5. $r$ (modus ponens z 3 a 4)

6. $p \Rightarrow r$ (zavedení implikace z 3–5)

Abyste opravdu věřili, že tato metoda je lepší než pravdivostní tabulky, tak se pojďme u příkladu **??** zamyslet nad velikostí tabulky. Vzhledem k tomu, že máme 5 proměnných, tak abychom dosáhli všech možných kombinací, musí mít tabulka $2^5 = 32$ řádků! Představte si, že je všechny musíte vyplňovat a pak z toho něco vyčíst.

Nebudeme vás nadále trápit, ale ještě si ukážeme odkud se berou vzorečky negací složených výroků.

**Příklad 1.3.8 (De Morganovy zákony)** De Morganovy zákony jsou zákony, které nám říkají, jak se neguje konjunkce a disjunkce. Jsou to následující vzorečky:

$$\begin{aligned} \neg(p \wedge q) &\dashv\vdash \neg p \vee \neg q \\ \neg(p \vee q) &\dashv\vdash \neg p \wedge \neg q \end{aligned} \tag{1.2}$$

[3] Pokud se vám to povede, tak gratuluji. Nejsou zde vypsaná pravidla, takže se ani nepředpokládá, že byste to měli zvládnout.

Tyto zákony se dají dokázat pomocí pravdivostní tabulky, ale my si je zde formálně dokážeme. Dají se zobecnit metematickou indukcí (už se brzy dozvíte co to je) na libovolný počet výroků následujícím způsobem:

$$\begin{aligned} \neg\left(\bigwedge_{i=1}^{n} p_i\right) &\dashv\vdash \bigvee_{i=1}^{n} \neg p_i \\ \neg\left(\bigvee_{i=1}^{n} p_i\right) &\dashv\vdash \bigwedge_{i=1}^{n} \neg p_i. \end{aligned} \tag{1.3}$$

Uvedeme zde důkaz prvního De Morganova zákona. Zbytek necháme jako cvičení pro čtenáře.

1. $\neg(p \wedge q)$ (předpoklad)
    2. $\neg(\neg p \vee \neg q)$ (pomocný předpoklad)
        3. $\neg p$ (pomocný předpoklad)
        4. $\neg p \vee \neg q$ (zavedení disjunkce z 3)
        5. $\perp$ (eliminace negace z 4 a 2)
    6. $p$ (reductio ad absurdum z 3–5)
        7. $\neg q$ (pomocný předpoklad)
        8. $\neg p \vee \neg q$ (zavedení disjunkce z 7)
        9. $\perp$ (eliminace negace z 8 a 2)
    10. $q$ (reductio ad absurdum z 7–9)
    11. $p \wedge q$ (zavedení konjunkce z 6 a 10)
    12. $\perp$ (eliminace negace z 11 a 1)
13. $\neg\neg(\neg p \vee \neg q)$ (reductio ad absurdum z 1–12)
14. $\neg p \vee \neg q$ (eliminace dvojí negace z 13)

1. $\neg p \vee \neg q$ (předpoklad)
    2. $p \wedge q$ (pomocný předpoklad) 3. $p$ (eliminace konjunkce z 2)
    4. $q$ (eliminace konjunkce z 2)
        5. $\neg p$ (pomocný předpoklad)
        6. $\perp$ (eliminace negace z 3 a 5)
        7. $\neg q$ (pomocný předpoklad)
        8. $\perp$ (eliminace negace z 4 a 7)
    9. $\perp$ (eliminace konjunkce z 6 a 8)
10. $\neg(p \wedge q)$ (reductio ad absurdum z 2–9)

Mohli bychom pokračovat dál, ale máme tu ještě spoustu dalších zajímavých věcí, které chceme probrat. Pokud vás téma logiky zaujalo, tak si doporučuji přečíst si knihu

Jiří Velebil, *Velmi jemný úvod do matematické logiky*, Praha 2007

Chcete-li jít více do hloubky a dozvědět se i více to těch prapodivných boxech, které jsme používali, tak si přečtěte knihu

M. Demlová a B. Pondělíček, *Matematická logika*, skriptum FEL ČVUT, Praha, 1997

## 1.4 Důkazy

Důkazy jsou základním nástrojem matematiky a bez nich bychom se nedostali daleko. V této kapitole si ukážeme několik základních typů důkazů, které se v matematice používají. V úvodní kapitole byl zmíněn systém definice-věta-důkaz. Než tedy přejdeme k důkazům, tak si ještě jednou připomeneme co tento systém znamená.

**Definice** je vymezení pojmu, ze kterým hodláme pracovat. Definice obsahuje název a charakteristické vlastnosti daného pojmu.
**Věta** je výrok, který je pravdivý a musí být dokázán. Většinou rozvíjíme nějaký pojem, který jsme si definovali.
**Důkaz** je postup, který nám ukazuje, proč je věta pravdivá. Důkaz se skládá z předpokladů a závěru. Předpoklady jsou věty, které už máme dokázané a závěr je věta, kterou chceme dokázat.

**Příklad 1.4.1** Vyzkoušejme si zde jak by vypadal jednoduchý důkaz. V matematické literatuře by to vypadalo následovně:

**Věta 1.2.3**[4] **(O součtu dvou sudých čísel)**: Součet dvou sudých čísel je sudé číslo.
DůKAZ. Nechť $a$ a $b$ jsou sudá čísla. Pak existují taková čísla $k, l \in \mathbb{Z}$, že $a = 2k$ a $b = 2l$. Potom

$$a + b = 2k + 2l = 2(k + l), \tag{1.4}$$

kde $k + l \in \mathbb{Z}$. Tedy $a + b$ je sudé číslo. ■

Důkaz není úplně korektní, ale za předpokladu, že víme, co znamená, že číslo je sudé[5], tak bychom mohli tento důkaz přijmout.

**Cvičení 1.4.2** Zkuste si nyní dokázat, že součet dvou lichých čísel je sudé číslo.

**Řešení 1.4.2**
DůKAZ. Nechť $a$ a $b$ jsou lichá čísla. Pak existují taková čísla $k, l \in \mathbb{Z}$, že $a = 2k + 1$ a $b = 2l + 1$. Potom

$$a + b = 2k + 1 + 2l + 1 = 2(k + l + 1), \tag{1.5}$$

kde $k + l + 1 \in \mathbb{Z}$. Tedy $a + b$ je sudé číslo. ■

Pojďme si nyní ukázat několik základních typů důkazů, které se v matematice používají. Mějme předpoklad $p$ a závěr $q$.
**Důkaz přímý**: Důkaz, kde se jde *přímo* z předpokladu k závěru. V jazyku logických spojek to znamená, že se použije implikace $p \Rightarrow q$. Tento typ důkazu jsme si ukázali v příkladu 1.4.1.
**Důkaz nepřímý**: Důkaz, kde se používá takzvaná obměněná implikace. V jazyku logických spojek to znamená, že se použije implikace $\neg q \Rightarrow \neg p$. To jsme si odvodili v příkladu 1.3.2.
**Důkaz sporem**: Důkaz, kde se zneguje výraz $p \Rightarrow q$ a dokáže se, že z toho vyplývá nějaký spor. Zde můžeme použít příklad 1.3.3 ve kterém jsme si dokázali, že $p \Rightarrow q \vdash \neg p \vee q$. Pokud tento výrok znegujeme za pomoci De Morganových zákonů, tak dostaneme $p \wedge \neg q$. Toto je nyní náš předpoklad, ze kterého se snažíme vyvodit spor.

Poslední typ zde úplně nezapadá, takže si ho uvedeme za chvíli samostatně.

[4] Nenechte se zmást značením. Je zde uvedeno jako příklad, nezapadá však do našeho číslování.
[5] Správná definice je ovšem, že číslo je sudé, pokud lze napsat jako 2k, kde $k \in \mathbb{Z}$. U lichých je to 2k + 1, kde $k \in \mathbb{Z}$

**Příklad 1.4.3** Ukažme si nyní příklad přímého důkazu. Mějme následující větu: *Pokud je číslo $n$ sudé, tak je i $n^2$ sudé.*. Zde opět využijeme naší definice sudých čísel z předchozích příkladů. Máme tedy číslo $n$, které je sudé. To znamená, že lze napsat jako $2k$, kde $k \in \mathbb{Z}$. Nyní si spočítáme $n^2$:

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2). \tag{1.6}$$

S trochou důvtipu lze vidět, že $2k^2 \in \mathbb{Z}$.[6] To znamená, že se nám podařilo $n^2$ napsat jako $2l$, kde $l \in \mathbb{Z}$. Tedy $n^2$ je sudé číslo.

**Cvičení 1.4.4** Zkuste si nyní dokázat, že pokud je číslo $n$ liché, tak je i $n^2$ liché. Postupujte podobně jako v předchozím příkladu.

**Příklad 1.4.5** Představte si, že máte dokázat větu: *Pokud je číslo $n^2$ sudé, tak je i $n$ sudé.* Zde zkusíme použít nepřímý důkaz. Provedeme obměněnou implikaci a dostaneme výrok $\neg p \Rightarrow \neg q$. Tedy pokud je $n$ liché, tak je i $n^2$ liché. Toto jste již udělali ve cvičení 1.4.4.

**Příklad 1.4.6** Přejděme na důkaz sporem. Oblíbeným příkladem je důkaz iracionality čísla $\sqrt{2}$. Chceme ukázat, že $\sqrt{2} \in \mathbb{Q}$. Provedením negace dostaneme tedy předpoklad, že $\sqrt{2}$ je racionální číslo. To znamená, že existují čísla $p$ a $q$ taková, že $\sqrt{2} = \frac{p}{q}$.[7] Dále si můžeme předpokládat, že $p$ a $q$ jsou nesoudělná čísla. To znamená, že nemají žádný společný dělitel. Nyní si můžeme napsat:

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2. \tag{1.7}$$

To znamená, že $p^2$ je sudé číslo. Z předchozích příkladů víme, že to znamená, že $p$ je sudé číslo. To znamená, že existuje číslo $k$ takové, že $p = 2k$. Dosadíme zpět do našeho vztahu:

$$2q^2 = (2k)^2 \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2. \tag{1.8}$$

To znamená, že $q^2$ je sudé číslo. Z předchozích příkladů víme, že to znamená, že $q$ je sudé číslo. To je ale spor s naším předpokladem, že $p$ a $q$ nemají žádný společný dělitel. Tedy jsme dokázali, že $\sqrt{2}$ je iracionální číslo.

K důkazům se určitě ještě vrátíme v dalších kapitolách u konkrétních vět, které stojí za dokázání. Teď si uvedeme ještě jeden běžný typ důkazu, který se v matematice používá.

**Důkaz matematickou indukcí**: Důkaz, který se používá pro dokazování vět, které platí pro všechna přirozená čísla. Důkaz se skládá ze tří kroků:

- **Základní krok**: Dokážeme, že věta platí pro první přirozené číslo.
- **Indukční krok**: Předpokládáme, že věta platí pro nějaké přirozené číslo $n$. Tomuto se říká indukční předpoklad.
- **Závěr**: Využitím indukčního předpokladu dokážeme, že věta platí i pro $n+1$ čísel.

**Příklad 1.4.7** Ukažme si nyní důkaz matematickou indukcí na příkladu. Mějme následující větu: *Pro každé přirozené číslo $n$ platí, že* $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.[8]
Důkaz.
**Základní krok**: Pro $n = 1$ platí, že $1 = \frac{1(1+1)}{2} = 1$. Tedy věta platí pro $n = 1$.
**Indukční krok**: Předpokládejme, že věta platí pro nějaké přirozené číslo $n$. To znamená, že platí rovnost $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.
**Závěr**: Nyní se pokusíme dokázat, že věta platí i pro $n+1$. Tedy

$$1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}. \tag{1.9}$$

Tímto jsme dokázali, že věta platí i pro $n+1$. Tedy věta platí pro všechna přirozená čísla. ■

[6] Zde bychom potřebovali něco o teorii celých čísel. Nám postačí, když tomu budete věřit.
[7] Definice racionálních čísel.
[8] Zkuste první se zamyslet, proč byt to mohlo platit. Legenda praví, že toto tvrzení objevil slavný matematik Gauss, když byl ještě dítě.

# Kapitola 2

# Množiny, relace a čísla

*From the paradise that Cantor created for us no-one shall be able to expel us.*

David Hilbert

## 2.1 Odbočka — Axiomatická teorie množin

Než se pustíme do pro nás více relevatních témat, pojďme se seznámit s rigorózní teorií množin na které je postavena celá matematika. Tato teorie byla vytvořena Georgem Cantorem na konci 19. století a je základem pro všechny matematické koncepty, které se týkají množin. Tato teorie je ale velice složitá a zmiňuji ji zde jen proto, abychom měli představu o tom, jak by mohla matematika vypadat, kdybychom se snažili být formální.

Hlavní roli v této teorii hrají axiomy, což jsou základní pravidla, která musíme přijmout jako pravdivá, abychom mohli dále pracovat. Než se pustíme na samotné axiomy, vysvětleme si rychle následující znaky, které nám usnadní zápis. Množiny značíme velkými písmeny, například $X$, $Y$, $Z$, atd. Prvky množin značíme malými písmeny, například $x$, $y$, $z$, atd. Pokud prvek $x$ patří do množiny $X$, značíme to $x \in X$ a pokud nepatří, tak $x \notin X$. Systém množin je vlastně také množina, která obsahuje množiny a značíme ji $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, atd. Projděme si nyní axiomy množinové teorie a pak si ukážeme základní příklady a vysvetlení těchto axiomů.

**Axiomy množinové teorie**

1. **Axiom of extension**: Dvě množiny jsou rovny právě tehdy, když obsahují stejné prvky.
2. **Axiom of the empty set**: Existuje množina, která neobsahuje žádné prvky. Tato množina se nazývá prázdná množina a značí se $\emptyset$.
3. **Axiom schema of separation**: Pro každou množinu $x$ a každou vlastnost $P$ existuje množina, která obsahuje všechny prvky množiny $x$ splňující vlastnost $P$.
4. **Axiom of pairing**: Pro každé dvě množiny $X$ a $Y$ existuje množina, která obsahuje všechny prvky množin $X$ a $Y$.
5. **Axiom of union**: Pro každý systém množin $\mathcal{S}$ existuje množina, která obsahuje všechny prvky všech množin v systému $\mathcal{S}$. Tato množina se nazývá sjednocení množin v systému $\mathcal{S}$ a značí se $\bigcup \mathcal{S}$. Pokud bychom chtěli sjednotit pouze množiny $X$ a $Y$, značili bychom to $X \cup Y$.
6. **Axiom of power set**: Pro každou množinu $X$ existuje systém všech podmnožin množiny $X$. Tento systém se nazývá potenční množina množiny $X$ a značí se $\mathcal{P}(X)$.
7. **Axiom of infinity**: Existuje systém množin $\mathcal{S}$ takový, že $\emptyset \in \mathcal{S}$ a pro každou množinu $x \in \mathcal{S}$ platí $x \cup \{x\} \in \mathcal{S}$.

8. **Axiom of choice**: Pro každý systém neprázdných množin $\mathcal{S}$ existuje funkce $f$, která každé množině $X \in \mathcal{S}$ přiřazuje prvek $f(X)$, který je prvkem množiny $X$.
9. **Axiom schema of replacement**: Pro každou množinu $X$ a každou funkci $f$ existuje množina, která obsahuje všechny prvky $f(x)$ pro každý prvek $x \in X$.

V poslední řadě chci dodat, že na přesných axiomech množinové teorie se zdroje moc neshodují a můžete najít různé formulace. Nám výše uvedené axiomy postačí pro naše účely. Pojďme si nyní podrobněji vysvětlit jednotlivé axiomy a ukázat si nějaké příklady.

### 2.1.1 Axiom of extension

K tomuto axiomu moc slov nepotřebujeme. Vezměme například tři množiny definované následovně[1]:

$$
\begin{aligned}
X &= \{1, 2, 3\},\\
Y &= \{1, 2, 3\},\\
Z &= \{1, 2, 3, 4\}.
\end{aligned}
$$

Množiny $X$ a $Y$ jsou rovny, protože obsahují stejné prvky, zatímco množina $Z$ je odlišná, protože obsahuje navíc prvek 4.

### 2.1.2 Axiom of the empty set

I tento axiom je poměrně jednoduchý. Prázdná množina je množina, která neobsahuje žádné prvky. Můžeme ji zapsat následovně: $\emptyset = \{\}$.

### 2.1.3 Axiom schema of separation

Tento axiom nám říká, že pro každou množinu $x$ a každou vlastnost $P$ existuje množina, která obsahuje všechny prvky množiny $x$ splňující vlastnost $P$. Například, pokud máme množinu $X = \{1, 2, 3, 4, 5\}$ a vlastnost $P$, že prvek $x$ je sudý, můžeme vytvořit množinu $Y = \{2, 4\}$.

### 2.1.4 Axiom of pairing

Tento axiom nám říká, že pro každé dvě množiny $X$ a $Y$ existuje množina, která obsahuje všechny prvky množin $X$ a $Y$. Například, pokud máme množiny $X = \{1, 2\}$ a $Y = \{3, 4\}$, můžeme vytvořit množinu $Z = \{\{1, 2\}, \{3, 4\}\}$. Tento axiom využijeme při důležité definici kartézského součinu množin.

### 2.1.5 Axiom of union

Tento axiom nám říká, že pro každý systém množin $\mathcal{S}$ existuje množina, která obsahuje všechny prvky všech množin v systému $\mathcal{S}$. Například, pokud máme množiny $X = \{1, 2\}$ a $Y = \{2, 3\}$, můžeme vytvořit množinu $Z = X \cup Y\{1, 2, 3\}$.

### 2.1.6 Axiom of power set

Tento axiom nám říká, že pro každou množinu $X$ existuje systém všech podmnožin množiny $X$. Například, pokud máme množinu $X = \{1, 2\}$, můžeme vytvořit množinu $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Této množině se říká potenční množina množiny $X$.

### 2.1.7 Axiom of infinity

Tento axiom nám říká, že existuje systém množin $\mathcal{S}$ takový, že $\emptyset \in \mathcal{S}$ a pro každou množinu $x \in \mathcal{S}$ platí $x \cup \{x\} \in \mathcal{S}$. Tento axiom nám zaručuje existenci nekonečných množin. Pomocí tohoto axiomu

[1] Všimněte si, že množiny zde zapisujeme pomocí závorek a prvky množiny oddělujeme čárkami.

můžeme definovat například množinu přirozených čísel $\mathbb{N}$ a to následovně:

$$\begin{aligned}
0 &= \emptyset, \\
1 &= \{0\} = \{\emptyset\}, \\
2 &= \{0,1\} = \{\emptyset, \{\emptyset\}\}, \\
3 &= \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\
&\vdots
\end{aligned}$$

### 2.1.8 Axiom of choice

Tento axiom je nejkontroverznější z celé množinové teorie, protože pokud ho pokud ho nepřijmeme, spousta zajímavých matematických konceptů se nám zhroutí. Například bez tohoto axiomu nefungují limity, protože potřebujeme vybrat prvek z nekonečné množiny posloupností a tento axiom nám zaručuje, že tam nějaký takový prvek je. K tomuto axiomu se ještě vrátíme, až se budeme zabývat konkrétními matematickými koncepty. Známým paradoxem spojeným s tímto axiomem je Banach-Tarski paradox, který říká, že můžeme rozložit kouli na konečně mnoho koulí, které mají stejný objem jako původní koule.

### 2.1.9 Axiom schema of replacement

Tento axiom nám říká, že pro každou množinu $X$ a každou funkci $f$ existuje množina, která obsahuje všechny prvky $f(x)$ pro každý prvek $x \in X$. Například, pokud máme množinu $X = \{1,2,3\}$ a funkci $f(x) = x^2$[2], můžeme vytvořit množinu $Y = \{1,4,9\}$.

## 2.2 Množiny

Nebudeme se zde zabývat, co přímo množina je, protože bychom se pohybovali na hranici mezi matematikou a filozofií. Množinou tedy rozumíme určitou kolekci prvků, které mohou být cokoliv. Pokud jste nečetli předchozí odbočku, zopakujme si nyní základní definice a pojmy spojené s množinami.

**Značení**: Množiny značíme velkými písmeny, například $X$, $Y$, $Z$. Prvky množin značíme malými písmeny, například $x$, $y$, $z$.
**Prvek množiny**: Prvek $x$ je prvkem množiny $X$, pokud $x \in X$. Opak platí, pokud $x \notin X$.
**Prázdná množina**: Množina, která neobsahuje žádné prvky. Značíme ji $\emptyset$.
**Podmnožina**: Množina $Y$ je podmnožinou množiny $X$, pokud každý prvek množiny $Y$ je také prvkem množiny $X$. Značíme to $Y \subseteq X$.
**Rovnost množin**: Množiny $X$ a $Y$ jsou rovny, pokud obsahují stejné prvky. Značíme to $X = Y$.
**Sjednocení množin**: Sjednocení množin $X$ a $Y$ je množina, která obsahuje všechny prvky množin $X$ a $Y$. Značíme to $X \cup Y$.
**Průnik množin**: Průnik množin $X$ a $Y$ je množina, která obsahuje pouze ty prvky, které jsou zároveň v množinách $X$ a $Y$. Značíme to $X \cap Y$.
**Rozdíl množin**: Rozdíl množin $X$ a $Y$ je množina, která obsahuje pouze ty prvky, které jsou v množině $X$ a nejsou v množině $Y$. Značíme to $X \setminus Y$.
**Potenční množina**: Potenční množina množiny $X$ je množina všech podmnožin množiny $X$. Značíme to $\mathcal{P}(X)$.

**Příklad 2.2.1** Mějme množiny $X = \{1,2,3\}$ a $Y = \{2,3,4\}$. Potom platí:

$$\begin{aligned}
X \cup Y &= \{1,2,3,4\}, \\
X \cap Y &= \{2,3\}, \\
X \setminus Y &= \{1\}, \\
Y \setminus X &= \{4\}. \\
\mathcal{P}(X) &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.
\end{aligned}$$

[2] Zde předpokládáme, že víte, co dělá základní operace na druhou.

**Cvičení 2.2.2** Mějme množiny $X = \{1,2,3,4\}$ a $Y = \{3,4,5\}$. Zjistěte $X \cup Y$, $X \cap Y$, $X \setminus Y$, $Y \setminus X$ a $\mathcal{P}(Y)$.

**Řešení 2.2.2** Máme:

$$\begin{aligned} X \cup Y &= \{1,2,3,4,5\}, \\ X \cap Y &= \{3,4\}, \\ X \setminus Y &= \{1,2\}, \\ Y \setminus X &= \{5\}, \\ \mathcal{P}(Y) &= \{\emptyset, \{3\}, \{4\}, \{5\}, \{3,4\}, \{3,5\}, \{4,5\}, \{3,4,5\}\}. \end{aligned}$$

## 2.3 Relace

Když už nyní víme, co jsou množiny, je na čase se zabývat vztahy mezi nimi. Takovým vztahům se říká relace a jsou základem pro spoustu dalších matematických koncept. Relace můžeme chápat jako způsob, jakým jsou prvky množin propojeny. Nejprve si zopakujme základní definice a pojmy spojené s relacemi. Než si řekneme, co je to relace, musíme nejdříve definovat kartézský součin množin.

**Kartézský součin množin**: Kartézský součin množin $X$ a $Y$ je množina všech uspořádaných dvojic $(x, y)$, kde $x \in X$ a $y \in Y$. Značíme to $X \times Y$.

**Příklad 2.3.1** Mějme množiny $X = \{1,2\}$ a $Y = \{3,4\}$. Potom platí:

$$X \times Y = \{(1,3), (1,4), (2,3), (2,4)\}.$$

**Relace**: Relace $\mathcal{R}$ mezi množinami $X$ a $Y$ je podmnožina kartézského součinu $X \times Y$. Pokud máme relaci $\mathcal{R}$ mezi množinami $X$ a $Y$, značíme to $\mathcal{R} \subseteq X \times Y$. Prvek $(x, y) \in R$ značíme $x\mathcal{R}y$ a říkáme, že prvek $x$ je v relaci $R$ s prvkem $y$. Je to ve zkratce jakási omezující vlastnost na kartézský součin množin.

**Příklad 2.3.2** Mějme množiny $X = \{1,2\}$ a $Y = \{3,4\}$ a relaci $\mathcal{R} = \{(1,3), (2,4)\}$. Potom platí:

$$\begin{aligned} &1\mathcal{R}3, \\ &2\mathcal{R}4. \end{aligned}$$

V tomto případě máme relaci zadanou explicitně a slouží jen na ukázání poněkud zvláštního zápisu[3].

**Příklad 2.3.3** Nyní si pojďme ukázat příklad, kde je relace zadaná jako nějaká vlastnost, kterou prvky množin splňují. Mějme množiny $X = \{1,2,3\}$ a $Y = \{3,4,5\}$ a relaci $\mathcal{R} = \{(x, y) \in X \times Y \mid x < y\}$. Což v překladu znamená, že prvek $x$ je v relaci s prvkem $y$, pokud $x$ je menší než $y$. Potom platí:

$$\begin{aligned} &1\mathcal{R}3, \\ &1\mathcal{R}4, \\ &1\mathcal{R}5, \\ &2\mathcal{R}3, \\ &2\mathcal{R}4, \\ &2\mathcal{R}5. \end{aligned}$$

[3] Tento zápis, jak brzy uvidíte, moc používat nebudeme.

**Cvičení 2.3.4** Mějme množiny $X = \{1, 2, 3\}$ a $Y = \{3, 4, 5\}$ a relaci $\mathcal{R} = \{(x, y) \in X \times Y \mid x + y = 5\}$. Zjistěte, které dvojice prvků množin $X$ a $Y$ splňují vlastnost $x + y = 5$.

**Řešení 2.3.4** Máme:

$$1\mathcal{R}4,$$
$$2\mathcal{R}3.$$

**Poznámka 2.3.5** Jak již bylo zmíněno v definice kartézského součinu, prvek $(x, y)$ je uspořádaná dvojice, což znamená, že pořadí prvků má význam. To znamená, že ve většině případů $(x, y) \neq (y, x)$.

**Vlastnosti relací**.
Nechť $\mathcal{R}$ je relace na množině $X$. Potom můžeme definovat následující vlastnosti relací:

**Reflexivita**: Relace $\mathcal{R}$ je reflexivní, pokud pro každý prvek $x \in X$ platí $x\mathcal{R}x$.

**Symetrie**: Relace $\mathcal{R}$ je symetrická, pokud pro každý prvek $x, y \in X$ platí, že pokud $x\mathcal{R}y$, tak $y\mathcal{R}x$.

**Antisymetrie**: Relace $\mathcal{R}$ je antisymetrická, pokud pro každý prvek $x, y \in X$ platí, že pokud $x\mathcal{R}y$ a $y\mathcal{R}x$, tak $x = y$.

**Tranzitivita**: Relace $\mathcal{R}$ je tranzitivní, pokud pro každý prvek $x, y, z \in X$ platí, že pokud $x\mathcal{R}y$ a $y\mathcal{R}z$, tak $x\mathcal{R}z$.

Pokud je relace reflexivní, symetrická a tranzitivní, říkáme, že je **relace ekvivalence**.

Vlastnosti relací se nejlépe ukazující na číselných množinách a proto si nejprve pojďme říct něco o nich.

## 2.4 Odbočka — Tělesa

Těleso je ve zkratce množina prvků, který splňuje 'hezké' vlastnosti. Jdou mezi sebou 'hezky' sčítat a násobit. Pojďme si nyní zadefinovat co přesně těleso je.

**Těleso** je zadáno množinou $\mathbb{F}$ a obsahuje dvě funkce, které jdou abstraktně zadefinovat, ale pro nás bude stačit, že to je sčítaní a násobení. Těleso musí splňovat následující axiomy:

1. Axiomy pro sčítání skalárů (Skaláry jsou prvky tělesa. Například v případě $\mathbb{R}$ jsou skaláry reálná čísla. To že jsou reálná čísla těleso si řekneme později.):
   (a) Existence nulového prvku: Pro každý prvek $x \in \mathbb{F}$ existuje prvek $0 \in \mathbb{F}$ takový, že $x + 0 = x$. Tento prvek se nazývá nulový prvek.
   (b) Komutativita sčítání: Pro každé dva prvky $x, y \in \mathbb{F}$ platí, že $x + y = y + x$.
   (c) Asociativita sčítání: Pro každé tři prvky $x, y, z \in \mathbb{F}$ platí, že $(x + y) + z = x + (y + z)$.
   (d) Existence opačného prvku: Pro každý prvek $x \in \mathbb{F}$ existuje prvek $-x \in \mathbb{F}$ takový, že $x + (-x) = 0$.
2. Axiomy pro násobení skalárů:
   (a) Existence jednotkového prvku: Pro každý prvek $x \in \mathbb{F}$ existuje prvek $1 \in \mathbb{F}$ takový, že $x \cdot 1 = x$. Tento prvek se nazývá jednotkový prvek.
   (b) Komutativita násobení: Pro každé dva prvky $x, y \in \mathbb{F}$ platí, že $x \cdot y = y \cdot x$.
   (c) Asociativita násobení: Pro každé tři prvky $x, y, z \in \mathbb{F}$ platí, že $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Distributivní zákon: Pro každé tři prvky $x, y, z \in \mathbb{F}$ platí, že $x \cdot (y + z) = x \cdot y + x \cdot z$.
4. Test invertibility: Pro každý nenulový prvek $x \in \mathbb{F}$ existuje prvek $x^{-1} \in \mathbb{F}$ takový, že $x \cdot x^{-1} = 1$. Tento prvek se nazývá inverzní prvek.

## 2.5 Čísla

O číslech jste pravděpodobně již slyšeli, ale stejně je nutné si představit základní číselné množiny, se kterými budeme pracovat.

### 2.5.1 Přirozená čísla

Přirozená čísla, jak jejich název napovídá, jsou čísla, která se nejčastěji vyskutují v našem životě. Je to také první množina, která se považovala za číselnou množinu po překvapivě dlouhou dobu.[4]

**Přirozená čísla** jsou množina čísel, která začínají od jedničky a pokračují dál. Značíme je $\mathbb{N} = \{1, 2, 3, \ldots\}$. Pokud si vzpomínáte na odbočku o axiomech, tak konkrétně v 2.1.7 jsme si ukázali, jak můžeme přirozená čísla definovat pomocí množinové teorie.
V případě, že chceme zahrnout nulu, mluvíme o **přirozených číslech včetně nuly** a značíme je $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.

**Cvičení 2.5.1** Jsou přirozená čísla těleso?

**Nápověda 2.5.1** Zkuste si projít axiomy tělesa a zjistit, zda přirozená čísla splňují všechny axiomy.

**Řešení 2.5.1** Nejsou.
DŮKAZ. Přirozená čísla nesplňují axiomy tělesa, protože například neexistuje inverzní prvek pro sčítání. Pokud vezmeme libovolné přirozené číslo $n$, tak jeho inverzní prvek by měl být $-n$, ale toto číslo není přirozené. ■

### 2.5.2 Celá čísla

**Celá čísla** jsou množina čísel, která zahrnují přirozená čísla, ale také záporná čísla a nulu. Značíme je $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

**Cvičení 2.5.2** Jsou přirozená čísla těleso?

**Řešení 2.5.2** Nejsou.
DŮKAZ. Celá čísla nesplňují axiomy tělesa, protože například neexistuje inverzní prvek pro násobení. Pokud vezmeme libovolné celé číslo $n$, tak jeho inverzní prvek by měl být $\frac{1}{n}$, ale toto číslo není celé. ■

### 2.5.3 Racionální čísla

**Racionální čísla** jsou množina čísel, která zahrnují celá čísla, ale také zlomky. Značíme je $\mathbb{Q} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$.

Tato definice je trochu složitější, ale znamená to, že racionální čísla jsou všechna čísla, která můžeme zapsat jako zlomek, kde čitatel i jmenovatel jsou celá čísla a jmenovatel není nula.

**Cvičení 2.5.3** Jsou racionální čísla těleso?

**Řešení 2.5.3** Ano.
DŮKAZ. Racionální čísla splňují axiomy tělesa, protože jsou uzavřená na sčítání, násobení, existuje nulový prvek, existuje opačný prvek, existuje jednotkový prvek, jsou komutativní a asociativní. Pokud tomu nevěříte, zkuste si projít axiomy tělesa a zjistit, zdali racionální čísla splňují všechny axiomy. ■

[4] Nula byla často rozporuplná a někteří matematikové ji neuznávali jako číslo a jejich argument byl, že není potřeba číslo, které značí nic.

### 2.5.4 Reálná čísla

**Reálná čísla** jsou množina čísel, která zahrnují racionální čísla, ale také iracionální čísla. Značíme je $\mathbb{R}$. Přesnou definici zde nebudeme uvádět, protože je složitější.

Proč ale existují reálná čísla? Proč nestačí racionální čísla? Odpověď je jednoduchá, ale zároveň složitá. Ukažme si příklad, který nám ukáže číslo, které není racionální.

**Příklad 2.5.4** Mějme číslo čtverec o stranách délky 1. Jaká je délka úhlopříčky čtverce? Pokud si vzpomenete na Pythagorovu větu[5], tak délka úhlopříčky je $\sqrt{1^2+1^2}=\sqrt{2}$. Nyní si pojďme ukázat, že číslo $\sqrt{2}$ není racionální.
Důkaz. Sporem. Předpokládejme, že číslo $\sqrt{2}$ je racionální. To znamená, že existují nesoudělná[6] celá čísla $a$ a $b$ taková, že $\sqrt{2}=\frac{a}{b}$. Potom můžeme napsat:

$$\begin{aligned}\sqrt{2} &= \frac{a}{b},\\ 2 &= \frac{a^2}{b^2},\\ 2b^2 &= a^2.\end{aligned}$$

To znamená, že $a^2$ je sudé číslo, což znamená, že $a$ je také sudé číslo. Toto tvrzení víme z příkladu 1.4.5. Takže existuje celé číslo $c$ takové, že $a=2c$. Dosadíme zpět do rovnice:

$$\begin{aligned}2b^2 &= (2c)^2,\\ 2b^2 &= 4c^2,\\ b^2 &= 2c^2.\end{aligned}$$

To znamená, že $b^2$ je sudé číslo, což znamená, že $b$ je také sudé číslo. To ale znamená, že čísla $a$ a $b$ mají společného dělitele a došli jsme ke sporu. Tedy jsme dokázali, že číslo $\sqrt{2}$ není racionální. ■

Když tedy $\sqrt{2}$ není racionální číslo, co tedy je? Těmto číslům se říká iracionální čísla a je to podmnožina čísel reálných. Velice známým iracionálním číslem je $\pi$ nebo $e$.

**Cvičení 2.5.5** Ukažte, že realná čísla jsou těleso.

**Poznámka 2.5.6** Reálná čísla jsou takzvaně nespočetná množina. To zjednodušeně znamená, že jich je více než přirozených čísel. Těch je ale také nekonečně mnoho. Ve zkratce, počet prvků množiny reálných čísel je větší nekonečno než počet prvků množiny přirozených čísel. Více se tím zde zabývat nebudeme.

### 2.5.5 Komplexní čísla

**Komplexní čísla** jsou množina čísel, která zahrnují reálná čísla, ale také imaginární čísla. Značíme je $\mathbb{C}=\{a+bi \mid a,b\in\mathbb{R}\}$, kde $i$ je imaginární jednotka, která splňuje $i^2=-1$.

Proč potřebujeme další číselnou množinu? Odpověď je jednoduchá, ale zároveň složitá. Komplexní čísla nám umožňují řešit rovnice, které nemají řešení v reálných číslech. Například rovnice $x^2+1=0$ nemá řešení v reálných číslech, protože $\sqrt{-1}$ není definované, ale má řešení v komplexních číslech.

[5] K této větě se ještě dostaneme, takže pokud nevíte o co jde, tak stačí, když mi budete věřit.
[6] Nemají žádného společného dělitele.