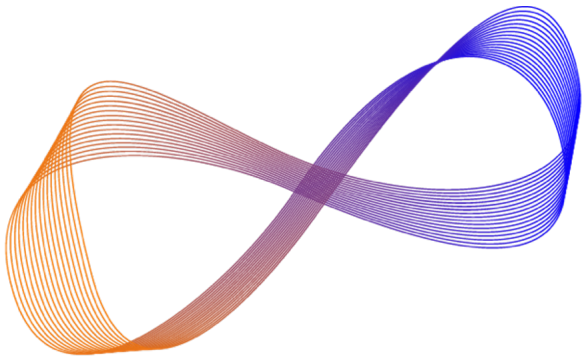
Gymnázium Evolution Jižní Město



Jakýsi úvod do matematické analýzy

Áďula vod Klepáčů

7. prosince 2023

Předmluva

Matematická analýza je věda o reálných číslech; tuším ovšem, že kolegové analytici mě za ono nedůstojně zjednodušující tvrzení rádi mít příliš nebudou. Snad mohou nicméně souhlasit, že v jejím jádru je pojem *nekonečna*. Nikoli nutně ve smyslu čísla, jež převyšuje všechna ostatní, ale spíše myšlenky, jež zaštiťuje přirozené jevy jako *okamžitá změna*, *blížení* či *kontinuum*.

O zrod matematické analýzy, jež zvláště v zámoří sluje též *kalkulus*, se bez pochyb podělili (nezávisle na sobě) Sir Isaac Newton a Gottfried Wilhelm Leibniz v 17. století po Kristu. Sir Isaac Newton se tou dobou zajímal o dráhy vesmírných těles a učinil dvě zásadní pozorování – zemská tíže působí na objekty zrychlením a zrychlení je *velikost okamžité změny* rychlosti. Potřeboval tedy metodu, jak onu velikost spočítat. Vynález takové metody po přirozeném zobecnění vede ihned na teorii tzv. *limit*, které právě tvoří srdce kalkulu. Pozoruhodné je, že Gottfried Leibniz, nejsa fyzik, dospěl ke stejným výsledkům zpytem geometrických vlastností křivek. V jistém přirozeném smyslu, který se zavazujeme rozkrýt, jsou totiž tečny *limitami* křivek. Ve sledu těchto rozdílů v přístupu obou vědců se v teoretické matematice dodnes, s mírnými úpravami, používá při studiu limit značení Leibnizovo, zatímco ve fyzice a diferenciální geometrii spíše Newtonovo.

Následující text je shrnutím – lingvistickým, vizuálním a didaktickým pozlacením – teorie limit. Hloubka i šíře této teorie ovšem přesáhla původní očekávání a kalkulus se stal součástí nespočtu matematických (samozřejmě i fyzikálních) odvětví bádání. První kapitola je věnována osvěžení nutných pojmů k pochopení textu. Pokračují pojednání o limitách posloupností a reálných číslech, limitách součtů, limitách funkcí a, konečně, derivacích. Tento sled není volen náhodně, nýbrž, kterak bude vidno, znalost předšedších kapitol je nutná k porozumění příchozích.

Jelikož se jedná o text průběžně doplňovaný a upravovaný, autor vyzývá čtenáře, by četli okem kritickým a myslí čistou, poskytovali připomínky a návrhy ke zlepšení.

Obsah

Kapitola 1

Předpoklady

Očekáváme, že čtenář je již dobře seznámen se základními pojmy teorie množin a logiky. Pro pohodlí je zde však uvedeme. Upozorňujeme však, že jejich výklad nemá za cíl být jakkolivěk podrobný či vyčerpávající.

1.1 Základní pojmy z logiky

Obyčejnou podobou matematické logiky je jazyk o

- dvou konstantách:
  - 0 (též $\bot$) – **lež**,
  - 1 (též $\top$) – **pravda**;
- dvou binárních operátorech $\wedge$ (**a**, též **konjunkce**) a $\vee$ (**nebo**, též **disjunkce**) definovaných rovnostmi
  - $(0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0)$ a $(1 \wedge 1 = 1)$,
  - $(0 \vee 0 = 0)$ a $(0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1)$.
- unárním operátoru $\neg$ (**ne** či **negace**) definovaném rovnostmi $(\neg 1 = 0)$ a $(\neg 0 = 1)$;
- proměnných;
- dvou kvantifikátorech $\forall$ (**pro všechny**, též **universální**) a $\exists$ (**existuje**, též **existenční**).

K množině binárních operátorů se často též pro praktické účely přidávají $\Rightarrow$ (**implikace**, **když ..., tak ...**) a $\Leftrightarrow$ (**ekvivalence**, **... právě tehdy, když ...**) definované rovnostmi

$$(x \Rightarrow y) = (\neg x \vee y) \quad \text{a} \quad (x \Leftrightarrow y) = ((x \Rightarrow y) \wedge (y \Rightarrow x)).$$

Užitím konstant 0 a 1 by implikace byla definována rovnostmi

$$(0 \Rightarrow 0 = 0 \Rightarrow 1 = 1 \Rightarrow 1 = 1) \quad \text{a} \quad (1 \Rightarrow 0 = 0),$$

zatímco ekvivalence rovnostmi

$$(0 \Leftrightarrow 0 = 1 \Leftrightarrow 1 = 1) \quad \text{a} \quad (0 \Leftrightarrow 1 = 1 \Leftrightarrow 0 = 0).$$

K matematické logice se též váže pojem *výroku*. Výrokem nepřesně řečeno míníme jakoukoli větu, o které lze tvrdit, že platí, nebo neplatí. Formálně se výrok definuje poněkud obtížněji a význam natolik abstraktní definice pro účely tohoto textu je přinejmenším sporný. Pochopitelně, výraz vzniklý z kratších výroků užitím logických operátorů a kvantifikátorů je rovněž výrokem.

Příklad 1.1.1

Ať x je výrok „Mám hlad.“ a y je „Jdu do hospody.“ Pak

- výrok $x \wedge y$ zní „Mám hlad a jdu do hospody.“
- výrok $x \vee y$ zní „Mám hlad nebo jdu do hospody.“
- výrok $\neg x$ zní „Nemám hlad.“ a $\neg y$ zní „Nejdu do hospody.“
- výrok $x \Rightarrow y$ zní „Když mám hlad, tak jdu do hospody.“
- výrok $x \Leftrightarrow y$ zní „Mám hlad právě tehdy, když jdu do hospody.“

Sémantická hodnota uvedených výroků se pochopitelně liší.

Varování 1.1.2

- Operátor $\vee$ **není** výlučný. To jest, výrok $x \vee y$ je pravdivý i v případě, že x je pravdivý a y je pravdivý.
- Jazykové vyjádření výroku $x \Rightarrow y$ je v mírném rozporu s běžnou intuicí. Totiž, $x \Rightarrow y$ je pravdivý, kdykoli x je lživý, neboť na základě lži nelze rozhodnout o pravdivosti žádného výroku. To znamená, že výrok „Když mám hlad, tak jdu do hospody.“ je pravdivý i tehdy, když nemám hlad, a přesto do hospody jdu.

Při zjišťování pravdivosti výroků na základě pravdivosti „elementárních výroků“ (tedy výroků, které již nelze více dělit), které je tvoří, je užitečná tzv. *pravdivostní tabulka*. Jde o tabulku, která ve sloupcích obsahuje stále složitější spojení elementárních výroků, a v posledním onen původní výrok. V řádcích pak obsahuje pravdivostní hodnoty. Není obtížné si rozmyslet, že je-li výrok složen z n elementárních výroků spojených logickými operátory, pak má jeho pravdivostní tabulka 2^n řádků – každý pro jedno možné přiřazení n pravdivostních hodnot (tj. 0 nebo 1) jeho elementárním výrokům.

Pro práci s výroky je užitečné si pamatovat (a není ani těžké si rozmyslet), že negace výroku způsobí nahrazení každého elementárního výroku jeho negací, prohození všech operátorů $\wedge$ a $\vee$ a rovněž prohození kvantifikátorů $\exists$ a $\forall$. Například

$$\neg(\exists x : (x \vee y \wedge \neg z)) = (\forall x : (\neg x \wedge \neg y \vee z)).$$

V případě implikace ($\Rightarrow$) pracujeme zkrátka s definicí a dostaneme

$$\neg(x \Rightarrow y) = (x \wedge \neg y).$$

Negovat ekvivalenci je mírně složitější, bo je konjunkcí dvou implikací. Výpočtem dostaneme

$$\begin{aligned}\neg(x \Leftrightarrow y) &= \neg((x \Rightarrow y) \wedge (y \Rightarrow x)) \\ &= (\neg(x \Rightarrow y) \vee \neg(y \Rightarrow x)) \\ &= ((x \wedge \neg y) \vee (y \wedge \neg x)).\end{aligned}$$

Ověříme si pravdivostní tabulkou na příkladě ekvivalence, že tento „selský“ přístup k negování výroků funguje (to samozřejmě **není** důkaz, že funguje obecně).

Ekvivalence $x \Leftrightarrow y$ je pravdivá tehdy, když x má stejnou hodnotu jako y. Její negace je tudíž pravdivá, když x a y nabývají hodnot opačných. Sestrojíme pravdivostní tabulku pro výrok $(x \wedge \neg y) \vee (y \wedge \neg x)$.

x	y	$\neg x$	$\neg y$	$x \wedge \neg y$	$y \wedge \neg x$	$(x \wedge \neg y) \vee (y \wedge \neg x)$
0	0	1	1	0	0	0
0	1	1	0	0	1	1
1	0	0	1	1	0	1
1	1	0	0	0	0	0

Tabulka 1.1: Pravdivostní tabulka výroku $(x \wedge \neg y) \vee (y \wedge \neg x)$.

Vidíme, že $(x \wedge \neg y) \vee (y \wedge \neg x)$ je skutečně negací ekvivalence, neboť je pravdivý přesně ve chvíli, kdy x a y mají navzájem opačné pravdivostní hodnoty.

1.2 Základní pojmy z teorie množin

Teorie množin tvoří společně s logikou základ moderní matematiky. Jedno možné přirovnání je, že množiny tvoří svět, který lze zkoumat pomocí logiky. Pojem „množina“ (podobně jako i „pravda“ a „lež“ v logice) není možné v teorii množin definovat, poněvadž je její základní stavební jednotkou. Stejně jako všechny teorie současné matematiky je i teorie množin definována *axiomaticky*. Axiomy jsou logické výroky, které v dané teorii nelze dokázat, a jsou a priori označeny za pravdivé. Jsou vlastně jakousi matematickou verzí zázraku. Přestože znalost a porozumění axiomům teorie množin se považuje za základ matematického vzdělání, jejich podoba je tomuto textu irelevantní a zmiňovat je nebudeme. Snad kromě toho prvního, asi nejpřirozenějšího možného – „Existuje množina“.

Intuitivně asi každý matematik přemýšlí o množinách jako o souborech prvků, které spolu nějakým způsobem souvisejí. Fakt, že prvek x je součástí množiny A, zapisujeme jako $x \in A$ a čteme „x náleží/je prvkem A“ (symbol $\in$ je pochroumané *e* v angl. slově **e**lement). Když B je množina, jejíž každý prvek leží rovněž v A, pak píšeme $B \subseteq A$ a čteme tento výrok jako „B je podmnožinou A“ (případně „A je nadmnožinou B“). Pomocí symbolu náležení ($\in$) lze tento vztah též logicky vyjádřit jako

$$(B \subseteq A) \Leftrightarrow (x \in B \Rightarrow x \in A),$$

tedy výrokem „Když x je prvkem B, pak x je prvkem A.“

Naopak, fakt, že y *není* prvkem A, nezapisujeme krkolomně $\neg(y \in A)$, nýbrž zkrátka $y \notin A$, a fakt, že C *není* podmnožinou A, nepřekvapivě jako $C \nsubseteq A$. Potřebujeme-li zdůraznit, že C je podmnožinou A, ale není celou množinou A, píšeme $C \subsetneq A$.

Varování 1.2.1

Mnoho začínajících matematiků pěstuje slabě nepřesnou intuici o pojmu množiny. Totiž, množinu lze vnímat jako soubor prvků; není však radno chovat představu, že tyto prvky mají uvnitř množiny nějaké „umístění“ či „pořadí“ nebo „četnost“ či „počet výskytů“. Že řada lidí z počátku přisuzuje množinám a jejich prvkům tyto vlastnosti, je vrub na úsudku velmi přirozený.

Množina jako taková je koncept, který nemá přesný ekvivalent ve světě vnímaném smysly. Na kupce sena vždy dokážeme říct, které stéblo je nahoře a které dole; rozlišujeme, zda máme v lednici deset pivo nebo jedno. V množině nikolivěk.

Existuje speciální množina, $\emptyset$, jíž říkáme *prázdná*, nemajíc z definice žádný prvek. Jako názorný příklad užití universálního kvantifikátoru lze za definici prázdné množiny považovat výrok

$$\forall x : x \notin \emptyset.$$

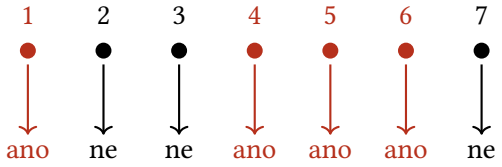
Je dobré si povšimnout, že $\emptyset$ je z definice podmnožinou každé množiny. Totiž, $x \in \emptyset$ je výrok vždy lživý a, pamatujte, ze lži plyne (aspoň v matematické logice) jak lež, tak pravda. Tedy, výrok $x \in \emptyset \implies x \in A$ je vždy pravdivý. Filosofickou otázku, zda dává smysl, že „nic“ je vždy součástí „něčeho“, s lehkým srdcem přenecháváme kroužkům nadšených bakalantů teologické fakulty.

Podobně, množina je též vždy svojí vlastní podmnožinou, neboť výrok $x \in A \implies x \in A$ je rovněž vždy pravdivý. Speciálně, každá množina kromě prázdné má přinejmenším dvě podmnožiny – prázdnou množinu a sebe samu. Snad pichlavější otázku, zda dává smysl, že každá věc je svou vlastní součástí, s lehkým srdcem přenecháváme doktorandům teologické fakulty.

Velikostí množiny A myslíme (v intuitivním smyslu) počet jejích prvků a zapisujeme ji $\#A$. Je-li A nekonečná, píšeme výmluvně $\#A = \infty$. Často je též užitečné přemýšlet o všech podmnožinách dané množiny rovněž jako o množině. Značíme ji jako 2^A. Za původem tohoto značení stojí fakt, že má-li A n prvků, pak má 2^n podmnožin. Totiž, představme si například všechny prvky A seřazené nějak náhodně za sebou. Libovolnou podmnožinu A získám tak, že začnu s prázdnou „krabicí“ a u každého prvku se postupně rozhodnu, zda jej do ní „hodím“, či ne. Pro každý prvek mám 2 možnosti, proto celkově pro n prvků mám

$$\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n-\text{krát}}$$

možností, jak vyrobit unikátní podmnožinu. Symbolicky můžeme psát $\#2^A = 2^{\#A}$.



Obrázek 1.1: Výběr podmnožiny $\{1, 4, 5, 6\}$ z množiny $\{1, 2, 3, 4, 5, 6, 7\}$.

1.2.1 Množinové operace

Podobně jako na výrocích, i na množinách lze provádět různé operace. V rámci jejich vnímání jako *souborů* je přirozené, že takové soubory umíme slučovat, oddělovat a vybírat z více souborů pouze prvky jim všem společné. Tyto tři základní množinové operace se zde jmeme připomenout.

Jsou-li A, B množiny, pak

- *sjednocením* A a B, zapsaným $A \cup B$, myslíme množinu, která obsahuje prvky ležící aspoň v jedné z těchto množin; logicky, $A \cup B$ je množina splňující výrok

$$(x \in A \cup B) \Leftrightarrow (x \in A \vee x \in B).$$

(a) Množiny A a B. (b) Sjednocení $A \cup B$.

Obrázek 1.2: Operace sjednocení množin.

- *průnikem* A a B, zapsaným $A \cap B$, myslíme množinu obsahující pouze prvky ležící v obou množinách; logicky, $A \cap B$ je množina splňující

$$(x \in A \cap B) \Leftrightarrow (x \in A \wedge x \in B).$$

(a) Množiny A a B. (b) Průnik $A \cap B$.

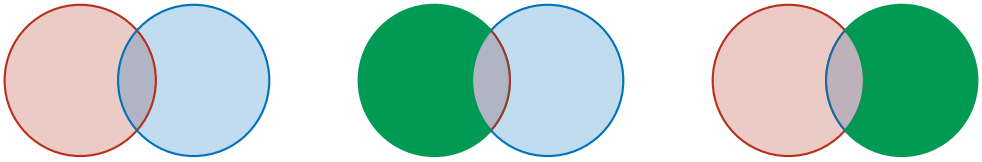
Obrázek 1.3: Operace průniku množin.

- *rozdílem* A a B, zapsaným $A \setminus B$, myslíme množinu obsahující prvky ležící v A, které však neleží v B; logicky, $A \setminus B$ je množina splňující

$$(x \in A \setminus B) \Leftrightarrow (x \in A \wedge x \notin B).$$

  Je dobré dbát faktu, že $A \setminus B$ a $B \setminus A$ jsou obecně **různé** množiny.

Operace sjednocení a průniku mají své „hromadné“ varianty, tedy sjednocení a průnik většího (klidně nekonečného) počtu množin. V případech jako je tento, kdy potřebujeme provádět operace na libovolném množství objektů, se často užívá pomocné množiny, tzv. *množiny indexů*, která slouží jen k tomu, aby jednotlivé objekty v operované skupině od sebe odlišovala.



(a) Množiny A a B. (b) Rozdíl $A \setminus B$. (c) Rozdíl $B \setminus A$.

Obrázek 1.4: Operace rozdílu množin.

Konkrétně, zápisem

$$\bigcup_{i\in I} A_i, \text{ resp. } \bigcap_{i\in I} A_i,$$

myslíme množinu, která obsahuje prvky, které leží aspoň v jedné, resp. v každé, z množin A_i, $i \in I$, kde I je libovolná množina indexů. K formální logické definici je třeba použít kvantifikátorů, neboť množina I nemusí mít konečně prvků. Definujeme

$$(x \in \bigcup_{i\in I} A_i) \Leftrightarrow (\exists i \in I : x \in A_i)$$

a

$$(x \in \bigcap_{i\in I} A_i) \Leftrightarrow (\forall i \in I : x \in A_i).$$

Tyto definice jsou původem matematické pranostiky „Existenční kvantifikátor je sjednocení a universální kvantifikátor je průnik.“

Ve speciálním případě, kdy $I = \{1, \ldots, n\}$ je množina přirozených čísel od 1 do n, se také užívá zápisů

$$\bigcup_{i=1}^{n} A_i \quad \text{a} \quad \bigcap_{i=1}^{n} A_i.$$

Není obtížné si uvědomit, že pro rozdíl taková definice není možná, neboť u rozdílu množin záleží na jejich pořadí a, opakujeme (vizte výstrahu 1.2.1), množina indexů I *neurčuje pořadí*, v kterém se množiny A_i sjednocují či pronikají.

Dalším oblíbeným způsobem zápisu těchto operací, především v teorii kategorií, je $\bigcup \mathcal{A}$ a $\bigcap \mathcal{A}$, kde $\mathcal{A} \coloneqq \{A_i \mid i \in I\}$ je pomocná množina všech množin $A_i, i \in I$. **Pozor!** Množina $\mathcal{A}$ není v žádném smyslu sjednocením množin A_i; je to množina, která má za prvky ony samotné množiny A_i, ne jejich prvky. Obecně, žádný prvek žádné množiny A_i není zároveň prvkem $\mathcal{A}$, speciálně A_i obecně **nejsou** podmnožiny $\mathcal{A}$.

1.2.2 Kartézský součin a uspořádané n-tice

Anobrž holý pojem množiny neobsahuje v žádném smyslu koncept *pořadí* prvku, je tento však pochopitelně užitečný, a proto si jej definujeme.

Zápisem (x, y) myslíme tzv. *uspořádanou dvojici* prvků x a y. V této dvojici je x prvním prvkem a y druhým. Je proto odlišná od množiny $\{x, y\}$, protože $\{x, y\} = \{y, x\}$, ale $(x, y) \neq (y, x)$. V úvodu do této kapitoly jsme tvrdili, že teorie množin tvoří svět matematiky. Pojem *dvojice*, který není shodný s pojmem *množiny* tudíž musel bedlivé čtenáře vylekat. Darmo se však lekati, uspořádané

dvojice jsou rovněž množiny. Než jej odhalíme, vybízíme čtenáře, aby našli způsob, kterak definovat uspořádanou dvojici jako množinu.

Běžně užívaná definice (prve formulována Kazimierzem Kuratowskim) je

$$(x, y) \coloneqq \{\{x\}, \{x, y\}\}.$$

Ta říká, že uspořádaná dvojice (x, y) je vlastně množina obsahující množinu s jediným prvkem x a množinu $\{x, y\}$. Ta je pak rozdílná od dvojice (y, x), což je množina $\{\{y\}, \{x, y\}\}$. Tato definice je z formálního hlediska nutná, protože vytvářet matematické objekty nedefinovatelné v teorii množin rodí chaos, ale intuitivně zcela nepoužitelná. Představme si dva lidi za sebou ve frontě vnímat jako skupinu, v níž je skupina jenom s tím prvním a pak ještě skupina obou. Tvrdíme, že je dobré udržet si pročež představu uspořádané dvojice jakožto množiny, ve které mají navíc prvky svá pořadí.

Definice uspořádané dvojice se rekurzivně rozšíří na libovolný počet prvků. Kupříkladu, uspořádanou trojici definujeme předpisem

$$(x, y, z) \coloneqq (x, (y, z)),$$

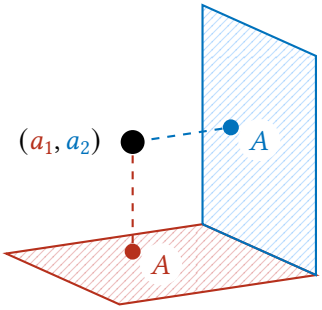
to jest jako uspořádanou dvojici obsahující prvek x a uspořádanou dvojici (y, z). Zápis pomocí množin se s rostoucím počtem prvků velmi rychle komplikuje. Všimněte si, že už v drobném případě tří prvků dostaneme

$$(x, y, z) = (x, (y, z)) = (x, \{\{y\}, \{y, z\}\}) = \{\{x\}, \{x, \{\{y\}, \{y, z\}\}\}\}.$$

Máme-li n prvků $x_1, \ldots, x_n$, pak jejich uspořádanou n-tici zapisujeme $(x_1, \ldots, x_n)$.

Existence uspořádaných n-tic dává vzniknout jedné další množinové operaci – kartézskému součinu. Kartézský součin dvou množin A, B, zapsaný $A \times B$, definujeme jako množinu všech uspořádaných dvojic (a, b), kde $a \in A$ a $b \in B$. Název *kartézský* (po Reném Descartesovi) ona nese pro zřejmou souvislost se stejnojmenným systémem souřadnic. Totiž, souřadnice v rovině jsou přesně dvojice $(x, y) \in \mathbb{R} \times \mathbb{R}$, kde $\mathbb{R}$ značí množinu reálných čísel.

Rovina skýtá navíc užitečný způsob přemýšlení o kartézském součinu jako o „dimenzní“ operaci. Má-li totiž A dimenzi (v intuitivním slova smyslu) n a B dimenzi m, pak $A \times B$ má dimenzi $n + m$. Například, je-li A čtverec o délce strany 1, pak $A^2 = A \times A$ je krychle o délce strany 1.



Obrázek 1.5: Vizualizace kartézského součinu $A \times A$.

Jakož tomu bylo i v případě sjednocení a průniku, lze definovat kartézský součin více množin než dvou. Zde je však dlužen zřetel – u kartézského součinu rovněž (jako u rozdílu) záleží na pořadí

násobení množin. Není možné definovat kartézský součin množin A_i pro libovolnou množinu indexů I, ale pouze pro množinu *uspořádanou* (tento pojem rovněž posléze připomeneme). Pro teď budeme předpokládat, že $I = \{1, \dots, n\}$ a zápisem

$$\prod_{i=1}^{n} A_i$$

myslet množinu uspořádaných n-tic $(a_1, \dots, a_n)$, kde $a_i \in A_i$ pro každé $i \in \{1, \dots, n\}$. Kartézský součin nekonečného množství množin lze též definovat, ano akt to není přímočarý a naší věci zatím zbytečný.

Jsou-li všechny A_i, $i \in \{1, \dots, n\}$, vskutku jednou množinou, A, ujalo se – poněkud přirozeně – pro jejich kartézský součin mocninné značení. To jest,

$$A^n \coloneqq \prod_{i=1}^{n} A.$$

1.2.3 Relace

Relace, jak jejich název snad napovídá, jsou množiny, které kódují *vztahy* mezi prvky dvou různých množin. Jejich matematické pojetí je přímočaré a elegantní, ano trochu neintuitivní. Totiž, relace (či „vztah“) je zkrátka jen výpis prvků, které v něm jsou, nikoli žádný nezávislý popis jeho vlastností. Musíme-li načrtnout sociální rovnoběžku, můžeme si představit, že význam vztahu přátelství je přesně určen seznamem všech párů přátel. I když ona rovnoběžka vzbudila v mnohých čtenářích jistě značnou nedůvěru, taková definice vztahu v matematice je jednoduchá a téměř nesrovnatelně užitečná.

Definice 1.2.2 (Relace)

Ať A, B jsou množiny. *Relací* R mezi A a B míníme kteroukoli podmnožinu $R \subseteq A \times B$.

Milí čtenáři se již jistě s několika relacemi setkali. Například samotný vztah rovnosti ($=$) je relací. Podobně, vztahy „býti menší nebo rovno“ ($\leq$) či „býti ostře větší“ ($>$) jsou relacemi ve všech číselných oborech. Jak tyto příklady naznačují, historicky se symboly relací píšou obvykle *mezi* prvky v oné relaci jsoucí. Tohoto úzu se držíme i my a pro relaci $R \subseteq A \times B$ píšeme aRb, kdykoli $(a, b) \in R$. Jelikož je však zápis $a \not R b$ poněkud neuhlazený a nadevše obtížně rozpoznatelný od svého pozitivního protipólu, používáme množinové značení $(a, b) \notin R$, kdykoli prvek a není v relaci R s prvkem b.

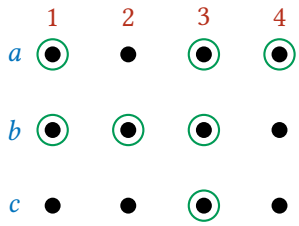
Máme-li k dispozici výčty prvků množin A a B, je pro představu dobré kreslit relace $R \subseteq A \times B$ do tzv. mříží. Ty tvoříme tak, že nakreslíme doslovnou mříž teček s $\#A$ sloupci, resp. $\#B$ řádky, pro každý prvek množiny A, resp. množiny B, a tečky na pozicích odpovídající párům $(a, b) \in A \times B$, které rovněž leží v R, například kroužkujeme. Zvolíme-li třeba

$$A = \{1, 2, 3, 4\}, B = \{a, b, c\}$$

a mezi nimi relaci

$$R = \{(1, a), (1, b), (2, b), (3, a), (3, b), (3, c), (4, a)\},$$

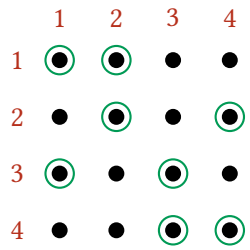
bude jejím vyobrazením mříž na obrázku 1.6.



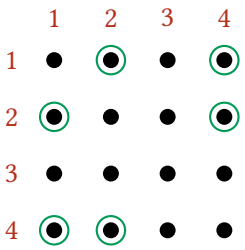
Obrázek 1.6: Mříž relace $R \subseteq A \times B$.

Relace zvláště zásadního významu jsou ty mezi dvěma totožnými množinami. Je-li R relace mezi A a A říkáme, výrazně lidštěji, že R je relace *na* A. U relací na množině stavíme na piedestal ty s jistými speciálními vlastnostmi. Konkrétně, řekneme, že relace $R \subseteq A \times A$ je

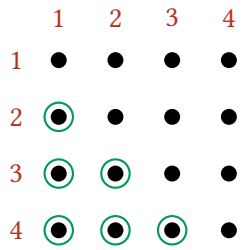
- *reflexivní*, když je každý prvek v relaci R sám se sebou, tj. $\forall x \in A : xRx$;
- *antireflexivní*, když žádný prvek není v relaci R sám se sebou, tj. $\forall x : (x, x) \notin R$;
- *symetrická*, když s každým párem prvků obsahuje i ten obrácený, tj. $\forall x, y \in A : xRy \Rightarrow yRx$;
- *antisymetrická*, když z každého páru dvojic (x, y) a (y, x) je v R vždy jen jedna, tj. $\forall x, y \in A : xRy \Rightarrow (y, x) \notin R$ (všimněme si, že antisymetrická relace je automaticky antireflexivní);
- ***slabě** antisymetrická*, když z každého páru dvojic (x, y) a (y, x) je v R vždy jen jedna za předpokladu, že x a y jsou od sebe různé, tj. $\forall x, y \in A : (xRy \wedge yRx) \Rightarrow (x = y)$;
- *transitivní*, když se přirozeně „přenáší“ přes prostřední prvek, tj. $\forall x, y, z \in A : (xRy \wedge yRz) \Rightarrow xRz$.



(a) Reflexivní a slabě antisymetrická, nikoli transitivní.



(b) Antireflexivní, symetrická a transitivní.



(c) Antisymetrická a transitivní (též *ostré uspořádání*, zde $<$).

Obrázek 1.7: Příklady relací R na množině $A = \{1, 2, 3, 4\}$.

Naprosto klíčovými typy relací pro rozvoj další teorie jsou *ekvivalence*, *uspořádání* a *zobrazení*. Každému typu je věnována jedna z následujících sekcí.

1.2.4 Relace ekvivalence

Ekvivalence je relací na množině, která umožňuje dělit ji na části tvořené ve smyslu daném touto relací „stejnými“/ekvivalentními prvky. Ačkoliv formálně nemá *relace* ekvivalence nic společného s *logickou operací* ekvivalence, důvody pro jejich jména souhlasí. Totiž, *logická* ekvivalence spojuje dva výroky, které jsou v pravdivostním smyslu stejné, a *relační* ekvivalence spojuje dva prvky množiny, které rovněž chceme (v daném kontextu) považovat za totožné.

Definice 1.2.3 (Relace ekvivalence)

Relaci R na množině A nazveme *ekvivalencí*, pokud je

- reflexivní ($\forall x \in A : xRx$),
- symetrická ($\forall x, y \in A : xRy \Rightarrow yRx$),
- transitivní ($\forall x, y, z \in A : (xRy \wedge yRz) \Rightarrow xRz$).

Spěšně si rozmyslíme smysluplnost této definice. Řekněme, že zkoumáme určité vlastnosti lidí v závislosti na jejich věku. Při takovéto studii pochopitelně uvažujeme o dvou různých lidech stejného věku jako o „totožných" subjektech. Je samozřejmé, že dva skutečně stejné lidi považujeme za totožné (to vysvětluje *reflexivitu*). Podobně, když je člověk *Jáchym* stejně starý jako člověk *Eric*, pak je i *Eric* stejně starý jako *Jáchym* (to vysvětluje *symetrii*). Konečně, když je člověk *Lenin* stejně starý jako člověk *Stalin* a *Stalin* je stejně starý jako *Trotsky*, pak je přirozeně *Lenin* stejně starý jako *Trotsky* (to vysvětluje *transitivitu*).

Díky relaci „býti stejného věku" můžeme nyní rozdělit množinu všech lidí na Zemi na 122 (nejstarší zaznamenaný lidský věk) chlívků; v každém chlívku všichni lidé stejně staří. Těmto „chlívkům" se v matematice přezdívá *třídy ekvivalence*. Třídy ekvivalence R na množině A jsou podmnožiny A, kde v každé podmnožině jsou přesně jen ty prvky, které jsou spolu v relaci R.

Definice 1.2.4 (Třída ekvivalence)

Ať A je množina a R ekvivalence na A. Vezměme $x \in A$. *Třídou ekvivalence* prvku x podle R, zapsanou $[x]_R$, myslíme množinu

$$[x]_R \coloneqq \{y \in A \mid xRy\}$$

všech prvků $y \in A$ v relaci R s x. O podmnožině $X \subseteq A$ řekneme, že je to *třída ekvivalence* A podle R, když existuje prvek $x \in A$ takový, že $X = [x]_R$.

Jak lze snadno vyčíst z příkladu studie vlastností lidí stejného věku, každý člověk je v právě jednom chlívku/třídě ekvivalence (jednomu člověku nemůže být různý počet let, metabolický věk ignorujeme) a navíc každý člověk je nutně v některém. Vladouce jazykem matematiky řčeme, že třídy ekvivalence dvou prvků jsou buď stejné (oba lidé v témž chlívku), nebo disjunktní (každý člověk v různém chlívku). Navíc, sjednocením všech tříd ekvivalence dostaneme původní množinu A, stejně jako spojením všech chlívků dostaneme jeden velký chlév s batolaty i kmety na jedné hromadě. Tento fakt je platný pro každou ekvivalenci a je oním klíčovým důvodem užitečnosti tohoto konceptu.

Tvrzení 1.2.5 (O třídách ekvivalence)

Ať R je ekvivalence na A a X, Y jsou třídy ekvivalence A podle R. Pak buď $X = Y$, nebo $X \cap Y = \emptyset$. Navíc, je-li

$$\mathcal{X} \coloneqq \{X \subseteq A \mid X \text{ třída ekvivalence } A \text{ podle } R\}$$

množina všech (podle předchozí věty navzájem disjunktních) tříd ekvivalence množiny A podle R, pak

$$A = \bigcup \mathcal{X}.$$

Pro nějaký číselný příklad relace ekvivalence – jenž zároveň ukazuje, že tříd ekvivalence nemusí být konečně mnoho – uvažme třeba relaci „býti mocninou“ na přirozených číslech. Řekneme, že číslo $n \in \mathbb{N}$ je *mocninou* $m \in N$, když existuje kladné **racionální** (abychom mohli uvažovat i odmocniny) číslo q takové, že $n = m^q$. Taková relace je jistě ekvivalence, neboť

- $\forall n \in \mathbb{N} : n = n^1$, tedy každé číslo je svou vlastní mocninou (reflexivita);
- když $n = m^q$, pak $m = n^{\frac{1}{q}}$, čili předpoklad, že n je mocninou m, implikuje, že m je mocninou n (symetrie);
- když $n = m^{q_1}$ a $m = l^{q_2}$, pak $n = l^{q_1 q_2}$, čili pokud je n mocninou m a m mocninou l, pak n je mocninou l (transitivita).

Obrázek 1.8 zobrazuje prvních několik tříd ekvivalence „býti mocninou“ na množině přirozených čísel.

1	2 4 8 ⋮	3 9 27 ⋮	5 25 125 ⋮	...

Obrázek 1.8: Třídy ekvivalence „býti mocninou“ na $\mathbb{N}$.

1.2.5 Relace uspořádání

V úvodu do této sekce jsme zdůraznili fakt, že množiny **nejsou** v žádném smyslu uspořádané, tedy nelze o jejich prvcích tvrdit, který jde první a poslední. Ovšem, čtenáři jsou si jistě vědomi, že kupříkladu přirozená čísla uspořádána *jsou* – číslo 1 je menší než číslo 5, 8 větší než 3. Tento výrok je však mírně nepřesný. Samotná množina přirozených čísel uspořádaná *není*, lze na ní však definovat jistý všudypřítomný typ relace (v tomto případě $\leq$) zvaný *uspořádání*. Definujeme si, které vlastnosti musí relace uspořádání na množině mít.

Definice 1.2.6 (Relace uspořádání)

Ať A je množina a $R \subseteq A \times A$ je relace na A. Řekneme, že R je *uspořádání* (někdy též nesoucí přívlastek *neostré*), když je

- reflexivní (tj. $\forall x \in A : xRx$),
- slabě antisymetrické (tj. $\forall x, y \in A : (xRy \wedge yRx) \Rightarrow (x = y)$),
- transitivní (tj. $\forall x, y, z \in A : (xRy \wedge yRz) \Rightarrow xRz$).

Je-li naopak R (silně) antisymetrické (tj. $\forall x, y \in A : xRy \Rightarrow (y, x) \notin R$), a tudíž antireflexivní (tj. $\forall x \in A : (x, x) \notin R$), řekneme, že je R ***ostré*** *uspořádání*.

Je-li A množina a R (ostré) uspořádání na A, říkáme, že dvojice (A, R) je *(ostře) uspořádaná množina* (podle R).

Zcela nejobyčejnější příklady (neostrých) uspořádání jsou relace $\leq$ a $\geq$ v číselných oborech. Vskutku, každý prvek je menší/větší nebo roven sám sobě, z každé dvojice prvek je buď jeden menší/větší

než ten druhý, nebo jsou stejné, a když je prvek x menší/větší než prvek y a ten zas menší/větší než prvek z, pak je x menší/větší než z. Speciálně, $(\mathbb{N}, \leq)$ a $(\mathbb{N}, \geq)$ jsou uspořádané množiny.

Příkladem *ostrých* uspořádání jsou relace $<$ a $>$, které se liší tím, že žádný prvek není ostře menší/větší než on sám.

Varování 1.2.7

Součástí definice uspořádání **není** podmínka, že **každé** dva prvky lze spolu porovnat. Pročež, v uspořádaných množinách obecně existují dvojice prvků, kde první není ani menší ani větší než ten druhý.

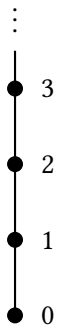
Uspořádáním (ať už ostrým či neostrým) naopak *splňujícím* onu podmínku říkáme *lineární*.

Za definicí uspořádání samozřejmě stojí myšlenka, že taková relace určuje *pořadí* prvků na množině. Z toho důvodu se obvykle uspořádání nekreslí jako obecné relace do mříží, ale do tzv. Hasseho (po číselném teoretiku Helmutu Hassem) diagramů, které získáme tím způsobem, že prvky nakreslíme jako puntíky a každé dva puntíky prvků, které jsou v daném uspořádání porovnatelné, spojíme úsečkou (nejsou-li již spojeny přes nějaký další puntík) a větší z nich nakreslíme nad menší. Chováme na vědomí, že kreslit obrázky je více uspokojující, než je popisovat, a tedy si závěrem této krátké sekce nakreslíme (Hasseho diagramy) tři takřkouce „učebnicové“ příklady uspořádání.

Příklad 1.2.8

(1) Uvažme jednoduchý příklad uspořádané množiny $(\mathbb{N}, \leq)$. Už jsme si rozmysleli, že $\leq$ je na $\mathbb{N}$ skutečně uspořádáním. Je triviální nahlédnout, že je rovněž lineární, neboť z každých dvou přirozených čísel lze vybrat to menší.

Lineární uspořádání mají velmi nezajímavý Hasseho diagram – řetěz prvků, který může končit nahoře nebo dole. V tomto případě je nejmenším prvkem 0 a nejvyšší neexistuje, tedy řetěz pokračuje nekonečně dlouho směrem nahoru.

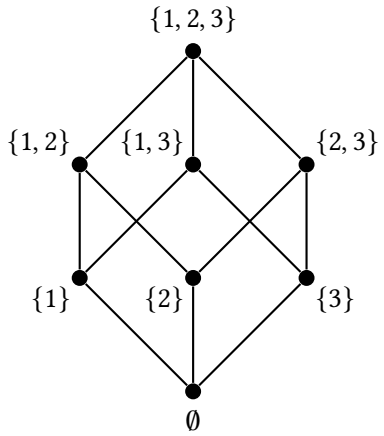


Obrázek 1.9: Hasseho diagram uspořádané množiny $(\mathbb{N}, \leq)$.

(2) O něco komplikovanější příklad je uspořádání inkluzí $\subseteq$. Pro libovolnou množinu A můžeme uvážit uspořádanou množinu $(2^A, \subseteq)$. Je téměř samozřejmé, že $\subseteq$ je skutečně (neostré) uspořádání, které však **není** lineární. Vizme příklad.

Ať $A \coloneqq \{1, 2, 3\}$. Pak jsou její podmnožiny $\{1, 2\}$ a $\{2, 3\}$ neporovnatelné pomocí $\subseteq$ – ani jedna není podmnožinou té druhé. Zajímavým geometrickým faktem je, že Hasseho

diagramem $(2^A, \subseteq)$ pro n-prvkovou množinu A je síť vrcholů krychle dimenze n.



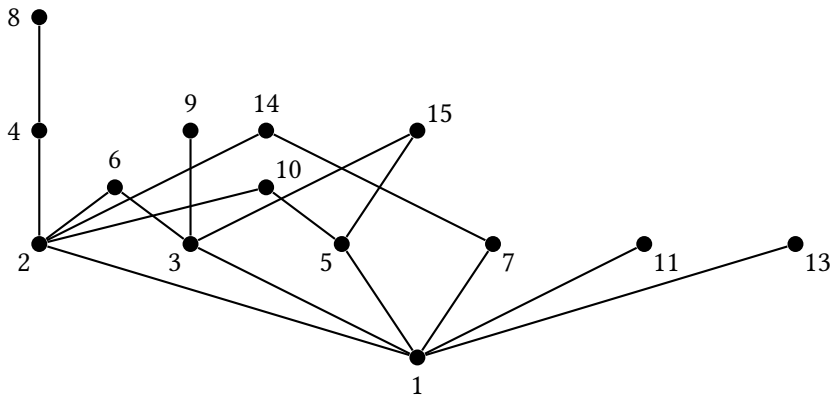
Obrázek 1.10: Hasseho diagram uspořádané množiny $(2^A, \subseteq)$ pro $A = \{1, 2, 3\}$.

(3) Poněkud méně pravidelný příklad než oba předchozí je uspořádání na přirozených číslech *dělitelností*. Dělitelnost jednoho přirozeného čísla jiným se definuje samozřejmě. Řekneme, že n *dělí* m, píšeme $n \mid m$, když existuje přirozené číslo k splňující $m = kn$. Kupříkladu $3 \mid 6$, protože existuje přirozené číslo – konkrétně 2 – takové, že $6 = 2 \cdot 3$.

Nyní, povšimněme sobě, že $\mid$ je uspořádání na $\mathbb{N}$. Vskutku, zřejmě každé číslo dělí samo sebe. Když n dělí m a m dělí n, pak jde nutně o téže číslo. Konečně, když n dělí m a m dělí l, pak v podstatě triviálně n dělí l. Nejde však jistě o uspořádání lineární, neboť například číslo 3 nedělí číslo 10 ani obráceně.

Uspořádání dělitelností na $\mathbb{N}$ má Hasseho diagram, který je nekonečný jak do šířky, tak do výšky. Totiž, žádné prvočíslo není dělitelné žádným číslem, které šlo před ním (pouze 1), a tedy je musíme umístit do druhé řady (nad 1) vedle ostatních prvočísel. Do výšky stoupá nekonečně pro to, že když spolu vynásobíme dvě čísla k-té úrovně, dostaneme číslo úrovně $(k + 1)$-ní.

Pro jednoduchost se spokojíme s Hasseho diagramem množiny přirozených čísel od 1 do 15 uspořádané relací dělitelnosti.



Obrázek 1.11: Hasseho diagram uspořádané množiny $(\{1, 2, \ldots, 15\}, \mid)$.

1.2.6 Relace zobrazení

Přišel na řadu poslední klíčový typ relace, a pro algebraika snad nejdůležitější myšlenka matematiky vůbec. Na rozdíl od relací uspořádání a ekvivalence, není zobrazení nutně relace na téže množině. Jak název napovídá, zobrazení má něco někam ... „zobrazovat“. Matematik zřídkakdy přemýšlí o zobrazení jako o relaci, nýbrž o popisu způsobu, kterak se prvky jedné množiny „přetvářejí v“ či „zobrazují na“ prvky množiny druhé.

Zobrazení je dáno vlastně jednou přímočarou podmínkou – každý prvek první množiny se může zobrazit na maximálně jeden prvek množiny druhé. Lidově řečeno, není prvku povoleno, aby se rozdvojil, roztřetil, rozčtvrtil, rozpětil, rozšestil, rozsedmil, rozosmil, rozdevítil a indukcí dále.

Ať tedy R je relace mezi A a B. Elegantním logickým zápisem podmínky, aby byl každý prvek $a \in A$ v relaci R s *maximálně jedním* prvkem $b \in B$, je výrok, že jsou-li dva prvky z A v relaci s týmž prvkem z B, pak se vskutku jedná o jediný prvek. Formální definice následuje.

Definice 1.2.9 (Zobrazení)

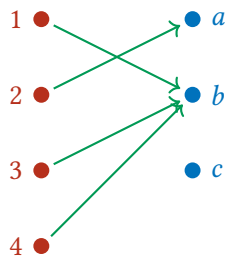
Ať $R \subseteq A \times B$ je relace mezi A a B. Nazveme R *zobrazením* (z A do B), pokud splňuje

$$\forall a_1, a_2 \in A\ \forall b \in B : a_1 R b \wedge a_2 R b \Rightarrow a_1 = a_2.$$

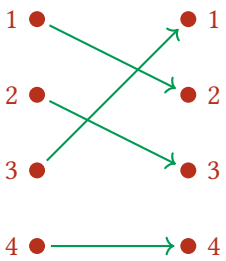
Zobrazení mezi množinami obvykle zapisujeme malými písmeny latinské abecedy počínaje písmenem f (od **f**unkce, jak se některým speciálním typům zobrazení často říká). Fakt, že f je zobrazení z A do B, symbolizujeme zápisem $f : A \to B$ nebo též $A \xrightarrow{f} B$.

Když $(a, b) \in f$, nepíšeme afb jako u obecné relace, ale spíše $f(a) = b$ či $f : a \mapsto b$.

Stejně jako uspořádání, i zobrazení se kreslí svým osobitým způsobem, který v sobě nese jejich mimořádnou povahu. Protože, opakujeme, bývají zobrazení vnímána vlastně jako „šipky“ mezi množinami nesoucí prvky z první do té druhé, i se tak kreslí. Konkrétně, zobrazení $f : A \to B$ nakreslíme například tak, že si prvky A postavíme nalevo, prvky B napravo, a pro každý vztah $f(a) = b$ nakreslíme šipku z a do b. Z definici zobrazení povede z každého $a \in A$ nejvýše jedna šipka. Vizte obrázek 1.12.



(a) Zobrazení $f = \{(1, b), (2, a), (3, b), (4, b)\}$.



(b) Zobrazení $g = \{(1, 2), (2, 3), (3, 1), (4, 4)\}$. Zobrazením „prohazujícím“ prvky na množině se říká *permutace*.

Obrázek 1.12: Příklady zobrazení.

K zobrazením se tokem historie navázaly přehoušle názvosloví. Zopakujeme je zde, bo pěstujeme zámysl je v dalším textu bez výstrah dštíti.

Ať f do konce sekce značí zobrazení $A \to B$. Množinu A nazýváme *doménou* zobrazení f, značíme $\operatorname{dom} f$, a množinu B jeho *kodoménou*, značíme $\operatorname{codom} f$. Množinu všech prvků z B, na které se zobrazuje nějaký prvek z A, nazýváme *obrazem* f, značíme $\operatorname{im} f$. Formálně

$$\operatorname{im} f \coloneqq \{b \in B \mid \exists a \in A : f(a) = b\}.$$

Triviálně platí $\operatorname{im} f \subseteq \operatorname{codom} f$, ale tyto množiny nemusejí být stejné. Například, zobrazení f z obrázku 1.12a má obraz $\{a, b\}$, ale kodoménu celou množinu $\{a, b, c\}$.

Pro každý prvek $b \in \operatorname{codom} f$ definujeme jeho *vzor* (při zobrazení f), značíme $f^{-1}(b)$, jako množinu **všech** prvků z A, které se na něj zobrazují. Formálně, pro $b \in \operatorname{codom} f$

$$f^{-1}(b) \coloneqq \{a \in A \mid f(a) = b\}.$$

Triviálně $f^{-1}(b) \subseteq \operatorname{dom} f$ pro každé $b \in \operatorname{codom} f$, ale tyto množiny jistě mohou být různé. Pro zobrazení f z obrázku 1.12a platí $f^{-1}(b) = \{1, 2, 4\}$ a $f^{-1}(c) = \emptyset$ a pro zobrazení g z obrázku 1.12b platí $g^{-1}(2) = \{1\}$. Přestože je vzor prvku při zobrazení oficiálně **množina**, budeme v případech jako byl tento poslední, kdy je vzorem množina jednoprvková, psát většinou $g^{-1}(2) = 1$ a tvrdit, že prvek 1 je *vzorem* prvku 2 při zobrazení g.

Sekci završíme zopakováním speciálních typů zobrazení. Říkáme, že zobrazení $f : A \to B$ je

- *prosté* (či *injektivní*), když na každý prvek B zobrazuje nejvýše jeden prvek A. Formálně lze psát, že
$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$
Ekvivalentně můžeme tvrdit, že zobrazení je prosté, když $f^{-1}(b)$ má nejvýš jeden prvek pro každé $b \in B$ a, **je-li** A **konečná**, pak je prostota f vyjádřena též v podmínce $\#\operatorname{im} f = \#A$. Nabádáme čtenáře, aby si ekvivalenci těchto výroků rozmysleli. Symbolicky budeme občas zapisovat prostá zobrazení jako $f : A \hookrightarrow B$.

- *na* (či *surjektivní*), když na každý prvek B zobrazuje nějaký prvek A. Formálně lze psát, že
$$\forall b \in B\ \exists a \in A : f(a) = b.$$
Ekvivalentně je f na, když $f^{-1}(b)$ není prázdná pro žádný prvek $b \in B$ anebo, **ať už je** B **konečná či ne**, když $\operatorname{im} f = B$. Opět nabádáme čtenáře k ověření této ekvivalence. Symbolicky budeme občas zapisovat surjektivní zobrazení jako $f : A \twoheadrightarrow B$.

- *vzájemně jednoznačné* (též *bijektivní*), když je prosté i na. Množiny, mezi kterými existuje bijektivní zobrazení, lze v mnoha situacích považovat za stejné, neboť mají vlastně tytéž prvky, akorát pod jinými „jmény“. Z ekvivalentních definic prostých a surjektivních zobrazení plyne, že zobrazení je bijektivní, právě když $f^{-1}(b)$ je jednoprvková pro každý prvek $b \in B$ a též, **jsou-li** A **i** B **konečné**, když $\#\operatorname{im} f = \#A = \#B$. Symbolicky budeme občas zapisovat bijektivní zobrazení jako $f : A \leftrightarrow B$.

Pojmu bijekce se používá při formální definici velikosti množiny. Pro libovolnou množinu X je její *velikost* definována jako takové přirozené číslo $n \in \mathbb{N}$, že existuje bijekce $\{1, \ldots, n\} \leftrightarrow X$. Píšeme $\#X = n$. Neexistuje-li takové přirozené číslo, říkáme, že X je nekonečná, a píšeme $\#X = \infty$.

Část I

Reálná čísla a limity

Kapitola 2

Číselné obory

Věříme, že čtenáři se setkali s pojmy *přirozených čísel*, *celých čísel* či *reálných čísel*. Máme však svých snadů, že bylo ono setkání více než intuitivní – „Přirozená čísla počítají, kolik je věcí; celá čísla jsou vlastně přirozená čísla, akorát některá mají před sebou takovou divnou čárku; reálná čísla jsou ... já vlastně nevím, něco jako $\sqrt{2}$?“

Jednou z našich snah v kapitole prvé bylo přesvědčit čtenáře, že většina moderní matematiky stojí na teorii množin. Čísla musejí být proto rovněž *množiny*. Ale jak vlastně? Jak bych – pro vše, což jest mi svaté – mohl množinami počítat věci? A co je jako „záporná“ množina? Všechny tyto otázky dočkají sebe svých odvět, jakož i vysvětlení onen záhadný pojem „obor“.

Započneme velmi teoreticky, algebraickými pojmy *grupy, pologrupy, monoidu, okruhu* a dalšími. Slibovaným významem takého výkladu je nabyté porozumění přirozené struktuře číselných oborů a pak, zcela bezděčné, protlačení abstraktní algebry na místa, kde by bývala snad byla ani nemusela být.

2.1 Základní algebraické struktury

První algebraické struktury počali lidé objevovat koncem 19. století, kdy jsme si všimli, že se mnoho skupin jevů – geometrických, fyzikálních, ... – „chová“ podobně jako čísla. Dnes bychom řekli, že „vykazují silnou symetrii“. Například, podobně jako můžeme přirozená čísla násobit, lze zobrazení *skládat* či křivky v rovině na sebe *napojovat*. Přirozená čísla „obracíme“, dávajíce vzniknout číslům celým. Po křivce umíme kráčet opačným směrem.

Taková pozorování vedla na pojem *grupy* – ve své podstatě množině všech symetrií nějakého objektu. *Symetrie* v tomto smyslu značí transformace/proměny tohoto objektu, které jej nemění. Dnes má samozřejmě grupa svou elegantní formální definici, z níž nelze vůbec poznat, o jakou strukturu vlastně jde. Uvedeme si ji.

Definice 2.1.1 (Grupa)

Ať G je libovolná neprázdná množina. Platí-li, že

- existuje binární operace $\cdot : G \times G \to G$, která je **asociativní** (tj. $(g \cdot h) \cdot k = g \cdot (h \cdot k)$),
- existuje prvek $1 \in G$ splňující pro každé $g \in G$ rovnost $g \cdot 1 = 1 \cdot g = g$, zvaný *neutrální*, a
- pro každý prvek $g \in G$ existuje prvek $g^{-1} \in G$ splňující $g \cdot g^{-1} = g^{-1} \cdot g = 1$, zvaný *inverz*,

pak nazveme čtveřici $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *grupou*.

Tato definice si zaslouží několika poznámek, varování a příkladů. Součástí definice grupy **není** komutativita její binární operace. Obecně, v grupě $\mathbf{G}$ není prvek $g{\cdot}h$ tentýž jako $h{\cdot}g$. Mezi algebraiky platí nepsaná dohoda, že grupy, které jsou *komutativní* (též *abelovské*) – tj. ty, kde $g{\cdot}h = h{\cdot}g$ opravdu pro všechny dvojice prvků $g, h \in G$ – se zapisují jako (tzv. *aditivní*) $\mathbf{G} = (G, +, -, 0)$. Naopak, grupy, které komutativní nutně nejsou, se obvykle píší stylem z definice 2.1.1.

Zadruhé, není vůbec zřejmé, proč by taková struktura měla jakýmkoli způsobem zrcadlit koncept *symetrie*. Ono „zrcadlo“ zde sestrojíme.

Příklad 2.1.2 (Dihedrální grupa)

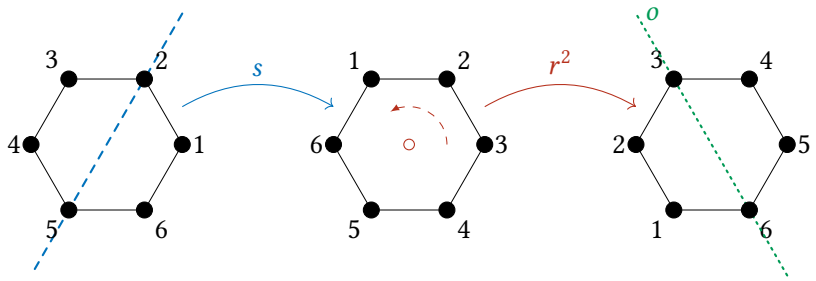
Ať P je pravidelný šestiúhelník v $\mathbb{R}^2$. Uvažme zobrazení $r : \mathbb{R}^2 \to \mathbb{R}^2$, které rotuje body v $\mathbb{R}^2$ o $60°$ (v kladném směru – proti směru hodinových ručiček) podle středu jeho uhlopříček, a zobrazení $s : \mathbb{R}^2 \to \mathbb{R}^2$, které reflektuje body v $\mathbb{R}^2$ podle kterékoli (ale fixní) jeho uhlopříčky.

Není těžké nahlédnout, že $r(P) = P$ a $s(P) = P$, čili tato zobrazení zachovávají P. Tvrdíme, že každé jejich složení je rovněž zobrazení, které zachovává P. Jinak řečeno, množina všech možných složení zobrazení r se zobrazením s tvoří *grupu*, kde binární operací je *složení* zobrazení, inverzem je *inverzní zobrazení* (pozřeme, že r i s jsou **bijekce**) a neutrálním prvkem je $\mathbb{1}_{\mathbb{R}^2}$ – *identické zobrazení* na $\mathbb{R}^2$.

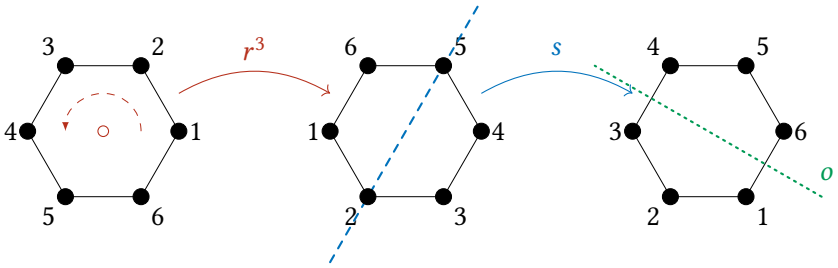
Po chvíli přemýšlení zjistíme, že rotace o $60, 120, 180, 240, 300$ a 360 stupňů zachovávají P. Všechny můžeme dostat jako složení r se sebou samým vícekrát. Například $r \circ r \circ r = r^3$ je rotace o $180°$. Přirozeně, rotace o $360°$ je identické zobrazení, což lze vyjádřit rovností $r^6 = \mathbb{1}_{\mathbb{R}^2}$.

S reflexemi je to mírně složitější. Jelikož s je reflexe, složení $s \circ s$ je identické zobrazení. Reflexi podle ostatních dvou uhlopříček dostaneme jeho složením s r. Například reflexi podle uhlopříčky, která svírá s s úhel $60°$ (proti směru hodinových ručiček) je rovna složení $r^2 \circ s$. Konečně, šestiúhelník P rovněž zachovávají reflexe podle os stran. Reflexi podle osy stran, která svírá s s úhel $90°$ dostanu (třeba) složením $s \circ r^3$.

Ponecháváme čtenáře, aby si rozmysleli, že různých zobrazení, která mohu dostat složením r a s je celkem 12, všechna jsou bijektivní a zachovávají P. Označíme-li jejich množinu D_{12} (jako **d**ihedrální grupa o 12 prvcích), pak je $(D_{12}, \circ, ^{-1}, \mathbb{1}_{\mathbb{R}^2})$ **nekomutativní** grupa.



(a) Složení $r^2 \circ s$ = reflexe podle o.



(b) Složení $s \circ r^3$ = reflexe podle o.

Obrázek 2.1: Příklady složení reflexí a rotací.

Příklad 2.1.3 (Permutační grupa)

Ať X je libovolná konečná množina velikosti $n \in \mathbb{N}$. Pak množina všech permutací na X (tj. bijekcí $X \leftrightarrow X$) tvoří spolu s operací skládání a invertování funkcí **nekomutativní** grupu. Skutečně, skládání funkcí je zřejmě *asociativní*, ke každé bijekci existuje *inverz* a *neutrálním* prvkem je $\mathbb{1}_X$. Z diskrétní matematiky víme, že permutací na n-prvkové množině je $n!$; označíme-li jejich množinu jako S_X (ze zaběhlého a zcestného názvu **s**ymetrická grupa), pak je $(S_X, \circ, ^{-1}, \mathbb{1}_X)$ nekomutativní grupa o $n!$ prvcích. Můžeme se na ni dívat jako na množinu všech transformací, které zachovávají množinu X.

Zajímavou otázkou je, kolik potřebujeme nejméně permutací, abychom jejich skládáním vyrobili všechny ostatní. V případě dihedrální grupy pravidelného šestiúhelníku (příklad 2.1.2) to byla zobrazení dvě. Ukazuje se, a není příliš obtížné to dokázat, že nám stačí všechny transpozice $(x\ y)$, kde $x \in X$ je nějaký fixní prvek a y probíhá všechny ostatní prvky X. Pokud by $X = \{1, \ldots, n\}$, pak by to byly třeba právě transpozice $(1\ 2), (1\ 3), \ldots, (1\ n)$. Tento fakt souvisí přímo s pozorováním z diskrétní matematiky, že každou permutaci lze rozložit na transpozice.

Příklad 2.1.4 (Odmocniny jednotky)

Každé komplexní číslo má přesně n n-tých odmocnin. Zapíšeme-li si komplexní číslo $z \in \mathbb{C}$ v tzv. „goniometrickém“ tvaru, pak je můžeme snadno najít. Totiž, je-li $z = r \cdot (\cos\theta + i \sin\theta)$, kde $r \in \mathbb{R}^+$ je jeho vzdálenost od počátku, θ úhel, který svírá s reálnou (typicky vodorovnou) osou, a i imaginární jednotka (z definice $i^2 = -1$), pak je

$$\left\{ \sqrt[n]{r} \cdot \left(\cos\left(\frac{\theta + 2\pi k}{n} \right) + i \cdot \sin\left(\frac{\theta + 2\pi k}{n} \right) \right) \mid k \in \{0, \ldots, n-1\} \right\}$$

množina všech jeho n-tých odmocnin.

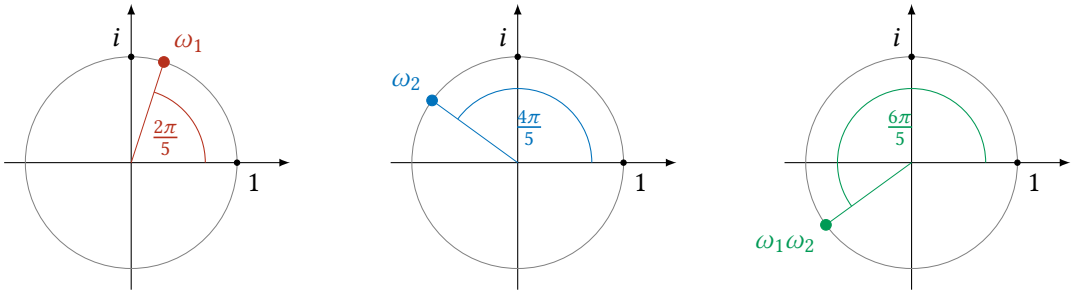
Tato množina obecně **není** grupa, neboť tím, že vynásobím dvě odmocniny komplexního čísla, nedostanu jeho jinou odmocninu – s jednou výjimkou, a tou je číslo 1. Totiž, $1 = \cos(2\pi) + i \cdot \sin(2\pi)$, a tedy všechny jeho třeba čtvrté odmocniny jsou

$$\left\{\cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right), \cos(\pi) + i\sin(\pi), \cos\left(\frac{3\pi}{2}\right) + i\sin\left(\frac{3\pi}{2}\right), \cos(2\pi) + i\sin(2\pi)\right\}$$
$$= \{i, -1, -i, 1\}.$$

Důležité pozorování k pochopení tohoto příkladu je, že když spolu násobím dvě komplexní čísla, jejich vzdálenosti od počátku (r) se násobí a jejich úhly svírané s reálnou osou (θ), se sčítají. Z toho plyne, že vzdálenost každé odmocniny z 1 od počátku je vždy 1 a že vynásobením dvou odmocnin z 1 dostanu další odmocninu z 1. Vskutku, jsou-li $\cos(2k\pi/n) + i\sin(2k\pi/n)$ a $\cos(2l\pi/n) + i\sin(2l\pi/n)$ dvě odmocniny z jedné, pak je jejich součin roven

$$\left(\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)\right)\left(\cos\left(\frac{2l\pi}{n}\right) + i\sin\left(\frac{2l\pi}{n}\right)\right) = \cos\left(\frac{2(k+l)\pi}{n}\right) + i\sin\left(\frac{2(k+l)\pi}{n}\right),$$

což je opět odmocnina z 1 (za předpokladu, že ztotožňujeme „přetočené úhly“ v tom smyslu, že třeba $7\pi/3 = \pi/3$). Označíme-li $\Omega(n)$ množinu všech n-tých odmocnin z 1, pak je čtveřice $(\Omega(n), \cdot, ^{-1}, 1)$ **komutativní** grupa, kde $\cdot$ značí běžné násobení komplexních čísel.



Obrázek 2.2: Komplexní čísla $\omega_1, \omega_2 \in \Omega(5)$ a jejich součin $\omega_1\omega_2$.

Doufáme, že jsme uspěli ve snaze vnímavé čtenáře přesvědčit, že grupy jsou přirozené struktury v různém smyslu reprezentující symetrie objektů spolu s jejich vzájemnými souvislostmi.

Avšak, grupy nezachycují *všechny* transformace, pouze ty, které lze zvrátit – tento požadavek je zachycen v podmínce existence inverzu ke každému prvku grupy. Není přehnané domnívat se, že tímto přístupem přicházíme o řád informací o studovaných jevech. Vskutku, matematici 19. století souhlasí a vymýšlejí strukturu *monoidu*, v podstatě jen grupy, u které nepožadujeme, aby každý prvek bylo lze invertovat. Monoidy jsou tudíž algebraické struktury objímající **všechny** transformace – jak symetrie, tak deformace.

Definice 2.1.5 (Monoid)

Ať M je libovolná neprázdná množina. Platí-li, že

- existuje binární operace $\cdot : M \times M \to M$, která je **asociativní** a
- existuje prvek $1 \in M$ takový, že $1 \cdot m = m \cdot 1 = m$ pro každé $m \in M$,

pak nazýváme trojici $(M, \cdot, 1)$ *monoidem*.

Přirozeně, pokud má každý prvek monoidu inverz, je tento monoid grupou. Některé příklady grup se dají zobecnit tak, aby se staly příklady monoidů, které však nejsou grupami. Vezměme příklad 2.1.3. Uvážíme-li místo pouhých permutací na X (tj. bijekcí $X \leftrightarrow X$) **všechna** zobrazení $X \to X$, pak dostaneme monoid. Vskutku, jak jsme již zmiňovali, skládání zobrazení je asociativní a máme k dispozici identické zobrazení $\mathbb{1}_X$, čili je trojice

$$(\{f \mid f \text{ je zobrazení } X \to X\}, \circ, \mathbb{1}_X)$$

monoidem. Tento příklad též ukazuje, že monoidy jsou v jistém smyslu „větší“ než grupy. Je-li X konečná množina velikosti n, pak je tento smysl dokonce absolutní. Všech permutací na X je totiž $n!$, zatímco všechna zobrazení $X \to X$ čítají n^n.

Příklady 2.1.2 a 2.1.4 žádných přirozených zobecnění nenabízejí. Přidáme-li k dihedrální grupě rotace a reflexe, které nemusejí daný mnohoúhelník zachovat, pak už můžeme rovnou uvážit úplně všechny rovinné rotace a reflexe. Je sice pravdou, že množina všech rotací a reflexí dvoudimenzionálního prostoru tvoří monoid, ale již nikterak nesouvisí s mnohoúhelníky. Podobně, když se nebudeme soustředit na komplexní odmocniny z 1, ale na komplexní odmocniny libovolného komplexního čísla, nedostaneme tak ani monoid – jak jsme uvedli, součin dvou n-tých odmocnin komplexního čísla obecně není n-tá odmocnina téhož čísla.

Předpokládáme, že čtenáři stále nevidí spojitost mezi grupy a monoidy a číselnými obory. Jedním (pravda zásadním) rozdílem je existence operací součtu a součinu v každém číselném oboru. Grupy a monoidy z definice dovolují jen jednu operaci. Pravdať, číselné obory jsou jakýmsi přirozeným „sloučením“ monoidu a grupy, které sluje *okruh*.

Okruhy jsou již vcelku komplikované struktury, jež v sobě mísí symetrie s destruktivními transformacemi a vlastně je „donucují“ ke spolupráci. Z jiného, více formálního, pohledu jsou prvky okruhů součty násobků všech transformací objektu.

Definice 2.1.6 (Okruh)

Ať R (od angl. výrazu pro okruh – **r**ing) je neprázdná množina, $+, \cdot$ jsou operace na R a $0, 1 \in R$. Je-li

- $(R, +, -, 0)$ **komutativní** grupa,
- $(R, \cdot, 1)$ (ne nutně komutativní) monoid

a platí-li

$$\begin{aligned} (r+s)\cdot t &= r\cdot t + s\cdot t, \\ t\cdot(r+s) &= t\cdot r + t\cdot s \end{aligned} \tag{2.1}$$

pro všechna $r, s, t \in R$, nazveme R okruhem.

Poznámka 2.1.7

- Symbol $-$ v popisu grupy $(R, +, -, 0)$ značí *inverz*, **nikoli binární operaci**! Odčítání nemůže být nikdy grupovou (ani monoidovou) operací, bo **není asociativní**. Zápis $r - s$

je pouze neformálním zkrácením zápisu $r + (-s)$, podobně jako se třeba $r \cdot s^{-1}$ zapisuje jako r/s.

- Definice okruhu vyžaduje, aby byla operace + komutativní, ale · nikoli. Mluvíme-li tedy o **komutativním** okruhu, znamená to, že i · je komutativní, a nemůže dojít ke zmatení, kterouže operaci máme na mysli.
- V literatuře se občas při definici okruhu nevyžaduje existence jednotky, tedy neutrálního prvku k násobení. Dvojice $(R, \cdot)$ je pak pouze tzv. *magma*, množina s binární operací bez žádných dalších předpokladů. Našemu pojmu okruhu se v takovém případě říká *okruh s jednotkou*. Možná překvapivě je teorie okruhů s jednotkou výrazně odlišná od teorie okruhů bez jednotky.
- Rovnice (2.1) jsou onou „vynucenou“ domluvou mezi symetrickou operací + a libovolnou transformací ·, říkáme jí *distributivita*. Je třeba specifikovat distributivitu jak zleva, tak zprava, protože · nemusí být komutativní.

Jednoduchých příkladů okruhů není mnoho a všechny vyžadují snad nepřirozené konstrukce. Ty přirozené vyplynou samovolně, až se jmeme tvořiti číselných oborů, v následující kapitole. S cílem představit jeden velmi naučný příklad/varování však tyto konstrukce dočasně přeskočíme a budeme předpokládat, že množina přirozených čísel $\mathbb{N}$ je čtenářům již plně známa.

Varování 2.1.8

V okruzích (a obecně v monoidech) může nastat situace, že $r \cdot s = 0$, přestože r ani s není nulový prvek. Uvažme například množinu přirozených čísel $\{0, 1, 2, 3, 4, 5\}$ se sčítáním a násobením „modulo 6“. Konkrétně, definujme operace $\oplus$ a $\odot$ předpisy

$$m \oplus n \coloneqq (m + n) \bmod 6,$$
$$m \odot n \coloneqq (m \cdot n) \bmod 6,$$

a položme $\ominus x \coloneqq (6 - x) \bmod 6$, kde $x \bmod y$ značí zbytek x po dělení y. Je poměrně snadné si uvědomit, že

$$(\{0, 1, 2, 3, 4, 5\}, \oplus, \ominus, 0, \odot, 1)$$

je (komutativní) okruh. V tomto okruhu platí

$$2 \odot 3 = (2 \cdot 3) \bmod 6 = 0,$$

ačkoli 2 ani 3 rovny 0 zřejmě nejsou.

Okruhy $(R, +, -, 0, \cdot, 1)$ s takovou vlastností jsou z číselného hlediska problematické, neboť na nich nelze žádným rozumným (vlastně ani nerozumným) způsobem definovat *dělení*, tj. inverz k ·.

Představme si totiž, že by na okruhu $(\{0, 1, 2, 3, 4, 5\}, \oplus, \ominus, 0, \odot, 1)$ existoval k prvku 2 inverzní prvek 2^{-1} vzhledem k $\odot$. Pak bychom měli následující rovnosti:

$$(2^{-1} \odot 2) \odot 3 = 1 \odot 3 = 3,$$
$$2^{-1} \odot (2 \odot 3) = 2^{-1} \odot 0 = 0,$$

čili by operace $\odot$ **nemohla být asociativní**! To by byl už kompletní binec.

Nepřítomnost takového problému v číselných oborech napovídá, že struktura okruhu stále ještě není dostatečně striktní, abychom jejím prvkům mohli přezdít „čísla“. Ukazuje se, že ale stačí zakázat součinu dvou nenulových prvků býti nulou, abychom se k číslům dostali. Taková struktura slove *obor integrity*; jmě, jež vrhá světlo na ustálené spojení *číselné obory*.

Definice 2.1.9 (Obor integrity)

Okruh $(R, +, -, 0, \cdot, 1)$ nazveme *oborem integrity*, pokud pro každé dva $r, s \in R$ platí

$$r \cdot s = 0 \Rightarrow r = 0 \vee s = 0.$$

Čtenáři dobře učiní, vejmou-li, že tato vlastnost číselných oborů je hojně využívána řekněme při řešení polynomiálních rovnic. Dokáži-li totiž rozložit polynom na součin jeho lineárních činitelů, pak vím, že řešení rovnice

$$(x - a)(x - b)(x - c) = 0$$

jsou právě čísla a, b a c. **To však není pravda v obecném okruhu!** Pouze struktura oboru integrity umožňuje činit takový závěr.

V oborech integrity lze „sčítat“, „odčítat“ a „násobit“. Nelze v nich však „dělit“. Součástí definice oboru integrity není existence inverzu k operaci násobení. Struktury, které toto splňují, se jmenují *tělesa* a tvoří základ moderní geometrie. Nezamýšlejíce formalizovat zmíníme, že z každého oboru integrity lze vyrobit těleso vlastně hrubým přidáním inverzů ke všem prvkům. Tomuto procesu se říká *lokalizace* a výsledné struktuře *podílové těleso*; lokalizace je způsobem, kterým se mimo jiné tvoří racionální čísla z čísel celých.

Definice 2.1.10 (Těleso)

Okruh $(F, +, -, 0, \cdot, 1)$ (z angl. názvu pro těleso – **f**ield) nazveme *tělesem*, existuje-li ke každému prvku $f \in F$ inverz vzhledem k $\cdot$, tj. prvek $f^{-1} \in F$ takový, že $f \cdot f^{-1} = f^{-1} \cdot f = 1$.

Pozorní čtenáři jistě sobě povšimli, že v definici tělesa *nepožadujeme*, aby byl výchozí okruh oborem integrity. Existence inverzů již tuto podmínku implikuje. Důkaz ponecháváme jako cvičení.

Cvičení 2.1.11

Dokažte, že každé těleso je oborem integrity.

2.2 Číselné obory

Konstrukce číselných oborů je symetrizační proces. Přirozená čísla nejsou z algebraického pohledu „hezký“ objekt, nejsou symetrická a všechny operace jsou destruktivní – ničí informaci o výchozím stavu. Kupříkladu operace + provedená na dvojici čísel dá číslo 5. Ovšem, nemám žádný způsob, jak se z čísla 5 vrátit zpět do čísel 2 nebo 3. V principu, v přirozených číslech se lze pohybovat pouze jedním směrem a všechny objekty ponechané vzadu upadají v trvalé zapomnění.

Varování 2.2.1

Nezasvěcený, zmatený a zcela pomýlený čtenář by snad měl odvahu tvrdit, že přeci mohu číslo 3 od čísla 5 **odečíst** a získat tím zpět číslo 2. Jistě, takové tvrzení by se kvapně stalo předmětem vášnivých diskusí v anarchistických kroužcích velebitelů teorie polomnožin, v kterékoli algebraické teorii však nemá nižádné místo.

Vyzýváme čtenáře, aby uvážili, že definovat „operaci minus“ na množině přirozených čísel, která vlastně není formálně operací, neboť funguje pouze tehdy, když je levý argument větší nebo roven pravému, není komutativní a není **ani asociativní**, byl by čin vskutku ohyzdný.

Znak − bude mít své místo až v celých číslech, kde však rovněž nebude operací (stále není asociativní), bude pouze značit inverz vzhledem k operaci +.

Tuto situaci vylepšují čísla celá, která přidávají inverzy k operaci + a tím ji symetrizují. Ovšem, operace · si stále drží svůj deformační charakter. Podobně jako tomu bylo u přirozených čísel s operacemi + a ·, v celých číslech operace · rovněž není zvratná. Dostat se ze součinu $-2 \cdot 3$ zpět na číslo -2 je nemožné.

Algebraicky nejdokonalejší jsou pak čísla racionální, která jsou již cele symetrickou strukturou – komutativním tělesem. Obě operace + i · jsou symetrické, zvratné prostřednictvím − a $^{-1}$. Pozor! Podobně jako odčítání, ani dělení **není operace**. Výraz p/q je pohodlným zápisem formálně korektního pq^{-1} vyjadřujícího součin čísla p s multiplikativním inverzem k číslu q.

Racionální čísla však stále mají, nikoli z algebraického, nýbrž z analytického pohledu, jednu podstatnou neduhu. Totiž, nerozumějí si dobře s pojmem *nekonečna*. Ukazuje se, že racionální čísla mají mezi sebou „nekonečně malé“ díry nejsouce pročež vhodná při modelování fyzického světa, který jsme si lidé zvykli vnímat jako *souvislý*. Tuto neduhu lze odstranit, a to konstrukcí čísel *reálných*. Ta však nebude zdaleka tak jednoduchá jako konstrukce ostatních číselných oborů, neboť z principu věci dožaduje sobě aparátu pro práci s nekonečně malými vzdálenostmi.

Vlastnosti číselných oborů (nebo korektněji, množin) shrnuje tabulka 2.1.

Množina	Struktura	Operace (symetrická?)	Díry
$\mathbb{N}$	polookruh	+(ne), ·(ne)	konstantní velikosti
$\mathbb{Z}$	obor integrity	+(ano), ·(ne)	konstantní velikosti
$\mathbb{Q}$	komutativní těleso	+(ano), ·(ano)	nekonečně malé
$\mathbb{R}$	komutativní těleso	+(ano), ·(ano)	pouze dvě ($-\infty$ a ∞)

Tabulka 2.1: Vlastnosti číselných množin.

Nyní k samotným konstrukcím. První výzvou je konstrukce množiny přirozených čísel $\mathbb{N}$. Stavebními kameny jsou množiny, tudíž přirozená čísla sama musejí být rovněž množiny. Existuje mnoho axiomatických systémů (z nich snad nejoblíbenější tzv. Peanova aritmetika) popisujících přirozená čísla, avšak, jako je tomu u axiomů vždy, nepodávají žádnou představu o výsledné struktuře.

My předvedeme jednu konstruktivní definici, jejíž korektnost vyplývá z axiomů teorie množin (speciálně z axiomu nekonečna), které zde však uvádět nechceme; žádáme pročež čtenáře o jistou míru tolerance.

Definice 2.2.2 (Přirozená čísla)

Definujme $0 \coloneqq \emptyset$ a „funkci následníka“ jako $s(a) \coloneqq a \cup \{a\}$. Množina $\mathbb{N}$ přirozených čísel je taková množina, že $0 \in \mathbb{N}$ a $s(n) \in \mathbb{N}$ pro každé $n \in \mathbb{N}$. Konkrétně, $\mathbb{N}$ jsou definována iterativně jako

$$\begin{aligned} 0 &\coloneqq \emptyset, \\ 1 &\coloneqq s(0) = 0 \cup \{0\} = \{\emptyset\} = \{0\}, \\ 2 &\coloneqq s(1) = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}, \\ 3 &\coloneqq s(2) = 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}, \\ &\vdots \end{aligned}$$

Intuitivně pojato, číslo n je definováno jako množina všech přirozených čísel menších než ono samo, tedy $\{0, \ldots, n-1\}$.

Na přirozených číslech lze definovat operace + a ·. Ukážeme si zběžně jak.

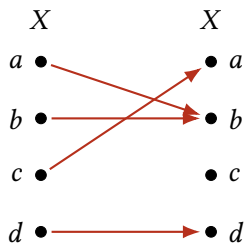
Přirozená čísla splňují tzv. axiom rekurze, který se obvykle zavádí v axiomatické definici přirozených čísel. V rámci našeho konstruktivního přístupu je třeba ho dokázat. My si ho zde však pouze uvedeme, neboť onen důkaz je silně logický a zdlouhavý.

Tvrzení 2.2.3 (Axiom rekurze)

Ať X je neprázdná množina a $x \in X$. Pak pro každé zobrazení $f : X \to X$ existuje jednoznačně určené zobrazení $F : \mathbb{N} \to X$ takové, že $F(0) = x$ a $F(s(n)) = f(F(n))$ $\forall n \in \mathbb{N}$.

Lidsky řečeno, axiom rekurze říká, že přirozenými čísly je možné „číslovat“ opakované (*rekurzivní*) aplikace zobrazení f na prvky množiny X počínaje jakýmsi pevně zvoleným prvkem. Vlastně vyrábíme nekonečný řetěz šipek zobrazení f.

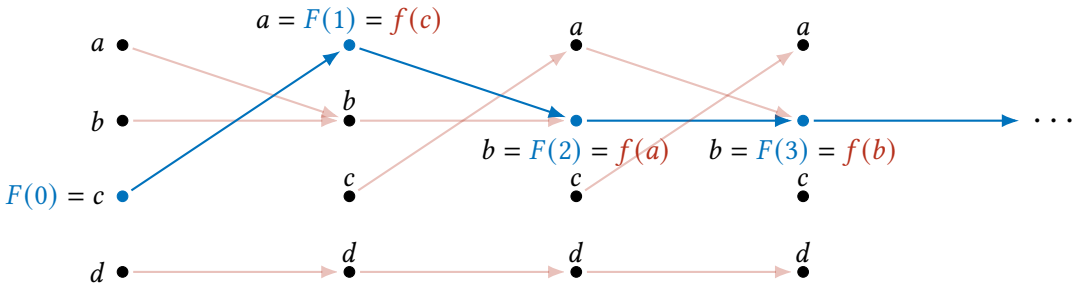
Uvažme například zobrazení na obrázku 2.3.



Obrázek 2.3: Zobrazení f z axiomu rekurze.

Zde $X = \{a, b, c, d\}$ a za počáteční prvek zvolme třeba c. Podle tvrzení 2.2.3 existuje zobrazení $F : \mathbb{N} \to X$ začínající v c (tj. $F(0) = c$), které zobrazuje číslo 1 na prvek, na který f zobrazuje c; číslo 2 na prvek, na který f zobrazuje ten prvek, na který zobrazuje c; číslo 3 na prvek, na který f zobrazuje ten prvek, na který zobrazuje ten prvek, na který zobrazuje c; číslo 4 ... radši nic ... Snad lepší představu poskytne obrázek 2.4.

Vybaveni axiomem rekurze, můžeme nyní definovat operaci $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Začneme tím, že defi-



Obrázek 2.4: Zobrazení F jako „rekurzor“ zobrazení f s počátečním bodem $F(0) = c$.

nujeme zobrazení „přičti n“. Zvolme za zobrazení f v axiomu rekurze funkci následníka $s : \mathbb{N} \to \mathbb{N}$ definovanou $s(n) = n \cup \{n\}$. Je zřejmé, že zobrazení „přičti n“, pracovně označené $+_n$, musí číslo 0 zobrazit na n. Podle axiomu rekurze však existuje pouze jediné zobrazení $+_n : \mathbb{N} \to \mathbb{N}$ splňující

$$\begin{aligned} +_n(0) &= n, \\ +_n(s(m)) &= s(+_n(m)) \ \forall m \in \mathbb{N}. \end{aligned}$$

Uvědomme si, že druhá rovnost je též velmi přirozeným požadavkem pro operaci sčítání. Říká totiž, že následník čísla $m + n$ je tentýž jako následník čísla m sečtený s n.

Konečně, na $\mathbb{N}$ definujeme operaci $+$ předpisem

$$m + n \coloneqq +_n(m).$$

V každé učebnici základů teorie množin a matematické logiky dá nyní nějakou práci osvětlit, že takto definovaná operace $+$ je komutativní a asociativní a že se obdobným způsobem dá definovat operace násobení. Naštěstí! Tento text není výkladem ani jedné z pokulhávajících disciplín, a tedy těchto několik malých kroků pro člověka a stejně tak malých kroků pro matematiku přeskočíme a věnovati sebe dalším oborům číselným budeme.

Zcela striktně vzato, $\mathbb{N}$ ještě nejsou *oborem*. Nejsou vlastně ani okruhem. Přestože $(\mathbb{N}, \cdot, 1)$ je komutativní monoid, $(\mathbb{N}, +, 0)$ zcela jistě není komutativní grupa, ano rovněž pouze komutativní monoid. Takovým strukturám se často říká (snad jen proto, aby se jim prostě nějak říkalo, ačkoliv nikoho zvlášť nezajímají) *polookruhy*. Situaci vylepšují čísla celá.

Podobně jako čísla přirozená, i čísla celá lze definovat mnoha způsoby. Uvedeme si jeden. Na množině $\mathbb{N} \times \mathbb{N}$ dvojic přirozených čísel definujme relaci $\sim_{\mathbb{Z}}$ předpisem

$$(a, b) \sim_{\mathbb{Z}} (c, d) \overset{\text{def}}{\iff} a + d = b + c.$$

Třídám ekvivalence dvojic přirozených čísel podle $\sim_{\mathbb{Z}}$ budeme říkat *celá čísla*.

Definice 2.2.4 (Celá čísla)

Množinu celých čísel $\mathbb{Z}$ definujeme jako

$$\mathbb{Z} \coloneqq \{[(a, b)]_{\sim_{\mathbb{Z}}} \mid (a, b) \in \mathbb{N} \times \mathbb{N}\}.$$

Operace $+$ a $\cdot$ na $\mathbb{N}$ indukují operace na $\mathbb{Z}$, které budeme označovat stejnými symboly. Kon-

krétně, definujme

$$[(a,b)]_{\sim_{\mathbb{Z}}} + [(c,d)]_{\sim_{\mathbb{Z}}} \coloneqq [(a+c, b+d)]_{\sim_{\mathbb{Z}}},$$
$$[(a,b)]_{\sim_{\mathbb{Z}}} \cdot [(c,d)]_{\sim_{\mathbb{Z}}} \coloneqq [(a\cdot c + b\cdot d, a\cdot d + b\cdot c)]_{\sim_{\mathbb{Z}}}.$$

Pro všechna $a, b \in \mathbb{N}$ navíc platí

$$[(a,b)]_{\sim_{\mathbb{Z}}} + [(b,a)]_{\sim_{\mathbb{Z}}} = [(a+b, b+a)]_{\sim_{\mathbb{Z}}} = [(0,0)]_{\sim_{\mathbb{Z}}},$$

kde poslední rovnost platí, protože + je komutativní. Čili, prvek $[(b,a)]_{\sim_{\mathbb{Z}}}$ je inverzní k prvku $[(a,b)]_{\sim_{\mathbb{Z}}}$ vzhledem k +. Značíme ho $-[(a,b)]_{\sim_{\mathbb{Z}}}$. Odtud plyne, že $(\mathbb{Z}, +, -, [(0,0)]_{\sim_{\mathbb{Z}}})$ je komutativní grupa, pročež je

$$(\mathbb{Z}, +, -, [(0,0)]_{\sim_{\mathbb{Z}}}, \cdot, [(1,0)]_{\sim_{\mathbb{Z}}})$$

komutativní okruh. Je snadné si uvědomit, že je to rovněž obor integrity.

Čtenáře snad povaha množiny $\mathbb{Z}$ z předchozí definice zaráží. Zcela jistě to není ta „obvyklá“. Ovšem, přechod od této verze celých čísel k té běžně užívané je zcela bezbolestný. Stačí se totiž dívat na třídy ekvivalence $[(a,b)]_{\sim_{\mathbb{Z}}}$ jako na „čísla“ $a - b$. Ponecháváme na čtenáři, aby ověřil, že definice operací + a − v naší verzi $\mathbb{Z}$ odpovídají těm na celých číslech v jejich zvyk ctící podobě. My budeme této korespondence drze využívat bez varování a mluvit o oboru integrity $(\mathbb{Z}, +, -, 0, \cdot, 1)$.

Cvičení 2.2.5 (Hrátky s celými čísly)

Množinou $\mathbb{Z}$ zde myslíme tu z definice 2.2.4. Ověřte, že

(1) relace $\sim_{\mathbb{Z}}$ je skutečně ekvivalence;

(2) operace + a · jsou dobře definované. To znamená, že nezávisí na volbě konkrétního reprezentanta z každé třídy ekvivalence. Ještě konkrétněji, dobrá definovanost zde značí fakt, že

$$[(a,b)]_{\sim_{\mathbb{Z}}} + [(c,d)]_{\sim_{\mathbb{Z}}} = [(a',b')]_{\sim_{\mathbb{Z}}} + [(c',d')]_{\sim_{\mathbb{Z}}},$$
$$[(a,b)]_{\sim_{\mathbb{Z}}} \cdot [(c,d)]_{\sim_{\mathbb{Z}}} = [(a',b')]_{\sim_{\mathbb{Z}}} \cdot [(c',d')]_{\sim_{\mathbb{Z}}},$$

kdykoli $(a,b) \sim_{\mathbb{Z}} (a',b')$ a $(c,d) \sim_{\mathbb{Z}} (c',d')$;

(3) operace +, − a inverz − podle naší definice souhlasí s operacemi danými stejnými symboly na „běžné“ verzi celých čísel při korespondenci

$$[(a,b)]_{\sim_{\mathbb{Z}}} \leftrightarrow a - b.$$

Konkrétně, pro operaci + toto znamená, že platí korespondence

$$[(a,b)]_{\sim_{\mathbb{Z}}} + [(c,d)]_{\sim_{\mathbb{Z}}} \leftrightarrow (a-b) + (c-d)$$

a nezávisí na výběru reprezentanta z tříd ekvivalence $[(a,b)]_{\sim_{\mathbb{Z}}}$ a $[(c,d)]_{\sim_{\mathbb{Z}}}$.

Přechod od celých čísel k racionálním obnáší definovat na celých číslech „dělení“ – v algebraické hantýrce definovat inverz k operaci · a učiniti tímť z oboru $(\mathbb{Z}, +, -, 0, \cdot, 1)$ těleso. Ten je překvapivě snadný úkol a proces „racionalizace“, nazývaný oficiálně *lokalizace*, lze v podstatě krok po kroku

replikovat pro libovolný obor integrity.

Snad není překvapením, že racionální čísla budou třídy ekvivalence dvojic (a, b) celých čísel (s $b \neq 0$), které budeme ovšem zapisovat tradičně a/b. Princip za konstrukcí racionálních čísel z čísel celých není nepodobný tomu za konstrukcí celých čísel z čísel přirozených. Totiž, *zlomky* pro nás budou rovněž třídy ekvivalence. Čtenář dobře učiní, přesvědčí-li sebe, že se zlomky jako s třídami ekvivalence vlastně zachází od doby, kdy mu byly představeny. Totiž, mám-li $a, b \in \mathbb{Z}$ obě dělitelná číslem $n \in \mathbb{Z}$, řekněme $a = nk$ a $b = nl$ pro vhodná $k, l \in \mathbb{Z}$, pak píšeme

$$\frac{a}{b} = \frac{nk}{nl} = \frac{k}{l},$$

ačkoli ve skutečnosti $a \neq k$ a $b \neq l$, čili rovnost výše dlužno nevejmouti absolutně. Zlomek a/b jsme totiž zvyklí vnímat jako třídu ekvivalence představující nějakou část celku. Tento pohled je snadné formalizovat.

Definice 2.2.6 (Racionální čísla)

Definujme ekvivalenci $\sim_{\mathbb{Q}}$ na dvojicích $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ předpisem

$$(a, b) \sim_{\mathbb{Q}} (c, d) \overset{\text{def}}{\iff} a \cdot d = b \cdot c.$$

Třídu ekvivalence $[(a, b)]_{\sim_{\mathbb{Q}}}$ budeme zapisovat a/b a položíme

$$\mathbb{Q} \coloneqq \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \right\}.$$

Operace + a − indukují operace na $\mathbb{Q}$, jež budeme značit stejně. Konkrétně,

$$\frac{a}{b} + \frac{c}{d} \coloneqq \frac{a \cdot d + b \cdot c}{b \cdot d},$$
$$\frac{a}{b} \cdot \frac{c}{d} \coloneqq \frac{a \cdot c}{b \cdot d}.$$

Navíc, prvek b/a je inverzní k prvku a/b vzhledem k $\cdot$, pokud $a \neq 0$. Budeme ho značit $(a/b)^{-1}$. Snadno se ověří, že

$$(\mathbb{Q}, +, -, 0, \cdot, ^{-1}, 1)$$

je těleso, kde jsme ztotožnili prvky $a/1 \in \mathbb{Q}$ s prvky $a \in \mathbb{Z}$.

Cvičení 2.2.7 (Hrátky s racionálními čísly)

Ověřte, že $\sim_{\mathbb{Q}}$ je skutečně ekvivalence a že operace + a $\cdot$ na $\mathbb{Q}$ jsou dobře definované (nezávisejí na výběru reprezentanta) a odpovídají „obvyklým“ operacím zlomků.

Konstrukce reálných čísel z racionálních je zcela jistě nejnáročnější úkol a nelze ho docílit čistě algebraicky. Potíž dlí už v samotné intuici. Totiž, jak již zmiňechom, racionální čísla mají mezi sebou „díry“. Formalizovat tento pojem však není přímočaré. Zatím nejlepší představu, kterou jsme schopni nastínit, je ta, že „racionální úsečka“ je „tečkovaná“ – každému jejímu bodu mohu přiřadit nějaké přirozené číslo. To znamená, že každé její dva body jsou od sebe vzdáleny, neboť je dokáži od sebe rozlišit dost na to, abych jim přiřadil dvě různá čísla. Naopak, s „reálnou úsečkou“ toto učinit nemohu. Jednotlivé body do sebe splývají a vytvářejí „plynulý“ obraz.

Přenosu této intuitivní představy do praxe brání fakt, že dvě racionální čísla jsou od sebe sice vzdálena, ale „nekonečně málo“. Další kapitola je věnována rigoróznímu pohledu na tuto problematiku a konstrukci reálných čísel.

Kapitola 3

Posloupnosti, limity a reálná čísla

Kritickým opěrným bodem při konstrukci reálných čísel i při jejich následném studiu je pojem *limity* (v češtině se tomuto slovu přiřazuje ženský rod). Limita je bod, k němuž se zvolená posloupnost čísel „blíží“, ale nikdy jeho „nedosáhne“, pokud takový existuje. Přidruženým pojmem je třeba *asymptota* reálné funkce, se kterou se čtenáři, očekáváme, setkali.

Samotná definice limity je zpočátku poněkud neintuitivní. Vlastně i samotná představa býti něčemu „nekonečně blízko“ je do jisté míry cizí. Pokusíme se vhodnými obrázky a vysvětlivkami cestu k pochopení dláždit, avšak, jakož tomu bývá, intuice přichází, až člověk s ideou takřkouce sroste.

3.1 Definice limity posloupnosti

Koncept posloupnosti je, na rozdíl od limity, velmi triviální. Je to vlastně „očíslovaná množina čísel“. Z každé množiny lze vyrobit posloupnost jejích prvků tím, že jim přiřkneme nějaké pořadí. Tento *přírok* se nejsnadněji definuje jako zobrazení z přirozených čísel – to totiž přesně na každý prvek kodomény zobrazí jeho pořadí.

Definice 3.1.1 (Posloupnost)

Ať X je množina. *Posloupností* prvků z X nazveme libovolné zobrazení

$$a : \mathbb{N} \to X.$$

Pro úsporu zápisu budeme psát a_n místo $a(n)$ pro $n \in \mathbb{N}$. Navíc, je-li kodoména X zřejmá z kontextu, říkáme stručně, že $(a_n)_{n=0}^{\infty}$ je *posloupnost.*

Poznámka 3.1.2

Vnímaví čtenáři sobě jistě povšimli, že jsme na $\mathbb{N}$ nedefinovali žádné *uspořádání.* Ačkoliv ěk není tímto definice posloupnosti formálně nijak postižena, neodpovídá přirozenému vnímání, že prvek s číslem 1 stojí před prvkem s číslem 5 apod.

Naštěstí, naše konstruktivní definice přirozených čísel nabízí okamžité řešení. Využijeme toho, že každé přirozené číslo je podmnožinou svého následníka, a definujeme zkrátka uspořádání $\leq$ na $\mathbb{N}$ předpisem

$$a \leq b \overset{\text{def}}{\iff} a \subseteq b.$$

Fakt, že $\subseteq$ je uspořádání, okamžitě implikuje, že $\leq$ je rovněž uspořádání.

Rozmyslíme si nyní dva pojmy pevně spjaté s posloupnostmi – *konvergence* a *limita*. Brzo si též ukážeme, že tyto dva pojmy jsou záměnné, ale zatím je vnímáme odděleně. Navíc, budeme se odteď soustředit speciálně na posloupnosti racionálních čísel, tj. zobrazení $\mathbb{N} \to \mathbb{Q}$, neboť jsou oním klíčem k sestrojení své reálné bratří.

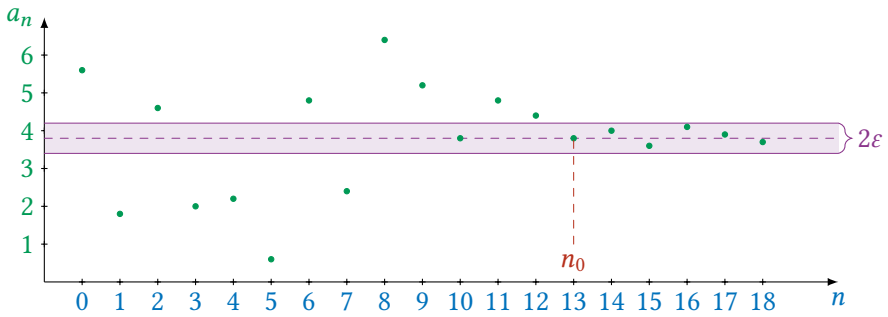
Ze všech posloupností $\mathbb{N} \to \mathbb{Q}$ nás zajímá jeden konkrétní typ – posloupnosti, vzdálenosti mezi jejichž prvky se postupně zmenšují. Tyto posloupnosti, nazývané *konvergentní* (z lat. con-vergere, „ohýbat k sobě“), se totiž vždy blíží k nějakému konkrétnímu bodu – ke své *limitě*. Představa ze života může být například následující: říct, že se blížíme k nějakému místu, je totéž, co tvrdit, že se vzdálenost mezi námi a oním místem s každým dalším krokem zmenšuje. V moment, kdy své kroky směřujeme stále stejným směrem, posloupnost vzdáleností mezi námi a tím místem tvoří konvergentní posloupnost. Jestliže se pravidelně odkláníme, k místu nikdy nedorazíme a posloupnost vzdáleností je pak *divergentní* (tj. **ne**konvergentní).

Do jazyka matematiky se věta „vzdálenosti postupně zmenšují“ překládá obtížně. Jeden ne příliš elegantní, ale výpočetně užitečný a celkově oblíbený způsob je následující: řekneme, že prvky posloupnosti jsou k sobě stále blíž, když pro jakoukoli vzdálenost vždy dokážeme najít krok, od kterého dál jsou již k sobě dva libovolné prvky u sebe blíž než tato daná vzdálenost. Důrazně vyzýváme čtenáře, aby předchozí větu přečítali tak dlouho, dokud jim nedává dobrý smysl. Podobné formulace se totiž vinou matematickou analýzou a jsou základem uvažování o nekonečnu.

Definice 3.1.3 (Konvergentní posloupnost)

Řekneme, že posloupnost $a : \mathbb{N} \to \mathbb{Q}$ je *konvergentní*, když platí výrok

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \; \exists n_0 \in \mathbb{N} \; \forall m, n \geq n_0 : |a_m - a_n| < \varepsilon.$$



Obrázek 3.1: Konvergentní posloupnost. Zde pro $\varepsilon = 0.2$ lze volit například $n_0 = 13$. Vodorovná přímka procházející bodem a_{n_0} je vlastně „středem“ pruhu o šíři 2ε, ve kterém se nacházejí všechny členy posloupnosti s pořadím vyšším než 13.

Poznámka 3.1.4

Radíme, aby se čtenáři sžili s intuitivním (přesto velmi přesným) ponětím absolutní hodnoty $|x-y|$ jako *vzdálenosti* mezi čísly x a y. V tomto smyslu je pak $|x| = |x-0|$ vzdálenost čísla x od čísla 0, což cele odpovídá definici tohoto symbolu.

Poznámka 3.1.5

Aplikujeme intuitivní vysvětlení *zmenšování vzdálenosti* z odstavce nad definicí 3.1.3 na jeho skutečnou definici.

Výrok

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall m, n \geq n_0 : |a_m - a_n| < \varepsilon$$

říká, že pro jakoukoli vzdálenost (ε) dokáži najít krok (n_0) takový, že vzdálenost dvou prvků v libovolných dvou následujících krocích (m, n) už je menší než daná vzdálenost ($|a_n - a_m| < \varepsilon$).

Slovo „krok“ je třeba vnímat volně – myslíme pochopitelně *pořadí* či *indexy* prvků v posloupnosti. Pohled na racionální posloupnosti jako na „kroky“ činěné v racionálních číslech může být ovšem užitečný.

Cvičení 3.1.6

Dokažte, že posloupnost $a : \mathbb{N} \to \mathbb{Q}$ je konvergentní právě tehdy, když

$$\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall m, n \geq n_0 : |a_m - a_n| < C\varepsilon$$

pro libovolnou **kladnou** konstantu $C \in \mathbb{Q}$.

Pojem *limity*, představuje jakýsi bod, k němuž se posloupnost s každým dalším krokem přibližuje, je vyjádřen výrazem podobného charakteru. Zde však přichází na řadu ona *děravost* racionálních čísel. Může se totiž stát, a příklady zde uvedeme, že limita racionální posloupnosti není racionální číslo.

Učiňmež tedy dočasný obchvat a před samotnou definicí limity vyrobme reálná čísla jednou z přehoušlí možných cest.

Ať $C(\mathbb{Q})$ značí množinu všech **konvergentních** racionálních posloupností. Uvažme ekvivalenci $\simeq$ na $C(\mathbb{Q})$ danou

$$a \simeq b \overset{\text{def}}{\iff} \forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0 : |a_n - b_n| < \varepsilon.$$

Přeloženo do člověčtiny, $a \simeq b$, právě když se rozdíl mezi prvky těchto posloupností se stejným pořadím neustále zmenšuje – řekli bychom, že se *blíží k nule*. V rámci (zatím intuitivní) představy, že konvergentní posloupnosti se blíží k nějakému bodu, dává smysl ztotožňovat posloupnosti, které se blíží k bodu *stejnému* – stav, který vyjadřujeme tak, že se jejich rozdíl blíží k nule.

Ve výsledku budeme definovat reálná čísla jako limity všech možných konvergentních racionálních posloupností. Pozbývajíce leč aparátu, bychom koncepty limity a konvergence stmelili v jeden, jsme nuceni učinit mezikrok.

Definice 3.1.7 (Reálná čísla)

Množinu *reálných čísel* tvoří všechny třídy ekvivalence konvergentních racionálních posloupností podle $\simeq$. Symbolicky,

$$\mathbb{R} \coloneqq \{[a]_\simeq \mid a \in C(\mathbb{Q})\}.$$

Nyní definujeme pojem limity. Nemělo by snad být příliš překvapivé, že se od definice konvergence příliš neliší. Významný rozdíl odpočívá pouze v předpokladu existence *cílového bodu*.

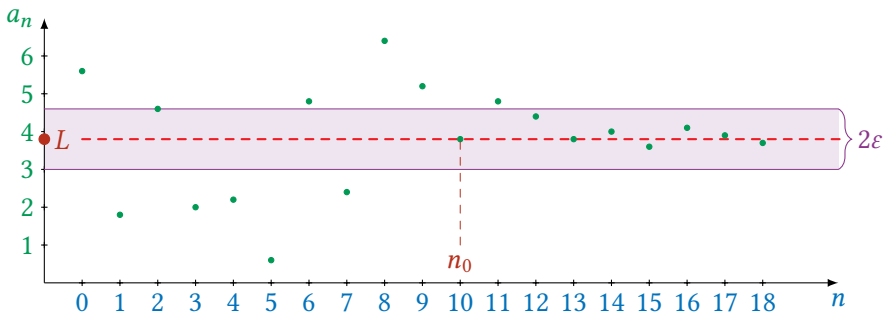
Definice 3.1.8 (Limita posloupnosti)

Ať $a : \mathbb{N} \to \mathbb{Q}$ je posloupnost. Řekneme, že a *má limitu* $L \in \mathbb{R}$, když

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \; \exists n_0 \in \mathbb{N} \; \forall n \geq n_0 : |a_n - L| < \varepsilon,$$

neboli, když jsou prvky a_n bodu L s každým krokem stále blíž.

Fakt, že $L \in \mathbb{R}$ je limitou a značíme jako $\lim a = L$.



Obrázek 3.2: Posloupnost s limitou L. Zde pro $\varepsilon = 0.4$ lze volit například $n_0 = 10$. Vodorovná přímka procházející bodem L je vlastně „středem“ pruhu o šíři 2ε, ve kterém se nacházejí všechny členy posloupnosti s pořadím vyšším než 10.

3.2 Limity konvergentních posloupností

V této sekci dokážeme, že konvergentní posloupnosti mají limitu. Opačná implikace, tj. že posloupnosti jmajíce limitu konvergují, je téměř triviální. K jejímu důkazu potřebujeme jen jednu vlastnost absolutní hodnoty.

Lemma 3.2.1 (Trojúhelníková nerovnost)

Ať $x, y \in \mathbb{Q}$. Pak

$$|x + y| \leq |x| + |y|.$$

Důkaz. Absolutní hodnota $|x + y|$ je rovna buď $x + y$ (když $x + y \geq 0$) nebo $-x - y$ (když $x + y < 0$). Zřejmě $x \leq |x|$ a $-x \leq |x|$, podobně $y \leq |y|$ a $-y \leq |y|$.

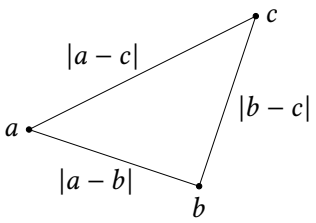
Pak je ale $x + y \leq |x| + |y|$ a též $-x + (-y) \leq |x| + |y|$. Tím je důkaz hotov. ∎

Poznámka 3.2.2

Název *trojúhelníková* obvykle přiřazovaný nerovnosti 3.2.1 vyplývá z její přirozené geometrické interpretace. Ať a, b, c jsou body v rovině. Dosazením $x = a - b$, $y = b - c$, dostává nerovnost 3.2.1 tvar

$$|a - c| \leq |a - b| + |b - c|,$$

tj. vzdálenost a od c je nanejvýš rovna součtu vzdáleností a od b a b od c pro libovolný bod b. Vizte obrázek 3.3.



Obrázek 3.3: Trojúhelníková nerovnost

Trojúhelníková nerovnost poskytuje snadné důkazy mnoha užitečných dílčích tvrzení o posloupnostech. Příkladem je následující cvičení.

Cvičení 3.2.3 (Jednoznačnost limity)

Dokažte, že každá posloupnost $a : \mathbb{N} \to \mathbb{Q}$ má nejvýše jednu limitu. Hint: použijte trojúhelníkovou nerovnost.

Ježto bychom však rádi dokazovali všechna tvrzení již pro reálná čísla, ukažme si nejprve, jak se dají sčítat a násobit. Dokážeme rovněž, že $\mathbb{R}$ – stejně jako $\mathbb{Q}$ – tvoří těleso. Začneme tím, že se naučíme sčítat a násobit konvergentní posloupnosti.

Ať $a, b \in C(\mathbb{Q})$ jsou dvě konvergentní racionální posloupností. Operace + a · na $C(\mathbb{Q})$ definujeme velmi přirozeně. Zkrátka, $(a + b)(n) \coloneqq a(n) + b(n)$ a $(a \cdot b)(n) \coloneqq a(n) \cdot b(n)$, tj. prvek na místě n posloupnosti $a + b$ je součet prvků na místech n posloupností a a b. Abychom ovšem získali skutečně operace na $C(\mathbb{Q})$, musíme ověřit, že $a + b$ i $a \cdot b$ jsou konvergentní.

Nechť dáno jest $\varepsilon > 0$. Chceme ukázat, že umíme najít $n_0 \in \mathbb{N}$, aby

$$|(a_n + b_n) - (a_m + b_m)| < \varepsilon,$$

kdykoli $m, n \geq n_0$. Protože jak a tak b konverguje, již umíme pro libovolná $\varepsilon_a, \varepsilon_b > 0$ najít n_a a n_b taková, že $|a_n - a_m| < \varepsilon_a$, kdykoli $m, n \geq n_a$, a podobně $|b_n - b_m| < \varepsilon_b$, kdykoli $m, n \geq n_b$. Položme tedy $\varepsilon_a = \varepsilon_b \coloneqq \varepsilon/2$ a $n_0 \coloneqq \max(n_a, n_b)$. Potom můžeme užitím trojúhelníkové nerovnosti pro $m, n \geq n_0$ odhadnout

$$|(a_n + b_n) - (a_m + b_m)| = |(a_n - a_m) + (b_n - b_m)| \leq |a_n - a_m| + |b_n - b_m| < \varepsilon_a + \varepsilon_b = \varepsilon,$$

čili $a + b$ konverguje.

Předchozí odstavec se může snadno zdát šílenou směsicí symbolů. Ve skutečnosti však formálně vykládá triviální úvahu. Máme najít pořadí, od kterého jsou prvky součtu $a + b$ u sebe blíž než nějaká daná vzdálenost. Poněvadž a i b konvergují, stačí přeci vzít větší z pořadí, od kterých je jak rozdíl prvků a, tak rozdíl prvků b, menší než polovina dané vzdálenosti.

Velmi obdobnou manipulaci lze provést k důkazu konvergence $a \cdot b$. Ponecháváme jej čtenářům jako (ne zcela snadné) cvičení.

Cvičení 3.2.4

Dokažte, že jsou-li a, b konvergentní posloupnosti racionálních čísel, pak je posloupnost $a \cdot b$ rovněž konvergentní. Kromě trojúhelníkové nerovnosti je zde třeba použít i zatím nedokázané lemma 3.2.10.

Racionální čísla jsou přirozeně součástí reálných prostřednictvím zobrazení

$$\begin{aligned} \xi : \mathbb{Q} &\hookrightarrow \mathbb{R}, \\ q &\mapsto [(q)], \end{aligned} \tag{3.1}$$

kde (q) značí posloupnost $a : n \mapsto q$ pro všechna $n \in \mathbb{N}$ a $[(q)]$ její třídu ekvivalence podle $\simeq$.

Varování 3.2.5

Tvrdíme pouze, že $\mathbb{Q}$ jsou *součástí* $\mathbb{R}$, kde slovu *součást* záměrně není dán rigorózní smysl. Racionální čísla totiž (aspoň po dobu naší dočasné definice reálných čísel) nejsou v žádném smyslu podmnožinou čísel reálných.

Matematici ale často ztotožňujeme doménu prostého zobrazení s jeho obrazem (neboť mezi těmito množinami vždy existuje bijekce). V tomto smyslu mohou být $\mathbb{Q}$ vnímána jako podmnožina $\mathbb{R}$, ztotožníme-li racionální čísla s obrazem zobrazení ξ z (3.1). Toto ztotožnění znamená vnímat racionální číslo $q \in \mathbb{Q}$ jako konvergentní posloupnost samých čísel q.

Cvičení 3.2.6

Dokažte, že zobrazení ξ z (3.1) je

- dobře definované – tzn. že když $p = q$, pak $[(p)] = [(q)]$ – a
- prosté.

Jelikož $\mathbb{Q}$ je těleso, speciálně tedy obsahuje 0 a 1, $\mathbb{R}$ je (prostřednictvím ξ z (3.1)) obsahuje rovněž. Pro stručnost budeme číslem $0 \in \mathbb{R}$ značit třídu ekvivalence posloupnosti samých nul a číslem $1 \in \mathbb{R}$ třídu ekvivalence posloupnosti samých jednotek. Ověříme, že se skutečně jedná o neutrální prvky ke sčítání a násobení.

Je třeba si rozmyslet, že pro každou posloupnost $a \in C(\mathbb{Q})$ platí $a + 0 = a$ a $a \cdot 1 = a$, kde, opět, čísla 0 a 1 ve skutečnosti znamenají nekonečné posloupnosti těchto čísel. Obě rovnosti jsou však zřejmé z definice, neboť $(a + 0)(n) = a_n + 0 = a_n = a(n)$ a $(a \cdot 1)(n) = a_n \cdot 1 = a_n = a(n)$ pro všechna $n \in \mathbb{N}$.

Konečně, rozšíříme rovněž $-$ a $^{-1}$ na $\mathbb{R}$. Pro libovolnou posloupnost $x \in C(\mathbb{Q})$ definujeme zkrátka $(-a)(n) \coloneqq -a(n)$. S $^{-1}$ je situace lehce komplikovanější. Totiž, pouze **nenulová** racionální čísla mají svůj inverz k násobení. Zde je třeba zpozorovat, že **konvergentní** posloupnost, která by však měla nekonečně mnoho prvků nulových, už musí mít od nějakého kroku **všechny** prvky nulové, jinak by totiž nemohla konvergovat. Vskutku, představme si, že a je posloupnost taková, že $a_n = 0$ pro nekonečně mnoho přirozených čísel $n \in \mathbb{N}$. Pak ale ať zvolím $n_0 \in \mathbb{N}$ jakkoliv, vždy existuje $m \geq n_0$ takové, že $a_m = 0$. Vezměme $n \geq n_0$ libovolné. Pokud $a_n \neq 0$, pak můžeme vzít třeba

$\varepsilon \coloneqq |a_n|/2$ a bude platit, že $|a_n - a_m| > \varepsilon$, což je dokonalý zápor definice konvergence. Z toho plyne, že a_n musí být 0 pro $n \geq n_0$ a odtud dále, že $a \simeq 0$. Čili, pouze posloupnosti ekvivalentní nulové posloupnosti nemají v $\mathbb{R}$ inverz vzhledem k $\cdot$.

Právě provedená úvaha nám umožňuje definovat $^{-1}$ pro posloupnosti $a \in C(\mathbb{Q})$ takové, že $a \not\simeq 0$, následovně:

$$(a^{-1})(n) \coloneqq \begin{cases} a(n)^{-1}, & \text{když } a(n) \neq 0, \\ 0, & \text{když } a(n) = 0. \end{cases}$$

Je snadné uvidět, že $-a$ je inverzem k a vzhledem k $+$ a a^{-1} je inverzem k $a \not\simeq 0$ vzhledem k $\cdot$. Vskutku, máme

$$(a + (-a))(n) = a_n + (-a_n) = 0,$$

tedy v tomto případě je $(a + (-a))$ přímo **rovna** nulové posloupnosti. V případě $^{-1}$ dostáváme pro $a \not\simeq 0$

$$(a \cdot a^{-1})(n) = \begin{cases} a_n \cdot a_n^{-1} = 1, & \text{když } a_n \neq 0, \\ a_n \cdot 0 = 0, & \text{když } a_n = 0. \end{cases}$$

Ergo, $a \cdot a^{-1}$ je rovna posloupnosti samých jedniček, až na konečně mnoho nul, protože, jak jsme si již rozmysleli, a nemůže mít nekonečně 0 a zároveň nebýt v relaci $\simeq$ s nulovou posloupností, jinak by nebyla konvergentní. To však přesně znamená, že $a \cdot a^{-1} \simeq 1$, čili $[a] \cdot [a^{-1}] = [1]$.

Shrneme-li řád předchozích úvah, získáme oprávnění tvrdit, že

$$(\mathbb{R}, +, -, [(0)], \cdot, ^{-1}, [(1)])$$

je těleso. Tento fakt je do budoucna pochopitelně zásadní; teď se však můžeme těšit znalostí, že jsme přechodem od $\mathbb{Q}$ k $\mathbb{R}$ neztratili symetrické rysy původní množiny.

Přikročmež již však k důkazu existence limity každé konvergentní posloupnosti. Fakt, že existence limity implikuje konvergenci, plyne přímo z trojúhelníkové nerovnosti.

Lemma 3.2.7

Každá posloupnost mající limitu je konvergentní.

Důkaz. Ať $a : \mathbb{N} \to \mathbb{Q}$ je posloupnost s limitou L. Pak pro každé $\varepsilon_L > 0$ existuje $n_L \in \mathbb{N}$ takové, že $|a_n - L| < \varepsilon_L$ pro všechna $n \geq n_L$.

Ať je dáno $\varepsilon > 0$. Chceme ukázat, že $|a_m - a_n| < \varepsilon$ pro všechna m, n větší než vhodné $n_0 \in \mathbb{N}$. Položme tedy $n_0 \coloneqq n_L$ a $\varepsilon_L \coloneqq \varepsilon/2$. Potom pro všechna $m, n \geq n_0 = n_L$ máme

$$|a_m - a_n| = |a_m - a_n - L + L| = |(a_n - L) + (L - a_m)| \leq |a_n - L| + |L - a_m| < \varepsilon_L + \varepsilon_L = \varepsilon,$$

čili a konverguje. ∎

3.2.1 Úplnost reálných čísel

K důkazu existence limity každé konvergentní posloupnosti potřebujeme prozpytovat vztah racionálních a reálných čísel podrobněji. Konkrétně potřebujeme ukázat, že $\mathbb{Q}$ jsou tzv. *hustá* v $\mathbb{R}$, tj.

že ke každému reálnému číslu existuje racionální číslo, které je mu nekonečně blízko. Zde jsme opět implicitně ztotožnili racionální čísla s třídami ekvivalence konstantních posloupností. Na základě toho budeme totiž moci tvrdit, že reálná čísla jsou tzv. *úplná*, což přesně znamená, že každá konvergentní posloupnost reálných čísel má reálnou limitu.

Nejprve si ovšem musíme rozmyslet, co vlastně míníme posloupností *reálných* čísel. Pochopitelně, zobrazení $x : \mathbb{N} \to \mathbb{R}$ poskytuje validní definici, ale uvědomme sobě, že teď vlastně uvažujeme posloupnosti, jejichž prvky jsou třídy ekvivalence konvergentních racionálních posloupností.

Abychom směli hovořit o konvergentních *reálných* posloupnostech, rozšíříme absolutní hodnotu $|\cdot|$ z $\mathbb{Q}$ na $\mathbb{R}$ zkrátka předpisem $|[(x_n)]| \coloneqq [(|x_n|)]$ pro $(x_n) \in C(\mathbb{Q})$. Napíšeme-li tedy $|x| \leq K$ pro reálná čísla $x, K \in \mathbb{R}$, pak tím doslova myslíme $[(|x_n|)] \leq [(K_n)]$, což ale **neznamená** $|x_n| \leq K_n$ pro všechna $n \in \mathbb{N}$, kde x_n, K_n jsou nyní již čísla ryze rozumná čili racionální, anobrž $|x_n| > K_n$ jen pro **konečně mnoho** $n \in \mathbb{N}$.

Varování 3.2.8

Důležitá myšlenka, již je dlužno snovat v srdci při práci s třídami ekvivalence konvergentních posloupností, je ta, že při porovnávání dvou tříd nás nezajímá libovolný **konečný počet** jejich prvních prvků.

Například, vztah $x = y$ pro $x, y \in \mathbb{R}$ znamená, že $x_n = y_n$ pro každé $n \in \mathbb{N}$ až na libovolný konečný počet prvních přirozených čísel. To se lépe vyjadřuje pomocí negace. Je snazší říct, že $x = y$, když $x_n \neq y_n$ pro jenom konečně mnoho $n \in \mathbb{N}$.

Rozepíšeme-li si tedy podrobně, co znamená, že je posloupnost $x : \mathbb{N} \to \mathbb{R}$ konvergentní, dostaneme pro dané $\varepsilon > 0$, vhodné $n_0 \in \mathbb{N}$ a $m, n \geq n_0$ nerovnost $|x_n - x_m| < \varepsilon$. Ovšem, x_n i x_m jsou samy o sobě třídy ekvivalence konvergentních **posloupností** racionálních čísel, tedy poslední nerovnost plně rozepsána dí

$$|[((x_n)_k - (x_m)_k)_{k=0}^{\infty}]| < \varepsilon,$$

což lze rovněž vyjádřit tak, že

$$|(x_n)_k - (x_m)_k| \geq \varepsilon$$

jen pro konečně mnoho $k \in \mathbb{N}$.

Nepřináší však žádný hmotný užitek nad konvergencí reálných posloupností uvažovat takto složitě. Čtenáři dobře učiní, uvědomí-li si plný význam předchozího odstavce, ovšem zůstanou-li věrni intuitivnímu vnímání výrazu $|x - y|$ jako „vzdálenosti“ čísel x a y.

Definice 3.2.9 (Omezená posloupnost)

Řekneme, že posloupnost $x : \mathbb{N} \to \mathbb{R}$ je *omezená*, když existuje $K \in \mathbb{R}$ takové, že $|x_n| \leq K$ pro všechna $n \in \mathbb{N}$. Píšeme $|x| \leq K$.

Lemma 3.2.10

Každá konvergentní posloupnost $x : \mathbb{N} \to \mathbb{R}$ je omezená.

Důkaz. Ať je $\varepsilon > 0$ dáno. Z definice konvergence nalezneme $n_0 \in \mathbb{N}$ takové, že pro každé $m, n \geq n_0$ je $|x_m - x_n| < \varepsilon$. Speciálně tedy pro každé $n \geq n_0$ platí

$$|x_n| = |x_n - x_{n_0} + x_{n_0}| \leq |x_n - x_{n_0}| + |x_{n_0}| < \varepsilon + |x_{n_0}|,$$

tudíž všechny členy posloupnosti s pořadím větším než n_0 jsou omezeny číslem $\varepsilon + |x_{n_0}|$. Ovšem, členů posloupnosti s pořadím menším než n_0 je konečně mnoho, a tedy z nich můžeme vzít ten největší – nazvěme ho s. Položíme-li $K \coloneqq \max(s, \varepsilon + |x_{n_0}|)$, pak $|x_n| \leq K$ pro každé $n \in \mathbb{N}$, čili x je omezená číslem K. ∎

Tvrzení 3.2.11 (Hustota $\mathbb{Q}$ v $\mathbb{R}$)

Množina racionálních čísel $\mathbb{Q}$ je hustá v $\mathbb{R}$, tj. ke každému $x \in \mathbb{R}$ a každému $\varepsilon > 0$ existuje $r \in \mathbb{Q}$ takové, že $|x - r| < \varepsilon$.

Důkaz. Ať $\varepsilon > 0$ je dáno a označme $x \coloneqq [(x_n)]$, $(x_n) \in C(\mathbb{Q})$. Najdeme $n_0 \in \mathbb{N}$ takové, že $\forall m, n \geq n_0$ je $|x_m - x_n| < \varepsilon$. Zvolme $r \coloneqq x_{n_0} \in \mathbb{Q}$. Pak ovšem máme

$$|x_n - r| = |x_n - x_{n_0}| < \varepsilon$$

pro všechna $n \geq n_0$. To přesně znamená, že $|x - r| < \varepsilon$. ∎

Lemma 3.2.12

Ať $a : \mathbb{N} \to \mathbb{Q}$ je konvergentní posloupnost racionálních čísel. Pak $\lim a = [(a)]$.

Důkaz. Položme $x \coloneqq [(a)]$. Ať je dáno $\varepsilon > 0$. Protože a je konvergentní, nalezneme $n_0 \in \mathbb{N}$, že $|a_m - a_n| < \varepsilon$ pro všechna $m, n \geq n_0$. Potom ale $|a_n - x| < \varepsilon$ pro všechna $n \geq n_0$, což z definice znamená, že $\lim a = x$. ∎

Důsledek 3.2.13 ($\mathbb{R}$ jsou úplná)

Každá konvergentní reálná posloupnost $x : \mathbb{N} \to \mathbb{R}$ má limitu v $\mathbb{R}$.

Důkaz. Ať $a : \mathbb{N} \to \mathbb{Q}$ je racionální posloupnost taková, že $|x_n - a_n| < 1/n$ pro všechna $n \in \mathbb{N}$. Tu nalezneme opakovaným použitím tvrzení 3.2.11 pro $\varepsilon \coloneqq 1/n$ a $x \coloneqq x_n$. Ukážeme nejprve, že a je konvergentní. Ať je dáno $\varepsilon > 0$. Zvolme n_1 takové, že $\forall m, n \geq n_1$ platí $1/m + 1/n < \varepsilon$. Dále, x je konvergentní z předpokladu. Čili, pro každé $\varepsilon_x > 0$ nalezneme $n_2 \in \mathbb{N}$ takové, že $\forall m, n \geq n_2$ máme $|x_n - x_m| < \varepsilon_x$. Volme tedy speciálně

$$\varepsilon_x \coloneqq \varepsilon - \frac{1}{m} - \frac{1}{n}.$$

a $n_0 \coloneqq \max(n_1, n_2)$. Potom pro všechna $m, n \geq n_0$ platí nerovnosti

$$\begin{aligned} |a_n - a_m| &= |a_n - a_m - x_n + x_n| \leq |a_n - x_n| + |x_n - a_m| = |a_n - x_n| + |x_n - a_m - x_m + x_m| \\ &\leq |a_n - x_n| + |x_n - x_m| + |x_m - a_m| < \frac{1}{n} + \varepsilon_x + \frac{1}{m} = \varepsilon, \end{aligned}$$

tedy a konverguje.

Jistě platí $\lim x - a = 0$, neboť pro každé $\varepsilon > 0$ lze najít $n \in \mathbb{N}$ takové, že $1/n < \varepsilon$. Odtud plyne, že x má limitu právě tehdy, když a má limitu. Ovšem, podle lemmatu 3.2.12 má a limitu $[(a)] \in \mathbb{R}$. Tím je důkaz hotov. ∎

Důsledek 3.2.14

Platí

$$\mathbb{R} \cong \{\lim a \mid a \in C(\mathbb{Q})\},$$

čili reálná čísla jsou přesně limity všech konvergentních racionálních posloupností.

Důkaz. Zkonstruujeme bijekci $f : \mathbb{R} \to \{\lim a \mid a \in C(\mathbb{Q})\}$. Vezměme $x \in \mathbb{R}$. Pak z definice existuje konvergentní racionální posloupnost $a \in C(\mathbb{Q})$ taková, že $x = [a]$. Podle lemmatu 3.2.12 má a limitu v $\mathbb{R}$. Definujme tedy $f(x) \coloneqq \lim a$.

Ověříme, že je f dobře definované, prosté a na.

Nejprve musíme ukázat, že $f(x)$ nezávisí na volbě konkrétní posloupnosti a z třídy ekvivalence $[a]$. Ať tedy $b \simeq a$ a označme $L_a \coloneqq \lim a, L_b \coloneqq \lim b$. Pak pro každé $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ takové, že $\forall n \geq n_0$ platí tři nerovnosti:

$$|a_n - b_n| < \varepsilon, \quad |a_n - L_a| < \varepsilon, \quad |b_n - L_b| < \varepsilon.$$

Velmi obdobnou úpravou jako v důkaze důsledku 3.2.13 dostaneme, že

$$|L_a - L_b| \leq |L_a - a_n| + |a_n - b_n| + |b_n - L_b| < 3\varepsilon,$$

odkud $L_a = L_b$, neboť L_a, L_b jsou třídy ekvivalence konvergentních posloupností. Společně s faktem, že každá konvergentní posloupnost má přesně jednu limitu (cvičení 3.2.3), plyne z předchozí úvahy, že f je dobře definováno.

Dokážeme, že f je prosté. To je snadné, neboť pokud $[a] = [b]$, neboli $a \simeq b$, potom $\lim a = \lim b$, což jsme již vlastně dokázali v odstavci výše.

Nakonec zbývá ověřit, že f je na. Ať tedy $L \coloneqq \lim a$ pro nějakou $a \in C(\mathbb{Q})$. Potom ovšem $[(a)] \in \mathbb{R}$ a podle lemmatu 3.2.12 platí $\lim a = [(a)]$. To ovšem přesně znamená, že $f([(a)]) = L$.

Tím je důkaz hotov. ∎

3.3 Poznatky o limitách posloupností

Účelem této sekce je shrnout základní poznatky o limitách posloupností, jež umožní čtenářům limity konkrétních posloupností efektivně počítat a navíc široké jejich použití v následujících kapitolách.

Začneme technickým, ale nezbytným, konceptem *rozšířené reálné osy* a pokračovati budeme jedním z nejdůležitějších a dle našeho názoru též nejkrásnějších výsledků – tzv. Bolzanovou-Weierstraßovou větou. Ta tvrdí v podstatě toto: mám-li omezenou posloupnost, pak z ní již umím vybrat nekonečně mnoho prvků, které tvoří posloupnost *konvergentní*.

Ona krása takového tvrzení spočívá v principu, kterým se podrobně zabývá kombinatorická disciplína zvaná Ramseyho teorie; v principu, že v téměř libovolně chaotické struktuře lze nalézt řád,

jakmile jest tato dostatečně velká. Nejedná se jistě o čistě matematický princip, nýbrž dost možná o princip vzniku vesmíru a života, popsaný již starým Aristotelem ve výmluvném výroku, „Celek je více než součet svých částí.“ V mnoha zpytech se tomuto jevu přezdívá Emergent Behavior a představuje stav, kdy chování systému nelze plně popsat pouze studiem jeho jednotlivých prvků.

Pro důkaz Bolzanovy-Weierstraßovy věty potřebujeme jedné pomocné konstrukce, tzv. *systému vnořených intervalů*. Nejprve si však pořádně definujeme samotný pojem *intervalu*. K tomu se nám bude hodit rozšířit množinu reálných čísel o prvky $-\infty$ a ∞.

3.3.1 Rozšířená reálná osa

Definice 3.3.1 (Rozšířená reálná osa)

Definujme množinu $\mathbb{R}^* \coloneqq \mathbb{R} \cup \{-\infty, \infty\}$, kde ∞, resp. $-\infty$, je z definice prvek takový, že $\infty \geq x$, resp. $-\infty \leq x$, pro každé $x \in \mathbb{R}$. Množině $\mathbb{R}^*$ budeme někdy říkat *rozšířená reálná osa*. Rozšíříme rovněž operace $+$ a $\cdot$ na prvky ∞ a $-\infty$ následovně.

$$\begin{aligned}
\infty + a = a + \infty = \infty, &\quad \text{pro } a \in \mathbb{R} \cup \{\infty\},\\
-\infty + a = a + (-\infty) = -\infty, &\quad \text{pro } a \in \mathbb{R} \cup \{-\infty\},\\
\infty \cdot a = a \cdot \infty = \infty, &\quad \text{pro } a > 0 \text{ nebo } a = \infty,\\
\infty \cdot a = a \cdot \infty = -\infty, &\quad \text{pro } a < 0 \text{ nebo } a = -\infty,\\
-\infty \cdot a = a \cdot (-\infty) = -\infty, &\quad \text{pro } a > 0 \text{ nebo } a = \infty,\\
-\infty \cdot a = a \cdot (-\infty) = \infty, &\quad \text{pro } a < 0 \text{ nebo } a = -\infty,\\
a \cdot \infty^{-1} = a \cdot (-\infty)^{-1} = 0, &\quad \text{pro } a \in \mathbb{R}.
\end{aligned}$$

Varování 3.3.2

Definice 3.3.1 stručně řečeno říká, že se s prvky ∞ a $-\infty$ zachází podobně jako s ostatními reálnými čísly. Ovšem, následující operace zůstávají nedefinovány.

$$\infty + (-\infty), -\infty + \infty, \pm\infty \cdot 0, 0 \cdot (\pm\infty), (\pm\infty) \cdot (\pm\infty)^{-1}.$$

Čtenáři možná zpozorovali, že jsme při své definici limity nerozlišili mezi posloupnostmi, které nemají limitu, protože jejich prvky „skáčou sem a tam“, a posloupnostmi, které ji nemají naopak pro to, že „stále klesají či stoupají“. Pro další studium záhodno se tohoto nedostatku zlišit.

Definice 3.3.3 (Limita v nekonečnu)

Ať $x : \mathbb{N} \to \mathbb{R}$ je reálná posloupnost. Řekneme, že x má limitu ∞, resp. $-\infty$, když pro každé $K > 0, K \in \mathbb{R}$, existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $n \geq n_0$ platí $x_n > K$, resp. $x_n < -K$. Píšeme $\lim x = \infty$, resp. $\lim x = -\infty$.

Na reálných číslech existuje uspořádání $\leq$, které zdědila z čísel přirozených, prostřednictvím čísel celých a konečně čísel racionálních. Protože, vděkem naší konstrukci, jsou celá čísla třídy ekvivalence dvojic čísel přirozených, čísla racionální třídy ekvivalence dvojic čísel celých a čísla reálná limity konvergentních racionálních posloupností, bylo by vskutku obtížné a neproduktivní vypsat konkrétní množinovou definici tohoto uspořádání na reálných číslech. Přidržíme se pročež

intuitivního pohledu na věc a důkaz, že $\leq$ je skutečně uspořádání na reálných číslech, necháváme laskavému čtenáři k promyšlení.

Existence uspořádání umožňuje dívat se na podmnožiny $\mathbb{R}$ z jistého „souvislého“ pohledu. Nemusejí již být vňaty (jako tomu je u ostatních představených číselných okruhů) jako výčty jednotlivých prvků, ale oprávněně jako „provázky“ či „úsečky“. Úplnost reálných čísel zaručuje, že z každého reálného čísla mohu plynule dorazit do každého jiného reálného čísla aniž reálná čísla opustím.

Předchozí odstavec vágně motivuje definici *intervalu* – „souvislé“ omezené podmnožiny reálných čísel. V souhlasu s definicí intervalu vzniká i pojem *otevřenosti* a *uzavřenosti* množiny – pojem, který je klíčem k definici *topologie* na obecné množině a tím pádem vlastně i základem tak zhruba poloviny celé moderní matematiky.

Směrem k definici intervalu učiňmež koliksi mezikroků.

Definice 3.3.4 (Maximum a minimum)

Ať $X \subseteq \mathbb{R}$ je množina. Řekneme, že prvek $M \in X$, resp. $m \in X$, je *maximem*, resp. *minimem*, množiny X, když pro každé $x \in X$ platí $x \leq M$, resp. $x \geq m$. Píšeme $M = \max X$, resp. $m = \min X$.

Definice 3.3.5 (Horní a dolní závora)

Ať $X \subseteq \mathbb{R}$ je množina. Řekneme, že prvek $Z \in \mathbb{R}^*$ resp. $z \in \mathbb{R}^*$, je *horní*, resp. *dolní*, *závora* množiny X, když pro každé $x \in X$ platí $x \leq Z$, resp. $x \geq z$.

Má-li množina X horní, resp. dolní, závoru, **která leží v** $\mathbb{R}$ (tedy není rovna $\pm\infty$), říkáme, že je *shora*, resp. *zdola*, *omezená*. Je-li navíc X omezená shora i zdola, říkáme krátce, že je *omezená*.

Definice 3.3.6 (Supremum a infimum)

Ať $X \subseteq \mathbb{R}$ je množina. Řekneme, že prvek $S \in \mathbb{R}^*$, resp. $i \in \mathbb{R}^*$, je *supremum*, resp. *infimum*, množiny X, když je to její *nejmenší horní závora*, resp. *největší dolní závora*. Píšeme $S = \sup X$, resp. $i = \inf X$.

Vyjádřeno symbolicky, prvek $S \in \mathbb{R}$ je *supremem* množiny X, když $x \leq S$ pro všechna $x \in X$, a kdykoli $x \leq Z$ pro nějaký prvek $Z \in \mathbb{R}$ a všechna $x \in X$, pak $S \leq Z$. Prvek $i \in \mathbb{R}$ je *infimem* množiny X, když $x \geq i$ pro všechna $x \in X$, a kdykoli $x \geq z$ pro nějaký prvek $z \in \mathbb{R}$ a všechna $x \in X$, pak $i \geq z$.

Varování 3.3.7

Vřele radíme čtenářům, aby sobě bedlivě přečetli předchozí tři definice a uvědomili si – velmi zásadní, leč lehko přehlédnuté – jejich vzájemné rozdíly.

- Maximum a minimum množiny X je z definice **vždy prvkem této množiny**. Maximem množiny $\{1, 2, 3\}$ je prvek 3 a jeho minimem je prvek 1.
- Horní, resp. dolní, závora množiny X je **libovolné rozšířené reálné číslo** (tedy klidně

i $\pm\infty$), které je větší, resp. menší, než všechny prvky X. Horní závorou množiny $\{1, 2, 3\}$ je číslo 69, též ∞ a též číslo 3. Horní a dolní závora **může, ale nemusí**, být prvkem X.

- Supremum, resp. infimum, množiny X je **rozšířené reálné číslo**, které je větší, resp. menší, než všechny prvky X, ale **zároveň menší, resp. větší, než každá jeho horní, resp. dolní, závora**. Supremum a infimum **může, ale nemusí, ležet v množině** X. Touto vlastností se přesně rozlišují *uzavřené* a *otevřené* intervaly – interval je uzavřený, když jeho supremum v něm leží, kdežto otevřený, když nikoliževěk. Supremem množiny $\{1, 2, 3\}$ je číslo 3 a jeho infimem je číslo 1.

Daná podmnožina $X \subseteq \mathbb{R}$ **nemusí nutně mít maximum a minimum**, ale, a to si dokážeme, **má vždy supremum, resp. infimum**. Je-li navíc shora, resp. zdola, omezená, pak toto supremum, resp. infimum, leží v $\mathbb{R}$.

Cvičení 3.3.8

Určete z definice suprema a infima $\inf \emptyset$ a $\sup \emptyset$.

Cvičení 3.3.9

Dokažte, že $\sup X$ a $\inf X$ jsou určeny jednoznačně.

Axiomatická definice reálných čísel

Přestože jsme konstrukci reálných čísel úspěšně dokončili použitím konvergentních racionálních posloupností, stojí snad za zmínku i jejich axiomatická definice, která se obvykle uvádí v úvodních učebnicích matematické analýzy.

Překvapivě není v principu tak odlišná od jejich konstrukce, kromě jednoho konkrétního axiomu, jenž právě zaručuje úplnost; není z něj však vůbec na první, v zásadě ani na druhý, pohled vidno, že takovou vlastnost skutečně implikuje.

Definice 3.3.10 (Axiomatická definice reálných čísel)

Množina $\mathbb{R}$ se v zásadě definuje jako nekonečné uspořádané těleso s vlastností úplnosti. Tedy,

- existují prvky $0, 1 \in \mathbb{R}$ a operace $+, \cdot : \mathbb{R}^2 \to \mathbb{R}$ s inverzy $-, ^{-1} : \mathbb{R} \to \mathbb{R}$ takové, že

  $$(\mathbb{R}, +, -, 0, \cdot, ^{-1}, 1)$$

  je nekonečné těleso;
- existuje uspořádání $\leq$ na $\mathbb{R}$, které je lineární (každé dva prvky lze spolu porovnat);
- (**axiom úplnosti**) každá shora omezená podmnožina $\mathbb{R}$ má supremum.

Je to právě on poslední axiom v předchozí definici, jehož použití jsme se chtěli vyhnout, bo dohlédnout jeho hloubky je obtížné a neintuitivní.

Dokážeme si zde ovšem, že naše definice reálných čísel odpovídá jejich axiomatické. Otázky neko-

nečnosti, podmínek tělesa i uspořádání jsme již zodpověděli. Zbývá dokázat axiom úplnosti. Pro stručnost vyjádření se nám bude hodit následující definice.

Definice 3.3.11 (Monotónní posloupnost)

O posloupnosti $x : \mathbb{N} \to \mathbb{R}$ řekneme, že je

- *rostoucí*, když $x_{n+1} > x_n \ \forall n \in \mathbb{N}$;
- *klesající*, když $x_{n+1} < x_n \ \forall n \in \mathbb{N}$;
- *neklesající*, když $x_{n+1} \geq x_n \ \forall n \in \mathbb{N}$;
- *nerostoucí*, když $x_{n+1} \leq x_n \ \forall n \in \mathbb{N}$.

Ve všech těchto případech díme, že posloupnost x je *monotónní*.

Tvrzení 3.3.12 (Axiom úplnosti)

Ať $X \subseteq \mathbb{R}$ je shora omezená množina. Pak existuje $\sup X$.

Důkaz. Ježto naše pojetí úplnosti se překládá do znění, „Každá konvergentní posloupnost má limitu“, není snad nečekané, že se důkaz *axiomu úplnosti* o tuto vlastnost opírá.

Je-li X prázdná, pak má supremum podle cvičení 3.3.8. Ať je tedy X neprázdná a shora omezená a $Z \in \mathbb{R}$ je libovolná horní závora X. Protože X je neprázdná, existuje $q \in \mathbb{R}$ takové, že $q < x$ pro nějaké $x \in X$. Definujeme posloupnosti Z_n a q_n podle následujících pravidel.

- Položme $Z_0 \coloneqq Z$ a $q_0 \coloneqq q$.
- Uvažme číslo $p_n \coloneqq (Z_n + q_n)/2$.
- Je-li p_n horní závorou X, položme $Z_{n+1} \coloneqq p_n$ a $q_{n+1} \coloneqq q_n$.
- Není-li p_n horní závorou X, položme $Z_{n+1} \coloneqq Z_n$ a $q_{n+1} \coloneqq p_n$.

Pak jsou posloupnosti Z_n a q_n konvergentní (**proč?**) a indukcí lze snadno dokázat (**dokažte!**), že q_n **není** horní závorou X a Z_n **je** horní závorou X pro všechna $n \in \mathbb{N}$. Navíc platí $\lim |Z_n - q_n| = 0$ (**proč?**), a tedy $\lim Z_n = \lim q_n$.

Označme $S \coloneqq \lim Z_n = \lim q_n$. Dokážeme, že $S = \sup X$. Je třeba ukázat, že

(1) S je horní závorou X;

(2) S je nejmenší horní závorou.

Předpokládejme pro spor, že existuje $x \in X$ takové, že $x > S$. To znamená, že existuje konstanta $c > 0$ taková, že $x - S = c$. Volme $\varepsilon \coloneqq c/2$. Pro toto ε z definice limity existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $n \geq n_0$ platí $|Z_n - \lim Z_n| = |Z_n - S| < \varepsilon$. Jelikož (Z_n) je nerostoucí a $S \leq Z_n$ pro každé $n \in \mathbb{N}$, je absolutní hodnota v předchozím výrazu zbytečná a můžeme zkrátka psát $Z_n - S < \varepsilon$. Potom ale pro všechna $n \geq n_0$ máme

$$x - Z_n = x + S - S - Z_n = (x - S) + (S - Z_n) > c - \varepsilon = \frac{c}{2},$$

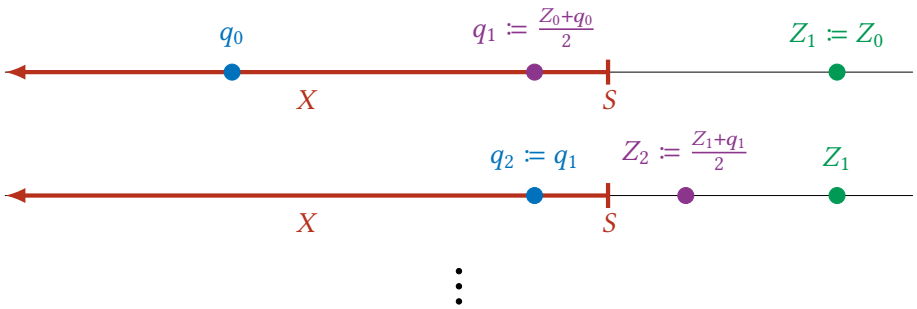
čili speciálně $x > Z_n$, což je ve sporu s tím, že Z_n je horní závora X. To dokazuje (1).

Tvrzení (2) lze dokázat obdobně, akorát využitím posloupnosti (q_n) spíše než (Z_n). Opět ať pro spor existuje $Z \in \mathbb{R}$, které je horní závorou X, a $Z < S$. Pak nalezneme konstantu $c > 0$ takovou, že $S - Z = c$. Opět z definice limity vezmeme $\varepsilon \coloneqq c/2$ a k němu $n_0 \in \mathbb{N}$ takové, že $\forall n \geq n_0$ platí $S - q_n < \varepsilon$, kde absolutní hodnotu jsme mohli vynechat, ježto jest posloupnost (q_n) neklesající a $S \geq q_n$ pro každé $n \in \mathbb{N}$. Nyní pro $n \geq n_0$ platí

$$q_n - Z = q_n - S + S - Z = (q_n - S) + (S - Z) > c - \varepsilon = \frac{c}{2},$$

čili speciálně $q_n > Z$, což je ve sporu s tím, že q_n není horní závora X pro žádné $n \in \mathbb{N}$, zatímco Z je.

Tím je důkaz dokončen. ∎



Obrázek 3.4: Důkaz axiomu úplnosti

Cvičení 3.3.13

Dokažte všechna (**proč?**) a (**dokažte!**) v důkazu předchozího tvrzení.

Jako každé poctivé tvrzení, jmá i axiom úplnosti svých důsledkův. Tyto bychom pochopitelně dokázati uměli i bez něj, neboť axiom úplnosti z naší konstrukce reálných čísel přímo plyne. Nicméně, zcela jistě jej lze použít jako nástroj ke zkrácení některých důkazů.

Nejprve duální tvrzení.

Tvrzení 3.3.14

Každá zdola omezená podmnožina $\mathbb{R}$ má infimum.

Důkaz. Cvičení. Doporučujeme čtenářům se zamyslet, jak tvrzení snadno plyne z axiomu úplnosti, aniž opakují konstrukci z jeho důkazu. ∎

Jedno, jak bude časem vidno, mimořádně užitečné tvrzení dí, že shora omezené rostoucí či neklesající posloupnosti a zdola omezené klesající či nerostoucí posloupnosti mají vždy limitu. To je opět intuitivně zřejmý fakt (jistě?), ale, kterak čtenáři doufáme již pozřeli, tvrzení o věcech nekonečných řídce radno nechati pouze intuici.

Lemma 3.3.15 (Limita monotónní posloupnosti)

(a) Každá rostoucí nebo neklesající shora omezená posloupnost je konvergentní.

(b) Každá klesající nebo nerostoucí zdola omezená posloupnost je konvergentní.

Důkaz. Dokážeme pouze část (a), část (b) je ponechána jako cvičení.

Ať $x : \mathbb{N} \to \mathbb{R}$ je neklesající posloupnost. Důkaz pro rostoucí posloupnost je téměř dokonale stejný, liše se akorát ostrými nerovnostmi v několika výrazech. Z předpokladu je x shora omezená, tudíž má množina jejích členů $\{x_n \mid n \in \mathbb{N}\}$ horní závoru. Z axiomu úplnosti má tato množina též supremum; označíme je S.

Ukážeme, že $\lim x = S$. Ať je $\varepsilon > 0$ dáno. Z definice suprema není $S - \varepsilon$ horní závora množiny $\{x_n \mid n \in \mathbb{N}\}$. Tedy existuje $n_0 \in \mathbb{N}$ takové, že $x_{n_0} > S - \varepsilon$. Protože x je neklesající – tj. $x_n \geq x_{n_0}$, kdykoli $n \geq n_0$ – platí rovněž $x_n > S - \varepsilon$ pro všechna $n \geq n_0$. Jelikož S je horní závora množiny členů x, platí $S \geq x_n$ pro všechna $n \in \mathbb{N}$. To však znamená, že $|x_n - S| = S - x_n$, a tedy z nerovnosti $x_n > S - \varepsilon$ po úpravě plyne, že $\varepsilon > S - x_n = |x_n - S|$, čili $\lim x = S$. ∎

Posledním důsledkem axiomu úplnosti, který si uvedeme, je tzv. *Archimédova vlastnost reálných čísel*. Obecně, těleso se nazývá *Archimédovo*, když vágně řečeno neobsahuje žádné nekonečně velké ani nekonečně malé prvky **vzhledem ke zvolené absolutní hodnotě**. Ukazuje se, že na reálných číslech lze definovat jen dva typy funkcí absolutní hodnoty – jednu „obvyklou“, též vyjádřitelnou vztahem $|x| = \sqrt{x^2}$, a pak tzv. *p*-adickou absolutní hodnotu pro p prvočíslo. Libovolná další konstrukce absolutní hodnoty (mající přirozené vlastnosti) již je ekvivalentní absolutní hodnotě jednoho z těchto typů. Reálná čísla jsou Archimédova vzhledem k obvyklé absolutní hodnotě, ale nikoliv vzhledem k libovolné p-adické absolutní hodnotě.

Lemma 3.3.16 (Archimédova vlastnost reálných čísel)

Pro každé $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, existuje $n \in \mathbb{N}$ takové, že $1/n < \varepsilon$.

Důkaz. Stačí dokázat, že

$$\inf \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\} = 0,$$

neboť potom z definice infima pro každé $\varepsilon > 0$ není $0 + \varepsilon = \varepsilon$ dolní závorou $\{1/n \mid n \in \mathbb{N}\}$, čili existuje $n \in \mathbb{N}$ takové, že $1/n < \varepsilon$.

Číslo 0 je zřejmě dolní závorou množiny $\{1/n \mid n \in \mathbb{N}\}$. Podle tvrzení 3.3.14 má tato množina infimum, označme je i. Pro spor ať $i > 0$. Potom $1/i \in \mathbb{R}$ a z nerovnosti $1/n \geq i$ (i je dolní závora) plyne, že $n \leq 1/i$ pro všechna $n \in \mathbb{N}$. Potom je ovšem číslo $1/i$ horní závorou množiny $\mathbb{N}$ a podle axiomu úplnosti má množina $\mathbb{N}$ supremum; označme je S. Pro každé $n \in \mathbb{N}$ tudíž platí $n \leq S$. Ovšem, z definice přirozených čísel platí $n + 1 \in \mathbb{N}$ pro každé $n \in \mathbb{N}$. Speciálně toto tedy znamená, že $n + 1 \leq S$ pro každé $n \in \mathbb{N}$. Pak je ovšem $S - 1$ horní závorou množiny $\mathbb{N}$, což je spor, neboť S bylo z předpokladu supremum $\mathbb{N}$.

Musí pročež platit $i = 0$, což bylo dokázati. ∎

Poznámka 3.3.17

Lemma 3.3.16 v podstatě říká, že $\lim_{n\to\infty} 1/n = 0$.

Bedliví čtenáři si mohou pamatovat, že jsme ono lemma již v předchozím textu bez uvedení použili (například v důkaze důsledku 3.2.13). Jedná se však z naší strany o drzost pouze malou. Totiž, jeho platnost je téměř okamžitým důsledkem tvrzení 3.2.11, jak si čtenáři rádi ověří v následujícím cvičení.

Cvičení 3.3.18

Dokažte, že lemma 3.3.16 je důsledkem tvrzení 3.2.11.

3.3.2 Bolzanova-Weierstraßova věta

Konečně kráčíme cestou definice intervalu a důkazu slibované Bolzanovy-Weierstraßovy věty. Vybaveni pojmy maxima (minima) a suprema (infima), můžeme intuitivní představě intervalu dát formální ráz. Vágně řečeno je interval *souvislá* podmnožina $\mathbb{R}$. Formálně je no ... vlastně totéž.

Definice 3.3.19 (Interval)

Podmnožinu $I \subseteq \mathbb{R}$ nazveme *intervalem*, pokud pro každé dva prvky $x < y \in I$ a $z \in \mathbb{R}$ platí

$$x < z < y \Rightarrow z \in I.$$

Intervaly mohou být otevřené, uzavřené a polouzavřené (či polootevřené?). Tyto vlastnosti intervalů jsou definovány pomocí existence maxim a minim.

Definice 3.3.20 (Typy intervalů)

Ať $I \subseteq \mathbb{R}$ je interval. Řekneme, že I je

- *otevřený*, když **nemá** maximum ani minimum;
- *uzavřený*, když **má** maximum i minimum;
- *shora uzavřený*, když má pouze maximum, ale nikoli minimum;
- *zdola uzavřený*, když má pouze minimum, ale nikoli maximum.

Otevřený interval I zapisujeme jako $I = (a, b)$, kde $a = \inf I$ a $b = \sup I$. Čísla a, b mohou být i $\pm\infty$, pokud I není shora či zdola omezený.

Uzavřený interval I zapisujeme jako $I = [a, b]$, kde $a = \min I$ a $b = \max I$. **Pozor!** Zde prvky a i b jsou striktně reálná čísla, tedy například $[0, \infty]$ **není** interval, neboť se nejedná o podmnožinu $\mathbb{R}$.

Definice 3.3.21 (Délka intervalu)

Délkou intervalu $I \subseteq \mathbb{R}$ s $a \coloneqq \inf I$ a $b \coloneqq \sup I$ myslíme číslo $\lambda(I) \coloneqq b - a$, je-li toto definováno.

Poznámka 3.3.22

Čtenáře snad mohlo zarazit značení $\lambda(I)$ pro délku intervalu, oproti zvyku podlehnuvšímu $|I|$. Písmeno λ zde není spojeno s angl. slovem **l**ength, jak by se snad mohlo prve zdát, nýbrž pochází ze jména **L**ebesgue. Totiž, *délka* intervalu je jeho *objemem* či *velikostí* vzhledem k tzv. Lebesgueově míře – mnohem obecnější konstrukci umožňující měřit velikosti všemožných podmnožin reálných čísel.

Příklad 3.3.23 (Pár intervalů)

Množina

- $I = (4, 6)$ je otevřený interval. Zřejmě platí $4 = \inf I$ a $6 = \sup I$. Ovšem, I nemá maximum ani minimum.
- $I = [-5, 4]$ je uzavřený interval. Zřejmě platí $-5 = \min I = \inf I$ a $4 = \max I = \sup I$.
- $I = [-2, \infty)$ je zdola uzavřený interval. Platí $-2 = \min I = \inf I$ a $\infty = \sup I$.
- $\mathbb{R} = (-\infty, \infty)$ je otevřený interval. Platí $-\infty = \inf \mathbb{R}$ a $\infty = \sup \mathbb{R}$.
- $I = (4, 4)$ je prázdná, neboť je to z definice množina čísel $x \in \mathbb{R}$ takových, že $4 < x < 4$.
- $I = [\exp(\tan(\log^3(\sqrt[7]{\pi/4}))), \exp(\tan(\log^3(\sqrt[7]{\pi/4})))]$ je rovna $\{\exp(\tan(\log^3(\sqrt[7]{\pi/4})))\}$, neboť je to z definice množina čísel $x \in \mathbb{R}$ takových, že

$$\exp(\tan(\log^3(\sqrt[7]{\pi/4}))) \leq x \leq \exp(\tan(\log^3(\sqrt[7]{\pi/4}))).$$

K pojmu intervalu se váže jedna speciální konstrukce zvaná *systém vnořených intervalů*. Definujeme si ji a ihned poté si povíme, čím je speciální.

Definice 3.3.24 (Systém vnořených intervalů)

Systém vnořených intervalů je posloupnost $(I_n)_{n=0}^{\infty}$ podmnožin $\mathbb{R}$ (čili zobrazení $\mathbb{N} \to 2^{\mathbb{R}}$) splňující následující podmínky:

- I_n je **uzavřený** interval pro každé $n \in \mathbb{N}$;
- $I_{n+1} \subseteq I_n$ pro každé $n \in \mathbb{N}$;
- $\lim_{n\to\infty} \lambda(I_n) = 0$.

Následující tvrzení je dalším ekvivalentem axiomu úplnosti a důsledku 3.2.13. V některých definicích reálných čísel se jím axiom úplnosti nahrazuje.

Tvrzení 3.3.25 (O vnořených intervalech)

Ať $(I_n)_{n=0}^{\infty}$ je systém vnořených intervalů. Pak $\#(\bigcap_{n=0}^{\infty} I_n) = 1$, čili v průniku všech intervalů I_n leží přesně jeden prvek.

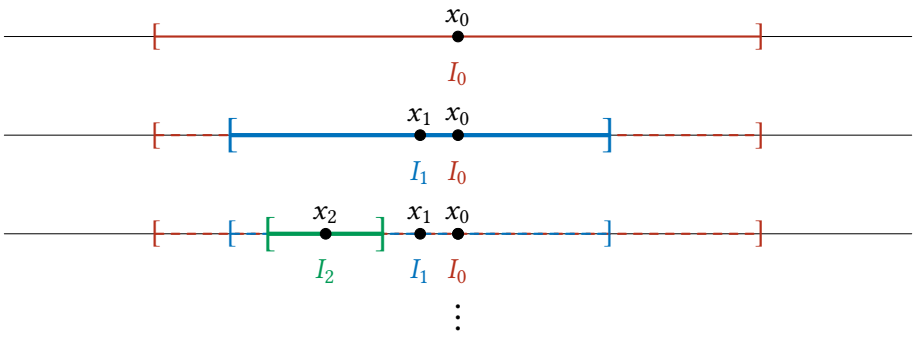
Důkaz. Je třeba dokázat, že takový prvek existuje a že je právě jeden. Začněme jednoznačností.

Předpokládejme, že existují prvky $x, y \in \bigcap_{n=0}^{\infty} I_n$ a $x \neq y$. Pak ale existuje konstanta $c > 0$ taková, že $|x - y| = c$. Protože však $x, y \in I_n$ pro každé $n \in \mathbb{N}$, speciálně platí $\lambda(I_n) \geq c$ pro každé $n \in \mathbb{N}$. To je spor s tím, že $\lim_{n\to\infty} \lambda(I_n) = 0$.

Dokážeme existenci. Označme $I_n = [a_n, b_n]$. Definujme posloupnost $x : \mathbb{N} \to \mathbb{R}$, $x_n \coloneqq (a_n + b_n)/2$. Na volbě čísla $(a_n + b_n)/2$ není nic speciálního. Stačí volit jakékoliv $x_n \in I_n$. Ukážeme, že x konverguje. Ať je dáno $\varepsilon > 0$. Protože $\lim_{n\to\infty} \lambda(I_n) = 0$, nalezneme $n_0 \in \mathbb{N}$ takové, že $\lambda(I_{n_0}) < \varepsilon$. Potom ale platí $|x_n - x_m| < \varepsilon$ pro všechna $m, n \geq n_0$, neboť $x_n, x_m \in I_{n_0}$, což je zaručeno podmínkou $I_n, I_m \subseteq I_{n_0}$.

Podle důsledku 3.2.13 má x limitu, označme ji L. Chceme ukázat, že $L \in \bigcap_{n=0}^{\infty} I_n$. K tomu je třeba ověřit, že $L \in I_n$ pro každé $n \in \mathbb{N}$. Ať pro spor existuje $n_L \in \mathbb{N}$ takové, že $L \notin I_{n_L}$. Protože intervaly jsou vnořené, znamená toto, že $L \notin I_n$ pro $n \geq n_L$. Volme libovolné $\varepsilon > 0$. K němu nalezneme $n_I \in \mathbb{N}$ takové, že $\lambda(I_n) < \varepsilon$ pro $n \geq n_I$. Ať $n_0 \coloneqq \max(n_L, n_I)$. Pak na jednu stranu pro $n \geq n_0$ platí $\lambda(I_n) < \varepsilon$ a na druhou stranu $L \notin I_n$. Sloučením obou vztahů dostaneme $|x_n - L| \geq \varepsilon/2$ pro $n \geq n_0$, neboť x_n leží v polovině intervalu I_n a L mimo něj pro každé $n \in \mathbb{N}$. To je spor s tím, že $\lim x = L$.

Důkaz je hotov. ∎



Obrázek 3.5: Důkaz tvrzení 3.3.25.

Definice 3.3.26 (Podposloupnost)

Řekneme, že $y : \mathbb{N} \to \mathbb{R}$ je *podposloupností* posloupnosti $x : \mathbb{N} \to \mathbb{R}$, když pro každé $n \in \mathbb{N}$ existuje $m \in \mathbb{N}$ takové, že $y_n = x_m$. Jinak řečeno, každý prvek y je rovněž prvkem x.

Již máme všechny ingredience k formulaci a důkazu Bolzanovy-Weierstraßovy věty. Je stěžejním tvrzením pro matematickou analýzu a pro matematiku obecně. Jeho filosofický význam dlí v poznání, že v „příliš velkých“ strukturách přirozeně vzniká řád.

Věta 3.3.27 (Bolzanova-Weierstraßova)

*Ať $x : \mathbb{N} \to \mathbb{R}$ je **omezená** posloupnost. Pak existuje podposloupnost y posloupnosti x, která konverguje.*

Důkaz. Z omezenosti x existují $s, S \in \mathbb{R}$ taková, že $s \leq x_n \leq S$ pro všechna $n \in \mathbb{N}$. Induktivně vyrobíme systém vnořených intervalů. Položme $I_0 \coloneqq [s, S]$. Za předpokladu, že $I_n = [a_n, b_n]$

je dán, sestrojíme I_{n+1} následovně:

$$I_{n+1} \coloneqq \begin{cases} [a_n, (a_n + b_n)/2], & \text{pokud } x_k \in [a_n, (a_n + b_n)/2] \text{ pro nekonečně mnoho } k \in \mathbb{N}, \\ [(a_n + b_n)/2, b_n], & \text{jinak.} \end{cases} \tag{3.2}$$

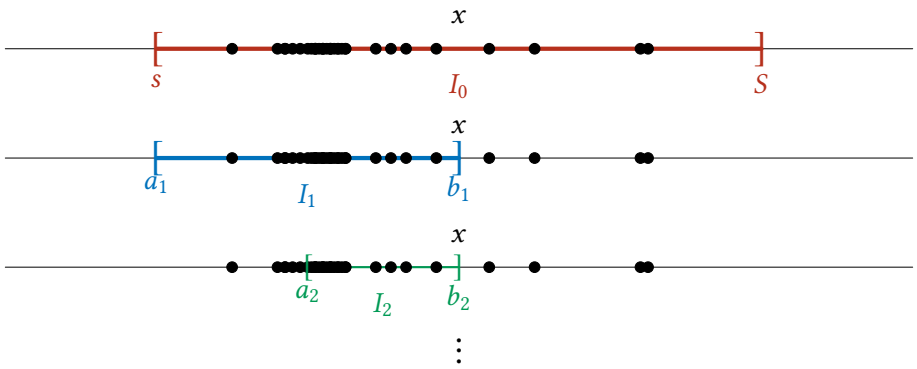
Rozmyslíme si lehce neformálním použitím matematické indukce, že tato konstrukce je korektní. První interval I_0 jistě obsahuje nekonečně mnoho prvků x, neboť obsahuje celou tuto posloupnost. Podobně, pokud I_n obsahuje nekonečně mnoho prvků x, pak aspoň jedna z jeho polovin musí rovněž obsahovat nekonečně mnoho prvků x. Z konstrukce (3.2) pak plyne, že rovněž I_{n+1} obsahuje nekonečně mnoho prvků x.

Ověříme, že $(I_n)_{n=0}^{\infty}$ je systém vnořených intervalů podle definice 3.3.24.

- Zcela jistě je I_n uzavřený interval pro každé $n \in \mathbb{N}$.
- Rovněž zcela jistě $I_{n+1} \subseteq I_n$ pro každé $n \in \mathbb{N}$, neboť I_{n+1} je jedna z polovin intervalu I_n.
- Délky intervalů I_n klesají k 0, neboť $\lambda(I_{n+1}) = \lambda(I_n)/2$, a tedy $\lambda(I_n) = \lambda(I_0)/2^n$. Zřejmě

$$\lim_{n\to\infty} \lambda(I_n) = \lim_{n\to\infty} \frac{\lambda(I_0)}{2^n} = 0.$$

Vyberme nyní z x libovolnou podposloupnost $y : \mathbb{N} \to \mathbb{R}$ takovou, že $y_n \in I_n$. To jistě lze, neboť každý z intervalů I_n obsahuje nekonečně mnoho prvků posloupnosti x. Pak ovšem podle tvrzení 3.3.25 existuje prvek $L \in \bigcap_{n=0}^{\infty} I_n$ a podle důkazu téhož tvrzení platí $\lim y = L$. To však znamená, se znalostí lemmatu 3.2.7, že y konverguje. ∎



Obrázek 3.6: Důkaz Bolzanovy-Weierstraßovy věty.

Seznam cvičení

Číselné obory

(1) Dokažte, že každé těleso je oborem integrity.

(2) Množinou $\mathbb{Z}$ zde myslíme tu z definice 2.2.4. Ověřte, že

(a) relace $\sim_{\mathbb{Z}}$ je skutečně ekvivalence;

(b) operace + a · jsou dobře definované. To znamená, že nezávisí na volbě konkrétního reprezentanta z každé třídy ekvivalence. Ještě konkrétněji, dobrá definovanost zde značí fakt, že

$$[(a,b)]_{\sim_{\mathbb{Z}}} + [(c,d)]_{\sim_{\mathbb{Z}}} = [(a',b')]_{\sim_{\mathbb{Z}}} + [(c',d')]_{\sim_{\mathbb{Z}}},$$
$$[(a,b)]_{\sim_{\mathbb{Z}}} \cdot [(c,d)]_{\sim_{\mathbb{Z}}} = [(a',b')]_{\sim_{\mathbb{Z}}} \cdot [(c',d')]_{\sim_{\mathbb{Z}}},$$

kdykoli $(a,b) \sim_{\mathbb{Z}} (a',b')$ a $(c,d) \sim_{\mathbb{Z}} (c',d')$;

(c) operace +, − a inverz − podle naší definice souhlasí s operacemi danými stejnými symboly na „běžné“ verzi celých čísel při korespondenci

$$[(a,b)]_{\sim_{\mathbb{Z}}} \leftrightarrow a - b.$$

Konkrétně, pro operaci + toto znamená, že platí korespondence

$$[(a,b)]_{\sim_{\mathbb{Z}}} + [(c,d)]_{\sim_{\mathbb{Z}}} \leftrightarrow (a-b) + (c-d)$$

a nezávisí na výběru reprezentanta z tříd ekvivalence $[(a,b)]_{\sim_{\mathbb{Z}}}$ a $[(c,d)]_{\sim_{\mathbb{Z}}}$.

(3) Ověřte, že $\sim_{\mathbb{Q}}$ z definice 2.2.6 je skutečně ekvivalence a že operace + a · na $\mathbb{Q}$ jsou dobře definované (nezávisejí na výběru reprezentanta) a odpovídají „obvyklým“ operacím zlomků.

Posloupnosti, limity a reálná čísla

(1) Dokažte, že posloupnost $a : \mathbb{N} \to \mathbb{Q}$ je konvergentní právě tehdy, když

$$\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall m, n \geq n_0 : |x_m - x_n| < C\varepsilon$$

pro libovolnou **kladnou** konstantu $C \in \mathbb{Q}$.

(2) Dokažte, že každá posloupnost $a : \mathbb{N} \to \mathbb{Q}$ má nejvýše jednu limitu. Hint: použijte trojúhelníkovou nerovnost.

(3) Dokažte, že jsou-li x, y konvergentní posloupnosti racionálních čísel, pak je posloupnost $x \cdot y$ rovněž konvergentní. Kromě trojúhelníkové nerovnosti je zde třeba použít i lemma 3.2.10.

(4) Dokažte, že zobrazení ξ z (3.1) je
   - dobře definované – tzn. že když $p = q$, pak $[(p)] = [(q)]$ – a
   - prosté.

(5) Určete z definice suprema a infima $\inf \emptyset$ a $\sup \emptyset$.

(6) Dokažte, že $\sup X$ a $\inf X$ jsou určeny jednoznačně.

(7) Dokažte všechna (**proč?**) a (**dokažte!**) v důkazu tvrzení 3.3.12.

(8) Dokažte tvrzení 3.3.14. Doporučujeme čtenářům se zamyslet, jak tvrzení snadno plyne z axiomu úplnosti, aniž opakují konstrukci z jeho důkazu.

(9) Dokažte část (b) lemmatu 3.3.15.

(10) Dokažte, že lemma 3.3.16 je důsledkem tvrzení 3.2.11.