Gymnázium Evolution Jižní Město

Jakýsi úvod do matematické analýzy

Áďula vod Klepáčů

12. října 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

Část I

Reálná čísla a limity

Kapitola 1

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.

1.1 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 1.1.1 (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 1.1.1.

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

Příklad 1.1.2 (Dihedrální grupa)

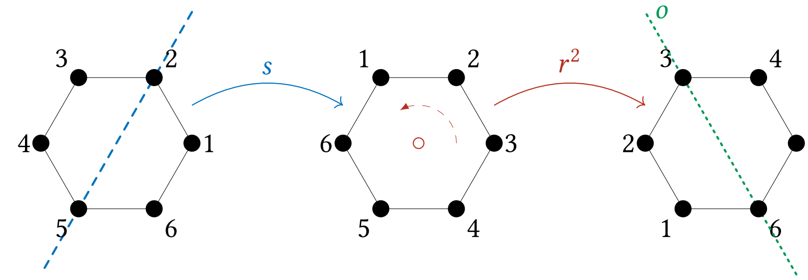
Ať P je pravidelný šestiúhelník v $\mathbb{R}^2$. Uvažme zobrazení $r : \mathbb{R}^2 \to \mathbb{R}^2$, které rotuje body v $\mathbb{R}^2$ o $60°$ (v kladném směru – proti směru hodinových ručiček) podle středu jeho uhlopříček, a zobrazení $s : \mathbb{R}^2 \to \mathbb{R}^2$, které reflektuje body v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

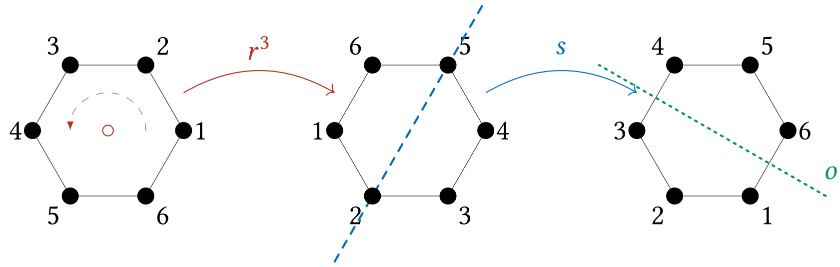
Po chvíli přemýšlení zjistíme, že rotace o $60, 120, 180, 240, 300$ a 360 stupňů zachovávají P. Všechny můžeme dostat jako složení r se sebou samým vícekrát. Například $r \circ r \circ r = r^3$ je rotace o $180°$. Přirozeně, rotace o $360°$ je identické zobrazení, což lze vyjádřit rovností $r^6 = \mathbb{1}_{\mathbb{R}^2}$.

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 1.1: Příklady složení reflexí a rotací.

Příklad 1.1.3 (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 1.1.2) 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 $X = \{1, \dots, n\}$, pak by to byly třeba právě transpozice $(1\ 2), (1\ 3), \dots, (1\ n)$. Tento fakt souvisí přímo s pozorováním z diskrétní matematiky, že každou permutaci lze rozložit na transpozice.

Příklad 1.1.4 (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

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

množina všech jeho n-tých odmocnin.

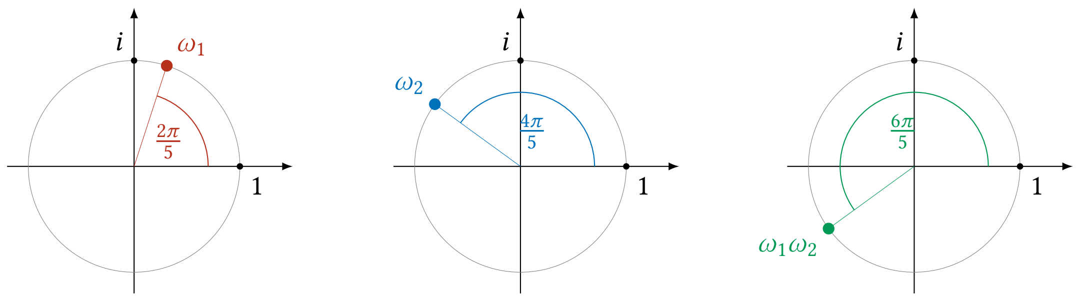
Tato množina obecně **není** grupa, neboť tím, že vynásobím dvě odmocniny komplexního čísla, nedostanu jeho jinou odmocninu – s jednou výjimkou, a tou je číslo 1. Totiž, $1 = \cos(2\pi) + i \cdot \sin(2\pi)$, a tedy všechny jeho třeba čtvrté odmocniny jsou

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

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 1.2: 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 1.1.5 (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 1.1.3. 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 1.1.2 a 1.1.4 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 1.1.6 (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

$$\begin{aligned} (r+s)\cdot t &= r\cdot t + s\cdot t, \\ t\cdot(r+s) &= t\cdot r + t\cdot s \end{aligned} \tag{1.1}$$

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

Poznámka 1.1.7

- 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 (1.1) 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 1.1.8

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

$$
\begin{aligned}
m \oplus n &\coloneqq (m + n) \bmod 6, \\
m \odot n &\coloneqq (m \cdot n) \bmod 6,
\end{aligned}
$$

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:

$$
\begin{aligned}
(2^{-1} \odot 2) \odot 3 &= 1 \odot 3 = 3, \\
2^{-1} \odot (2 \odot 3) &= 2^{-1} \odot 0 = 0,
\end{aligned}
$$

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 1.1.9 (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 1.1.10 (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 1.1.11

Dokažte, že každé těleso je oborem integrity.

1.2 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 1.2.1

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 pravý argument větší nebo roven levému, 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 tuto operaci symetrizují. Ovšem, operace $\cdot$ si stále drží svůj deformační charakter. Podobně jako tomu bylo u přirozených čísel s operacemi $+$ a $\cdot$, v celých číslech operace $\cdot$ 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 dokonale symetrickou strukturou – komutativním tělesem. Obě operace $+$ i $\cdot$ 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 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 aparátu pro práci s nekonečně malými vzdálenostmi.

Nyní k samotným konstrukcím. Naší 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 1.2.2 (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

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

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

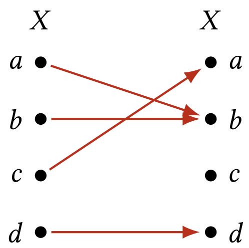
Přirozená čísla splňují tzv. axiom rekurze, který se obvykle zavádí v axiomatické definici přirozených čísel. V rámci našeho konstruktivního přístupu je třeba ho dokázat. My si ho zde však pouze uvedeme, neboť onen důkaz je silně logický a zdlouhavý.

Tvrzení 1.2.3 (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 1.3.

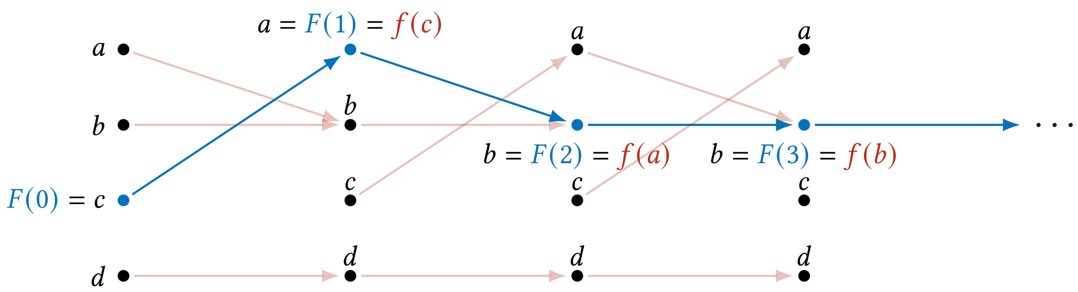


Obrázek 1.3: Zobrazení f z axiomu rekurze.

Zde $X = \{a, b, c, d\}$ a za počáteční prvek zvolme třeba c. Podle tvrzení 1.2.3 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 1.4.

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

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



Obrázek 1.4: Zobrazení F jako „rekurzor“ zobrazení f s počátečním bodem $F(0) = c$.

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 1.2.4 (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. Konkrétně, definujme

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

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 předposlední 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 obvyklé podobě. My budeme této korespondence drze využívat bez varování a mluvit o oboru integrity $(\mathbb{Z},+,-,0,\cdot,1)$.

Cvičení 1.2.5 (Hrátky s celými čísly)

Množinou $\mathbb{Z}$ zde myslíme tu z definice 1.2.4. Ověřte, že

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

(2) operace $+$ a $\cdot$ 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 znamená definovat na celých číslech „dělení“ – v algebraické hantýrce definovat inverz k operaci $\cdot$ 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 nelze vejmout absolutně. Zlomek a/b jsme totiž zvyklí vnímat jako třídu ekvivalence představující nějakou část celku. Tento pohled je snadné formalizovat.

Definice 1.2.6 (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 prvek $a/1 \in \mathbb{Q}$ s prvkem $a \in \mathbb{Z}$.

Cvičení 1.2.7 (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 jsme již zmiňovali, 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 2

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, ke kterému se zvolená posloupnost čísel „blíží“, ale nikdy ho „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 toho, že jsem 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 když člověk s ideou takřka sroste.

2.1 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. Toto *přiřčení* se nejsnadněji definuje jako zobrazení z přirozených čísel – to totiž přesně na každý prvek kodomény zobrazí jeho pořadí.

Definice 2.1.1 (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 2.1.2

Vnímaví čtenáři sobě jistě povšimli, že jsme na $\mathbb{N}$ nedefinovali žádné *uspořádání*. Ačkoliv 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 2.1.3 (Konvergentní posloupnost)

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

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

Poznámka 2.1.4

Aplikujeme intuitivní vysvětlení *zmenšování vzdálenosti* z odstavce nad definicí 2.1.3 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 2.1.5

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 naší (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. Ježto však pozbýváme aparátu, abychom koncepty limity a konvergence stmelili v jeden, jsme nuceni učinit mezikrok.

Definice 2.1.6 (Reálná čísla)

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

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

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 2.1.7 (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 $\lim a = L$.

2.2 Limity konvergentních posloupností

V této sekci dokážeme, že konvergentní posloupnosti mají limitu. Opačná implikace, tj. že posloupnosti majíce limitu konvergují, je téměř triviální. Potřebujeme dokázat jen jednu vlastnost absolutní hodnoty.

Lemma 2.2.1 (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. ■

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

Cvičení 2.2.2 (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 $\cdot$ 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 2.2.3

Dokažte, že jsou-li a, b konvergentní posloupnosti racionálních čísel, pak je posloupnost $a \cdot b$ rovněž konvergentní.

Racionální čísla jsou přirozeně součástí reálných prostřednictvím zobrazení

$$\begin{aligned} \xi : \mathbb{Q} &\hookrightarrow \mathbb{R}, \\ q &\mapsto [(q)], \end{aligned} \tag{2.1}$$

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

Varování 2.2.4

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 (2.1). Toto ztotožnění znamená vnímat racionální číslo $q \in \mathbb{Q}$ jako konvergentní posloupnost samých čísel q.

Cvičení 2.2.5

Dokažte, že zobrazení ξ z (2.1) 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 (2.1)) 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 nulové posloupnosti v $\mathbb{R}$ nemají 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.

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 2.2.6

Každá posloupnost majíc 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. ∎

2.2.1 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. *kompletní*, 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 si, 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 2.2.7

Důležitá myšlenka, jiř 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.

Konkrétně, 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

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

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 věrni intuitivnímu vnímání výrazu $|x - y|$ jako „vzdálenosti" čísel x a y.

Definice 2.2.8 (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 $n \in \mathbb{N}$.

Lemma 2.2.9

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 2.2.10 (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 2.2.11

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 2.2.12 ($\mathbb{R}$ 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 2.2.10 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 2.2.11 má a limitu $[(a)] \in \mathbb{R}$. Tím je důkaz hotov. ■

Důsledek 2.2.13

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 2.2.11 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 2.2.12 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 2.2.2), 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 2.2.11 platí $\lim a = [(a)]$. To ovšem přesně znamená, že $f([(a)]) = L$.

Tím je důkaz hotov. ∎

Seznam cvičení

Číselné obory

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

(2) Množinou $\mathbb{Z}$ zde myslíme tu z definice 1.2.4. Ověřte, že

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

(b) operace $+$ a $\cdot$ 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 1.2.6 je skutečně ekvivalence a že operace $+$ a $\cdot$ 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.

(4) Dokažte, že zobrazení ξ z (2.1) je

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