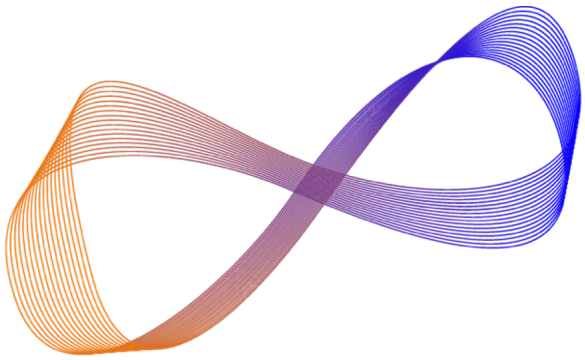
Gymnázium Evolution Jižní Město



Jakýsi úvod do matematické analýzy

Áďula vod Klepáčů

3. 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)

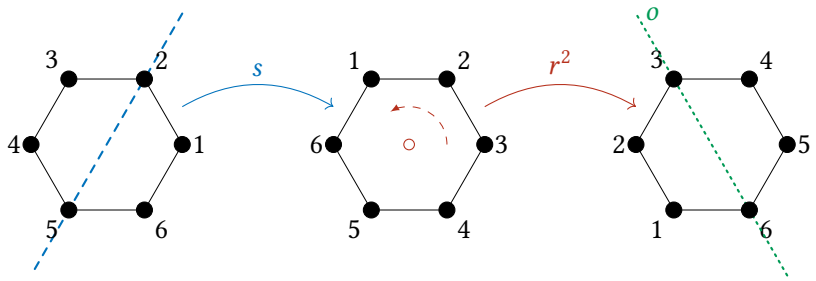
Ať P je pravidelný šestiúhelník v $\mathbb{R}^2$. Uvažme zobrazení $r : \mathbb{R}^2 \to \mathbb{R}^2$, které rotuje body v $\mathbb{R}^2$ o $60°$ (v kladném směru – proti směru hodinových ručiček) podle středu jeho uhlopříček, a zobrazení $s : \mathbb{R}^2 \to \mathbb{R}^2$, které reflektuje body v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

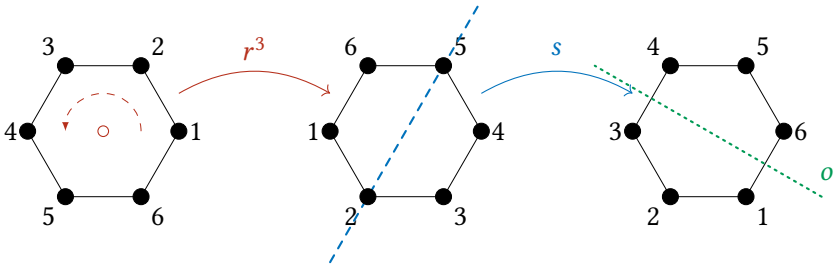
Po chvíli přemýšlení zjistíme, že rotace o $60, 120, 180, 240, 300$ a 360 stupňů zachovávají P. Všechny můžeme dostat jako složení r se sebou samým vícekrát. Například $r \circ r \circ r = r^3$ je rotace o $180°$. Přirozeně, rotace o $360°$ je identické zobrazení, což lze vyjádřit rovností $r^6 = \mathbb{1}_{\mathbb{R}^2}$.

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 $X = \{1, \ldots, n\}$, 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 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

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

množina všech jeho n-tých odmocnin.

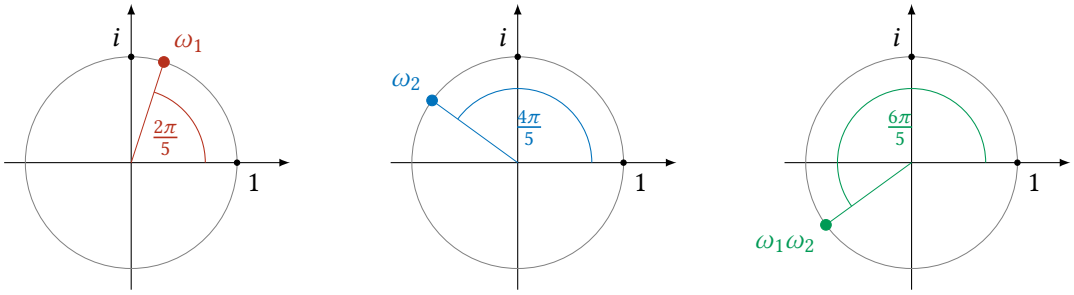
Tato množina obecně **není** grupa, neboť tím, že vynásobím dvě odmocniny komplexního čísla, nedostanu jeho jinou odmocninu – s jednou výjimkou, a tou je číslo 1. Totiž, $1 = \cos(2\pi) + i \cdot \sin(2\pi)$, a tedy všechny jeho třeba čtvrté odmocniny jsou

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

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 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

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

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 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.

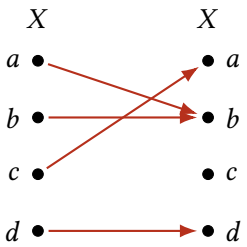
Přirozená čísla splňují tzv. axiom rekurze, který se obvykle zavádí v axiomatické definici přirozených čísel. V rámci našeho konstruktivního přístupu je třeba ho dokázat. My si ho zde však pouze uvedeme, neboť onen důkaz je silně logický a zdlouhavý.

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.

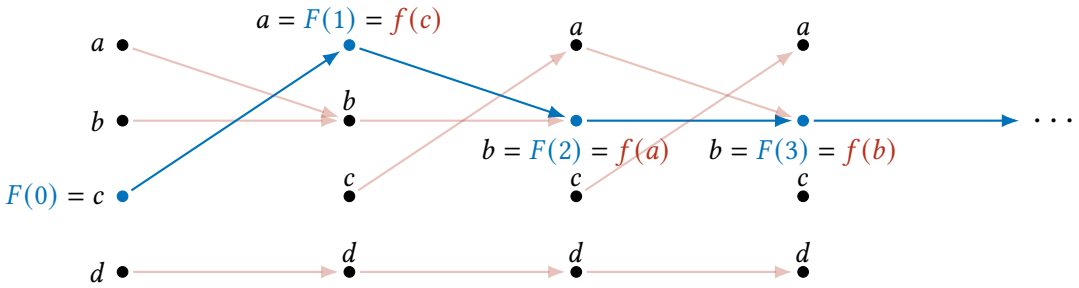


Obrázek 1.3: Zobrazení f z axiomu rekurze.

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

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

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 · 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.

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 · 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 $[(c,d)]_{\sim_{\mathbb{Z}}}$.