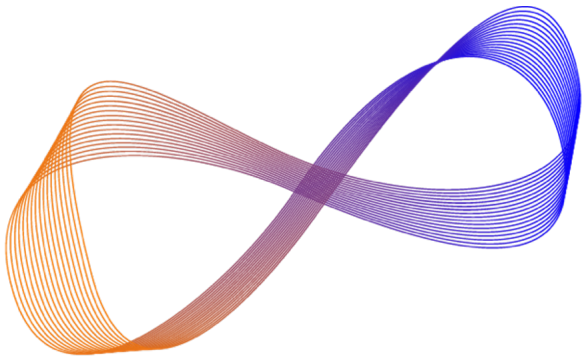
Gymnázium Evolution Jižní Město



Jakýsi úvod do matematické analýzy

Áďula vod Klepáčů

20. září 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 $C \not\subseteq A$. 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

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

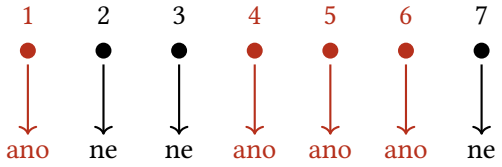
Je dobré si povšimnout, že $\emptyset$ je z definice podmnožinou každé množiny. Totiž, $x \in \emptyset$ je výrok vždy lživý a, pamatujte, ze lži plyne (aspoň v matematické logice) jak lež, tak pravda. Tedy, výrok $x \in \emptyset \implies x \in A$ je vždy pravdivý. Filosofickou otázku, zda dává smysl, 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 $A \cap B$.

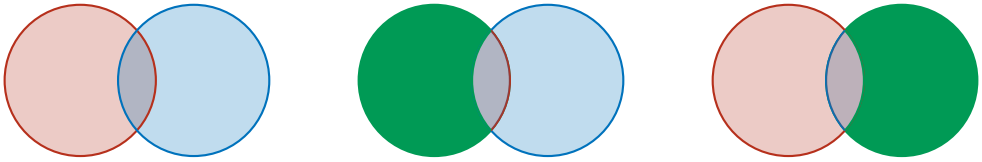
Obrázek 1.3: Operace průniku množin.

- *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

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

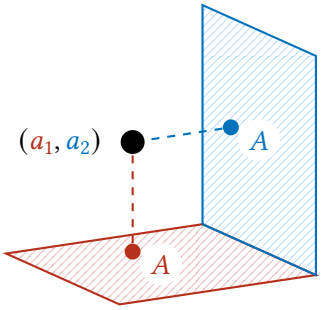
to jest jako uspořádanou dvojici obsahující prvek x a uspořádanou dvojici (y, z). Zápis pomocí množin se s rostoucím počtem prvků velmi rychle komplikuje. Všimněte si, že už v drobném případě tří prvků dostaneme

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

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.

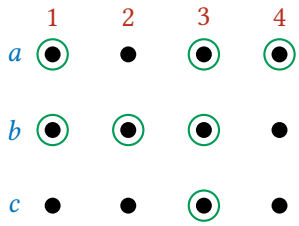
Máme-li k dispozici výčty prvků množin A a B, je pro představu dobré kreslit relace $R \subseteq A \times B$ do tzv. mříží. Ty tvoříme tak, že nakreslíme doslovnou mříž teček s $\#A$ sloupci, resp. $\#B$ řádky, pro každý prvek množiny A, resp. množiny B, a tečky na pozicích odpovídající párům $(a, b)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

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

a mezi nimi relaci

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

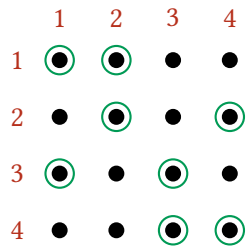
bude jejím vyobrazením mříž na obrázku 1.6.



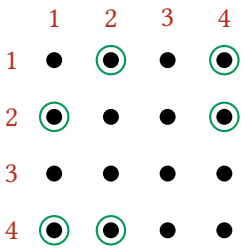
Obrázek 1.6: Mříž relace $R \subseteq A \times B$.

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

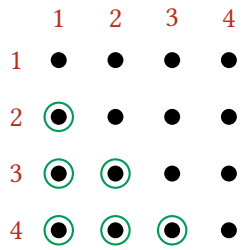
- *reflexivní*, když je každý prvek v relaci R sám se sebou, tj. $\forall x \in A : xRx$;
- *antireflexivní*, když žádný prvek není v relaci R sám se sebou, tj. $\forall x : (x, x) \notin R$;
- *symetrická*, když s každým párem prvků obsahuje i ten obrácený, tj. $\forall x, y \in A : xRy \Rightarrow yRx$;
- *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.

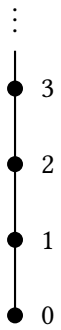
Uspořádáním (ať už ostrým či neostrým) naopak *splňujícím* onu podmínku říkáme *lineární*.

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.

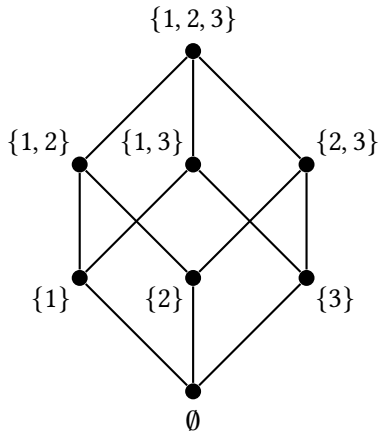


Obrázek 1.9: Hasseho diagram uspořádané množiny $(\mathbb{N}, \leq)$.

(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.



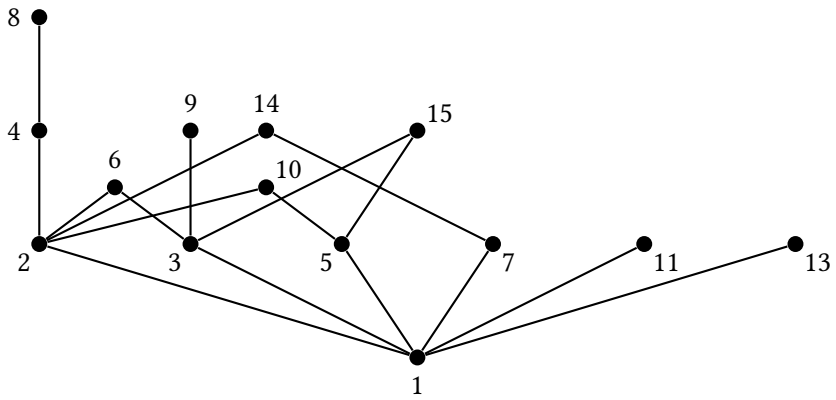
Obrázek 1.10: Hasseho diagram uspořádané množiny $(2^A, \subseteq)$ pro $A = \{1, 2, 3\}$.

(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)

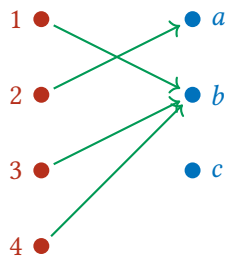
Ať $R \subseteq A \times B$ je relace mezi A a B. Nazveme R *zobrazením* (z A do B), pokud splňuje

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

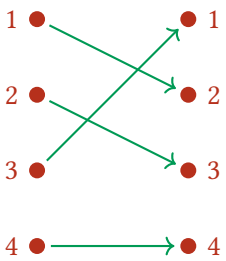
Zobrazení mezi množinami obvykle zapisujeme malými písmeny latinské abecedy počínaje písmenem f (od **f**unkce, jak se některým speciálním typům zobrazení často říká). Fakt, že f je zobrazení z A do B, symbolizujeme zápisem $f : A \to B$ nebo též $A \xrightarrow{f} B$.

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. $(g \cdot h) \cdot k = g \cdot (h \cdot k)$),
- pro každý prvek $g \in G$ existuje prvek $g^{-1} \in G$ splňující $g \cdot g^{-1} = g^{-1} \cdot g = 1$, zvaný *inverz*, a
- existuje prvek $1 \in G$ splňující pro každé $g \in G$ rovnost $g \cdot 1 = 1 \cdot g = g$, zvaný *neutrální*,

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

Tato definice si zaslouží několik 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 odrážet koncept *symetrie*. Uvedeme si několik příkladů.

Příklad 2.1.2 (Dihedrální grupa)

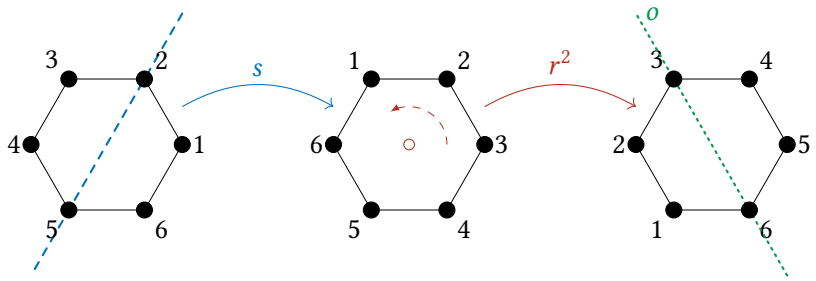
Ať P je pravidelný šestiúhelník v $\mathbb{R}^2$. Uvažme zobrazení $r : \mathbb{R}^2 \to \mathbb{R}^2$, které rotuje body v $\mathbb{R}^2$ o $60°$ podle středu jeho uhlopříček, a zobrazení $s : \mathbb{R}^2 \to \mathbb{R}^2$, které reflektuje body v $\mathbb{R}^2$ podle kterékoli (ale fixní) jeho uhlopříčky.

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* (uvědomme si, že r i s jsou **bijekce**) a neutrálním prvkem je *identické zobrazení* na $\mathbb{R}^2$.

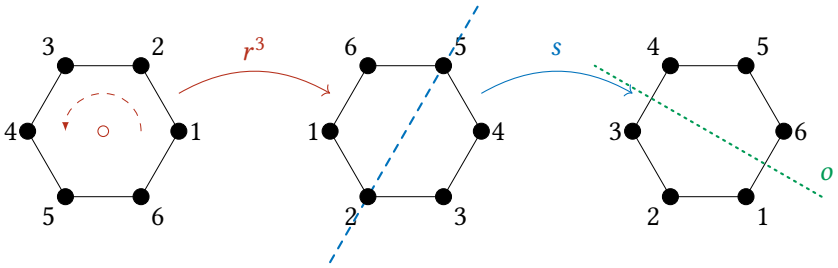
Po chvíli přemýšlení zjistíme, že rotace o $60, 120, 180, 240, 300$ a 360 stupňů zachovávají P. Všechny můžeme dostat jako složení r se sebou samým vícekrát. Například $r \circ r \circ r = r^3$ je rotace o $180°$. Přirozeně, rotace o $360°$ je identické zobrazení, což lze vyjádřit rovností $r^6 = \mathbb{1}_{\mathbb{R}^2}$.

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 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 zobrazení r a s.

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 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 dostali 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)

V komplexních číslech má každé číslo 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, 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.

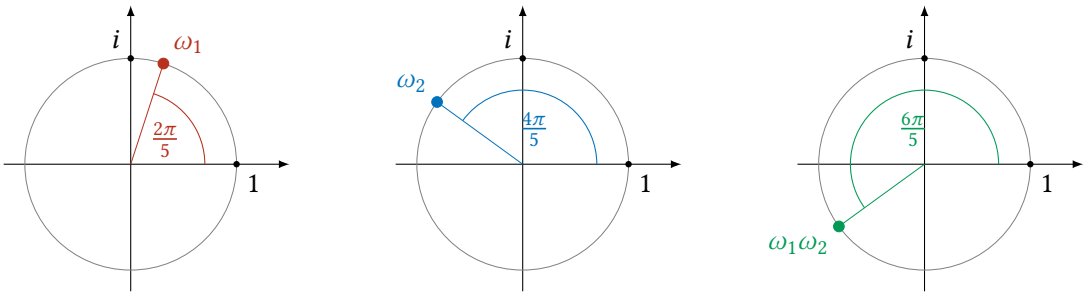
Tato množina obecně **není** grupa, neboť tím, že vynásobím dvě odmocniny komplexního čísla, nedostanu jeho jinou odmocninu – s jednou výjimkou, a tou je číslo 1. Totiž, $1 = \cos(2\pi) + i \cdot \sin(2\pi)$, a tedy všechny jeho třeba čtvrté odmocniny jsou

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

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 se nám podařilo 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 se každý prvek dal 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 monoid 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 $X \to X$) **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 všech zobrazení $X \to X$ je n^n.

Příklady 2.1.2 a 2.1.4 žádných přirozených zobecnění nenabízejí. Přidáme-li k dihedrální grupě transformace 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. Neboť, 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. Vskutku, 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) je 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 vytvářeti 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.