Logika a teorie množin (NMTM503)

Martin Rmoutil

17. ledna 2023

Obsah

Předmluva ii

1 Motivace 1

1.1 Paradoxy nekonečna . . . 1
1.2 Porovnávání nekonečných množin podle počtu prvků . . . 3
1.3 Trocha historie – důvody pro vznik a upřesňování TM . . . 9

2 Základní pojmy TM 12

2.1 Naivní teorie množin . . . 12
2.1.1 Definice množiny . . . 12
2.1.2 Rovnost množin v NTM . . . 13
2.1.3 Způsoby zadání množin v NTM . . . 14
2.2 Operace s množinami a vztahy mezi nimi . . . 17
2.2.1 Jednoduché základní operace s konečně mnoha množinami . . . 17
2.2.2 Operace s nekonečně mnoha množinami . . . 19
2.2.3 Důkazy rovností množin a De Morganovy vzorce . . . 23
2.3 Binární relace . . . 26
2.3.1 Základní pojmy . . . 29
2.3.2 Typy relací . . . 31
2.3.3 Relace ekvivalence . . . 33
2.4 Relace uspořádání . . . 37
2.4.1 Příklady . . . 38
2.4.2 Maximum, maximální prvek, supremum . . . 43
2.5 Funkce . . . 48

3 Základní výsledky TM 52

3.1 Cantorova-Bernsteinova věta . . . 52
3.1.1 Věta o pevném bodě . . . 52
3.1.2 Důkaz Cantorovy-Bernsteinovy věty . . . 54

Předmluva

Toto je můj doprovodný text k přednášce *Logika a teorie množin* pro studenty učitelství na MFF UK. Nelze ho vnímat jako učebnici a sám o sobě aktuálně nestačí k přípravě na zkoušku: na textu pracuji ve volných chvílích a vzniká pozvolna. Lze ovšem říci, že v zásadě sleduje program přednášky, takže dokud věci z přednášky budete nacházet v tomto textu, můžete se na něj spolehnout. K úplné přípravě ke zkoušce však budete muset pracovat i s vlastními poznámkami.

Mým cílem je, aby se tyto poznámky postupně proměnily v ucelená skripta, která budou vhodným způsobem doplňovat přednášku. Je to potřeba mimo jiné kvůli tomu, že délka kurzu je v příslušném ročníku učitelského studia omezena každoročními učitelskými praxemi, které zaberou zhruba první čtyři týdny semestru. Každému, kdo o obsahu tohoto předmětu něco ví, je přitom jasné, že i plný kurz s hodinovou dotací 2/0, sotva stačí k důstojnému představení těchto základních matematických disciplín. Skripta, jejichž zárodek právě čtete, by ve finále měla všem zájemcům poskytnout doplnění látky do přiměřeně úplného celku. Zároveň by měla nabídnout aspoň nějaká, vesměs lehká, cvičení, která by studenty podnítila k procvičení práce s probíranými pojmy: ta totiž pro začátečníky obvykle není snadná a správnému způsobu přemýšlení o teorii množin se většina z nich musí teprve naučit.

V tomto semestru budu pokračovat v psaní a doufejme, že na jeho konci, tedy v čase, kdy se mnozí začnete intenzivněji připravovat na zkoušku, už bude tento text k něčemu.

Aby se rozsah materiálu udržel v rozumných mezích a zároveň podstatné myšlenky nezanikly ve vřavě technických detailů, dovolím si u čtenářů předpokládat praktické seznámení s mnoha základními pojmy, byť je současně budu upřesňovat a učit jejich správnému používání (které je někdy v rozporu se zažitými zlozvyky). Příklady takových pojmů jsou různé matematické značky, číselné obory nebo funkce; třeba se symboly pro kvantifikátory jste už všichni seznámeni, a tak je budu používat bez obav z možného nedorozumění. Od jistého momentu (který bez obtíží rozpoznáte) však s nimi budeme pracovat v jistém smyslu přesněji.

Struktura tohoto kurzu se liší od jiných podobných kurzů, totéž lze říci o tomto učebním textu. V první fázi vám představím několik motivačních úvah (to je zřejmě běžné). Pak ale nenaskočíme rovnou do formální teorie, nýbrž budeme se nějakou dobu pohybovat v tzv. *naivní teorii množin*, byť budeme od začátku vědět, že tato teorie nenaplňuje moderní standardy matematické přesnosti. Formální teorii se nicméně budeme věnovat až o něco později: popíšeme si pak způsob, jak konstruovat formule (tj. smysluplná vyjádření) v jazyce teorie množin pomocí formálních symbolů (které už vlastně znáte) a některé takové formule prohlásíme za axiomy teorie množin. Z nich pak odvodíme vše potřebné k tomu, aby vše dříve budované v naivní teorii bylo postaveno na pevné základy teorie axiomatické. Hlavní smysl tohoto postupu je vyhnout se přílišnému počátečnímu náporu formálních pojmů, které mohou leckterého studenta předčasně odradit; místo toho budeme ze začátku pracovat s pojmy v zásadě dobře známými, jen trochu jinak, a později si ukážeme, jak tyto (známé) věci zapadají do axiomatické teorie množin. Chovám naději, že se tak látka tohoto kurzu teorie stane stravitelnější a srozumitelnější.

Autor

Kapitola 1

Motivace

1.1 Paradoxy nekonečna

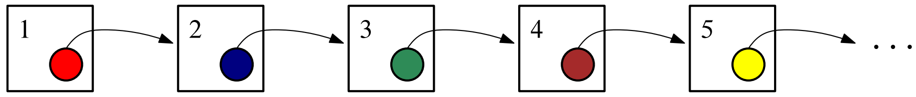
Teorie množin, jak ji známe dnes, vznikla na přelomu 19. a 20. století zásluhou německého matematika Georga Cantora (1845 – 1918). Velká část moderní matematiky se neobejde bez práce s pojmem nekonečna a právě Cantor byl tím, kdo s tímto konceptem začal pracovat bez předsudků vyplývajících z naší intuice ovlivněné světem plným konečných veličin. To, čemu se před Cantorem říkalo „paradoxy nekonečna“, se po Cantorovi stalo běžně přijímanými vlastnostmi, které jen málokterý matematik nějak zpochybňuje. Pojďme si na úvod představit konkrétní takový „paradox“.

1.1 Příklad (Hilbertův hotel)**.** V jednom hotelu v turistickém centru jistého krásného města pracoval recepční s kvalifikací, která by se na první pohled mohla zdát poněkud nepřiměřenou – byl to německý matematik David Hilbert (1862 – 1943).

Návštěvník znalý moderní matematiky by v něm rychle rozpoznal vůdčí osobnost matematiky přelomu století: Hilbert například jako první uspokojivě vybudoval axiomatickou teorii eukleidovské geometrie a patří mu celá řada dalších významných výsledků. Možná nejvíce se však zapsal do historie svým seznamem 23 nejdůležitějších problémů matematiky, které nevyřešil, místo toho je souhrnně představil na Mezinárodním matematickém kongresu v Paříži roku 1900: nasměroval tím úsilí matematiků na další století.

Proč tedy Hilbert pracoval jako recepční v hotelu? Na takovou práci obvykle není potřeba geniálního mozku; tento hotel – Hilbertův hotel – byl ale speciální. Byl totiž nekonečný! Přesněji, pro každé přirozené číslo od 1 až do nekonečna měl přesně jeden (jednolůžkový a bez přistýlky!) pokoj a každý pokoj měl jediné přirozené číslo. Zvládnout ubytování hostů v takovém hotelu už může být netriviální, zvlášť, když je hotel plně obsazený.

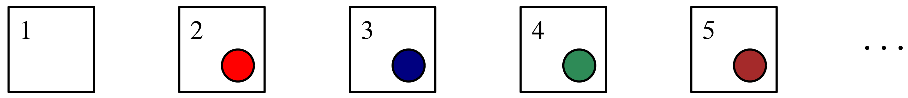
Při plně obsazeném nekonečném hotelu by běžný recepční patrně poslal nově příchozího zájemce o ubytování pryč s tím, že mají plno, a promeškal by tím hotelu příležitost vydělat více peněz. Ale ne Hilbert! Ten si snadno uvědomil, že nového hosta snadno ubytuje i v plně obsazeném Hilbertově hotelu. Jak? Stačí *každého už ubytovaného hosta přestěhovat do pokoje*



Obrázek 1.1: Původní plné obsazení hotelu

s číslem o jedna větším, čímž se uvolní pokoj 1 pro nového hosta.

V běžném hotelu by to pochopitelně nefungovalo, neboť některý z pokojů má největší číslo a tam ubytovaného hosta by tedy šlo přestěhovat leda tak na střechu. V Hilbertově hotelu však tato logistická operace bude fungovat, neboť největší číslo nemá žádný pokoj.

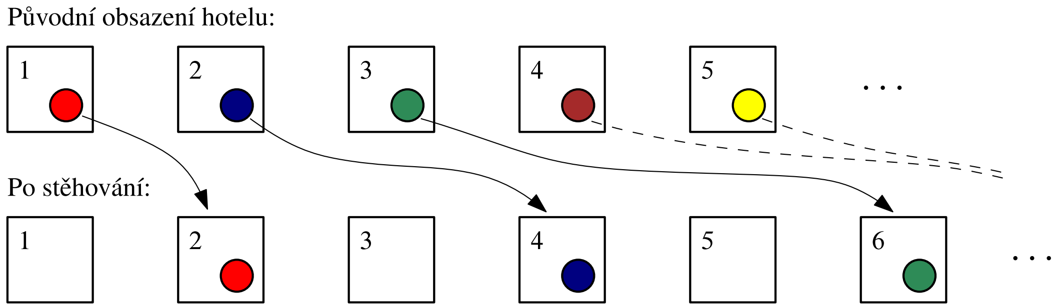


Obrázek 1.2: Obsazení hotelu po stěhovací akci

Po ubytování nového hosta však přijede celý autobus plný čínských turistů. Běžný recepční by po zkušenosti s předchozím trikem zajásal: stačilo by přece pro každého nového hosta zopakovat předchozí postup. Jestliže by přijelo k nových hostů, každý už ubytovaný host by se k-krát přestěhoval do pokoje s číslem o jedničku vyšším a bylo by hotovo. Mírně nadprůměrný recepční by pak možná pochopil, že stačí provést pouze jedno stěhování – pro každé n hosta ubytovaného v n-tém pokoji přestěhujeme do pokoje s číslem $n + k$.

Hilbert se však podíval pořádně. Z recepce viděl předek autobusu, který zrovna zastavil před hlavním vchodem, neviděl však jeho konec. Šel se tedy podívat ven ze dveří a zjistil něco nečekaného: autobus žádný konec neměl, byl nekonečný! A v něm bylo nekonečně mnoho sedaček: pro každé přirozené číslo přesně jedna a na každé z nich seděl jeden čínský turista se zájmem o ubytování. Zde by běžný recepční mohl zkoušet různé postupy. Je jasné, že posunout všechny už ubytované hosty do pokoje s číslem o k větším, je zbytečné pro $k = 1$. Mohl by tedy zkusit $k = 9^{9^{9^9}}$. Tím by ubytoval prvních $9^{9^{9^9}}$ turistů z autobusu, což není špatný výsledek. Stále by jich však drtivá většina čekala. Postup by tedy mohl opakovat; i po $9^{9^{9^9}}$ opakováních by však měl ubytováno jen $\left(9^{9^{9^9}}\right)^2$ nových zájemců a drtivá většina by jich stále čekala v autobusu. Vynalézavý recepční by mohl v každé další iteraci ubytovat dvojnásobný počet hostů; tím by počet nových hostů ubytovaných na jedno stěhování rostl geometrickou řadou, stále by však bylo nutné provést nekonečně mnoho takových iterací, přičemž po každé z nich by stále bylo ubytováno přesně 0% zájemců z čínského autobusu.

Právě pro takové případy pracoval v hotelu Hilbert: vymyslel způsob, jak všechny nové zájemce ubytovat na jediné stěhování. Jednoduše každého už ubytovaného hosta nechal přestěhovat do pokoje s dvojnásobným číslem. Tím se uvolní všechny pokoje s lichými čísly, kterých je nekonečně mnoho; je jich ale dost na to, aby do nich Hilbert umístil všechny hosty z autobusu, v němž je pro každé, tedy liché i sudé, přirozené číslo jeden host? Odpověď je kladná: host ze sedačky s číslem k bude ubytován v pokoji číslo $2k - 1$.



Obrázek 1.3: Stěhování do sudých pokojů

Zdálo by se, že tím výčet možných problémů skončil a recepční už více nápadů nepotřebuje. Náhle však k plně obsazenému Hilbertovu hotelu přijelo nekonečně mnoho plně obsazených nekonečných čínských autobusů. Jejich řidiči se postupně dostavili za recepčním Hilbertem a když Hilbert dokončil tyto postupné rozmluvy s nekonečně mnoha řidiči (patrně jeho superschopnost), měl jasno v tom, že všichni hosté ze všech autobusů se v hotelu chtějí ubytovat. Hilbert by mohl pro každý autobus provést stejný proces, jako nedávno pro jediný nekonečný autobus; tak by ale bylo potřeba nekonečně mnoho iterací: pro každý nový autobus jedna. Hilbert to však zvládl na jediné, byť komplikované, stěhování. Zvládli byste to i vy? A zvládli byste to tak, abyste obtěžovali 0% už ubytovaných hostů? $\triangle$

Myslím, že podstata právě uvedeného příkladu je jasná: nekonečno má jisté překvapivé vlastnosti. Ubytování jednoho hosta tak trochu připomíná fakt, který znáte už z prvního semestru, kdy jsme pracovali s rozšířenou reálnou osou: $1 + \infty = \infty$. Přičteme-li jednoho hosta k nekonečnu, dostaneme zase to stejné nekonečno. Příjezd nekonečného autobusu by se dal intuitivně popsat rovností $\infty + \infty = \infty$, i ta podle naší definice operací na $\mathbb{R}^*$ platí.[1] Jde ovšem jen o přirovnání, matematickou podstatu triků recepčního Hilberta budeme vysvětlovat poněkud jinak, a to pomocí teorie množin, v níž pojem „nekonečna“ dostane zcela konkrétní obsah (na rozdíl od prvního semestru, kdy jsme symbol ∞ používali v podstatě jen jako pomůcku k vyjadřování).

1.2 Porovnávání nekonečných množin podle počtu prvků

Můžeme hovořit o množině hostů a množině pokojů, přičemž chceme umět poznat, že množiny mají stejný počet prvků. U konečných množin, řekněme u nějakých dvou množin A, B, jsme zvyklí to zjišťovat tak, že prostě spočítáme jejich prvky a oba počty porovnáme:

$$|A| = m, \quad |B| = n;$$

[1] Příjezd nekonečného počtu nekonečných autobusů by v této hrubé analogii odpovídal platné (podle definice aritmetiky na $\mathbb{R}^*$) rovnosti $\infty + \infty \cdot \infty = \infty$.

množiny A a B mají stejný počet prvků, pokud $m = n$. Jak ale máme postupovat, pokud A a B jsou nekonečné, třeba $A = \mathbb{Q}$ a $B = \mathbb{R}$? Je jasné, že prvky už nelze „spočítat"; můžeme je ovšem spárovat. Pokud se nám podaří uspořádat prvky do dvojic a „vyjde nám to", mají obě množiny stejný počet prvků; pokud to není možné, počty prvků jsou různé.

To, že dvě nekonečna jsou „stejně velká" definujeme v teorii množin: dvě množiny jsou stejně velké, pokud mezi nimi existuje vzájemně jednoznačné zobrazení (tj. zobrazení prosté a na, neboli bijekce). V našem příkladě s Hilbertovým hotelem vlastně hledáme bijekci mezi množinami hostů a pokojů, přičemž konkrétní host je zobrazen na konkrétní pokoj prostřednictvím ubytování. Když tedy například přijel jeden nekonečný autobus, Hilbertovo řešení této situace lze interpretovat jako bijekci mezi množinou $\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$ a množinou $\mathbb{N}$: dvojici $(k, 0)$, která reprezentuje hosta už ubytovaného v pokoji s číslem k, jsme přiřadili číslo $2k$ a dvojici $(k, 1)$ reprezentující cestujícího na sedačce k jsme přiřadili přirozené číslo $2k - 1$. To dohromady dává bijekci; formálně jde o funkci $f : \mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\} \to \mathbb{N}$ definovanou předpisem

$$f(k,l) = \begin{cases} 2k, & \text{pokud } l = 0 \\ 2k - 1, & \text{pokud } l = 1. \end{cases}$$

Zobrazení f je zjevně prosté a na (snadno najdete inverzní zobrazení), takže jsme vlastně dokázali, že sjednocení dvou „paralelních kopií $\mathbb{N}$" je stejně velké (učeně: má stejnou mohutnost) jako množina $\mathbb{N}$ sama.[2]

Situace, kdy k Hilbertovu hotelu přijede nekonečně mnoho nekonečných autobusů plně obsazených zájemci o ubytování, se dá interpretovat jako hledání bijekce $\mathbb{N} \times \mathbb{N}$ na $\mathbb{N}$, kde dvojice $(k, l) \in \mathbb{N} \times \mathbb{N}$ reprezentuje cestujícího na k-té sedačce l-tého autobusu. I takové bijekce existují (pochopitelně je jich možných více) a není obtížné některé z nich popsat (podíváme se na to dále, ale můžete se nad tím zamyslet už zde). Konstatujeme tedy (prozatím bez důkazu), že množina $\mathbb{N} \times \mathbb{N}$ má stejnou mohutnost jako $\mathbb{N}$.

1.2 Příklad. Další příklady dvojic množin o stejné mohutnosti jsou třeba následující. Pro snazší zápis si vypůjčíme značení, které pořádně zavedeme a probereme až později: píšeme

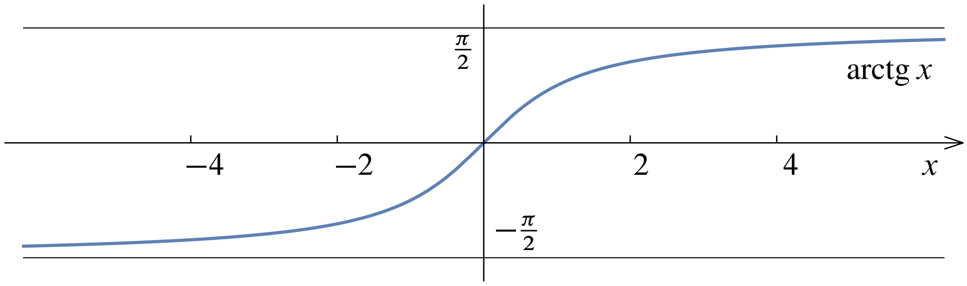
$$A \approx B,$$

pokud množiny A a B mají stejnou mohutnost, tj. existuje bijekce A na B.

- $\mathbb{N} \approx \underbrace{\{k \in \mathbb{N} :\ 2|k\}}_{=:\, S}$, tj. množina všech sudých přirozených čísel má stejnou mohutnost jako množina všech přirozených čísel (včetně lichých). O této skutečnosti svědčí například bijekce $f_1 : \mathbb{N} \to S$, $f_1(n) = 2n$.[3]
- $\mathbb{R} \approx \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Příslušná bijekce je $f_2 := \operatorname{arctg}$.

[2]Pokud nějaká množina A má stejnou mohutnost jako $\mathbb{N}$, neboli existuje bijekce A na $\mathbb{N}$, říkáme, že množina A je *spočetná*. Formálně tuto definici odložíme na později, je ale dobré mít ji na paměti.

[3]Je zřejmé, že jde o bijekci, její inverzní zobrazení je $(f_1)^{-1} : S \to \mathbb{N}$, $(f_1)^{-1}(k) = k/2$.



Obrázek 1.4: Graf funkce arctg

- $\mathbb{R} \approx (0,1)$: jak asi tušíte, jde o podobný příklad jako výše, stačí modifikovat funkci arctg. Funguje třeba funkce $f_3\colon \mathbb{R} \to (0,1)$, $f_3(x) = \frac{1}{\pi}\left(\frac{\pi}{2} + \operatorname{arctg} x\right)$. (Nakreslete si graf!)

- Protože $\mathbb{R} \approx \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ a zároveň $\mathbb{R} \approx (0,1)$, o čemž svědčí bijekce f_2 a f_3, můžeme snadno odvodit, že $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \approx (0,1)$. Skutečně, složená funkce $g := f_3 \circ (f_2)^{-1}$ je totiž bijekce $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to (0,1)$, což snadno ověříte (napište si vzorec: $g(x) = \ldots$).

- $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \approx (0,1)$: pochopitelně existuje mnohem jednodušší důkaz tohoto faktu, než je ten uvedený v předchozím bodě. Třeba funkce $f_4\colon (0,1) \to \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, $f_4(x) = -\frac{\pi}{2} + \pi x$, je jednoduchým vzorcem daná bijekce mezi oběma intervaly: to jistě dovedete snadno ověřit, jde totiž o rostoucí lineární funkci, jejíž limity v krajních bodech definičního oboru $(0,1)$ snadno spočtete.

  Poznamenávám ještě, že $f_4\colon (0,1) \to \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, je tedy v opačném směru, „než jsme chtěli“. Je jasné, že na tom nezáleží, protože $(f_4)^{-1}\colon \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to (0,1)$ je samozřejmě také bijekce (ve „správném“ směru). Toto pozorování jde pochopitelně zobecnit: inverzní zobrazení k libovolné bijekci je opět bijekce, a to v opačném směru. Jinými slovy, relace $\approx$ je *symetrická*, tj. $A \approx B \Leftrightarrow B \approx A$. △

Konečnost a nekonečnost: Pojďme se stručně zamyslet nad filosofickými důsledky toho, co jsme právě na různých příkladech (včetně Hilbertova hotelu) viděli, zejména nad rozdíly v chování konečných a nekonečných množin. Pojem *konečnosti* zatím chápeme spíše intuitivně a máme jím na mysli konečný počet prvků.[4] Třeba množina $\{-\infty, \infty\}$ konečná je (obsahuje dva prvky, a to $-\infty$ a ∞), zatímco interval $(0,1)$ je množina nekonečná (obsahuje všechna reálná čísla ostře mezi nulou a jedničkou, kterých je „nekonečně mnoho“).

Uvažujme libovolnou neprázdnou „konečnou“ množinu A a nějakou její vlastní podmnožinu $B \subset A$.[5] Jestliže A má n prvků a B má k prvků, pak nám naše intuice velí očekávat, že

[4] Mohli bychom to poněkud upřesnit a říci, že množina je konečná, jestliže počet jejích prvků odpovídá některému přirozenému číslu. Nebo třeba ještě rigorózněji: A je konečná, jestliže $\exists n \in \mathbb{N}\colon A \approx \{0, 1, \ldots, n-1\}$. Protože však přirozená čísla (tím spíše množinu $\mathbb{N}$) také zatím chápeme spíše intuitivně, příliš si tím nepomůžeme.

[5] Na rozdíl třeba od matematické analýzy, v teorii množin je zvykem rozlišovat symboly $\subset$ a $\subseteq$, z nichž pouze druhý připouští rovnost mezi oběma množinami. Této konvence se zde budeme držet.

nezbytně $k < n$. U konečných množin to skutečně funguje tímto způsobem: podmnožina, v níž „některé prvky chybí“ je skutečně „menší“, má (ostře) menší mohutnost; rozdíl těchto mohutností je přitom roven počtu „chybějících“ prvků. Speciálně mezi množinami A a B neexistuje žádná bijekce.

Naproti tomu v příkladu výše jsme viděli několik dvojic nekonečných množin o stejné mohutnosti (tj. bijekce existuje), přičemž ve všech čtyřech případech byla jedna z obou množin vlastní podmnožinou druhé: $S \subset \mathbb{N}$, $(0,1) \subset \mathbb{R}$ atd. Opakovaně jsme tedy byli svědky porušení „principu“, že *část je menší než celek*: u nekonečných množin tomu tak nemusí být – a právě to je ve skutečnosti to podstatné, co je odlišuje od množin konečných.

Množina je totiž nekonečná, právě když existuje její vlastní podmnožina o stejné mohutnosti (tj. existuje bijekce na vlastní podmnožinu).

Ve světě konečných množin toto možné není, což je intuitivně zřejmé. Netriviální informace, kterou výše uvedený výrok přináší, je, že u libovolné nekonečné množiny toto naopak možné je. (Tj. pokud ne, množina není nekonečná.)

Jsou všechny nekonečné množiny stejně velké? Ještě jsme se zde přímo nesetkali s dvojicí množin, jejichž mohutnosti by byly různé. Pokud by platilo, že ve skutečnosti mezi libovolnými dvěma nekonečnými množinami existuje bijekce, muselo by platit i $\mathbb{N} \approx \mathbb{R}$. Pojďme si nyní pomocí klasického důkazu tzv. *Cantorovou diagonální metodou* dokázat, že tomu tak není, a že tedy existují různě velké nekonečné množiny:

1.3 Věta (Cantor)**.** $\mathbb{R} \not\approx \mathbb{N}$.

Důkaz. Pro potřeby tohoto důkazu musíme předpokládat, že víme, co jsou reálná čísla, a známe některé jejich základní vlastnosti, zejména to, že každé z nich se dá nejméně jedním způsobem vyjádřit pomocí nekonečného desetinného rozvoje. Zároveň se zaměříme pouze na reálná čísla z intervalu $(0,1)$, striktně vzato tedy dokážeme, že $(0,1) \not\approx \mathbb{N}$.[6] Je-li $x \in (0,1)$, existuje vyjádření pomocí desetinného rozvoje, které neobsahuje periodu $\overline{9}$ (tj. „nekončí samými devítkami“).[7] Budeme uvažovat výhradně takové rozvoje: kdykoliv má nějaké reálné číslo dva různé desetinné rozvoje, jeden z nich obsahuje periodu $\overline{9}$ a druhý ne[8] – vezmeme ten druhý.

Důkaz povedeme sporem. Pro spor tedy předpokládejme, že existuje bijekce $f : \mathbb{N} \to (0,1)$.[9] Můžeme si nyní představit nekonečný „seznam“ čísel $f(1), f(2), f(3), \ldots$; tento seznam podle našeho předpokladu, že f je na (a také prosté, což nás ale nezajímá),

[6] Protože z Příkladu 1.2 víme, že $(0,1) \approx \mathbb{R}$, bude nám to k úplnému důkazu stačit. Kdyby totiž neplatilo tvrzení věty, tj. platilo by $\mathbb{R} \approx \mathbb{N}$, složením obou bijekcí bychom dostali $(0,1) \approx \mathbb{N}$, což je ovšem opak toho, co se chystáme dokázat. Je to jasné i intuitivně: automaticky totiž chápeme, že se snažíme dokázat, že množina $\mathbb{R}$ je „větší“ než množina $\mathbb{N}$. A pokud to dokážeme pro $(0,1)$, tím spíše to bude platit pro celé $\mathbb{R}$.

[7] Trochu více košer by mohla být formulace, že použijeme takový desetinný rozvoj, který obsahuje nekonečně mnoho cifer různých od 9.

[8] To si lze snadno rozmyslet pomocí znalostí o reálných číslech, které dávno máte.

[9] Formálně vzato je f posloupnost reálných čísel, jak ji znáte z prvního semestru analýzy. My o ní budeme přemýšlet jako o číslovaném „seznamu“ všech reálných čísel intervalu $(0,1)$.

$$\begin{array}{rcccccc} f(1) = & 0, & 4 & 1 & 5 & 9 & 2 \\ f(2) = & 0, & 2 & 2 & 3 & 3 & 7 \\ f(3) = & 0, & 9 & 0 & 0 & 6 & 4 \\ f(4) = & 0, & 4 & 2 & 0 & 8 & 7 \\ f(5) = & 0, & 4 & 4 & 5 & 1 & 7 \\ & \vdots & & & & & \end{array}$$

Obrázek 1.5: „seznam“

$$\begin{array}{rcccccc} f(1) = & 0, & 4 & 1 & 5 & 9 & 2 \\ f(2) = & 0, & 2 & 2 & 3 & 3 & 7 \\ f(3) = & 0, & 9 & 0 & 0 & 6 & 4 \\ f(4) = & 0, & 4 & 2 & 0 & 8 & 7 \\ f(5) = & 0, & 4 & 4 & 5 & 1 & 7 \\ & \vdots & & & & & \end{array}$$

Obrázek 1.6: diagonála

obsahuje všechna čísla intervalu $(0, 1)$. Představme si dále, že čísla našeho seznamu napíšeme ve formě nekonečných desetinných rozvojů (bez periody $\overline{9}$) do řádků pod sebe. Výsledná představa by měla odpovídat Obrázku 1.5.

Vidíme, že cifry desetinných rozvojů jednotlivých čísel jsou uspořádány v nekonečné matici; zanedbáme-li první sloupec, ve kterém na všech řádcích máme „0,“, můžeme si představovat, že se jedná o nekonečnou čtvercovou matici, která má nekonečnou diagonálu – tu vidíme vyznačenou na Obrázku 1.6

Nyní se podívejme na posloupnost cifer na této diagonále; v případě znázorněném na obrázku tato posloupnost začíná $4, 2, 0, 8, 7, \ldots$. Pokud před tyto cifry představíme „0,“, dostaneme desetinný rozvoj nějakého reálného čísla: $x := 0{,}42087\ldots$. Můžeme se nyní ptát, jestli toto číslo je na našem seznamu – což by mělo, neboť seznam má přece obsahovat všechna taková čísla. Odpověď je nejasná. Při nešťastném uspořádání našeho seznamu by se například mohlo stát, že máme co do činění s číslem $0{,}999\ldots = 0{,}\overline{9} = 1 \notin (0, 1)$, které na seznamu není. Obecně ale nic nebrání tomu, aby toto číslo na seznamu bylo, a na našem obrázku je hned na 4. řádku (předpokládejme, že obě zvýrazněné posloupnosti cifer pokračují stejně až do nekonečna).

Věnujme pozornost cifře, v níž se obě posloupnosti protínají; na obrázku je to cifra 8. Kdybychom definovali číslo $\tilde{x}$ stejným rozvojem jako číslo x až na čtvrtou cifru, již bychom změnili z 8 třeba na 0, tj. $\tilde{x} = 0{,}42007\ldots$, je náhle zřejmé, že toto číslo není na čtvrté pozici našeho seznamu (neboť se od $f(4)$ liší ve 4. cifře). Podobně, změníme-li k tomu ještě 5. cifru, výsledné číslo nebude na 4. ani na 5. pozici v našem seznamu.

Protože nám nic nebrání vhodně změnit všechny cifry našeho desetinného rozvoje, provedeme to; tím najdeme číslo z $(0, 1)$, které se nenachází na žádné pozici našeho seznamu, což bude spor s jeho předpokládanou úplností. Přesněji: Označme, pro všechna i přirozená, $a_i \in \{0, 1, 2, \ldots, 9\}$ cifru na i-té pozici za desetinnou čárkou rozvoje čísla $f(i) \in (0, 1)$. Tím pádem je $\{a_i\}_{i=1}^{\infty}$ přesně ona posloupnost cifer „na diagonále“. Nyní položíme

$$b_i = \begin{cases} 1, & \text{pokud } a_i \neq 1, \\ 2, & \text{pokud } a_i = 1, \end{cases}$$

takže $b_i \neq a_i$ pro všechna i. Definujme číslo z desetinným rozvojem určeným posloupností $\{b_i\}_{i=1}^{\infty}$, tj.

$$z = 0{,}b_1 b_2 b_3 \ldots .$$

Uvedený rozvoj je v povoleném tvaru (nekončí periodou $\overline{9}$), navíc evidentně $z \in (0, 1)$. Číslo z s tímto rozvojem by tedy mělo být na některém řádku našeho seznamu. To ale není možné, protože rozvoj čísla z se (minimálně) v cifře na diagonále liší od každého řádku našeho seznamu. Přesněji: pro každé i, z se liší od čísla $f(i)$ v i-té cifře desetinného rozvoje, a tedy (díky tomu, že jsme vyloučili dvojakost rozvojů) $z \neq f(i)$. To je spor s naším předpokladem, že f je *na* interval $(0, 1)$. □

Důsledek. *Existují nekonečné množiny více různých mohutností.*

Podívejme se ještě na jeden pozoruhodný úkaz podobného typu jako Hilbertův hotel: tak zvaný Hyper-Webster. Označení je odvozeno z názvu jednoho z nejznámějších slovníků anglického jazyka zvaného Merriam-Webster.

1.4 Příklad (Hyper-Webster)**.** Uvažujme libovolnou konečnou množinu znaků $\mathcal{A}$; pro větší názornost předpokládejme, že $\{A, B, C, D, \dots, Z\} \subseteq \mathcal{A}$. Množinu $\mathcal{A}$ nazýváme *abeceda*. Libovolnou konečnou posloupnost znaků z $\mathcal{A}$ nazýváme *slovo*. Označme $N = |\mathcal{A}|$, tj. N je počet prvků abecedy. Existuje tedy právě N slov délky 1, N^2 slov délky 2 atd.; pro libovolné $k \in \mathbb{N}$ existuje přesně N^k slov délky k. Existuje také jediné slovo délky 0, a to $\emptyset$, neboli prázdná posloupnost.[10] Množinu všech slov délky k značíme $\mathcal{A}^k$, čímž máme na mysli kartézský součin k kopií abecedy $\mathcal{A}$, tj.

$$\mathcal{A}^k = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \times \mathcal{A}}_{k\text{-krát}} = \big\{(a_1, a_2, \dots, a_k) \colon\ a_1, a_2, \dots, a_k \in \mathcal{A}\big\}.$$

Navíc značíme $\mathcal{A}^0 = \{\emptyset\}$, což je v souladu s naší dohodou o tom, že $\emptyset$ je jediná posloupnost délky 0.

Označme HW množinu všech slov, tj.

$$\mathrm{HW} := \bigcup_{k=0}^{\infty} \mathcal{A}^k = \{\emptyset\} \cup \mathcal{A}^1 \cup \mathcal{A}^2 \cup \mathcal{A}^3 \cup \dots .$$

Je zřejmé, že HW je nekonečná, neboť obsahuje slova libovolné (konečné) délky.

Protože prvky HW jsou slova, dává smysl o HW hovořit jako o slovníku – a to o slovníku dosti obsáhlém. Mohlo by nás proto napadnout ho rozdělit do svazků podle počátečního písmene. Budeme tak mít N svazků, které si označíme $\mathrm{HW}(x)$, kde $x \in \mathcal{A}$. Speciálně tedy máme i svazky $\mathrm{HW}(A), \mathrm{HW}(B), \dots, \mathrm{HW}(Z)$. Pojďme se podívat na jeden z nich, třeba na svazek $\mathrm{HW}(A)$, který obsahuje právě všechny konečné posloupnosti znaků z abecedy $\mathcal{A}$, jejichž první člen je znak A, tj. všechna slova začínající na A.

Když budeme ve svazku $\mathrm{HW}(A)$ listovat, uvidíme slova jako A, AA, AB, AAA, ale také $ASFJKSDIFGN$ nebo $ADELAJESTENEVECERELA$ a $ASKETA$. Můžeme si všimnout, že je zde určitá redundance: první znak je vždycky A, což je dáno tím, že prohlížíme slova

[10] Týmtéž symbolem samozřejmě značíme i prázdnou množinu. Nejde o kolizi značení, neboť formálně jde o stejný objekt. Zde se nám pouze víc hodí mu říkat „posloupnost“ místo „množina“.

z $\mathrm{HW}(A)$; informace o prvním znaku je tedy dána naší volbou svazku a vlastně by tak první znak mohl být – pro úsporu místa – u jednotlivých hesel vynechán. Místo výše uvedených příkladů bychom pak viděli pouze: $\emptyset$, A, B, AA, $SFJKSDIFGN$ atd. Protože $\mathrm{HW}(A)$ obsahuje nekonečně mnoho hesel, odstraňujeme tak nekonečně mnoho znaků A, a lesy tím tedy šetříme poměrně značně.

Nové vydání $\mathrm{HW}(A)$ tedy už zahrnuje naše úsporné opatření: všechna hesla byla ochuzena o počáteční A. Aby se odlišilo od vydání starého, značíme ho $\widetilde{\mathrm{HW}}(A)$.

Třikrát běda, však! Nekonečno nás převezlo!

Tisk nabral zpoždění a netrpěliví zákazníci tvoří fronty na první výtisky. Ukázalo se, že

$$\widetilde{\mathrm{HW}}(A) = \mathrm{HW}.$$

Naše úsporné opatření způsobilo, že tiskneme místo jednoho svazku zase celý slovník – jak smutné. Rozmyslete si to! $\triangle$

1.3 Trocha historie – důvody pro vznik a upřesňování TM

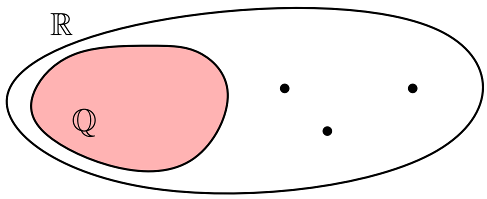
Za zakladatele teorie množin je všeobecně považován německý matematik Georg Cantor (1845-1918), který jako první vymyslel a přijal za svůj specifický způsob přemýšlení a práce s množinami, který přijímá v předchozí kapitole zmiňované paradoxy („nekonečná množina je stejně velká jako nějaká její vlastní část“ apod.). Skok mezi (do té doby) klasickou a cantorovskou matematikou je tak velký, že bych se nebál ho přirovnat ke změně paradigmatu ve fyzice, která nastala objevem teorie relativity; zároveň jsem přesvědčen, že k tomu, aby Cantor mohl takto velký skok uskutečnit, musel mít srovnatelně otevřenou a originální mysl, jako Albert Einstein. Na rozdíl od Einsteina však Cantor musel na uznání svých myšlenek širší vědeckou komunitou čekat dlouhá desetiletí a během této doby musel odrážet různé, často dost nevybíravé, útoky od svých „kolegů“. Tato skutečnost dlouhodobě nahlodávala jeho duševní zdraví (u geniálních lidí často i tak dost křehké) a poslední léta svého života strávil v léčebně pro duševně nemocné.

Původní motivací pro Cantorův originální směr přemýšlení bylo studium jistých složitých podmnožin $\mathbb{R}$, rychle se však z jeho nápadů stala samostatná nová teorie. Cantor teorii množin vybudoval do podoby, v níž bylo možné na ní založit všechny ostatní matematické teorie a postavit je tak na jednotné a svou jednoduchostí elegantní matematické základy. Kromě tohoto sjednocujícího efektu navíc do matematiky přinesl řadu zcela nových metod, z nichž některé budily rozruch[11] svojí zcela odlišnou filosofickou podstatou.

Základním příkladem takové metody jsou tak zvané *nekonstruktivní důkazy existence*; až do Cantora byl v matematice jediný uznávaný princip důkazu existence nějakého objektu: pomocí vhodné konstrukce (vycházející z objektů, o jejichž existenci nebylo pochyb) najít konkrétní

[11] Od překvapení až po naprosté odmítání.

příklad požadovaného typu objektu – a samozřejmě také dokázat, že onen objekt skutečně má příslušnou vlastnost.



Obrázek 1.7: Puntíky představují *nějaká* iracionální čísla.

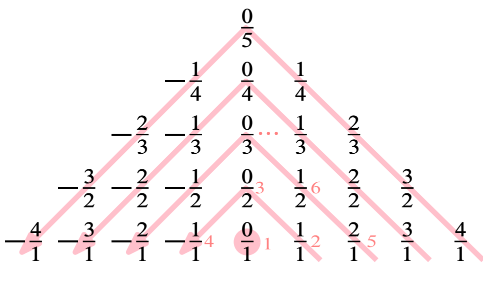
Tak například staří Řekové dokázali existenci iracionálních čísel tak, že podali příklad (aspoň) jednoho takového čísla, a to $\sqrt{2}$. Cantor ale skrze studium *mohutností* množin mohl podat důkaz existence iracionálních čísel, *aniž by znal jediné konkrétní iracionální číslo*: stačilo mu dokázat, že $\mathbb{R}$ má větší mohutnost než $\mathbb{Q}$, takže $\mathbb{R} \setminus \mathbb{Q}$ musí být neprázdná množina. (Ve skutečnosti tuto metodu aplikoval na čísla transcendentní místo iracionálních; o tom se můžete dočíst dále v tomto textu.)

Přesněji řečeno mohl postupovat takto: Stačilo dokázat níže uvedenou Větu 1.5, která v kombinaci s Větou 1.3 znamená, že $\mathbb{Q} \not\approx \mathbb{R}$, takže musí existovat nějaká iracionální čísla (tj. taková reálná čísla, která nejsou racionální) – viz Obrázek 1.7.

1.5 Věta. $\mathbb{Q} \approx \mathbb{N}$.

Náznak důkazu. Podrobněji (a přesněji) se k důkazu této věty vrátíme později (až budeme mít například přesnou definici racionálních čísel), nyní pouze naznačíme základní myšlenku:

Každému racionálnímu číslu odpovídá nějaký zlomek tvaru $\frac{k}{n}$, kde $k \in \mathbb{Z}$ a $n \in \mathbb{N}$. Ponecháme nyní stranou drobný problém, že každé racionální číslo je reprezentováno nekonečně mnoha různými zlomky (třeba zlomky $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \ldots$ reprezentují všechny totéž číslo). Nyní se spokojíme s tím, že zlomků je *nejméně tolik co racionálních čísel*, takže když se nám podaří očíslovat přirozenými čísly všechny zlomky (tj. vlastně je seřadit do nekonečné posloupnosti indexované přirozenými čísly), tím spíše je totéž možné i s racionálními čísly, a věta tedy platí. Důkaz provedeme obrázkem, formální popis bijekce mezi $\mathbb{N}$ a všemi zlomky by byl příliš dlouhý (a hůře srozumitelný): Je zřejmé, že při použití algoritmu číslování zlomků, který na-



Obrázek 1.8: Uspořádání zlomků do posloupnosti

značuje obrázek, nakonec se dostaneme k libovolnému zlomku a s trochou úsilí by šlo i určit, jaký přesně dostane daný zlomek (jako třeba $\frac{537}{1000}$) index. Tím pádem je zlomků stejný počet jako přirozených čísel (existuje bijekce daná naším očíslováním), a tedy racionálních čísel není víc než přirozených (takže je jich stejný počet). □

Cantor vytvořil to, čemu se dnes říká *Naivní teorie množin*. V ní se pokusil vymezit pojem množiny pomocí jednoduché „definice“, kterou si můžete přečíst na začátku další kapitoly. Dále už pracoval formálně přesně, ovšem s tím, že bez důkazu používal některé vlastnosti množin, které byly „evidentní“, respektive „plynuly“ z definice. Ačkoliv v tomto rámci vybudoval teorii, která je i z hlediska moderního standardu beze zbytku použitelná a správná, intuitivní přístup k práci se základním pojmem množiny nenaplňuje moderní standardy matematické přesnosti. Ty se začaly formovat na přelomu 19. a 20. století a které v podstatě znamenají axiomatizaci (a další formální charakteristiky) dnes běžně používané teorie množin.

Kapitola 2

Základní pojmy TM

V této kapitole se budeme věnovat některým pojmům teorie množin, aniž bychom pořádně vysvětlili, co to je teorie množin a co vůbec je „množina“; těmto otázkám se budeme podrobněji věnovat později. Nyní se spoléhám na to, že koncept množiny je všem „známý“ do takové míry, že nehrozí omyly v základních věcech jako množinové operace apod. Chci nicméně zdůraznit, že všechny uvedené pojmy a výsledky o nich budou stát na nejpevnějších možných základech v okamžiku, kdy začneme pracovat v *axiomatické teorii množin*.

2.1 Naivní teorie množin

Jak už bylo zmíněno, takzvanou Naivní teorii množin vytvořil Georg Cantor v sedmdesátých a osmdesátých letech 19. století.

2.1.1 Definice množiny

Prozatím se tedy spokojíme s prací v tzv. *naivní teorii množin* (NTM), která pojem množiny „definuje“ takto:

> *Množinou rozumíme každé srhnutí M určitých rozlišitelných předmětů našeho nazírání nebo myšlení v jeden celek; tyto předměty se nazývají prvky množiny M.*

Vidíme, že se přes veškerou snahu jedná o definici vágní, která navíc využívá nedefinovaná slova jako „shrnutí“ nebo „celek“, takže vzniká důvodné podezření na definici kruhem (neboť tyto pojmy mají – aspoň intuitivně – podobný význam jako samo slovo „množina“). Těžko by nás tedy tato definice uspokojila, i kdybychom měli jasnou představu o obsahu dalších zúčastněných pojmů jako třeba „předmět nazírání“, „rozlišitelný“ apod.[1]

[1] Lze si ovšem představit, že tyto pojmy uspokojivým způsobem vymezíme; hlavní problém je tedy v „definici kruhem“.

V NTM tedy nemáme úplně jasno v tom, co je to množina. Zdá se například bez problému přípustné, abychom uvažovali množinu všech lidí, případně nějakou její podmnožinu (jako množinu všech studentů MFF apod.), neboť jednotliví lidé jsou bez pochyby možnými předměty našeho nazírání i myšlení. Protože množiny samy jsou předměty našeho myšlení, je zároveň dovoleno, aby množiny byly prvky jiných množin. Totéž platí například pro čísla (jakkoliv tímto pojmem lze myslet více věcí) atd. *Množina* v pojetí NTM je tedy velmi obecný pojem: jakýkoliv myslitelný „soubor“ může být chápán jako množina. To nám na jednu stranu umožňuje vybudovat velmi zajímavou teorii; na stranu druhou se ukazuje, že právě obrovská obecnost pojmu *množina* je kamenem úrazu této teorie.

Jak víme, byl to Bertrand Russell, kdo si jako první uvědomil spornost NTM: stačilo uvažovat množinu všech množin, které nejsou svým vlastním prvkem, a zeptat se, je-li tato množina svým vlastním prvkem, nebo není (obě možnosti vedou ke sporu). Podrobněji viz úvod. Protože však teorie množin nabízela lákavou cestu, jak sjednotit matematiku skrze jedinou základní teorii, hledaly se cesty, jak pojem množiny vymezit o něco přísněji, zejména tak, aby nebylo možné zkonstruovat žádnou známou antinomii. Tak se prosadil axiomatický přístup k teorii množin.

My se zatím s NTM spokojíme, budeme však provádět (jak se později ukáže) pouze takové kroky, které jsou přípustné i v axiomatické teorii množin, kterou popíšeme později. Začneme tím, že v rámci teorie množin zkonstruujeme základní pojmy jako uspořádání nebo funkce. Samozřejmě si uvedeme také různé operace s množinami atd.; vše bude provedeno v souladu s pozdější výstavbou axiomatické teorie (takže tyto věci nebudeme muset dělat podruhé).

2.1.2 Rovnost množin v NTM

Základním pojmem naší teorie je v každém případě *množina*. Je tedy vhodné se hned od začátku shodnout na tom, co naše definice množiny vypovídá o rovnosti množin. Kdy se tedy dvě množiny rovnají (a jsou tedy jedna a ta samá)? Odpověď na tuto otázku rozdělíme do několika pozorování.

Různost prvků dané množiny: Všimněme si, že definice požaduje *rozlišitelnost* prvků; speciálně tedy prvky každé množiny musí být navzájem *různé*; jeden objekt tedy může být v každé množině zastoupen jakožto prvek nejvýše jednou. Z toho plyne, že přijmeme-li níže uvedené zadání množiny pomocí výčtu všech prvků, tj. například $\{a,b,c\}$, kde a,b,c jsou různé předměty, značí tříprvkovou množinu obsahující právě tyto tři objekty, pak platí rovnost $\{a,a\} = \{a\}$. Množina zadaná jako $\{a,a\}$ má tedy jediný prvek, a to předmět a. Toto pozorování je pochopitelně třeba zobecnit, takže například $\{1,2,2,3,3,3\} = \{1,2,3\}$ apod.

Prvky množiny nemají pořadí: Z definice skutečně nevyplývá, že by prvky množiny měly být jakkoliv uspořádány v rámci samotné množiny. Je tedy například $\{0,1\} = \{1,0\}$ apod. Pochopitelně nám ovšem nic nebrání podle potřeby přiřadit k dané množině M ještě další strukturu (složitější množinu), která by vypovídala o pořadí prvků M (viz níže pojem relace a uspořádání). Shrňme, že v množině není dáno žádné pořadí prvků, a tedy také nezáleží na tom, v jakém pořadí její prvky uvedeme apod.

Množina je určena právě všemi svými prvky. Tím se myslí, že rovnost množin $A = B$ nastává právě tehdy, když množiny A a B mají přesně stejné prvky. Formálněji bychom toto pozorování mohli zapsat takto:[2]

$$A = B \quad \longleftrightarrow \quad \Big(\forall x\colon x \in A \longleftrightarrow x \in B\Big). \tag{2.1}$$

„Důkaz." Máme tedy přesný popis toho, co mezi množinami znamená rovnost; chceme přitom tvrdit, že tento popis je důsledkem definice, a na místě je tedy provést důkaz. Abychom si uvědomili, že definice množiny v NTM skutečně implikuje (2.1), bude potřeba se zamyslet nad tím, co obecně rozumíme pojmem rovnosti mezi dvěma předměty. Standardní způsob nahlížení relace rovnosti je, že předměty A a B jsou si rovny, pokud cokoliv, co lze (v rámci dané teorie) pravdivě prohlásit o A, lze pravdivě prohlásit i o B.[3] Pak je ovšem zřejmé, že pokud jistý předmět náleží množině A, ale nenáleží množině B, nemůže být $A = B$. Tím je dokázáno, že rovnost množin implikuje stejnost prvků, neboli že stejnost prvků je *nutná* pro rovnost množin.

Pro důkaz opačné implikace, tj. že stejnost prvků je pro rovnost množin také *postačující* už musíme hodně číst mezi řádky. V definici množiny například není uvedeno, že by se od sebe množiny lišily tím, jakou mají vůni nebo tvar. Proto takovéto rozlišení připouštět nebudeme a budeme se soustředit pouze na to, co v definici zmíněno je, tedy prvky množiny. Množiny se tedy mohou od sebe navzájem lišit pouze v tomto jediném aspektu; neliší-li se tedy v tomto aspektu (tj., mají-li stejné prvky), jsou si rovny. □

Není divu, pokud vás výše uvedený „důkaz" příliš neuspokojil. Pokud bychom o něm chtěli diskutovat více, nevyhnutelně bychom zabředli do rozmlženého prostředí filosofie a výsledný závěr by nejspíše záležel na jazykové obratnosti jeho zastánce. Nic nám ovšem nebrání se na platnosti (2.1) prostě dohodnout a NTM budovat s tímto předpokladem (axiomem).

2.1.3 Způsoby zadání množin v NTM

Množina zadaná výčtem prvků: Už jsme se dohodli, že množina je určena právě svými prvky; prvky se přitom nemůžou opakovat a nezáleží na jejich pořadí. S tím je v bezvadném souladu základní způsob zadání množiny: výčtem prvků. Standardní způsob zápisu je jednotlivé

[2] Implikaci a ekvivalenci ve formálních výrocích budeme značit jednoduchými šipkami, dvojité šipky budeme příležitostně používat při neformálním vyjadřování. Podrobněji viz též ...

[3] Mohli bychom dodat: „... a naopak". Je užitečné si rozmyslet, že tento dodatek by byl zbytečný, neboť pokud libovolné prohlášení $\varphi(A)$ neplatí, pak tedy $\neg\varphi(A)$ platí. Proto (v případě $A = B$) platí i $\neg\varphi(B)$. Za předpokladu $A = B$ tedy platí $\neg\varphi(A) \Rightarrow \neg\varphi(B)$, neboli (obměna implikace) $\varphi(B) \Rightarrow \varphi(A)$, tj. ono „a naopak".

prvky oddělit čárkami a vše uzavřít do složených závorek. Zápisem

$$\{\text{pondělí, úterý, středa, čtvrtek, pátek}\}$$

tedy rozumíme množinu obsahující právě oněch pět prvků uvedených mezi složenými závorkami; podle výše uvedeného je tím množina jednoznačně určena, a nic nám tedy nebrání například označit

$$A = \{\text{pondělí, úterý, středa, čtvrtek, pátek}\}$$

a psát „středa $\in A$“ nebo „sobota $\in A$“ (přičemž první z obou výroků je pravdivý, druhý ne).

Občas je možné spatřit také zápisy podobné následujícímu:

$$\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \dots\right\}.$$

Takovýto zápis sice dává jasnou představu o tom, jaké prvky má uvažovaná množina obsahovat (a s vhodnou konvencí mezi autorem a čtenářem by snad i mohl být přípustný), nejde ale o úplný výčet prvků, nýbrž o popis jakéhosi algoritmu, který generuje všechny prvky. Podobný způsob konstrukce (zadání) množiny jistě potkáme, nebudeme ho však označovat za zadání výčtem prvků.

Za zmínku možná stojí ještě to, že prvky množin mohou být také jiné množiny. Dobrý smysl by tedy dával třeba i zápis

$$\left\{0, \frac{1}{2}, A, \{4, 5, 6, 7\}, \mathbb{R}\right\}.$$

Uvedená množina má přesně 5 prvků (ty nejsou „stejného typu“, což ovšem není potřeba) – tedy za předpokladu, že A se liší od každého z ostatních čtyř prvků (tj. 0, $\frac{1}{2}$, $\{4, 5, 6, 7\}$ a $\mathbb{R}$), takže všechny uvedené prvky jsou navzájem různé.[4]

Množina všech prvků s jistou vlastností: Další standardní způsob zadání množin je pomocí nějaké vlastnosti, kterou mají prvky množiny splňovat. Zápisem

$$\{x\colon\ \varphi(x)\}$$

myslíme množinu právě všech objektů, pro které platí výrok $\varphi(\cdot)$. Poněkud přesněji, $\varphi(x)$ je zde výroková forma (též výroková funkce), z níž po dosazení konkrétního objektu za x vznikne výrok, tj. získá jednoznačnou pravdivostní hodnotu.

Označíme-li například $\varphi(x)$ výrokovou formu

$$x \text{ je sudé celé číslo,}$$

[4] Často se používá výraz, že prvky jsou „po dvou různé“, čímž je míněno, že každé dva prvky x a y splňují $x \neq y$. Přesně to mám na mysli, když píšu, že „všechny prvky jsou navzájem různé“.

pak zápis $\varphi(x)$, kde x je proměnná, nemá žádnou pravdivostní hodnotu. Když ale za x dosazujeme různé objekty, např. $x = 6$, $x = -\sqrt{2}$ nebo $x = \mathbb{Q}$, dostáváme postupně výroky „6 je sudé číslo“, „$-\sqrt{2}$ je sudé číslo“, „$\mathbb{Q}$ je sudé číslo“; ty jsou buďto pravdivé, nebo nepravdivé (z uvedených případů je pravdivý pouze první).

Lze tedy definovat množinu $B = \{x\colon\ x \text{ je sudé celé číslo}\}$; ta obsahuje čísla 0, 2, -2, 4, $-4, \dots$, obecně právě všechna čísla n tvaru $n = 2k$, kde k je celé číslo. Poněkud neformálně by šlo tuto množinu zapsat také jako

$$\{\dots, -4, -2, 0, 2, 4, \dots\}.$$

Často budeme používat také zápis tvaru

$$\{x \in C : \psi(x)\},$$

kde C je nějaká množina a $\psi(x)$ výroková forma s proměnnou x. Máme tím na mysli množinu právě všech prvků x množiny C, pro něž platí výrok $\psi(x)$. Výše uvažovanou množinu všech sudých celých čísel bychom tak mohli zapsat například následujícími způsoby:

$$B = \{x \in \mathbb{Z}\colon\ \underbrace{x \text{ je sudé}}_{\psi(x)}\} = \{n \in \mathbb{Z}\colon\ \underbrace{\text{existuje } k \in \mathbb{Z} \text{ takové, že } n = 2k}_{\psi(n)}\}$$

2.1 Poznámka (Russellův paradox v NTM)**.** V souvislosti s odstavcem o zadání množiny pomocí vlastnosti je dobré si uvědomit, že nám v principu nic nebrání použít nějakou velmi univerzální vlastnost. Například $\mathbb{V}$ definovaná jako

$$\mathbb{V} = \{x\colon\ x \text{ je množina}\}$$

je množina všech množin (speciálně tedy i $\mathbb{V} \in \mathbb{V}$, což samo o sobě nepředstavuje zřejmý problém). Nyní[5] můžeme definovat

$$A = \{x \in \mathbb{V}\colon\ x \notin x\}$$

a dospět ke sporu v NTM, neboť nemůže platit ani $A \in A$, ani $A \notin A$ (obě možnosti vedou ke sporu, jak bylo vysvětleno už výše).

[5] Ve skutečnosti bychom mohli rovnou definovat $A = \{x\colon\ x \notin x\}$ a dostali bychom úplně stejný spor; pro snazší pochopení se ale nejprve omezujeme jen na objekty, které jsou množinami (což pro vznik paradoxu v NTM stačí).

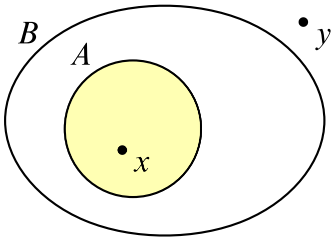
2.2 Operace s množinami a vztahy mezi nimi

Platnost obsahu tohoto oddílu už není omezena jen na NTM; budeme se sem odkazovat i při pozdějším studiu axiomatické teorie množin. Popíšeme základní množinové operace a vztahy mezi množinami, které lze používat v obou typech teorie množin.[6]

2.2.1 Jednoduché základní operace s konečně mnoha množinami

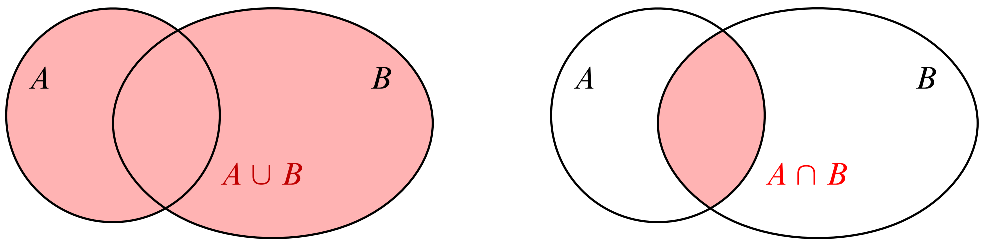
2.2 Definice (Operace s konečně mnoha množinami)**.** V následujícím výčtu definic jsou A, B a X množiny.

- Symbol $A \subseteq B$ je zkratka za výrok $\forall x\colon x \in A \rightarrow x \in B$. V tom případě říkáme, že A *je podmnožinou* B a relace $\subseteq$ se nazývá *inkluze*.



Obrázek 2.1: $x \in A \rightarrow x \in B$, tj. ekvivalentně $y \notin B \rightarrow y \notin A$

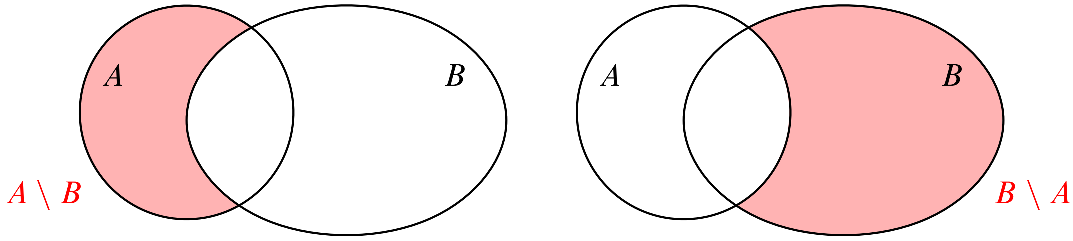
- *Sjednocení množin* A *a* B je množina $A \cup B = \{x\colon\ x \in A\ \vee x \in B\}$.
- *Průnik množin* A *a* B je množina $A \cap B = \{x\colon\ x \in A \wedge x \in B\}$.



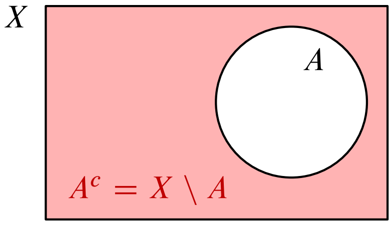
Obrázek 2.2: sjednocení a průnik množin A a B

- *Rozdíl množin* A *a* B je množina $A \setminus B = \{x\colon\ x \in A \wedge x \notin B\}$.
  Všimněte si, že na rozdíl od předchozích dvou operací není rozdíl komutativní, tj. záleží v něm na pořadí A a B.
- Je-li $A \subseteq X$, definujeme *doplněk množiny* A *v množině* X jako $A^c = X \setminus A$.

[6] S tím, že v axiomatické teorii budeme muset dodat důkazy, že aplikací těchto operací na množiny vzniknou opět množiny. Z axiomů například dokážeme, že sjednocení dvou množin je opět množina apod. V naivní teorii množin jsou to zcela zřejmá fakta a v tomto oddíle se tím nebudeme zabývat.

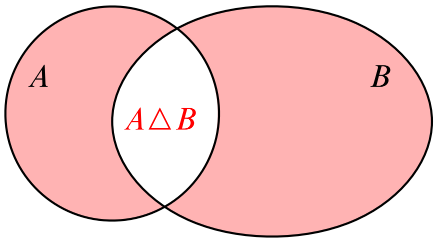


Obrázek 2.3: Množinový rozdíl není komutativní operace.



Doplněk (též komplement[7]) je tedy operace vztažená k nějaké pevně zvolené nadmnožině, v tomto případě X. Například uvažujeme-li interval $[5, 7) \subseteq \mathbb{R}$, pak $[5, 7)^c = (-\infty, 5) \cup [7, \infty)$.

- *Symetrická diference A a B* je množina $A \triangle B = (A \setminus B) \cup (B \setminus A)$.



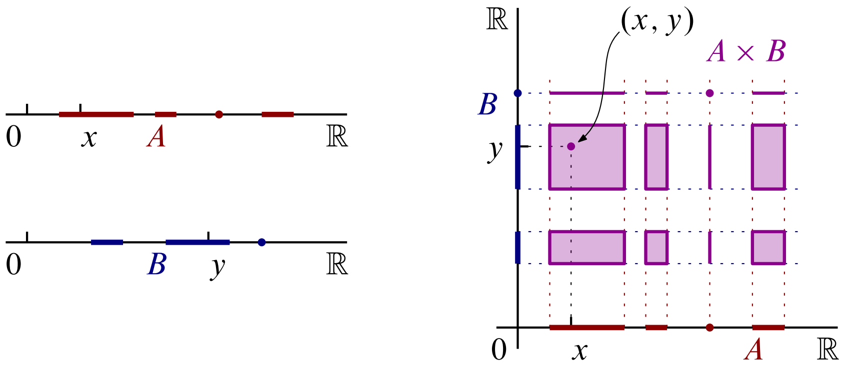
Z obrázku je snadno vidět, že platí $A \triangle B = (A \cup B) \setminus (A \cap B)$.

- *Kartézský součin* množin A a B je $A \times B = \{(a, b) \colon a \in A \wedge b \in B\}$, tj. množina všech uspořádaných dvojic prvků z A a z B (v tomto pořadí).

- *Prázdnou množinu* značíme symbolem $\emptyset$; prázdná množina neobsahuje žádný prvek. Protože množina je jednoznačně určena svými prvky, existuje jediná prázdná množina. Všimněte si, že pro libovolnou množinu A platí $\emptyset \subseteq A$.

- Řekneme, že množiny A a B jsou *disjunktní*, pokud $A \cap B = \emptyset$ (tj. mají prázdný průnik, tj. nemají žádný společný prvek).

[7] Angl. *complement*, odkud pochází písmenko „c“ v značení doplňku množiny.



Obrázek 2.4: kartézský součin A a B s vyznačeným bodem (x, y), kde $x \in A$ a $y \in B$

- Jsou-li $A_1, A_2, \ldots, A_N$ množiny, definujeme symboly $\bigcup_{i=1}^N A_i$ a $\bigcap_{i=1}^N A_i$ takto:

$$\bigcup_{i=1}^{N} A_i = A_1 \cup A_2 \cup \ldots \cup A_N \quad \text{a} \quad \bigcap_{i=1}^{N} A_i = A_1 \cap A_2 \cap \ldots \cap A_N .$$

  Protože jsou operace sjednocení a průniku asociativní[8] a komutativní, není potřeba v žádném smyslu udávat pořadí prováděných operací, a zápisy $A_1 \cup A_2 \cup \ldots \cup A_N$, resp. $A_1 \cap A_2 \cap \ldots \cap A_N$ (kde N je přirozené číslo) mají jednoznačný a jasný význam.

2.2.2 Operace s nekonečně mnoha množinami

Složitější situace vzniká, máme-li nekonečně mnoho množin, které je potřeba „proniknout“, „sjednotit“ apod. Pak už nelze postupovat přirozeným postupem z předchozího bodu, zápisy jako $A_1 \cap A_2 \cap A_3 \cap A_4 \ldots$ apod. v tuto chvíli nemají žádný jasně definovaný význam.

V první řadě je potřeba si rozmyslet, co vlastně mám na mysli, když píšu „máme nekonečně mnoho množin“. Jsou dvě hlavní možnosti, co to může znamenat:

(a) Máme nějakou nekonečnou množinu X, jejíž prvky jsou množiny, s nimiž chceme provádět operace – zejména sjednocení a průnik. Množina X obecně nemá žádnou strukturu; stačí, když všechny její prvky jsou množiny[9] a už je možné definovat sjednocení (resp. průnik) všech těchto prvků (viz níže).

Všimněte si, že prvky X jsou navzájem různé (žádný objekt není prvkem téže množiny „víckrát“), takže nekonečná množina X dává automaticky nekonečně mnoho navzájem různých prvků – množin. (Pozor, tyto množiny *nejsou podmnožiny* X, jsou to její *prvky*. Zvykněte si, že prvky množin mohou být zase množiny, třeba $X = \{\mathbb{N}, \mathbb{R}, [0, 1), \mathbb{Q}, \mathbb{C}\}$ je množina o přesně *pěti prvcích*, z nichž každý je množina (mimochodem nekonečná).)

[8] To jest, pro libovolné množiny A, B, C platí $A \cup (B \cup C) = (A \cup B) \cup C$ a $A \cap (B \cap C) = (A \cap B) \cap C$.

[9] Později, v axiomatické teorii množin, jiné objekty než množiny nebudeme připouštět. Tím pádem budou všechny prvky X množiny automaticky (nic jiného nebude existovat).

(b) Máme „indexovou" množinu I a pro každý prvek („index") $i \in I$ nějakou množinu označenou A_i. Přesněji řečeno to znamená, že máme zobrazení (označme ho φ) definované na I, které každému prvku $i \in I$ přiřadí nějakou množinu A_i.[10] V případě, že množina I je nekonečná, může se stát, že tím máme dáno nekonečně mnoho (různých) množin.[11]

Je dobré si všimnout, že na rozdíl od předchozího případu je zde celkem přirozené dát množině I nějakou dodatečnou strukturu, například uspořádání. (Typickým příkladem je $I = \mathbb{N}$, takže máme na I jasné uspořádání, které se „přenese" na příslušně indexované množiny A_i.)

Probrali jsme dva způsoby, jak zadat nekonečně mnoho množin. Nyní se podíváme na definice operací s těmito množinami, a to nejdřív v případě (a), pak (b).

2.3 Definice (Sjednocení a průnik prvků množiny $\mathcal{X}$)**.** Buď $\mathcal{X}$ množina, jejíž prvky jsou množiny. Takové množině můžeme pro přehlednost říkat *kolekce* (množin). Definujeme *sjednocení* (též *sumu*) $\mathcal{X}$ jako množinu

$$\bigcup \mathcal{X} = \{x\colon \exists A \in \mathcal{X} : x \in A\},$$

tedy jako množinu všech objektů x, které jsou prvkem *některé* množiny A z kolekce $\mathcal{X}$.

Podobně definujeme *průnik* $\mathcal{X}$ jako množinu

$$\bigcap \mathcal{X} = \{x\colon \forall A \in \mathcal{X} : x \in A\},$$

tedy jako množinu všech objektů x, které jsou prvkem *každé* množiny A z kolekce $\mathcal{X}$.

Pro odlišení „úrovní množin" můžeme někdy místo „množina množin" používat termín „kolekce", resp. „kolekce množin".[12] Volně řečeno, $\bigcup \mathcal{X}$ je sjednocení všech množin z kolekce $\mathcal{X}$, tj. „obsahy všech množin z $\mathcal{X}$ sesypeme do jedné velké množiny". Podobně $\bigcap \mathcal{X}$ je průnik všech množin z kolekce $\mathcal{X}$, tj. vezmeme právě ty prvky, které se vyskytují v každé množině z naší kolekce.

2.4 Příklad.

- Pokud $\mathcal{X} = \{A, B, C\}$, pak $\bigcup \mathcal{X} = A \cup B \cup C$. Konkrétně třeba pro $\mathcal{X}$ obsahující tři intervaly v $\mathbb{R}$, např. $\mathcal{X} = \{[0,2], (1,5), (7,10]\}$, dostaneme $\bigcup \mathcal{X} = [0,5) \cup (7,10]$.

[10] Tj. A_i je hodnota zobrazení φ v „bodě" i, neboli $\varphi(i) = A_i$. Je to stejný princip, jako definice číselné posloupnosti v prvním semestru analýzy: jednotlivé její členy zapisujeme (třeba) a_n, čímž myslíme hodnotu jistého zobrazení f v bodě $n \in \mathbb{N}$, neboli $a_n = f(n)$. Striktně vzato pak posloupnost $\{a_n\}_{n=1}^{\infty}$ *je* toto zobrazení f, tj. $\{a_n\}_{n=1}^{\infty} = f$. Rozdíl je v tom, že pro posloupnosti jsme jako „indexovou množinu" uvažovali $\mathbb{N}$, zatímco zde připouštíme absolutně jakoukoliv množinu I.

[11] Například v případě, že „indexové zobraení" φ je prosté, tj. pro různé indexy $i, j \in I$ dostaneme různé množiny A_i, A_j.

[12] Kromě tohoto terminologického odlišení úrovní „prvek $\in$ množina $\in$ kolekce" v tomto případě navíc používáme odlišení pomocí tvaru písma, tj. třeba $x \in X \in \mathcal{X}$ apod. Na to se ale nespoléhejte, v dalším můžeme a budeme různé tvary písmen používat vcelku libovolně.

- Samozřejmě můžeme také psát rovnou

  $$\bigcup\{A, B, C\} = A \cup B \cup C \quad \text{nebo} \quad \bigcap\big\{(-\infty, 0], [0, \infty)\big\} = \{0\}$$

  apod., tj. můžeme sjednocovat a pronikat kolekce i bez jejich předchozího označení písmeny jako $\mathcal{X}$ apod.

- Pokud $A = \{1, 2, 3\}$ a $B = \{3, 5, 7\}$, pak pro

  $$\mathcal{X} = \{A, B\} = \big\{\{1, 2, 3\}, \{3, 5, 7\}\big\}$$

  dostaneme $\bigcup \mathcal{X} = A \cup B = \{1, 2, 3\} \cup \{3, 5, 7\} = \{1, 2, 3, 5, 7\}$.

- Následující, poněkud umělý příklad, snad také ilustruje koncept sumy množiny. Nechť $\mathcal{X}$ je definována jako (zde už nekonečná) množina právě všech jednoprvkových množin obsahujících jednotlivá přirozená čísla, tj.

  $$\mathcal{X} = \big\{\{n\} \colon n \in \mathbb{N}\big\}. \quad \text{Pak}$$
  $$\bigcup \mathcal{X} = \{1\} \cup \{2\} \cup \{3\} \cup \ldots = \{1, 2, 3, \ldots\} = \mathbb{N};$$

  zde zápisy se třemi tečkami jsou neformální, používám je jen pro objasnění věci; správně bychom měli napsat rovnou $\bigcup \mathcal{X} = \mathbb{N}$. △

2.5 Definice (Operace na indexovaných množinách)**.** Nechť I je libovolná množina, jejíž prvky budeme chápat jako indexy;[13] nechť jsou dále dány množiny A_i pro všechna $i \in I$. Pak definujeme *sjednocení*, resp. *průnik* množin A_i jako

$$\bigcup_{i \in I} A_i = \big\{x \colon \exists i \in I : x \in A_i\big\}, \quad \text{resp.}$$
$$\bigcap_{i \in I} A_i = \big\{x \colon \forall i \in I : x \in A_i\big\}$$

Pokud $I = \mathbb{N}$, můžeme psát též

$$\bigcup_{i=1}^{\infty} \text{ místo } \bigcup_{i \in \mathbb{N}}, \quad \text{resp.} \quad \bigcap_{i=1}^{\infty} \text{ místo } \bigcap_{i \in \mathbb{N}},$$

případně (se zřejmým významem) lze psát také $\bigcup_{n=0}^{\infty}$ nebo $\bigcap_{n=13}^{\infty}$ apod.

2.6 Poznámka. Všimněte si, že nyní máme dvě různé definice sjednocení, resp. průniku ko-

[13] Povaha indexů, tedy prvků indexové množiny, může být jakákoliv. Nemusí to být přirozená čísla. Přípustné indexy jsou třeba také reálná čísla, funkce i libovolné jiné objekty vyskytující se v naší teorii.

nečně mnoha množin $A_1, A_2, \ldots, A_N$. Podle Definice 2.2 jest

$$\bigcup_{i=1}^{N} A_i \overset{\text{def.}}{=} A_1 \cup A_2 \cup \ldots \cup A_N, \quad \text{neboli}$$
$$x \in \bigcup_{i=1}^{N} A_i \quad \Longleftrightarrow \quad x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_N.$$

Naproti tomu Definice 2.5 říká toto: pro indexovou množinu $I = \{1, 2, \ldots, N\}$ definujeme

$$\bigcup_{i \in I} A_i = \{x\colon \exists i \in I : x \in A_i\}, \quad \text{neboli}$$
$$x \in \bigcup_{i \in I} A_i \quad \Longleftrightarrow \quad \exists i \in \{1, 2, \ldots, N\}\colon x \in A_i$$

Protože je jasné, že význam symbolů $\bigcup_{i=1}^{N} A_i$ a $\bigcup_{i \in I} A_i$ pro $I = \{1, 2, \ldots, N\}$ by měl být stejný, je dobré si uvědomit, že výroky na pravých stranách obou ekvivalencí říkají totéž. Je triviální si rozmyslet (a vy to udělejte), že skutečně platí

$$x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_N \quad \Longleftrightarrow \quad \exists i \in \{1, 2, \ldots, N\}\colon x \in A_i. \tag{2.2}$$

To znamená, že sjednocení konečně mnoha množin jsme sice definovali dvakrát a zdánlivě jinak, ničemu to ovšem nevadí, neboť definice jsou ve vzájemném souladu.

Je snad jasné, že analogickou poznámku bychom mohli zformulovat pro průnik konečně mnoha množin; abychom si v tom případě uvědomili, že si definice neodporují, stačí si rozmyslet platnost ekvivalence

$$x \in A_1 \wedge x \in A_2 \wedge \ldots \wedge x \in A_N \quad \Longleftrightarrow \quad \forall i \in \{1, 2, \ldots, N\}\colon x \in A_i. \tag{2.3}$$

Všimněte si, že v ekvivalenci (2.2) odpovídá logické spojce $\vee$ („nebo“) existenční kvantifikátor a v ekvivalenci (2.3) odpovídá logické spojce $\wedge$ („a zároveň“) kvantifikátor obecný.

Výhoda značení z Definice 2.3 je, že funguje i pro nekonečné kolekce množin, aniž by bylo potřeba množiny indexovat. Nicméně pokud máme třeba (spočetně) nekonečně mnoho indexovaných množin $A_1, A_2, \ldots$, můžeme je dát do kolekce $\{A_i\colon i \in \mathbb{N}\}$ a pak pochopitelně platí

$$\bigcup \{A_i\colon i \in \mathbb{N}\} = \bigcup_{i=1}^{\infty} A_i.$$

2.2.3 Důkazy rovností množin a De Morganovy vzorce

Jako hezká ilustrace na použití a vztahy některých základních množinových operací nám poslouží následující tvrzení. Jeho důkaz je velmi poučný, neboť (přesně podle definic zúčastněných operací) převádí množinovou aritmetiku na výrokovou logiku, s níž pracujeme mnohem jistěji.

Důkaz vypadá dlouhý, ale nevynechávejte ho, je totiž spojen s výkladem. Ve skutečnosti by se vešel na pár řádků: Je jednoduchý, já na něm však chci ukázat některé myšlenky, takže obsahuje i komentáře, v důsledku čehož nám poněkud nabobtnal.

2.7 Tvrzení (De Morganovy vzorce)**.** *Nechť X a A_i pro $i \in I$ jsou množiny (kde I je jakákoliv množina „indexů“). Pak platí vzorce*

$$X \setminus \bigcap_{i \in I} A_i = \bigcup_{i \in I} (X \setminus A_i) \quad a \quad X \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (X \setminus A_i). \tag{2.4}$$

Vzorce rovněž platí, nahradíme-li v nich N symbolem ∞. Speciálně (pro $I = \{1, 2\}$) tedy máme

$$X \setminus (A_1 \cap A_2) = (X \setminus A_1) \cup (X \setminus A_2) \quad a \quad X \setminus (A_1 \cup A_2) = (X \setminus A_1) \cap (X \setminus A_2).$$

Důkaz. Pojďme si rozmyslet nejprve důkaz speciálního případu pro $I = \{1, 2\}$. Mějme tedy množiny A_1, A_2 a X (nemusíme předpokládat, že by X obsahovala zbylé dvě množiny; a priori mezi těmito třemi množinami nemusí být žádný vztah).

Co to znamená dokázat rovnost dvou množin? Výše jsme tuto otázku řešili v rámci NTM – poněkud nepřesně – na základě „definice“ z oddílu 2.1.1. Dospěli jsme k závěru (2.1), tj. že dvě množiny jsou si rovny, právě když mají stejné prvky; jinými slovy: jsou si rovny, právě když cokoliv je prvkem jedné, je i prvkem druhé *a naopak*. Důkaz rovnosti dvou množin je tedy důkazem této ekvivalence (opět, viz (2.1)). Někdy se hodí ekvivalenci chápat jako konjunkci dvou implikací[14] a dokázat každou z nich zvlášť; jindy je možné ji dokázat naráz.

V našem případě, kdy chceme dokázat rovnost množin[15]

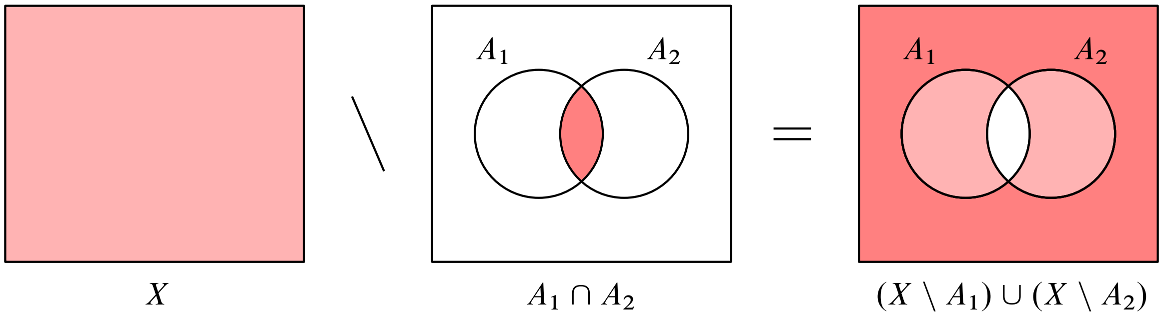
$$X \setminus (A_1 \cap A_2) = (X \setminus A_1) \cup (X \setminus A_2)$$

to tedy znamená dokázat, pro libovolný objekt x, ekvivalenci

$$x \in X \setminus (A_1 \cap A_2) \longleftrightarrow x \in (X \setminus A_1) \cup (X \setminus A_2).$$

[14] Jsou-li φ, ψ nějaké výroky, pak $(\varphi \leftrightarrow \psi)$ je ekvivalentní $(\varphi \to \psi) \wedge (\psi \to \varphi)$.

[15] Na levé straně rovnosti je nějaká množina (která vznikne pomocí operací z množin X, A_1 a A_2), podobně je jistá množina i na straně pravé.



Obrázek 2.5: První vzorec pro dvě množiny A_1, A_2. Tmavší odstín znamená, že se příslušné body vyskytnou v obou pronikaných (v prostředním obrázku) resp. sjednocovaných (vpravo) množinách. To sice není podstatné, je ale zajímavé si toho všimnout.

Pojďme tedy postupně dosazovat do definic jednotlivých zúčastněných množinových operací:

$$
\begin{aligned}
& x \in X \setminus (A_1 \cap A_2) & \\
\longleftrightarrow\ & x \in X \wedge \neg\big(x \in A_1 \cap A_2\big) & \text{(def. množinového rozdílu)} \\
\longleftrightarrow\ & x \in X \wedge \neg\big(x \in A_1 \wedge x \in A_2\big) & \text{(def. průniku množin)} \\
\longleftrightarrow\ & x \in X \wedge \big(x \notin A_1 \vee x \notin A_2\big) & \text{(negace konjunkce)} \\
\longleftrightarrow\ & \big(x \in X \wedge x \notin A_1\big) \vee \big(x \in X \wedge x \notin A_2\big) & \text{(distributivita)} \\
\longleftrightarrow\ & \big(x \in X \setminus A_1\big) \vee \big(x \in X \setminus A_2\big) & \text{(def. množinového rozdílu)} \\
\longleftrightarrow\ & x \in (X \setminus A_1) \cup (X \setminus A_2) & \text{(def. sjednocení)}
\end{aligned}
$$

První dvě ekvivalence jsou prostě dosazení do definic. Ekvivalence označená „negace konjunkce“ je snad také jasná: víme, že pro jakékoliv výroky φ, ψ obecně platí

$$\neg(\varphi \wedge \psi) \quad \longleftrightarrow \quad (\neg\varphi \vee \neg\psi),$$

tj. výše uvedená ekvivalence je *tautologie*.[16] O tom se lze snadno přesvědčit použitím selského rozumu, případně tabulku pravdivostních hodnot.

I další ekvivalence („distributivita“) využívá jednoduchého výrokového počtu, konkrétně tautologie

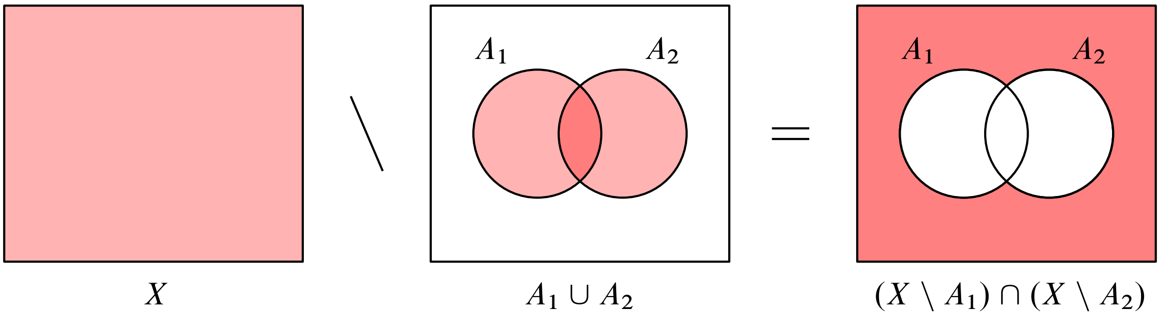
$$\varphi \wedge (\psi_1 \vee \psi_2) \quad \longleftrightarrow \quad (\varphi \wedge \psi_1) \vee (\varphi \wedge \psi_2).$$

I ta se dá nahlédnout pomocí tabulky (pokud vám to není jasné, napište si ji, měla by mít 8 řádků) ale i selským rozumem: platí-li φ a zároveň buďto ψ_1 nebo ψ_2 (popř. obojí), pak tedy buďto platí φ zároveň s ψ_1 nebo zároveň s ψ_2 (popř. obojí), tj. platí (nejméně) jedna z obou konjunkcí – a naopak.

[16] Tautologie je formule výrokového počtu, která má pravdivostní hodnotu 1 při libovolném pravdivostním ohodnocení všech zúčastněných proměnných, v tomto případe φ a ψ. Jinými slovy, tautologie „vždy platí“, a to z důvodu logické nutnosti.

Další dvě ekvivalence už využívají zase jen definic zúčastněných množinových operací, tedy rozdílu a sjednocení.

Tím je tedy dokázána první z obou rovností; důkaz rovnosti $X \setminus (A_1 \cup A_2) = (X \setminus A_1) \cap (X \setminus A_2)$ je analogický a doporučuji vám ho jako snadné cvičení, na kterém se ujistíte, že jste pochopili výše uvedené (příslušný obrázek platnost rovnosti také dobře ilustruje).



Obrázek 2.6: Druhý vzorec pro dvě množiny A_1, A_2.

Viděli jsme, že v případě De Morganových vzorců pro konečně mnoho množin si vystačíme s jednoduchým výrokovým počtem: stačí chápat zcela základní věci jako negaci konjunkce a podobně.

Nyní se podíváme na důkaz plné verze vzorců s tím, že se opět omezíme pouze na jednu z obou variant. Dokážeme tedy například druhý vzorec z (2.4). I zde se jedná o rovnost množin (na levé straně rovnosti je nějaká množina, stejně tak na straně pravé), chceme tedy dokázat, pro libovolné x, ekvivalenci

$$x \in X \setminus \bigcup_{i \in I} A_i \quad \longleftrightarrow \quad x \in \bigcap_{i \in I} (X \setminus A_i).$$

Postupným dosazováním do definic provedeme důkaz velmi podobně jako v předchozím případě.

$$\begin{aligned}
& x \in X \setminus \bigcup_{i \in I} A_i \\
\longleftrightarrow\ & x \in X \wedge \neg\Big(x \in \bigcup_{i \in I} A_i\Big) \\
\longleftrightarrow\ & x \in X \wedge \neg\big(\exists i \in I : x \in A_i\big) \\
\longleftrightarrow\ & x \in X \wedge \big(\forall i \in I : x \notin A_i\big) \\
\longleftrightarrow\ & \forall i \in I : x \in X \wedge x \notin A_i \\
\longleftrightarrow\ & \forall i \in I : x \in X \setminus A_i \\
\longleftrightarrow\ & x \in \bigcap_{i \in I} (X \setminus A_i)
\end{aligned}$$

Jak vidíte, je to velmi podobné, jako dříve. Hlavní změna je ve třetí ekvivalenci, kde negujeme výrok s kvantifikátorem. Není těžké si rozmyslet, že to funguje přesně uvedeným způsobem. □

2.3 Binární relace

Klíčovým pojmem pro další postup je právě relace: důležité pojmy jako zobrazení, uspořádání a ekvivalence jsou speciálními případy relací. Výklad k tomuto pojmu je společný pro NTM i pro axiomatickou teorii, k níž se dostaneme později (bude tedy možné se vrátit k tomuto oddílu v rámci studia axiomatické teorie).

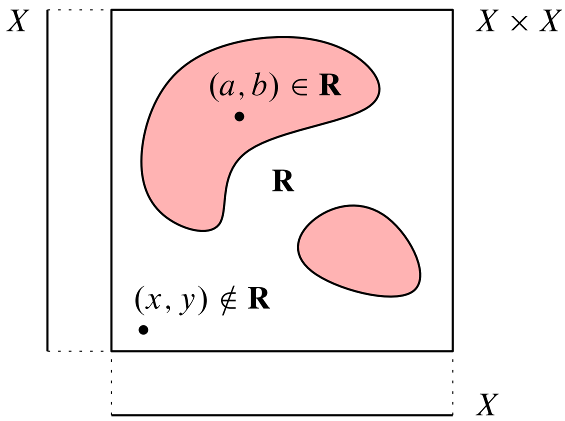
2.8 Definice (Relace)**.** Buď X libovolná množina.[17] Jakoukoliv podmnožinu $\mathbf{R}$ kartézského součinu $X \times X$ nazveme *relací na* X. Množinu X někdy nazýváme *nosnou množinou* relace $\mathbf{R}$.

Jsou-li A, B libovolné množiny, můžeme též definovat relaci mezi (prvky) A a B jako libovolnou podmnožinu součinu $A \times B$. Jedná se o speciální případ relace na X pro $X = A \cup B$.[18] Na druhou stranu je samozřejmě relace na X zároveň relací mezi prvky X a X, je tedy speciálním případem relace mezi prvky A a B (kde $A = X$ a $B = X$).

Vidíme, že obě definice relace, tedy relace na X a relace mezi A a B vyjdou v podstatě nastejno, a tak budeme pro jednoduchost pracovat převážně s první z nich.

Relace na X je tedy libovolná množina (třeba i prázdná) uspořádaných dvojic prvků X. Pokud jistá uspořádaná dvojice $(a, b) \in X \times X$ prvků X je prvkem $\mathbf{R}$, tj. $(a, b) \in \mathbf{R}$, řekneme, že a a b jsou spolu v relaci $\mathbf{R}$. Budeme používat zápis $a\mathbf{R}b$ jako zkratku za $(a, b) \in \mathbf{R}$.

Relace můžeme značit všelijakými symboly, nemusí to nutně být tučná velká písmena.



Obrázek 2.7: Relace, v níž $a\mathbf{R}b$ a $\neg(x\mathbf{R}y)$.

[17]Poznámka k axiomatické teorii: Připouštíme i možnost, že X je (vlastní) *třída*. Připouštíme tedy i relace na vlastních třídách, včetně celého univerza množin.

[18]Lze tedy říci, že relace $\mathbf{R}$ na X je relací mezi A a B, pokud $\mathrm{dom}(\mathbf{R}) \subseteq A$ a $\mathrm{rng}(\mathbf{R}) \subseteq B$. (Pojmy $\mathrm{dom}(\mathbf{R})$, resp. $\mathrm{rng}(\mathbf{R})$ definuji níže, jednoduše řečeno se ale jedná o definiční obor, resp. obor hodnot relace $\mathbf{R}$.

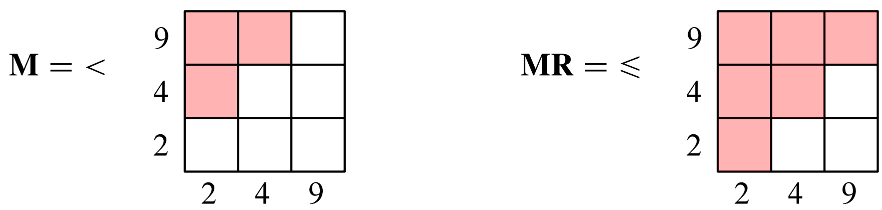
2.9 Poznámka. Na Obrázku 2.7 je množina X patrně nekonečná, v každém případě však jde pouze o zjednodušení: máme k dispozici pouze papír dimenze 2, takže při znázornění kartézského součinu nám nezbývá než jednotlivé činitele nakreslit dimenze 1, tj. typicky jako úsečky. Zde se tedy zdá, že X je nějaký interval, například $[1,6] \subseteq \mathbb{R}$, a $X \times X$ je tedy jistý plný čtverec v rovině. Je ale, doufám, jasné, že jde pouze o znázornění pro představu a X může být jakákoliv množina, například nějaká křivka v rovině nebo $\mathbb{N}$ atd. Podstatné je uvědomit si, že zde nás vlastně příliš nezajímá případná struktura na X: tuto množinu chápeme zcela abstraktně (a můžeme ji pak vlastně znázornit, jak cheme): třeba pokud $X = \mathbb{R}^3$, ignorujeme, že jde o vektorový prostor, ve kterém existují věci jako báze, velikost vektoru atd. Pro nás je to prostě konglomerát elementů. Chceme-li pak zadat nějakou relaci $\mathbf{R} \subseteq X \times X$, znamená to prostě nějakým způsobem jednoznačně určit, které dvojice (a, b), kde $a, b \in X$ do $\mathbf{R}$ patří a které ne.

2.10 Příklad. Vcelku jednoduše se dají znázornit relace na konečných množinách. Pokud X je konečná a má n prvků, pak $X \times X$ má n^2 prvků, které přirozeným způsobem tvoří tabulku $n \times n$, v níž každé „okénko“ odpovídá jednomu prvku $X \times X$.

Pojďme si tedy vzít konkrétní množinu, třeba $X = \{2, 4, 9\}$ a uvažujme na této množině relace

$$\mathbf{M} = \big\{(2,4), (2,9), (4,9)\big\} \quad \text{a} \quad \mathbf{MR} = \big\{(2,2), (2,4), (2,9), (4,4), (4,9), (9,9)\big\}.$$

Možná jste si všimli, že $\mathbf{M}$ je prostě relace $<$ („menší“) na množině X. Podobně $\mathbf{MR}$ je relace $\leqslant$ („menší nebo rovno“) na X. Pomocí tabulek lze tyto (dobře známé) relace zakreslit poněkud nezvyklým způsobem, který odpovídá přesně jejich definicím – viz Obrázek 2.8. Uspořádané dvojice, které do relace patří, odpovídají vybarveným okénkům, ostatní bílým.



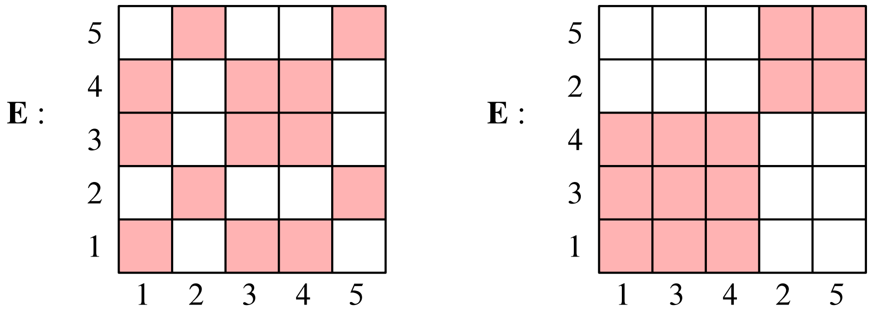
Obrázek 2.8: Tabulkové znázornění relací $<$ a $\leqslant$ na množině $X = \{2, 4, 9\}$

V dalším příkladě mějme nosnou množinu $X = \{1, 2, 3, 4, 5\}$, která má 5 prvků; příslušná tabulka tak bude mít 25 okének. Uvažujme nyní relaci $\mathbf{E}$ na této množině X, která je dána jako následující množina uspořádaných dvojic:

$$\mathbf{E} = \big\{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1), (1,4), (4,1), (3,4), (4,3), (2,5), (5,2)\big\}$$

Asi se shodneme, že z takovéhoto zápisu není snadné udělat si dobrou představu. Na Obrázku 2.9 vidíme příslušnou tabulku, v níž vybarvená okénka odpovídají prvkům relace $\mathbf{E}$.

V případě druhé tabulky jsme zvolili vhodnější pořadí prvků nosné množiny X, aby byla struktura relace $\mathbf{E}$ lépe patrná, jedná se o tutéž relaci, jak se lze snadno přesvědčit. Je dobré si uvědomit, že nám zde nezáleží na pořadí, ve kterém prvky nosné množiny X v tabulce uvedeme, neboť X je pro nás v tuto chvíli prostě pětiprvková množina bez jakékoliv struktury.[19]



Obrázek 2.9: Dvakrát ta stejná relace $\mathbf{E}$: záleží jen na tom, které dvojice do ní patří a které ne.

Místo $X = \{1, 2, 3, 4, 5\}$ bychom mohli uvažovat třeba množinu $Y = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit, \maltese\}$ a na ní relaci

$$\mathbf{F} = \big\{(\clubsuit, \clubsuit), (\diamondsuit, \diamondsuit), (\heartsuit, \heartsuit), (\spadesuit, \spadesuit), (\maltese, \maltese), (\clubsuit, \heartsuit),\\ (\heartsuit, \clubsuit), (\clubsuit, \spadesuit), (\spadesuit, \clubsuit), (\heartsuit, \spadesuit), (\spadesuit, \heartsuit), (\diamondsuit, \maltese), (\maltese, \diamondsuit)\big\}$$

Na množině Y nejsme zvyklí mít žádné „kanonické“ uspořádání, je tedy pro nás jednodušší Y chápat skutečně jako abstraktní množinu bez dodatečných struktur. Pořadí prvků Y při kreslení tabulky relace $\mathbf{F}$ (můžete si to zkusit) evidentně záleží na naší libovůli. Jde ovšem o situaci analogickou relaci $\mathbf{E}$ na X.[20] △

2.11 Příklad. Ať už si toho jste, nebo nejste vědomi, s relacemi jste se setkali už mnohokrát. Každé zobrazení a funkce je příkladem relace: třeba funkce $\sin x$ je z matematické analýzy dobře známá relace na $\mathbb{R}$. To uvidíme a podrobně rozebereme později.

Jiný příklad je třeba běžná relace uspořádání $\leqslant$ na $\mathbb{R}$. Striktně vzato je $\leqslant$ podmnožina $\mathbb{R} \times \mathbb{R}$,[21] tj. jde o množinu (některých) uspořádaných dvojic přirozených čísel. Dobře víme, že třeba $(3, 4) \in\, \leqslant$, $(5, 5) \in\, \leqslant$, ale $(7, 6) \notin\, \leqslant$. Pochopitelně tyto skutečnosti obvykle zapisujeme (v souladu s konvencí o zápisu $a\mathbf{R}b$ z Definice 2.8) raději takto: $3 \leqslant 4$, $5 \leqslant 5$, $7 \nleqslant 6$. Můžeme si všimnout, že $\nleqslant$ je vlastně také příkladem relace na $\mathbb{R}$, pro kterou platí:

$$\nleqslant\, = \mathbb{R} \times \mathbb{R} \setminus \leqslant \qquad \text{a také} \qquad \nleqslant\, = \,> .$$

Oba uvedené zápisy jsou skutečně korektní a vyjadřují pravdivé rovnosti množin. Skutečně,

[19] Tedy speciálně bez uspořádní či dokonce aritmetických operací apod.

[20] Obě relace, tady $\mathbf{E}$ a $\mathbf{F}$ jsou dokonce izomorfní v tom smyslu, že existuje bijekce $f : X \to Y$ taková, že pro všechna $a, b \in X$ je $a\mathbf{E}$, právě když $f(a)\mathbf{F} f(b)$. Jistě vám nebude dělat potíže tuto bijekci najít.

[21] Bizarní zápis „$\leqslant\, \subseteq \mathbb{R} \times \mathbb{R}$“ je tedy správný a pravdivý.

první zápis říká, že v relaci $\not\leqslant$ jsou právě všechny dvojice reálných čísel, které nejsou v relaci $\leqslant$. Druhý zápis vlastně říká, že pro libovolná čísla $a, b \in \mathbb{R}$ je $a \not\leqslant b$, právě když $a > b$. A takto bychom mohli pokračovat, například si můžete velmi snadno rozmyslet, že platí rovnost množin (relací na $\mathbb{R}$)

$$< \; = \mathbb{R} \times \mathbb{R} \setminus \geqslant$$

a tak dále. △

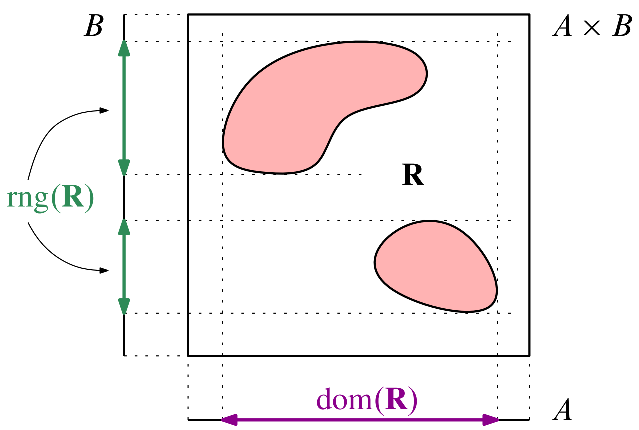
2.12 Poznámka. V teorii množin je nejzákladnější *relace náležení*, neboli $\in$. V axiomatické teorii později uvidíme, že jde o třídovou relaci (viz poznámka pod čarou 17) na univerzu množin. Relace náležení $\in$ je příkladem tzv. *primitivního pojmu*, tedy pojmu (v tomto případě relace), který přímo nedefinujeme (není „z čeho“) a jeho vlastnosti jsou místo toho vymezeny pomocí axiomů.

Další známé relace mezi množinami, jako třeba $\subseteq$, jsou už pojmy odvozené, tj. definované pomocí nástrojů logiky a pojmů primitivních, případně jiných (už definovaných) pojmů, jejichž definice se dají zapsat pomocí primitivních pojmů. Třeba právě zápis $A \subseteq B$ definujeme platností výroku $\forall x\colon\; x \in A \to x \in B$.

2.3.1 Základní pojmy

Mějme nyní libovolnou relaci $\mathbf{R} \subseteq A \times B$; jde tedy o relaci mezi prvky A a prvky B, kde A, B můžou být jakékoliv množiny.[22] Definujeme následující pojmy:

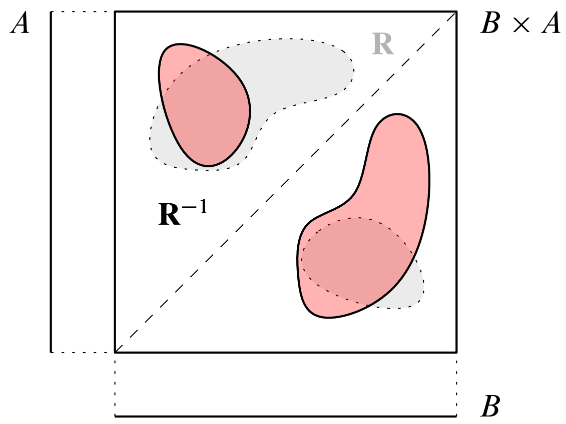
- $\mathrm{dom}(\mathbf{R}) = \{x \in A\colon\; \exists y \in B\colon x\mathbf{R}y\}$ je *definiční obor* relace $\mathbf{R}$, anglicky také *domain*.
- $\mathrm{rng}(\mathbf{R}) = \{y \in B\colon\; \exists x \in A\colon x\mathbf{R}y\}$ je *obor hodnot* relace $\mathbf{R}$, také známý jako *range*.



Obrázek 2.10: Domain a range relace **R** jsou projekce **R** na „osy“.

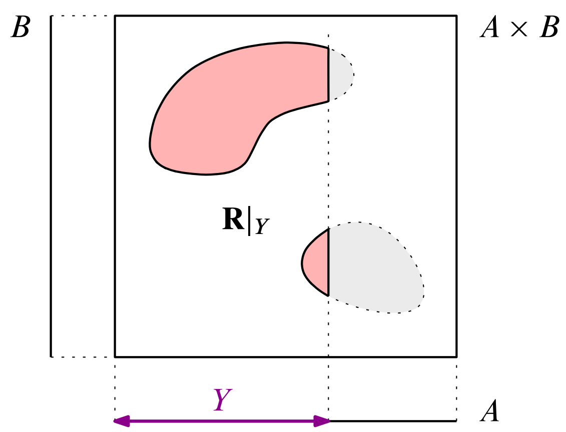
- $\mathbf{R}^{-1} = \{(x, y) \in B \times A\colon\; (y, x) \in \mathbf{R}\}$ je *inverzní relace* k relaci $\mathbf{R}$.

[22] Všechny následující definice lze samozřejmě použít i v případě, kdy $\mathbf{R}$ je relace na X, tj. $\mathbf{R} \subseteq A \times B$. U těchto definic chci rozlišovat „výchozí“ a „cílovou“ množinu relace hlavně kvůli přehlednosti a názornosti. Ovšem, jak



Obrázek 2.11: Relace $\mathbf{R}$ a $\mathbf{R}^{-1}$ jsou zrcadlově symetrické podle „diagonály“.

- $\mathbf{R}|_Y = \{(x, y) \in A \times B :\ (x, y) \in \mathbf{R} \wedge x \in Y\}$ je *restrikce* relace $\mathbf{R}$ na množinu Y.



Obrázek 2.12: Restrikce je „umělé“ omezení definičního oboru.

- Je-li C nějaká množina a $\mathbf{S} \subseteq B \times C$ je relace, pak definujeme *složenou relaci* takto: $\mathbf{R} \circ \mathbf{S} = \{(x, z) \in A \times C :\ \exists y \in B : x\mathbf{R}y \wedge y\mathbf{S}z\}$.

  Zde je namístě poznamenat, že pořadí zápisu $\mathbf{R}\circ\mathbf{S}$ u relací znamená, že nejprve „aplikujeme“ relaci $\mathbf{R}$ a až poté $\mathbf{S}$. Ovšem u zobrazení (viz níže) je tomu naopak: složení $f \circ g$ dvou zobrazení funguje tak, že nejprve aplikujeme g a potom f. Na to je potřeba si dávat pozor, z kontextu bude nicméně vždy jasné, kterou variantu máme na mysli.

2.13 Cvičení. (i) Buď X množina všech lidí a uvažujme na ní relaci „x je otec y“, kterou označme $\mathbf{O} \subseteq X \times X$. Platí jedna z rovností $X = \mathrm{dom}(\mathbf{O})$, $X = \mathrm{rng}(\mathbf{O})$? Vysvětlete.

(ii) Mějme těchto sedm relací mezi lidmi (tj. na množině X): být otec, matka, dítě, bratr, sestra, manžel (husband), manželka (wife). Označíme tyto relace pořadě symboly $\mathbf{O}$, $\mathbf{M}$,

víme, není to potřeba, stačilo by hovořit čistě o relaci na X.

D, **B**, **S**, **H**, **W**. Aplikujeme-li na tyto relace různé výše definované operace, dostaneme nové relace, pro něž někdy nalezneme jednoduché názvy v běžném jazyce; například $\mathbf{H} \circ \mathbf{D}$ označuje relaci „být zeť“. Najděte, pokud je to možné, jednoduché názvy pro tyto relace:

$$\mathbf{H}^{-1},\ \mathbf{B}^{-1},\ \mathbf{O} \cup \mathbf{M},\ \mathbf{O} \cup \mathbf{B},\ \mathbf{O} \circ \mathbf{M},\ \mathbf{M} \circ \mathbf{D}^{-1},\ \mathbf{B} \circ \mathbf{D}^{-1},$$
$$\mathbf{O} \circ (\mathbf{W} \cup \mathbf{H}),\ (\mathbf{B} \circ \mathbf{D}^{-1}) \cup \big(\mathbf{H} \circ (\mathbf{S} \circ \mathbf{D}^{-1})\big).$$

(iii) Pomocí symbolů pro relace mezi lidmi a operací mezi relacemi vyjádřete relace být rodičem, sourozencem, vnoučetem, snachou a tchyní.

(iv) Objasněte významy následujících formulí a určete, které z nich jsou pravdivé:

$$\mathbf{B}^{-1} = \mathbf{S},\ \mathbf{O} \cup \mathbf{M} = \mathbf{D}^{-1},\ \mathbf{H} \circ \mathbf{M} = \mathbf{O},\ \mathbf{B} \circ \mathbf{S} \subseteq \mathbf{B},\ \mathbf{S} \subseteq \mathbf{D} \circ \mathbf{D}^{-1},\ \mathbf{O} \subseteq X \times X \setminus \mathbf{M}$$

2.3.2 Typy relací

Následující definice už jste nejspíše potkali, přesto vám je ale připomenu.

2.14 Definice. Buď X libovolná množina a $\mathbf{R} \subseteq X \times X$. Řekneme, že relace **R** je:

- *reflexivní*, jestliže $\forall x \in X : x\mathbf{R}x$;
- *symetrická*, jestliže $\forall x, y \in X : x\mathbf{R}y \rightarrow y\mathbf{R}x$;
- *tranzitivní*, jestliže $\forall x, y, z \in X : x\mathbf{R}y \wedge y\mathbf{R}z \rightarrow x\mathbf{R}z$;
- *slabě antisymetrická*, jestliže $\forall x, y \in X : x\mathbf{R}y \wedge y\mathbf{R}x \rightarrow x = y$;
- *silně antisymetrická*, jestliže $\forall x, y \in X : x\mathbf{R}y \rightarrow \neg y\mathbf{R}x$;
- *trichotomická*, jestliže $\forall x, y \in X : x\mathbf{R}y \vee y\mathbf{R}x \vee x = y$.

2.15 Příklad. Pojďme se podívat na nějaké příklady ze života: buď X množina lidí. Na X můžeme uvažovat různé relace dané (například) příbuzenskými vztahy.[23]

Uvažujme relaci „sourozenectví“ **S**, pro niž $x\mathbf{S}y$, právě když x je sourozenec y (pro všechna $x, y \in X$). Které z výše uvedených vlastností tato relace má? Zkuste si to rozmyslet. Změní se něco, připustíme-li i „nevlastní sourozence“ (definované právě jedním společným rodičem)?[24]

[23] Relace = vztah. Pokud nám tedy nevadí matematické koncepty ilustrovat na příkladech ze života (mně to třeba vadí jen někdy), příbuzenské vztahy (tj. relace) se přímo nabízejí.

[24] Odpověď: Není reflexivní, je symetrická, je tranzitivní a není v žádném smyslu antisymetrická. Připustíme-li nevlastní sourozence, selže tranzitivita.

Dále můžeme vzít relaci „je předkem“, tj. $x\mathbf{P}y$, právě když x je předek y. Které z uvedených vlastností má tato relace?[25]

Zkuste si sami vymyslet nějaké další podobné příklady a promyslet si jejich vlastnosti. $\triangle$

2.16 Poznámka. Jak terminologie napovídá, *silná antisymetrie implikuje antisymetrii slabou*. Pojďme si uvědomit, že tomu tak skutečně je; mějme tedy libovolnou silně antisymetrickou relaci $\mathbf{R}$ na množině nějaké množině X; chceme dokázat její slabou antisymetrii.

Mějme tedy libovolné prvky $x, y \in X$. Ze silné antisymetrie relace $\mathbf{R}$ vyplývá, že nemůže současně platit $x\mathbf{R}y$ a $y\mathbf{R}x$; to znamená, že výrok $x\mathbf{R}y \wedge y\mathbf{R}x$, který je předpokladem implikace z definice slabé antisymetrie, je zaručeně nepravdivý. To ovšem znamená, že implikace je pravdivá (bez ohledu na platnost jejího závěru).[26] Tedy $\mathbf{R}$ je slabě antisymetrická.

Je dobré si správně rozmyslet, jak tato terminologie funguje: *slabou* vlastností se myslí podmínka, kterou je snadné splnit, tj. splní ji více individuí. *Silnou* podmínku naproti tomu splní jen některá individua. Kupříkladu můžeme definovat pojem *zdatný sprinter* zaběhnutým časem na 100 metrů pod 12 sekund a pojem *špičkový sprinter* časem na 100 metrů pod 10 sekund. Je zřejmé, že každý špičkový sprinter je zároveň zdatný, ale ne naopak. Stejně tak každá silně antisymetrická relace je zároveň slabě antisymetrická (ale ne naopak).

2.17 Definice. Buď X libovolná množina a $\mathbf{R} \subseteq X \times X$. Řekneme, že relace $\mathbf{R}$ je:

- *ekvivalence*, je-li reflexivní, symetrická a tranzitivní;
- *neostré uspořádání*, je-li reflexivní, slabě antisymetrická a tranzitivní;
- *ostré uspořádání*, je-li silně antisymetrická a tranzitivní.

Uspořádání (ostré nebo neostré), které je navíc trichotomické, se nazývá *lineární*. Uspořádání (ostré nebo neostré), které není lineární, se nazývá *částečné*.

Každé uspořádání je tedy lineární, nebo částečné; poznáme to tak, že u lineárního uspořádání jsou každé dva různé prvky porovnatelné, zatímco u částečného existují aspoň dva neporovnatelné prvky.

2.18 Příklad. V Příkladu 2.10 jsme diskutovali relace $\mathbf{M}$, $\mathbf{MR}$ a $\mathbf{E}$. Rozmyslete si, jakých typů (podle definice výše) tyto relace jsou.[27] Snadno je vidět symetrie relace $\mathbf{E}$ a antisymetrie zbylých dvou. Reflexivita je v tomto tabulkovém zápisu také jednoduše rozpoznatelná, znamená přesně to, že jsou vybarvena všechna políčka na diagonále (třeba u $\mathbf{MR}$ to znamená vybarvená políčka odpovídající dvojicím $(2, 2)$, $(4, 4)$, $(9, 9)$, podobně pro $\mathbf{E}$).

I tranzitivita se dá nahlédnout z obrázku; snadné je to třeba u relace $\mathbf{M}$, u níž vidíme $2\mathbf{M}4$, $4\mathbf{M}9$ a skutečně také $2\mathbf{M}9$, jak žádá tranzitivita. Zkuste si to podobně rozmyslet u relace $\mathbf{E}$. $\triangle$

[25] Tato relace není reflexivní, ani symetrická. Je ovšem tranzitivní a silně (a tedy i slabě – viz níže) antisymetrická.

[26] Stačí nahlédnout do tabulky pravdivostních hodnot implikace.

[27] Odpověď: $\mathbf{M}$ je ostré uspořádání, $\mathbf{MR}$ je neostré uspořádání a $\mathbf{E}$ je ekvivalence.

2.3.3 Relace ekvivalence

Nyní se podíváme podrobněji na některé relace ekvivalence, tedy relace, které jsou současně reflexivní, symetrické a tranzitivní.

2.19 Příklad (Příklady ekvivalencí). • Rovnost (identita) je triviálním příkladem ekvivalence na jakékoliv množině X. Všechny vlastnosti (tedy reflexivita, symetrie a tanzitivita) jsou triviálně platné, jde prostě o známé vlastnosti rovnosti. Například: pokud $x = y$ a zároveň $y = z$, pak také $x = z$, a to bez ohledu na to, o jaký typ objektu se jedná.

- Buď X množina všech trojúhelníků v $\mathbb{R}^2$. Na X budeme uvažovat tři relace: $=, \approx, \sim$, kde pro libovolné trojúhelníky $x, y \in X$ definujeme $x \approx y$ jako jejich shodnost, $x \sim y$ jako jejich podobnost (a samozřejmě $x = y$ znamená prostě jejich identitu, neboli že x a y jsou jeden a tentýž trojúhelník). U všech tří relací je snadné ověřit, že se jedná o ekvivalence (u rovnosti to víme na jakékoliv množině, tedy i na množině trojúhelníků). Například pokud $x \sim y$ a $y \sim z$, je také $x \sim z$. To lze odvodit třeba ze znalosti geometrické věty, že podobnost trojúhelníků znamená shodnost vnitřních úhlů.[28]

  Je jasné, že pokud $x = y$, pak také $x \approx y$. Podobně pokud $x \approx y$, pak také $x \sim y$. Tyto dva zřejmé fakty se dají zapsat také množinově takto: $= \ \subseteq \ \approx \ \subseteq \ \sim$. To je ovšem opravdu dosti obskurní zápis, který bych nikomu nedoporučil. Snad přehlednější by to bylo pokud bychom si rovnost na okamžik označili $\mathbf{R}$, shodnost $\mathbf{S}$ a podobnost $\mathbf{P}$. Nyní už nám asi nebude činit potíže $\mathbf{R}, \mathbf{S}, \mathbf{P} \subseteq X \times X$ vnímat jednoduše jako množiny (a to množiny uspořádaných dvojic trojúhelníků v rovině) a zápis $\mathbf{R} \subseteq \mathbf{S} \subseteq \mathbf{P}$ je snad o něco stravitelnější.

- Jiným přirozeným příkladem relace ekvivalence v geometrii je rovnoběžnost přímek, tj. na množině $X = \{p \subseteq \mathbb{R}^2 \colon p \text{ je přímka}\}$. Pro $p, q \in X$ definujeme $p \| q$, pokud p a q jsou rovnoběžné, tj. nemají právě jeden společný bod. (Tato definice mj. znamená, že $p \| p$ pro libovolnou $p \in X$.) Pak $\|$ je relace ekvivalence na X, jak si snadno ověříte sami. △

2.20 Příklad (Třídy ekvivalence). Buď X množina všech žijících lidí. Můžeme popsat relaci $\mathbf{T}$ mezi prvky X takto: pro $x, y \in X$ platí $x\mathbf{T}y$, právě když osoby x a y se narodily ve stejný den v týdnu (pondělí atd.). Pokud tedy například $a \in X$ i $b \in X$ se narodili v pondělí, platí $a\mathbf{T}b$, pokud ale osoba a se narodila v pátek, zatímco osoba b v sobotu, platí $\neg a\mathbf{T}b$, tj. neplatí $a\mathbf{T}b$.

Všimněme si nyní, že každý prvek X spadá do právě jedné ze sedmi množin: lidé narození v pondělí, lidé narození v úterý atd. až po narozené v neděli. Označíme-li si tyto množiny

[28] Známe-li pojem podobnosti jakožto zobrazení, pak je nám zřejmé, že složení dvou podobností je podobnost, čehož je tranzitivita uvedené relace triviálním důsledkem.

postupně $X_1, X_2, \ldots, X_7$, můžeme psát $X = X_1 \cup X_2 \cup \ldots \cup X_n$, neboli

$$X = \bigcup_{i=1}^{7} X_i,$$

přičemž každé dvě různé množiny X_i, X_j mají prázdný průnik: žádný člověk se nenarodil současně v i-tém a j-tém dni v týdnu, kde $i \neq j$.[29] Tento fakt lze zapsat formálně:

$$\forall i, j \in \{1, 2, \ldots, 7\}: i \neq j \longrightarrow X_i \cap X_j = \emptyset.$$

Vrátíme-li se nyní k naší relaci $\mathbf{T}$, je jasné, že pro libovolné dva lidi $x, y \in X$ je $x\mathbf{T}y$, právě když x, y jsou prvkem společné množiny X_i (oba se narodili v tomtéž, a to i-tém, dni týdne). Z druhé strany je jasné, že máme-li například nějaký prvek $x_1 \in X_1$ (tj. člověka narozeného v pondělí), pak $X_1 = \{y \in X : y\mathbf{T}x_1\}$, a podobně pro další X_i.

Vidíme tedy, že rozklad X na $X_1, X_2, \ldots, X_7$ s relací $\mathbf{T}$ úzce souvisí: relace určuje rozklad a naopak. Množinám X_i se v tomto kontextu říká *třídy ekvivalence* $\mathbf{T}$. △

2.21 Definice (Třídy ekvivalence)**.** Nechť $\mathbf{E}$ je relace ekvivalence na množině (třídě) X. Pak pro každé $x \in X$ definujeme *třídu ekvivalence* $\mathbf{E}$ příslušnou prvku x jako

$$[x]_{\mathbf{E}} = \big\{y \in X : y\mathbf{E}x\big\}.$$

Soubor všech tříd ekvivalence $\big\{[x]_{\mathbf{E}} : x \in X\big\}$ pak nazýváme *rozkladem* X *podle* $\mathbf{E}$ a často ho značíme $X/_{\mathbf{E}}$. Máme-li nějakou třídu ekvivalence $[x]_{\mathbf{E}}$, pak prvek x, ale také libovolný jiný její prvek, nazýváme *reprezentantem* té třídy.

2.22 Poznámka. Je dobré si všimnout, že máme-li dva prvky $x, y \in X$, pro něž $x\mathbf{E}y$ (kde $\mathbf{E}$ stále značí nějakou ekvivalenci na X), pak $[x]_{\mathbf{E}} = [y]_{\mathbf{E}}$. Řečeno slovy: navzájem ekvivalentní prvky určují tutéž třídu ekvivalence. Doporučuji vám si tento jednoduchý fakt samostatně dokázat pomocí tří axiomů ekvivalence (reflexivita, symetrie, tranzitivita).

Vidíme tedy, v definici rozkladu X podle $\mathbf{E}$ se mohou uvedené třídy opakovat. Pro názornost se vraťme k Příkladu 2.20 a předpokládejme, že množina X (všech lidí) má alespoň 8 různých prvků $x_1, x_2, \ldots x_8$. Vzhledem k tomu, že $\mathbf{T}$ určuje na X pouze 7 tříd ekvivalence, některé dva z uvedených 8 prvků musí ležet ve stejné třídě: nechť jsou to například prvky x_3 a x_8. To znamená, že $x_3\mathbf{T}x_8$ a $[x_3]_{\mathbf{T}} = [x_8]_{\mathbf{T}}$. Vypíšeme-li nyní výčet všech tříd ekvivalence $\mathbf{T}$ příslušných prvkům x_1 až x_8, dostaneme:

$$[x_1]_{\mathbf{T}}, [x_2]_{\mathbf{T}}, [x_3]_{\mathbf{T}}, [x_4]_{\mathbf{T}}, [x_5]_{\mathbf{T}}, [x_6]_{\mathbf{T}}, [x_7]_{\mathbf{T}}, [x_8]_{\mathbf{T}}.$$

My ovšem víme, že v tomto seznamu je nejméně jedna třída uvedena (nejméně) dvakrát, totiž

[29] Předpokládejme, že u každého člověka lze jednoznačně určit jediný den v týdnu, ve kterém se narodil.

$[x_3]_{\mathbf{T}}$. To ovšem znamená, že množina

$$\big\{[x_1]_{\mathbf{T}}, [x_2]_{\mathbf{T}}, [x_3]_{\mathbf{T}}, [x_4]_{\mathbf{T}}, [x_5]_{\mathbf{T}}, [x_6]_{\mathbf{T}}, [x_7]_{\mathbf{T}}, [x_8]_{\mathbf{T}}.\big\}$$

obsahuje nejvýše 7 prvků (a možná méně, pokud je v seznamu více opakování).[30] Pamatujte, že prvky množiny jsou navzájem různé, tj. jeden a tentýž prvek se dvěma různými zápisy (jako např. $[x_3]_{\mathbf{T}}$ a $[x_8]_{\mathbf{T}}$) se v množině objeví přesně jednou.

V našem konkrétním případě má množina X miliardy prvků a dělíme ji na pouhých 7 tříd ekvivalence (jednu pro každý den v týdnu). To znamená, že v zápisu $\big\{[x]_{\mathbf{T}} : x \in X\big\}$ se některé (vlastně skoro určitě každá) ze sedmi tříd mnohokrát opakují. Přesto má tato množina tříd ekvivalence (nejvýše, ale skoro jistě právě) sedm prvků.

2.23 Poznámka (Co je to „směr"?)**.** Nyní se na okamžik vrátíme k příkladu rovnoběžnosti přímek v eukleidovské rovině, kterou si nyní označíme E_2. Tj. buď opět $X = \{p \subseteq E_2 : p \text{ je přímka}\}$ a $\|$ buď relace rovnoběžnosti na X; o té jsme si už rozmysleli, že je to relace ekvivalence.

Pojďme se nyní zamyslet, co vlastně rozumíme abstraktním pojmem, jako je *směr přímky* v E_2. Jedna možnost je uvažovat E_2 jako $\mathbb{R}^2$, přímky popsat analyticky pomocí jejich rovnice tvaru $y = \alpha x + \beta$ a jejich „směr" ztotožnit se směrnicí α. Tím postihneme všechny směry až na ten odpovídající ose y, tj. „svislé" přímky; na ty nám nedělá problém nahlížet jako na speciální případ.

Uvedené řešení položené otázky je bohužel poněkud alibistické. Každé malé dítě totiž „pozná", když dvě přímky mají stejný směr, definici pomocí směrnice v analytickém vyjádření bychom ale dětem na prvním stupni vysvětlovali těžko. Je tedy vidět, že k popisu „základního" pojmu jako *směr* jsme sáhli k příliš hluboké teorii.[31] Ne náhodou jsem přitom napsal, že školáček dokáže rozeznat, že dvě přímky mají *stejný směr*; těžko bychom však téhož školáčka žádali, aby nám vysvětlil, co směr *je*.

V mnoha případech pro nás není obtížné nahlédnout obsah některých důležitých ekvivalencí. Školáček v podstatě rozumí významu ekvivalence $\|$, protože „neomylně" rozpozná dvojice rovnoběžných přímek od dvojic různoběžných. O čem už nejspíš většina dětí nepřemýšlí, jsou třídy ekvivalence, které relaci rovnoběžnosti odpovídají; ve skutečnosti jim ale v jistém smyslu rozumí: tyto třídy jsou totiž to, čemu dává velmi dobrý smysl říkat *směry*. Výhoda tohoto přístupu je zřejmá: k jeho definici potřebujeme pouze naprosto základní pojem relace ekvivalence; nepotřebujeme chápat podstatu reálných čísel ani žádná fakta pokročilejší matematiky.

Směry v E_2 tedy definujeme jako třídy ekvivalence $\mathbf{T}$, tj. každá třída ekvivalence je směr a naopak. Každé přímce $p \in X$ tedy odpovídá směr $[p]_{\|}$, jehož je přímka p reprezentantem (stejně jako kterákoliv jiná přímka q z téže třídy, tj. splňující $q \| p$).

[30] Vzpomeňte, že třeba množina $\{a, a\}$ má jediný prvek, a to a. Viz též oddíl 2.1.2.

[31] Ostatně na to lze nahlížet i z historického hlediska: staří Řekové jistě měli dobrou představu o obsahu pojmu *směr přímky*, přesto ale nemohli použít výše uvedenou definici, neboť analytická geometrie má své kořeny až u Descarta.

Že přímky p a q „mají stejný směr“, tedy znamená, že jsou reprezentanty téhož směru, neboli prvky téže třídy ekvivalence $\|$. To lze zapsat třeba tak, že existuje $r \in X$, že $p, q \in [r]_{\|}$, nebo jednodušeji $q \in [p]_{\|}$, resp. $p \in [q]_{\|}$. Je jasné, že všechny tři zápisy ve výsledku říkají totéž: v prvním případě máme $p \| r$ a $q \| r$, odkud jednoduše (pomocí symetrie a tranzitivity $\|$) odvodíme $p \| q$, druhý zápis říká přímo $p \| q$ a třetí zápis říká $q \| p$, což je ze symetrie stejné jako $p \| q$. Shrnuto: to, že přímky p a q mají stejný směr, lze chápat jedině tak, že patří do společné třídy ekvivalence $\|$, což znamená přesně $p \| q$.

Pojďme se podívat ještě na jeden zajímavý příklad ekvivalence, tentokrát v aritmetice.

2.24 Příklad. Nosná množina bude tentokrát $\mathbb{Z}$, tedy množina všech celých čísel a mějme nějaké přirozené číslo $n \geqslant 2$. Definujeme relaci $\mathbf{E_n}$ pro libovolná čísla $k, l \in \mathbb{Z}$ takto:

$$k \mathbf{E_n} l \quad \stackrel{\text{def.}}{\iff} \quad k \equiv l \mod n.$$

Předpokládejme nejprve, že $n = 2$. Pak $k \mathbf{E_2} l$, právě když obě čísla mají stejný zbytek po dělení 2, to jest právě když k, l jsou obě sudá, nebo k, l jsou obě lichá. Je tedy zřejmé, že

$$\mathbb{Z}/_{\mathbf{E_2}} = \big\{\{a \in \mathbb{Z} \colon a \text{ je sudé}\}, \{a \in \mathbb{Z} \colon a \text{ je liché}\}\big\}.$$

Slovy: Rozklad $\mathbb{Z}$ podle ekvivalence $\mathbf{E_2}$ má dva prvky, a sice množinu všech sudých čísel a množinu všech lichých čísel.

Asi je vám nyní jasné, že když budeme předpokládat $n = 3$, pak se celá čísla rozpadnou do tří tříd podle zbytku po dělení 3, a to pro zbytky 0 (tj. čísla třemi dělitelná), 1 a 2. Pro obecné číslo $n \geqslant 2$ máme tedy n tříd ekvivalence, které se dají zapsat také takto:

$$\begin{aligned}\mathbb{Z}/_{\mathbf{E_n}} = \big\{&\{0, n, -n, 2n, -2n, \dots\},\ \{1, 1+n, 1-n, 1+2n, 1-2n, \dots\},\ \dots \\ &\dots,\ \{(n-1), (n-1)+n, (n-1)-n, (n-1)+2n, (n-1)-2n, \dots\}\big\}.\end{aligned}$$

Rozklad $\mathbb{Z}/_{\mathbf{E_n}}$ má tedy n prvků, z nichž každý je nekonečná množina celých čísel se společným zbytkem po dělení n. △

Jako malý bonus nabízím ještě některé další příklady, které se samovolně vyskytly při diskusích se studenty u zkoušky.

2.25 Příklad. Mějme nějakou neprázdnou množinu lidí X a uvažujme na ní relaci $\mathbf{P}$ definovanou vztahem

$$x \mathbf{P} y \quad \stackrel{\text{def.}}{\iff} \quad x \text{ je kamarád(ka) } y.$$

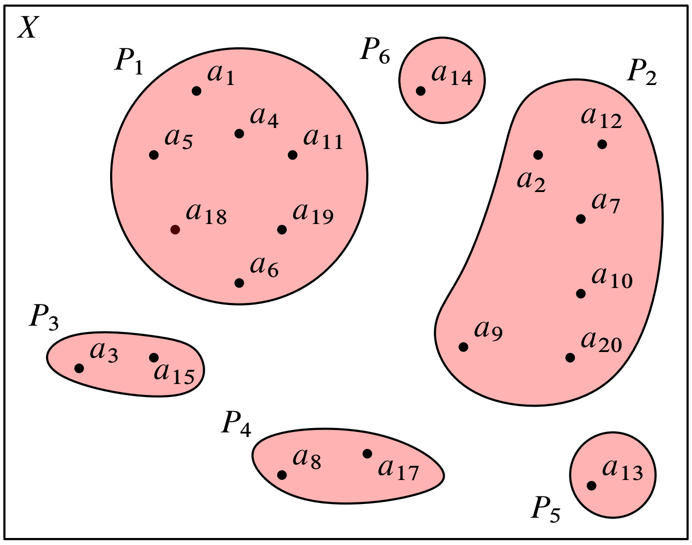
Zamyslete se, jestli je $\mathbf{P}$ relací ekvivalence na množině X, tj. jestli $\mathbf{P}$ splňuje reflexivitu, symetrii a tranzitivitu.

Reflexivita je patrně nejméně podstatná součást definice relace ekvivalence, a můžeme se tedy dohodnout, že podle naší definice je každý člověk sám sobě kamarádem. (I když je jasné, že u piva se o otázce reflexivity $\mathbf{P}$ dá vést celovečerní diskuse.) Při promýšlení platnosti dalších axiomů ekvivalence se ovšem nevyhneme otázce, které lidi množina X obsahuje.

Pokud například požadujeme, aby X obsahovala všechny žijící lidi, pak z vlastní zkušenosti asi každý zná případy, ve kterých selže tranzitivita: často se třeba stává, že x je kamarádka y a y je kamarádka z, přičemž x není kamarádka z.

Na druhou stranu pokud by nosná množina $X = \{a\}$ byla pouze jednobodová, byla by relace **P** ekvivalencí z triviálních důvodů: podle dohodnuté reflexivity bychom měli, že $\mathbf{P} = \{(a, a)\}$, symetrie i tranzitivita jsou zřejmé. V tomto případě si můžeme všimnout, že **P** má jedinou třídu ekvivalence, a to $\{a\}$, tj. X.

Vidíme tedy, že oba extrémní příklady jsou triviální, přičemž v prvním případě **P** ekvivalencí není a v druhém je. Představme si tedy, že $X = \{a_1, a_2, \ldots, a_{20}\}$ je množina žáků jisté třídy jisté základní školy. Může se stát, že žáci jsou rozděleni do několika *part* a v každé partě jsou všichni navzájem kamarádi a zároveň nikdo nekamarádí s nikým z žádné jiné party (připouštíme i jednoprvkové party). V takovém případě je snad jasné, že **P** je ekvivalence na X a příslušné třídy ekvivalence odpovídají jednotlivým partám. Třeba na Obrázku 2.13 vidíme schéma situace v případě, že **P** má na X šest tříd ekvivalence $P_1 = \{a_1, a_4, a_5, a_6, a_11, a_18, a_19\}$ atd. Ta samá relace se dá zakreslit také pomocí tabulky o 400 „okénkách“; pokud si na obě osy vyneseme jednotlivé body X ve vhodném pořadí „podle part“, budou třídy ekvivalence zřetelně rozpoznatelné i při tomto způsobu zobrazení.



Obrázek 2.13: Příklad relace **P** ve třídě s partami

△

2.26 Příklad. Zajímavá relace mezi body roviny $\mathbb{R}^2$ je „ležet na stejné přímce procházející počátkem“. Zkuste si rozmyslet, proč tato relace není relací ekvivalence a jak je potřeba upravit její nosnou množinu (tj. $\mathbb{R}^2$), aby se o ekvivalenci jednalo. △

2.4 Relace uspořádání

Nyní se o něco podrobněji podíváme na relace, které jsou buďto (a) reflexivní, slabě antisymetrické a tranzitivní (ostré uspořádání), nebo (b) silně antisymetrické a tranzitivní (ostrá uspořádání) a na některé související pojmy. Připomeňme, že uspořádání jsou buďto *lineární* (též: *úplná*), jestliže každé dva různé prvky jsou porovnatelné; v opačném případě se jedná o uspořádání *částečná*.

2.4.1 Příklady

2.27 Příklad. Základním příkladem, s nímž jsme všichni dobře obeznámeni už ze základní školy, je uspořádání na reálných číslech $(\mathbb{R}, \leqslant)$, resp. $(\mathbb{R}, <)$. Je známo, že libovolná dvě reálná čísla můžeme porovnat podle velikosti (tj. relace $\leqslant$, $<$ jsou trichotomické), což znamená, že obě tato uspořádání jsou lineární. Můžeme se také omezit na některé podmnožiny, je tedy jasné, jak chápat třeba uspořádání $(\mathbb{Z}, <)$ nebo $([0, 1], \leqslant)$ apod.

O něco hůře představitelná a méně známá mohou být mnohá uspořádání částečná, tedy nelineární. Můžeme kupříkladu X označit množinu všech lidí, co kdy žili (včetně stále žijících) a uspořádat je relací $\prec$ definovanou pro $a, b \in X$ tak, že $a \prec b$, pokud a je předek b (tj. b je potomek a).[32] Je jasné, že nelze toto uspořádání „vynést na přímku“, neboť není lineární: zdaleka ne každí dva lidé jsou v tomto uspořádání porovnatelní. Je zřejmé, že toto uspořádání úzce souvisí s rodokmeny, a jeho části jsou často zobrazovány pomocí tzv. rodinného stromu. Právě zobrazení pomocí podobných diagramů (tzv. Hasseových diagramů) je často vhodným způsobem, jak zachytit strukturu částečných uspořádání.

Viz též Příklad 2.10, kde **M** a **MR** jsou příklady uspořádání na množině $\{2, 4, 9\}$. △

Pro jednodušší a přesnější vyjadřování se nám bude hodit následující definice uspořádané množiny. Tato definice má pro nás hlavně formální význam, nejde o nic podstatného.

2.28 Definice. Nechť **R** je relace (ostrého nebo neostrého) uspořádání na množině X. Pak dvojici $(X, \mathbf{R})$ nazveme *uspořádanou množinou*. V případě, že uspořádání **R** je pouze částečné (tj. není lineární), můžeme dvojici $(X, \mathbf{R})$ nazvat *částečně uspořádanou množinou*.

Důležitým typem uspořádaných množin, se kterým budeme v dalším výkladu podstatným způsobem pracovat, je potenční množina uspořádána inkluzí. Definici potence následují některé základní příklady a níže se podíváme na zmíněné uspořádání.

2.29 Definice (Potenční množina)**.** Je-li X libovolná množina, pak symbolem $\mathcal{P}(X)$ značíme množinu všech podmnožin X, tj.

$$\mathcal{P}(X) = \{A\colon\ A \subseteq X\}.$$

Množinu $\mathcal{P}(X)$ nazýváme *potenční množinou* (množiny) X, případně *potencí* X.

Pojďme se pro začátek podívat na nějaké příklady.

2.30 Příklad (Hrátky s potencí)**.**

- $X = \{a, b\}$, kde $a \neq b$ jsou různé prvky. Pak $\mathcal{P}(X) = \big\{\emptyset, \{a\}, \{b\}, X\big\}$. Skutečně, prázdná množina je podmnožinou libovolné množiny. Pak má naše dvouprvková X dvě jednoprvkové podmnožiny, a to $\{a\}$ a $\{b\}$. Nakonec je samozřejmě sama sobě podmnožinou. Celkem tedy existují 4 podmnožiny, a ty jsou všechny uvedeny ve výčtu prvků $\mathcal{P}(X)$ výše.

[32] Sami si rozmyslete, že tato relace splňuje oba axiomy ostrého uspořádání.

- $\mathcal{P}(\emptyset) = \{\emptyset\}$. Tj. potence prázdné množiny má jeden prvek. Jinými slovy, prázdná množina má jedinou podmnožinu, a to sebe samu. Speciálně je tedy potence prázdné množiny neprázdná – pozor na to.

- $\mathcal{P}\big(\mathcal{P}(\emptyset)\big) = \mathcal{P}(\{\emptyset\}) = \big\{\emptyset, \{\emptyset\}\big\}$. Potenci můžeme chápat jako (unární) operaci, kterou můžeme aplikovat na kteroukoliv množinu, tedy i na potenční množinu (nějaké množiny, v tomto případě prázdné). Rozmyslete si pořádně, že uvedené rovnosti platí a pak se pokuste zapsat výčtem prvků $\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\emptyset))\big)$.[33] Dále si rozmyslete, že $\{\emptyset\} \neq \emptyset$, neboť první množina je neprázdná (má jeden prvek), zatímco druhá je prázdná. To ovšem znamená, že $\{\{\emptyset\}\} \neq \{\emptyset\}$ jsou dvě různé jednoprvkové množiny (právě jsme si totiž uvědomili, že jejich prvky, tj. $\{\emptyset\}$, resp. $\emptyset$, jsou různé).

- Kolik prvků má $\mathcal{P}\big(\{0, 1, 2, 3\}\big)$? Je záležitostí jednoduché kombinatoriky si rozmyslet, že má právě $16 = 2^4$ prvků. Skutečně, chci-li z daných 4 prvků (tj. $0, 1, 2, 3$) utvořit nějakou množinu, u každého z těchto prvků mohu učinit rozhodnutí, zda ho do množiny zařadím, či ne. Čtyřikrát po sobě musím učinit toto rozhodnutí, a je tedy $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ možností. Všimněte si, že když se pokaždé rozhodnu pro nezařazení prvku do utvářené množiny, skončím nakonec s prázdnou množinou; pokud se zcela naopak u každého prvku rozhodnu ho zařadit, dostanu celou množinu $\{0, 1, 2, 3\}$ (a kromě těchto uvedených existují ještě tři jednoprvkové a tři dvouprvkové podmnožiny).

- Kolik prvků má $\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))\big)$? A kolik jich má $\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))))\big)$?[34] $\triangle$

2.31 Příklad (Uspořádání potenční množiny)**.** Pojďme se nyní podívat ještě na jeden příklad potence, přičemž nyní budeme uvažovat všechny podmnožiny jisté tříprvkové množiny (počet prvků vlastně není důležitý, ale z didaktického pohledu se 3 jeví jako optimum): $\mathcal{X} = \mathcal{P}\big(\{a, b, c\}\big)$, kde a, b, c jsou nějaké navzájem různé objekty. Pro přehlednost můžeme (ale nepotřebujeme) označit $X = \{a, b, c\}$.[35] Pak tedy

$$\mathcal{X} = \mathcal{P}\big(\{a, b, c\}\big) = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\big\}.$$

[33] Řešení: $\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\emptyset))\big) = \big\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\big\}$.

[34] Řešení: První případ (se čtyřmi potencemi) odpovídá potenci čtyřprvkové množiny, tj. $2^4 = 16$ prvků. Druhý případ je tedy potencí 16-prvkové množiny, a obsahuje 2^{16} prvků. (Pokud znáte výsledek z hlavy, pravděpodobně studujete informatiku!)

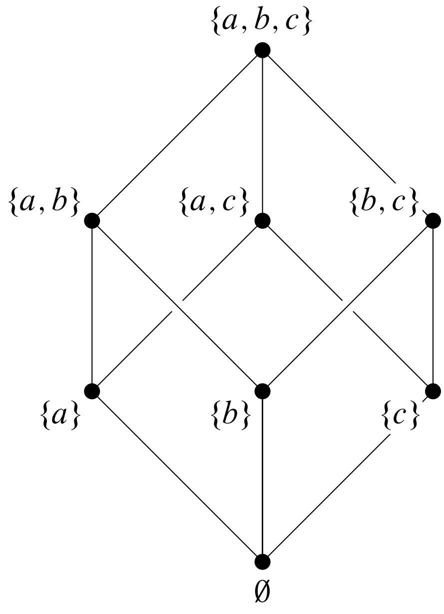
[35] V tomto případě pak dostaneme přehledné značení, při němž *základní objekty*, jmenovitě a, b a c, jsou značeny malými písmeny. *Množiny* těchto objektů jsou značeny velkými písmeny; např. X je množina všech základních objektů a dále můžeme psát kupříkladu $B = \{a, c\}$ a podobně. Konečně *množiny množin* základních objektů značíme kaligrafickými velkými písmeny, např. $\mathcal{X} = \mathcal{P}(X) = \mathcal{P}\big(\{a, b, c\}\big)$ je množina všech množin základních objektů a má, jak víme, 8 prvků; nebo můžeme psát třeba $\mathcal{D} = \{\emptyset, \{a\}, B, X\}$ – tato množina má 4 prvky – atd. Vidíme tedy docela přehlednou hierarchii objektů s nimiž v tomto příkladě pracujeme: (1) základní objekty; (2) množiny základních objektů; (3) množiny množin základních objektů; a tato hierarchie je zachycena ve stylu značení. Nečekejte ale, že značení vždy bude takto přehledně rozvrstvené, někdy je prostě potřeba dávat pozor, co je co.

Máme tedy 8-prvkovou množinu $\mathcal{X}$ a protože ony prvky nejsou ledajaké, ale úzce spolu souvisí, jsouce podmmnožinami dané tříprvkové množiny $X = \{a, b, c\}$, lze na $\mathcal{X}$ najít zcela přirozené jisté uspořádání, a to uspořádání inkluzí: Jsou-li A, B libovolné prvky $\mathcal{X} = \mathcal{P}(X)$, pak tedy $A, B \subseteq X$. To je jasné, neboť prvky potence jisté dané množiny jsou z definice podmnožinami této dané množiny. Má tedy smysl ptát se, platí-li $A \subseteq B$, případně $B \subseteq A$, případně nic z toho. Tak například pokud $A = \{a\}$ a $B = \{a, c\}$ (obě tyto množiny jsou skutečně prvky $\mathcal{X}$), pak platí $A \subseteq B$ a $B \nsubseteq A$, a tak podobně.

Uvažujme tedy strukturu $(\mathcal{X}, \subseteq)$; nyní si rozmyslíme, že se jedná o uspořádanou množinu, neboli že relace $\subseteq$ je uspořádání na $\mathcal{X}$. Je zřejmé, že relace je reflexivní, a tedy nemáme jinou možnost než ověřovat axiomy neostrého uspořádání. Zbývá ověřit slabou antisymetrii a tranzitivitu. Velmi vám na tomto místě doporučuji to vyzkoušet provést samostatně; pokud to nevidíte hned, bude to pro vás velmi snadné, a přitom poučné. Následující odstavec obsahuje návod.

Návod: Napište si definici slabé antisymetrie relace **R** a pak do ní za „**R**“ dosaďte „$\subseteq$“. Nyní si stačí uvědomit, že výsledný výrok v podstatě triviálně platí (a je intuitivně zcela zřejmý). Tytéž kroky proveďte i pro tranzitivitu, a budete s důkazem hotovi.

Víme tedy, že $\left(\mathcal{P}(\{a, b, c\}), \subseteq\right)$ je uspořádaná množina, resp. že relace $\subseteq$ je uspořádání na $\mathcal{X}$. Je ovšem zřejmé, že ne každé dva prvky $\mathcal{X}$ jsou v tomto uspořádání porovnatelné. Skutečně, třeba prvky $\{a\}, \{b\} \in \mathcal{X}$ porovnatelné nejsou: máme totiž $\{a\} \nsubseteq \{b\}$ a zároveň $\{b\} \nsubseteq \{a\}$. To znamená, že uspořádání není lineární, je částečné. Pohodlný způsob, jak si takové uspořádání představit (pochopit jeho strukturu) je pomocí tzv. *Hasseova diagramu* – viz obrázek.



Obrázek 2.14: Hasseův diagram $(\mathcal{X}, \subseteq)$.

$\triangle$

2.32 Cvičení. Množinu $X = \{1, 2, 3, 4, 5, 6, 12, 15, 60\}$ uspořádáme standardní relací dělitelnosti; raději ji připomenu: Pro dvě celá čísla k, l říkáme, že k *dělí* l a píšeme $k|l$, jestliže existuje celé číslo q takové, že $l = q \cdot k$. Je jasné, že $|$ je binární relace na $\mathbb{Z}$, my ji ovšem budeme uvažovat také na vybrané podmnožině X (tj. striktně vzato budeme pracovat s relací $| \cap X \times X$).

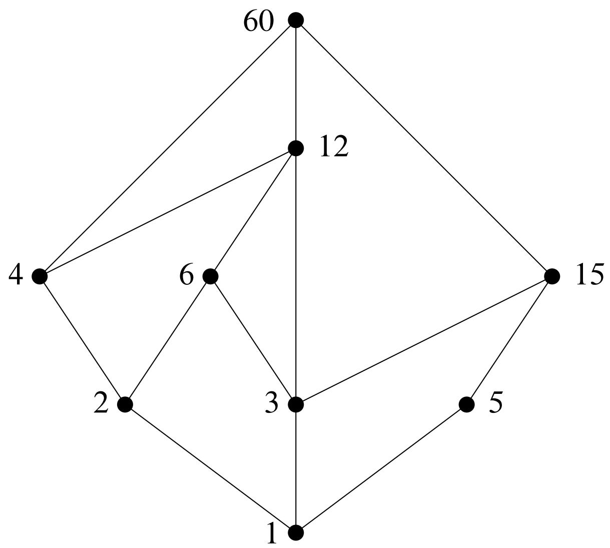
(i) Dokažte, že $(\mathbb{Z}, |)$ je uspořádaná množina, tj. že $|$ je uspořádání na $\mathbb{Z}$. Totéž si uvědomte i pro $(X, |)$.

(ii) Samostatně nakreslete Hasseův diagram $(X, |)$. (Viz obrázek níže.)

(iii) Jak se diagram změní, přidáme-li k X další prvky 7, 8, 9, 20, 25? Obrázek doplňte.

(iv) *Řetězec* v nějaké uspořádané množině $(A, \leqslant)$ je libovolná podmnožina $R \subseteq A$ taková, že $(R, \leqslant)$ je lineárně uspořádaná. Najděte nějaký řetězec maximální možné délky v $(X, |)$.

(v) *Antiřetězcem* v uspořádané množině rozumíme libovolnou podmnožinu takovou, že žádné dva její prvky nejsou v tom uspořádání porovnatelné. Najděte tři různé antiřetězce o třech prvcích v $(X, |)$.



Obrázek 2.15: Hasseův diagram uspořádání $\big(\{1, 2, 3, 4, 5, 6, 12, 15, 60\}, |\big)$.

Příklad uspořádání na $\mathbb{C}$

Na závěr tohoto oddílu se pojďme podívat ještě na jedno zajímavé uspořádání, tentokrát na nekonečné množině $\mathbb{C}$ všech komplexních čísel (tj. vlastně na $\mathbb{R}^2$). Jak víme, komplexní čísla nemají přirozené uspořádání podobné lineárnímu uspořádání na číslech reálných. Můžeme je sice porovnávat podle velikosti (tj. podle vzdálenosti od 0), to ale nemusí být uspořádání ve smyslu Definice 2.17. Pojďme se nejprve podívat, kdy srovnání podle velikosti nedává uspořádání. Definujme dvě relace na $\mathbb{C}$ následovně: pro každá čísla $a, b \in \mathbb{C}$ pišme:

- $a \lhd b$, právě když $|a| < |b|$.
- $a \blacktriangleleft b$, právě když $|a| \leqslant |b|$;

Tím jsou dány dvě relace na $\mathbb{C}$, tj. $\lhd \subseteq \mathbb{C} \times \mathbb{C}$ a také $\blacktriangleleft \subseteq \mathbb{C} \times \mathbb{C}$. Jde o uspořádání?

2.33 Pozorování. *Relace $\blacktriangleleft$ není uspořádání (ostré ani neostré) na $\mathbb{C}$.*

Důkaz. Zjevně nejde o ostré uspořádání, protože například pro $x, y = 1$ máme $x \blacktriangleleft y$ a zároveň $y \blacktriangleleft x$, což vyvrací silnou antisymetrii. Uvědomte si, že stačí dát jediný protipříklad; a pochopitelně bychom mohli dát i protipříklad, v němž $x \neq y$, kupříkladu $x = 1$ a $y = \mathrm{i}$ (imaginární jednotka), ale není to potřeba.

Zbývá zpozorovat, že relace $\blacktriangleleft$ není ani neostré uspořádání $\mathbb{C}$. K tomu by totiž musela být slabě antisymetrická. Ovšem právě příklad dvojice čísel 1 a i dokládá porušení této podmínky: Platí totiž $1 \blacktriangleleft \mathrm{i} \wedge \mathrm{i} \blacktriangleleft 1$, a přitom $1 \neq \mathrm{i}$. Slabá antisymetrie tedy neplatí, a relace není ani neostrým uspořádáním. □

2.34 Pozorování. *Relace $\lhd$ je ostré uspořádání na $\mathbb{C}$.*

Důkaz. Stačí ověřit oba axiomy ostrého uspořádání; začněme silnou antisymetrií; vezměme tedy dva prvky $x, y \in \mathbb{C}$ takové, že $x \lhd y$. To podle definice relace $\lhd$ znamená, že $|x| < |y|$, neboli že y je od počátku dál než x. Tím pádem ovšem samozřejmě není současně k počátku blíž, tj. neplatí $|y| < |x|$, tj. neplatí $y \lhd x$. Dokázali jsme silnou antisymetrii.

Zbývá prokázat tranzitivitu $\lhd$. Mějme tedy $x, y, z \in \mathbb{C}$ splňující $x \blacktriangleleft y$ a zároveň $y \blacktriangleleft z$. Podle definice $\blacktriangleleft$ to znamená, že $|x| < |y|$ a $|y| < |z|$. Ovšem to jsou dvě obyčejné nerovnosti mezi reálnými čísly a my víme, že $(\mathbb{R}, <)$ je uspořádání, je tedy tranzitivní, a ty dvě nerovnosti tak společně implikují $|x| < |z|$, neboli $x \blacktriangleleft z$. Tím je dokázána tranzitivita $\blacktriangleleft$, a jsme hotovi. □

Viděli jsme, že u „neostré verze“ $\blacktriangleleft$ selže slabá antisymetrie, zatímco $\lhd$ skutečně je ostré uspořádání. Znamená to, že pro $\lhd$ neexistuje příslušné neostré uspořádání? Nikoliv, jen je potřeba ho „vyrobit“ přímo z $\lhd$ takto: Pro $a, b \in \mathbb{C}$ definujeme

- $a \trianglelefteq b$, právě když $a \lhd b$ nebo $a = b$.

2.35 Cvičení. (i) S využitím už dokázaného faktu, že $(\mathbb{C}, \lhd)$ je ostré uspořádání, dokažte, že $(\mathbb{C}, \trianglelefteq)$ je neostré uspořádání.

(ii) Všimněte si, že libovolná polopřímka vycházející z počátku je řetězec (viz Cvičení 2.32) v $(\mathbb{C}, \lhd)$. Najděte další nekonečné řetězce, které nejsou obsažené v žádné polopřímce.

(iii) Jak vypadají antiřetězce?

2.4.2 Maximum, maximální prvek, supremum

V této části se podíváme na důležité pojmy související s uspořádáním; kromě těch jmenovaných v nadpisu se podíváme ještě na analogické pojmy „z druhé strany“, jmenovitě minimum, minimální prvek a infimum – a další. Kromě toho, že jsou znalosti těchto věcí důležité pro matematiku jako celek, brzy je využijeme bezprostředně v teorii množin pro důkaz jedné z jejích klíčových vět, tzv. Cantorovy-Bernsteinovy věty.

2.36 Úmluva (Neostré a ostré uspořádání)**.** V obecném kontextu budeme symbolem „$\leqslant$“ značit vždy *neostré* uspořádání. Není-li explicitně řečeno jinak, budeme v tom případě symbolem „$<$“ rozumět příslušnou ostrou relaci, která je definována ekvivalencí $x < y \leftrightarrow (x \leqslant y \wedge x \neq y)$.

Podobně, je-li dána relace $<$ ostrého uspořádání (na nějaké množině), pak definujeme relaci $\leqslant$ jako příslušné neostré uspořádání, neboli $x \leqslant y \leftrightarrow (x < y \vee x = y)$.

Kromě toho asi nepřekvapí, že dále definujeme relace $>$ a $\geqslant$ jednoduše ekvivalencemi $x > y \leftrightarrow y < x$ a podobně $x \geqslant y \leftrightarrow y \leqslant x$.

Kdykoliv je tedy dána relace uspořádání označená jedním ze symbolů „$<, \leqslant, >, \geqslant$“, budeme automaticky oprávněni používat i zbylé tři symboly pro příslušné přirozeně související relace tak, jak jsme tomu byli zvyklí dosud v kontextu $(\mathbb{R}, \leqslant)$.

2.37 Definice. Buď $(X, \leqslant)$ uspořádaná množina, $A \subseteq X$, $a \in X$. Řekneme, že a je:

- *horní závora* (množiny) A, jestliže $\forall x \in A\colon x \leqslant a$;
- *maximum* A, jestliže $a \in A$ a zároveň a je horní závora A;
- *maximální prvek* A, jestliže $a \in A$ a zároveň $\forall x \in A\colon \neg(a < x)$.
- *supremum* A, jestliže a je horní závora A a zároveň

$$\forall h \in X : h \text{ je horní závora } A \rightarrow a \leqslant h.$$

Existují i jiné názvy pro tyto pojmy, ke kolizi označení však nedochází: Pro horní závoru se občas používá také termín *majoranta*. Maximum je jinak také *největší prvek*. Pro pojmy maximálního prvku a suprema nejsou ustálená alternativní označení. Píšeme $a = \max A$ (resp. $a = \sup A$), pokud a je maximum (resp. supremum) množiny A. Chceme-li zdůraznit, že se jedná o maximum (resp. supremum) vzhledem k uspořádání $\leqslant$, píšeme také $\max_{\leqslant} A$ (resp. $\sup_{\leqslant} A$).

2.38 Poznámka.

(a) Není těžké si (třeba na příkladu $(\mathbb{R}, \leqslant)$) všimnout, že množina (třeba $[0, 1] \subseteq \mathbb{R}$) může mít více horních závor. Skutečně, libovolné $a \geqslant 1$ je v $\mathbb{R}$ horní závorou intervalu $[0, 1]$.

(b) Obecně může existovat nejvýše jedno maximum. Skutečně, je-li $(X, \leqslant)$ uspořádaná množina, $A \subseteq X$ a $a, b \in A$ jsou maxima A, pak z definice maxima a plyne, že $b \leqslant a$ a z definice maxima b zase $a \leqslant b$. Slabá antisymetrie neostrého uspořádání dává $a = b$, takže maximum je opravdu jen jedno. Zároveň je snad jasné, že maximum nemusí vždy existovat, třeba interval $(0, 1) \subseteq \mathbb{R}$ maximum nemá.

(c) Definice suprema se může zdát poněkud složitá, lze ji ale jednoduše a výstižně vyjádřit slovy: $a \in X$ je supremum A, jestliže a je (v rámci X) nejmenší horní závora A; jinými slovy, pokud a je minimem množiny horních závor.[36]

(d) Množina A může mít více maximálních prvků: Stačí se podívat na Příklad 2.31, kde $\mathcal{X} = \mathcal{P}\big(\{a, b, c\}\big)$ uspořádáváme relací $\subseteq$. Uvažujme nyní množinu $A = \mathcal{X} \setminus \big\{\{a, b, c\}\big\}$, tj. množinu A dostaneme odebráním největšího prvku z $\mathcal{X}$. Na Obrázku 2.14 si nyní odmyslete nejvyšší vrchol, tj. ten, který odpovídá prvku $\{a, b, c\}$, a uvidíte množinu A. O úroveň níž zůstanou tři vrcholy odpovídající různým dvouprvkovým množinám. Každá z nich je maximálním prvkem A: třeba $\{a, b\}$ je maximálním prvkem, protože (jak je z obrázku zřejmé) nad ní v množině A není už nic ostře většího. Stejný argument platí i pro zbývající dvě dvouprvkové množiny. Máme tedy tři různé (z logiky věci navzájem neporovnatelné) maximální prvky množiny A.

Rozmysleli jsme si, že maximum dané množiny je jednoznačně určeno. Analogickou úvahou lze zjistit, že stejně tak je jednoznačně určeno minimum (existuje-li). Dává proto smysl používat značení „max A" pro maximum množiny A a „min A" pro její minimum, neboť tyto symboly mají (jak musí) jednoznačně určený význam.

To dále znamená, že i značení „sup A" (resp. „inf A") pro supremum (resp. infimum) A je rozumné, neboť třeba supremum, jsouc minimem množiny všech horních závor A, je jednoznačně určeno.[37] Analogický argument dokazuje jednoznačnost infima A.

2.39 Cvičení. Zkuste si samostatně napsat definice analogických pojmů „zdola": Je-li $(X, \leqslant)$ uspořádaná množina, $A \subseteq X$, $a \in X$, pak definujte *dolní závoru* A, *minimum* A, *minimální prvek* A a *infimum* A. Porovnejte své řešení s následující definicí.

2.40 Definice. Buď $(X, \leqslant)$ uspořádaná množina, $A \subseteq X$, $a \in X$. Řekneme, že a je:

- *dolní závora* (množiny) A, jestliže $\forall x \in A\colon a \leqslant x$;
- *minimum* A, jestliže $a \in A$ a zároveň a je dolní závora A;
- *minimální prvek* A, jestliže $a \in A$ a zároveň $\forall x \in A\colon \neg(x < a)$.

[36] Zde ovšem používám dosud nedefinovaný pojem minima – definici najdete níže a můžete si sami rozmyslet, že všechny definice lze napsat v takovém pořadí, aby se nejednalo o definici kruhem.

[37] Dodávám, že jednoznačně určena je i množina všech horních závor A, což je ovšem samozřejmé.

- *infimum* A, jestliže a je dolní závora A a zároveň

$$\forall d \in X : d \text{ je dolní závora } A \to d \leqslant a.$$

Dolní závoru nazýváme též *minorantou*, minimum je jinak také *nejmenší prvek*. Píšeme $a = \min A$ (resp. $a = \inf A$), pokud a je minimum (resp. infimum) množiny A.

2.41 Poznámka. Nyní už je snad zřejmé, že pro podmnožinu A uspořádané množiny X je

$$\inf A = \max\{d \in X : d \text{ je dolní závora } A\} \quad \text{a} \quad \sup A = \min\{h \in X : h \text{ je horní závora } A\}.$$

Důležitější je poznamenat, že oba pojmy (tedy jak infimum, tak supremum) jsou jednoznačně určené, *pokud existují*. Existovat ale nemusí!

Asi si vzpomenete, že v matematické analýze prvního semestru se probírá tzv. Věta o supremu, která říká, že každá neprázdná shora omezená množina reálných čísel má supremum (a podobně pro infimum). Obohatíme-li reálnou osu o $\pm\infty$, tj. $\mathbb{R}^* = \mathbb{R} \cup \{-\infty, +\infty\}$, můžeme dokonce prohlásit, že libovolná podmnožina $\mathbb{R}$ má infimum i supremum (v $\mathbb{R}^*$). To je ovšem poměrně speciální vlastnost reálných čísel (související s tzv. jejich úplností), kterou například racionální čísla nesdílí. V obecném kontextu tedy není zaručena existence infim a suprem libovolných množin.

S tímto faktem souvisí Definice 3.3: v těch speciálních případech, kdy existence infim a suprem zaručena je, hovoříme o tzv. *úplném svazu*.

2.42 Cvičení. Buď $(X, \leqslant)$ uspořádaná množina, $A \subseteq X$. Dokažte následující výroky.

(i) Je $\sup A = \max A$, má-li pravá strana smysl.[38] (Podobně pro $\inf A$.)

(ii) Pokud $\inf A \in A$, pak $\inf A = \max A$.[39] (Podobně pro $\sup A$.)

(iii) Maximum je vždy zároveň maximální prvek a minimum je vždy minimální prvek.

(iv) Dokažte, že pokud má množina A aspoň dva různé maximální prvky, pak nemá maximum. Zároveň si uvědomte na vhodném příkladu, že opačná implikace neplatí. (Podobně pro minimum.)

Další příklad uspořádání na $\mathbb{C}$

Jedno zajímavé uspořádání (označené $\lhd$ a $\unlhd$) na $\mathbb{C}$ jsme už probrali výše. Nyní se podíváme na jinou verzi. Definujeme relaci $\lhd$ na $\mathbb{C}$ ekvivalencí pro $a, b \in \mathbb{C}$

$$a \lhd b \iff \exists r \in [0, 1) : a = r \cdot b.$$

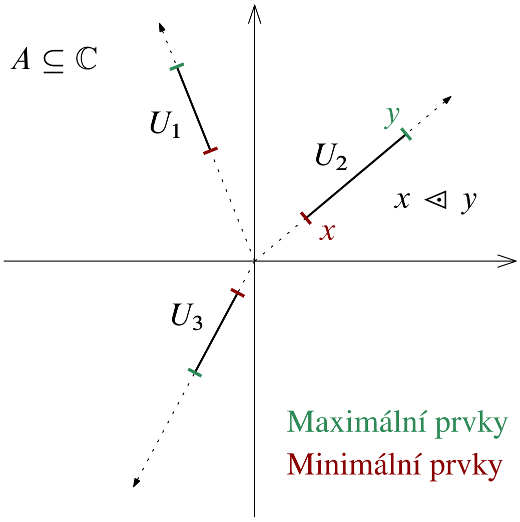
[38] Jinými slovy, existuje-li maximum, jde současně o supremum.
[39] Jinými slovy, pokud infimum je prvek množiny, je to současně její minimum.

Dále budeme psát $a \trianglelefteq b$, kdykoliv $(a \lhd b) \vee (a = b)$. Řečeno slovy, $a \lhd b$ platí, právě když a, b jsou na stejné polopřímce vycházející z počátku a bod a je počátku ostře blíže než b, neboli $|a| < |b|$. Tj. vidíme, že

$$a \lhd b \iff (a \lhd b) \wedge (a, b \text{ jsou na společné polopřímce z počátku}),$$

odkud je mimochodem snadno vidět, že relace $\lhd, \lhd \subseteq \mathbb{C} \times \mathbb{C}$ splňují $\lhd \subseteq \lhd$, protože relace $\lhd$ je více restriktivní, připouští méně dvojic. Třeba $\frac{1}{2} \lhd \mathrm{i}$ (kde i je imaginární jednotka), ale tato čísla nejsou porovnatelná v relaci $\lhd$, protože nejsou na společné polopřímce vycházející z počátku.

Nyní se podrobněji podíváme na vlastnosti $\lhd$. V první řadě si uvědomte, že se jedná o (ostré) uspořádání, neboli že relace je silně antisymetrická a tranzitivní.



Obrázek 2.16: Uspořádání $\lhd$ na množině $A = U_1 \cup U_2 \cup U_3$

2.43 Pozorování. *Relace $\lhd$ je ostré uspořádání na $\mathbb{C}$. Relace $\trianglelefteq$ je neostré uspořádání na $\mathbb{C}$.*

Důkaz. Silná antisymetrie $\lhd$ je takřka triviální – rozmyslete. Tranzitivitu můžeme ověřit třeba přímo z definice takto: Nechť $a, b, c \in \mathbb{C}$ a platí $a \lhd b$, resp. $b \lhd c$. To podle definice znamená, že existují čísla $r, s \in [0, 1)$ tak, že $a = r \cdot b$ a $b = s \cdot c$. Pak ale $a = rs \cdot c$, přičemž součin $rs \in [0, 1)$, takže skutečně $a \lhd c$. Máme tedy ostré uspořádání $\lhd$ a jemu příslušnou neostrou verzi $\trianglelefteq$ (že jde o neostré uspořádání, by vám už mělo být jasné). □

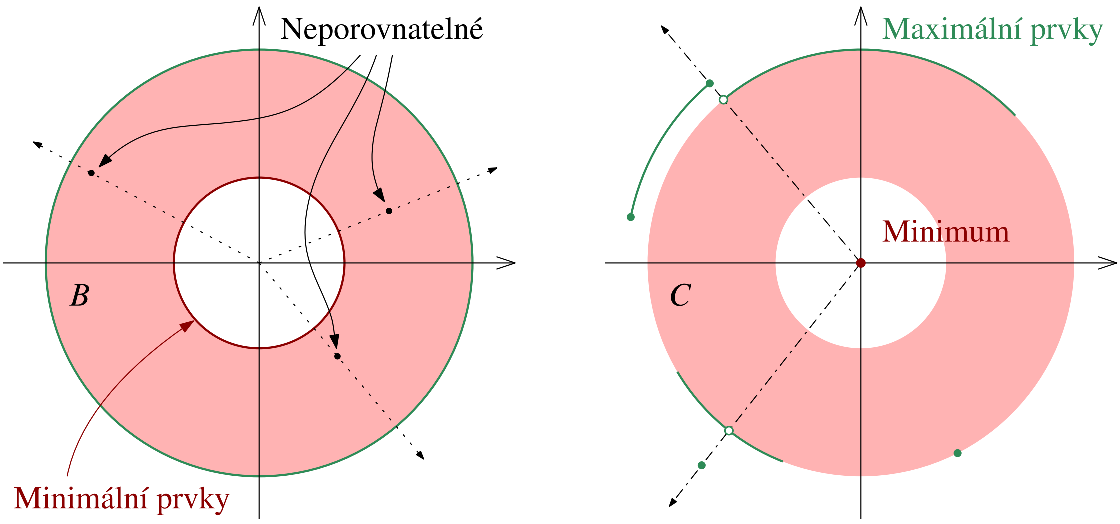
Obrázek 2.16 ilustruje strukturu uspořádání $\lhd$ na podmnožině $A \subseteq \mathbb{C}$, která je dána jako sjednocení tří vyobrazených úseček, tj. $A = U_1 \cup U_2 \cup U_3$. Na kterékoliv z těchto úseček uspořádání $\lhd$ funguje lineárně: každé dva body jsou porovnatelné, přičemž ty, které jsou blíže k počátku, jsou „menší“.[40] Naproti tomu žádné dva body na různých úsečkách, porovnatelné

[40] Je to tak díky tomu, že každá z těch tří úseček leží na nějaké polopřímce vycházející z počátku.

nejsou. Z toho je vidět, že množina A nemá maximum (tj. největší prvek), neboť to by muselo být větší než libovolný jiný prvek A, takže speciálně by muselo být se všemi prvky A porovnatelné; my ovšem víme, že žádný prvek A není porovnatelný se všemi ostatními. Ze stejného důvodu nemá množina A ani minimum (tj. nejmenší prvek): muselo by být porovnatelné se všemi prvky A.

Můžeme si ale všimnout, že množina A má tři maximální prvky, tedy prvky, „nad nimiž už v A nic není“: na každé úsečce je to ten bod, který je nejvzdálenější od počátku, tj. nutně jeden z krajních bodů. Zbývající krajní body jsou naopak minimální prvky množiny A, neboť „pod nimi už v množině A nic nenajdeme“. Celkem tedy existují tři maximální a tři minimální prvky množiny A.

Pokud bychom z množiny A odebrali všech šest krajních bodů úseček U_1, U_2, U_3 (a zůstaly by tedy „otevřené“ úsečky bez krajních bodů), výsledná množina by neměla žádné maximální ani minimální prvky. Každou úsečku bez krajních bodů s uspořádáním $\lhd$ si totiž můžeme představit jako otevřený interval $(a, b) \subseteq \mathbb{R}$, který ovšem zjevně nemá minimum ani maximum.



Obrázek 2.17: Vlevo mezikruží s hranicí; vpravo otevřené mezikruží + něco navíc

Podíváme-li se na Obrázek 2.17 vlevo, uvidíme mezikruží se zelenou vnější hraniční kružnicí a červenou vnitřní kružnicí; tuto množinu (včetně hranice) označíme B. Můžeme si nyní všimnout, že všechny body zelené kružnice jsou v B maximální a všechny body červené kružnice jsou v B minimální. Naznačené tři černé body na různých polopřímkách jsou vzájemně neporovnatelné, a tvoří tedy tříprvkový *antiřetězec* (množinu po dvou neporovnatelných prvků). Ve skutečnosti je jasné, že například žádné dva body zelené (vnější) kružnice nejsou porovnatelné, a tedy v B snadno najdeme nekonečné antiřetězce.

2.44 Cvičení. (i) Najděte nekonečné řetězce v B, které nejsou obsaženy v žádné kružnici se středem 0.

(ii) Jak vypadají maximální řetězce (lineárně uspořádané podmnožiny) v B?

(iii) Na Obrázku 2.17 vpravo je vyobrazena množina $C \subseteq \mathbb{C}$, která je sjednocením otevřeného mezikruží (tj. bez hraničních kružnic), zelené množiny a počátku (červený puntík). Rozmyslete si z definice, že $0 = \min C$ a také $0 = \inf C$. Je 0 minimálním prvkem C?

(iv) Rozmyslete si, že množina zelených bodů sestává výhradně z maximálních prvků C. Dále ukažte některé body C, které nad sebou nemají žádný maximální prvek.

2.5 Funkce

V řadě matematických disciplín je zvykem rozlišovat mezi pojmy „funkce“ a „zobrazení“, přičemž funkce je obvykle zobrazení s hodnotami v $\mathbb{R}$ nebo $\mathbb{C}$. V teorii množin tomu tak obvykle není, je naopak zvykem tyto výrazy považovat za synonyma se stejným významem, jako má v běžné terminologii slovo „zobrazení“. Funkce, resp. zobrazení, pro nás tedy není nic jiného než relace splňující jistou podmínku:

2.45 Definice (funkce)**.** Mějme relaci $\mathbf{R} \subseteq A \times B$. Řekneme, že $\mathbf{R}$ je:

- *funkce* (též *zobrazení*) z A do B, jestliže platí

$$\forall x \in A\ \forall y, y' \in B\colon x\mathbf{R}y \wedge x\mathbf{R}y' \longrightarrow y = y'; \tag{2.5}$$

- *prostá*, jestliže platí

$$\forall y \in B\ \forall x, x' \in A\colon x\mathbf{R}y \wedge x'\mathbf{R}y \longrightarrow x = x'; \tag{2.6}$$

- *na* B (též *surjektivní*[41]) , jestliže $\operatorname{rng}(\mathbf{R}) = B$, tj. jestliže

$$\forall y \in B\ \exists x \in A\colon x\mathbf{R}y.$$

2.46 Poznámka (Značení hodnot funkce)**.** Smyslem definice funkce je zařídit, aby s každým daným $x \in A$ byl v relaci nejvýše jeden prvek $y \in B$. Pokud pro dané x takové y existuje, je podle této definice jednoznačně určené, a dává tedy dobrý smysl toto y nazývat, jak jsme zvyklí, *hodnotou* funkce (v bodě x). Značíme-li onu funkci třeba „f“, jsme zvyklí její hodnotu příslušnou bodu x značit „$f(x)$“. Protože tato hodnota y je určena jednoznačně, je tedy $f(x) = y$, a značení dává dobrý smysl.

[41] Lze říci i „$\mathbf{R}$ je na“ bez upřesnění, na *kterou* množinu (v našem případě je to B) $\mathbf{R}$ je; v tomto smyslu tedy chápeme slova „surjektivní“ a „na“ jako přídavná jména a synonyma. Problém ovšem je, že informace o množině B, vzhledem k níž je funkce surjektivní, v tomto vyjádření není obsažena. Kupříkladu se podívejme na funkci $\sin\colon \mathbb{R} \to \mathbb{R}$: je jasné, že není *na*, neboť $\operatorname{rng}(\sin) = [-1, 1]$. Na druhou stranu je ale zcela správné říci, že funkce sin je *na* $[-1, 1]$.

Aby bylo co nejjasnější, že smysluplnost značení typu „$y = f(x)$“ vyplývá z jednoznačnosti hodnot, představme si relaci $\mathbf{f}$,[42] která má v jistém bodě dvě různé „hodnoty“ y_1, y_2, tj. přesně řečeno, platí $x\mathbf{f}y_1$ a zároveň $x\mathbf{f}y_2$. Kdybychom se v této situaci domáhali práva používat pro tyto „hodnoty“ funkční značení, tedy $\mathbf{f}(x) = y_1$, resp. $\mathbf{f}(x) = y_2$, ocitli bychom se ihned v potížích, neboť bychom museli uznat $y_1 = \mathbf{f}(x) = y_2$, odkud (vzhledem k tranzitivitě identity čili rovnosti) $y_1 = y_2$, což je ovšem v rozporu s předpokladem $y_1 \neq y_2$. Ještě jinak řečeno, symbol $\mathbf{f}(x)$ by měl nejméně dvě možné interpretace (zastupuje y_1, nebo y_2?), přičemž by nebylo jasné, které z nich bychom měli dát přednost.

Předchozí odstavec snad jasně dokládá, že aby značení typu $f(x) = y$ fungovalo, musí být hodnoty f jednoznačně určené, tj. musí být splněno (2.5), tj. f musí být funkce.

2.47 Značení. Pro funkce obvykle volíme jiné znaky než pro obecné relace, například f, g, F, φ, Φ apod. Také definiční obor a obor hodnot se u funkcí často značí jinými symboly než u obecných relací, například $\mathbb{D}_f = \mathbb{D}(f) = \mathrm{dom}(f)$, $\mathbb{H}_f = \mathbb{H}(f) = \mathrm{rng}(f)$.

Je-li f funkce a $\mathrm{dom}(f) = A$, hovoříme též o *funkci A do B*.[43]

Pokud f je funkce A do B (tedy $\mathrm{dom}(f) = A$), píšeme $f\colon A \to B$. Je důležité mít na paměti, že tento zápis obsahuje informaci, že f je definovaná na *celé* množině A.

V dalším se budeme držet standardního značení a pro relace $f \subseteq A \times B$, které splňují definici funkce (2.5), budeme místo „xfy“ psát „$y = f(x)$“.

2.48 Poznámka (O definicích funkce a prostoty)**.** Porovnejme formule (2.5) a (2.6), které definují funkci a prostou relaci; podobnost mezi nimi je patrná na první pohled. Podíváme-li se pozorně, vidíme, že při přechodu od jedné k druhé dojde pouze k záměně rolí obou proměnných (tj. složek uspořádaných dvojic, z nichž se relace skládá). Řečeno slovy, definice funkce požaduje, aby ke každému $x \in A$ existovalo nejvýše jedno $y \in B$, a definice prostoty zase žádá, aby ke každému $y \in B$ existovalo nejvýše jedno x tak, že (v obou případech) $x\mathbf{R}y$.

Nyní se znovu podívejme na definici inverzní relace (viz též 2.3.1):

$$\mathbf{R}^{-1} = \big\{(x, y) \in B \times A\colon\ (y, x) \in \mathbf{R}\big\}.$$

Tato jednoduchá definice vlastně pouze „prohodí proměnné“ – tak z $\mathbf{R}$ vznikne $\mathbf{R}^{-1}$. Co bylo původně y, je nyní x a naopak. Doufám, že v tomto světle (a ve světle Obrázku 2.18) není překvapivé, že platí:

$$\mathbf{R} \text{ je prostá} \quad\longleftrightarrow\quad \mathbf{R}^{-1} \text{ je funkce.} \tag{2.7}$$

Dodejme, že „být inverzní relací“ se dá chápat jako *vzájemný* vztah relací $\mathbf{R}$ a $\mathbf{R}^{-1}$ v tom smyslu, že také $\mathbf{R}$ je inverzní relací k $\mathbf{R}^{-1}$. Přesně vyjádřeno tím mám na mysli prostě rovnost $\big(\mathbf{R}^{-1}\big)^{-1} = \mathbf{R}$. (Že toto je pravda je zřejmé: „dvojím prohozením úloh x a y“ se totiž vrátíme do výchozího stavu.) Díky tomu k ekvivalenci (2.7) už vlastně není potřeba dodávat ještě její

[42] Nebudeme ji nazývat funkcí, neboť nesplňuje definici.

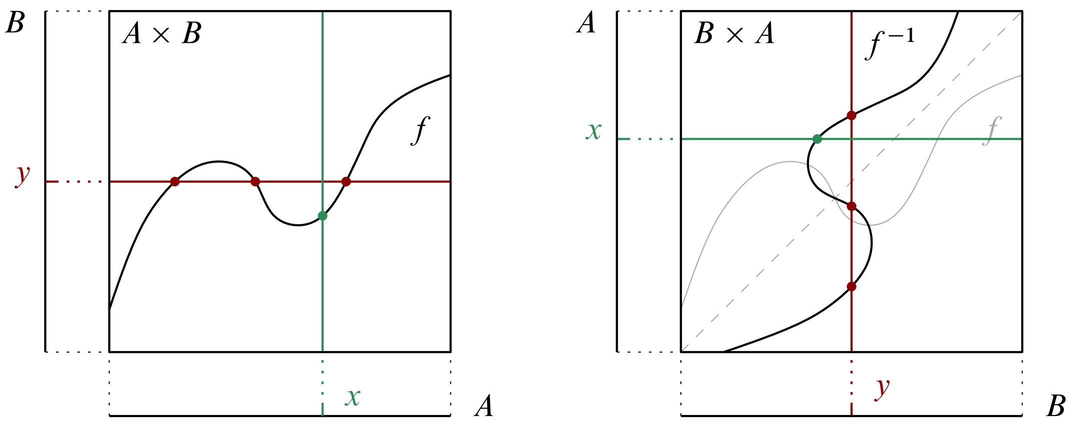
[43] Tj. bez předložky „z“ před „A“.

duální verzi, tj. ekvivalenci:

$$\mathbf{R} \text{ je funkce} \quad \longleftrightarrow \quad \mathbf{R}^{-1} \text{ je prostá.} \tag{2.8}$$

neboť ta v důsledku nese tutéž informaci.

Je určitě dobré si rozmyslet, proč přesně to tak je. Bezprostředním důsledkem (2.7) je ekvivalence: $\mathbf{R}^{-1}$ je prostá, právě když $(\mathbf{R}^{-1})^{-1}$ je funkce. (Stačí dosadit $\mathbf{R}^{-1}$ za $\mathbf{R}$.) Ale $(\mathbf{R}^{-1})^{-1} = \mathbf{R}$, takže dostáváme (2.8). Zcela stejným postupem lze odvodit také formuli (2.7) z formule (2.8). Jedna lze (navíc triviálně) odvodit z druhé, takže obě formule opravdu říkají totéž.



Obrázek 2.18: Vlevo: funkce není prostá; vpravo: inverzní relace je „prostá“, ale není to funkce.

2.49 Poznámka („Funkce a její graf jedno jsou“). (a) Funkce je definována jako speciální typ relace, jde tedy o podmnožinu kartézského součinu výchozí a cílové množiny (výše je to $A \times B$). Máme-li tedy kupříkladu nějakou funkci f $\mathbb{R}$ do $\mathbb{R}$, tj. $f : \mathbb{R} \to \mathbb{R}$, pak f není „pravidlo“ nebo „vzorec“ podle nějž z $x \in \mathbb{R}$ stanovíme příslušnou hodnotu $f(x)$. Tento pohled na pojem funkce je omezující (a nejasně definovaný) a my jsme ho v Definici 2.45 odmítli; místo toho takovouto funkci f chápeme jako jistou relaci, tedy $f \subseteq \mathbb{R} \times \mathbb{R}$. Funkce f je tak prostě množina bodů v rovině $\mathbb{R} \times \mathbb{R}$.

(b) Pokud „funkci“ chápeme jako nějaký „vzorec“, pak její graf, tj. jistá množina bodů, je objekt jiného typu než funkce sama,[44] byť má se samotnou funkcí úzkou souvislost. Při tomto chápání pojmu funkce bychom tak měli $f \neq \operatorname{graf} f$. Z předchozí poznámky ale vyplývá, že po přijetí naší definice funkce už nedává smysl rozlišovat mezi funkcí a jejím grafem. Mějte tedy na paměti, že toto rozlišení sice může někdy přidat na názornosti, striktně vzato je ale zbytečné.

(c) Pro úplnost si představme, jak by musela vypadat definice grafu funkce, pokud bychom se tento pojem rozhodli zavést: Je-li f funkce z A do B,

$$\operatorname{graf} f := \{(x, f(x)) \in A \times B : \ x \in \operatorname{dom}(f)\}.$$

[44] Graf přece není vzorec a vzorec zase není graf.

Jistě jsou i jiné možnosti, jak tuto definici zapsat, ty ale nutně budou ekvivalentní, přijměme tedy třeba tu právě uvedenou. Nyní ale dostáváme:

$$\begin{aligned}\operatorname{graf} f &= \{(x, f(x)) \in A \times B\colon\ x \in \operatorname{dom}(f)\}\\ &= \{(x, y) \in A \times B\colon\ x \in \operatorname{dom}(f) \wedge y = f(x)\}\\ &= \{(x, y) \in A \times B\colon\ x \in \operatorname{dom}(f) \wedge (x, y) \in f\}\\ &= \{(x, y) \in A \times B\colon\ (x, y) \in f\}\\ &= f.\end{aligned}$$

Předposlední rovnost platí, podmínka $x \in \operatorname{dom}(f)$ totiž samozřejmě plyne z toho, že $(x, y) \in f$, a je tam tedy zbytečná. Poslední rovnost je jasná z toho, že $f \subseteq A \times B$ podle předpokladu. Na předposledním řádku je tedy jen zbytečně složitě zapsaná množina f (v duchu zbytečného, leč pravdivého zápisu $A = \{x\colon\ x \in A\}$ apod.). Dostali jsme tedy, že $f = \operatorname{graf} f$, a graf funkce tedy nemá cenu definovat jako samostatný pojem.

(d) Z předchozích poznámek také plyne, že s funkcemi můžeme provádět všechny běžné množinové operace: jsou to přece relace, a relace jsou množiny. Jsou-li například $f, g \subseteq \mathbb{R} \times \mathbb{R}$ funkce (z $\mathbb{R}$ do $\mathbb{R}$), pak $f \cup g \subseteq \mathbb{R} \times \mathbb{R}$, takže $f \cup g$ je nějaká relace. Samozřejmě ale není zaručeno, že by relace $f \cup g$ musela být dokonce funkcí. Jistě si sami dovedete představit nespočet případů, kdy sjednocení dvou grafů funkcí (tj. dvou funkcí) není graf funkce (tj. funkce). Možná zajímavější je zkusit vymyslet případy, kdy sjednocení dvou funkcí je opět funkce (viz následující cvičení).

2.50 Cvičení.

(i) Dokažte, že pokud $f\colon A \to B$ je bijekce, pak f^{-1} je bijekce. (Viz též Poznámku 2.48.)

Pokud jste četli Poznámku 2.49, doporučuji také zamyslet se nad následujícími úlohami.

(ii) Ukažte příklad dvou funkcí f_1, f_2 tak, že $f_1 \cup f_2$ není funkce.

(iii) Ukažte příklad dvou funkcí f_1, f_2 tak, že $f_1 \cup f_2$ je funkce.

(iv) Ukažte příklad dvou funkcí f_1, f_2 tak, že $f_1 \neq f_1 \cap f_2 \neq \emptyset$.

(v) Napište běžnou funkci $\operatorname{sgn}\colon \mathbb{R} \to \mathbb{R}$ ve tvaru $\operatorname{sgn} = g_1 \cup g_2 \cup g_3$, kde g_i jsou konstantní funkce pro $i \in \{1, 2, 3\}$. Rozmyslete si platnost rovnosti

$$\operatorname{sgn} = (-\infty, 0) \times \{-1\} \cup \{(0, 0)\} \cup (0, \infty) \times \{1\}.$$

Kapitola 3

Základní výsledky TM

3.1 Cantorova-Bernsteinova věta

V této části si dokážeme jeden z klíčových výsledků teorie množin, Cantorovu-Bernsteinovu větu. Nejprve vyslovíme její znění s příslušnými definicemi a potom se chvíli budeme věnovat zdánlivě jiným věcem, abychom je posléze použili při důkazu této důležité věty.

3.1 Definice (Subvalence, ekvipotence)**.** Buďte A, B libovolné množiny. Řekneme, že A je *subvalentní* B a píšeme $A \preccurlyeq B$, jestliže existuje prosté zobrazení A do B (definované na celé množině A). Dále říkáme, že množiny A a B jsou *ekvipotentní* a píšeme $A \approx B$, existuje-li bijekce A na B.

3.2 Věta (Cantor-Bernstein)**.** *Buďte A, B množiny. Jestliže $A \preccurlyeq B$ a $B \preccurlyeq A$, potom $A \approx B$.*

3.1.1 Věta o pevném bodě

Tento pododdíl obsahuje pojmy a výsledky, které jsou zajímavé samy o sobě, my je ale probíráme hlavně kvůli naší snaze podat elegantní a přehledný důkaz Cantorovy-Bernsteinovy věty. Budeme potřebovat pojem potence množiny, tj. množiny všech podmnožin. S pojmem potence už jsme se seznámili výše v odstavcích 2.29, 2.30 a 2.31. Zejména posledně jmenovaný odstavec je pro nás nyní podstatný, neboť se v něm ukazuje, že potenci lze přirozeným způsobem uspořádat pomocí relace inkluze: máme-li kupříkladu $A, B \in \mathcal{P}(X)$, jsou A i B podmnožiny téže množiny X, a dává velmi dobrý smysl ptát se, platí-li $A \subseteq B$ nebo $B \subseteq A$ (popř. nic z toho, nebo naopak obojí v případě rovnosti $A = B$).

3.3 Definice (Úplný svaz)**.** Řekneme, že neprázdná uspořádaná množina $(\mathcal{X}, \leqslant)$ je *úplný svaz*, jestliže libovolná její neprázdná podmnožina má v $\mathcal{X}$ infimum i supremum.

3.4 Věta. *Je-li X libovolná množina, pak $(\mathcal{P}(X), \subseteq)$ je úplný svaz.*

Důkaz. Budiž dána libovolná neprázdná $\mathcal{A} \subseteq \mathcal{P}(X)$; máme dokázat, že $\mathcal{A}$ má vzhledem k uspořádání $\subseteq$ infimum i supremum v $\mathcal{P}(X)$. Protože $\mathcal{A}$ je jistá kolekce (tj. množina) podmnožin množiny X, je jistě $\bigcup \mathcal{A} \subseteq X$ a $\bigcap \mathcal{A} \subseteq X$: sjednotím-li několik podmnožin X (a to ty, které jsou v kolekci $\mathcal{A}$), dostanu jistě opět podmnožinu X a stejně tak i pro průnik. Tytéž fakty lze zapsat také takto:

$$\bigcup \mathcal{A} \in \mathcal{P}(X) \quad \text{a} \quad \bigcap \mathcal{A} \in \mathcal{P}(X).$$

Dokážeme, že $\bigcup \mathcal{A} = \sup_{\subseteq} \mathcal{A}$. To podle definice suprema (2.37) obnáší dokázat, že (a) $\bigcup \mathcal{A}$ je horní závora kolekce $\mathcal{A}$ a (b) je ze všech horních závor $\mathcal{A}$ nejmenší. Abychom nahlédli platnost (a), stačí si uvědomit, že skutečně pro libovolnou množinu B z kolekce $\mathcal{A}$, máme $B \subseteq \bigcup \mathcal{A}$. To je ale jasné, protože i B sama je jednou ze „sjednocovaných" množin, které dohromady dají $\bigcup \mathcal{A}$. Zbývá tedy pouze ukázat (b); budiž tedy dána $H \in \mathcal{P}(X)$, libovolná jiná horní závora kolekce $\mathcal{A}$. To, že H je horní závora $\mathcal{A}$ znamená, že „libovolný prvek $\mathcal{A}$ je pod H", neboli libovolná množina $B \in \mathcal{A}$ splňuje $B \subseteq H$. To ovšem triviálně implikuje, že i sjednocení všech takových B je podmnožinou H, neboli $\bigcup \mathcal{A} \subseteq H$.

Důkaz rovnosti $\bigcap \mathcal{A} = \inf_{\subseteq} \mathcal{A}$ je analogický: ukážeme, že (a) $\bigcap \mathcal{A}$ je dolní závora kolekce $\mathcal{A}$ a (b) je ze všech dolních závor $\mathcal{A}$ největší. Pokud o ně máte zájem, jistě si podrobnosti zvládnete doplnit. □

3.5 Definice (Neklesající funkce)**.** Nechť $(\mathcal{X}, \leqslant)$ je uspořádaná množina. Funkci $f : \mathcal{X} \to \mathcal{X}$ nazveme neklesající na $\mathcal{X}$, jestliže

$$\forall a, b \in \mathcal{X} : a \leqslant b \longrightarrow f(a) \leqslant f(b).$$

3.6 Poznámka. Právě uvedené je ve shodě s definicí neklesající funkce, kterou znáte ze základního kurzu matematické analýzy; jediný rozdíl je v tom, že nyní místo uspořádání $\leqslant$ na (podmnožině) $\mathbb{R}$ uvažujeme obecnou uspořádanou množinu. Jde tedy samozřejmě o výrazné zobecnění onoho pojmu známého z analýzy.

Připomeňme jednoduchou neformální poučku, podle které „neklesající funkce je jako rostoucí, ale má navíc povolené konstantní úseky".

3.7 Definice (Pevný bod)**.** Nechť f je libovolná funkce. Jestliže $f(u) = u$, nazveme u *pevným bodem* f. Pokud tedy existuje $u \in \mathrm{dom}(f)$ tak, že $f(u) = u$, říkáme že *f má pevný bod.*

3.8 Věta (O Pevném bodě)**.** *Buď $(\mathcal{X}, \leqslant)$ úplný svaz a buď $f : X \to X$ neklesající funkce. Pak f má pevný bod.*

Důkaz. Důkaz rozdělíme do několika kroků. V tom prvním si všimneme, že libovolný úplný svaz má minimum. Skutečně, $\mathcal{X}$ sama je jistě neprázdnou podmnožinou $\mathcal{X}$, a tedy má podle definice úplného svazu infimum. Označme ho $a = \inf_{\leqslant} \mathcal{X}$. Ovšem $a \in \mathcal{X}$, neboť $\mathcal{X}$ nyní představuje největší množinu, ze které přichází v úvahu brát infima (a suprema), jejichž existence se postuluje. Máme tedy

$$a = \inf_{\leqslant} \mathcal{X}, \quad \text{přičemž} \quad a \in \mathcal{X},$$

a tedy $a = \min \mathcal{X}$, neboť infimum je jistá dolní závora a je-li dolní závora množiny současně jejím prvkem, jde zjevně o minimum (viz též Cvičení 2.42).

V druhém kroku definujeme množinu

$$B := \{b \in \mathcal{X} : b \leqslant f(b)\}.$$

Všimněme si, že $a \in B$, neboli že platí $a \leqslant f(a)$. Skutečně, $a, f(a) \in \mathcal{X}$ (jelikož $f : \mathcal{X} \to \mathcal{X}$) a $a = \min \mathcal{X}$, takže nutně $a \leqslant f(a)$. Tedy $a \in B$, a B je tedy neprázdnou podmnožinou úplného svazu $\mathcal{X}$. Má tedy supremum; označme

$$u := \sup_{\leqslant} B.$$

V posledním kroku zjistíme, že u je pevný bod funkce f. Důkaz si rozdělíme do dvou částí.

- Tvrdím, že $f(u)$ je horní závora množiny B. Zvolme tedy libovolný prvek $b \in B$ a dokažme, že $b < f(u)$: Protože $u = \sup B$ a $b \in B$, je $b \leqslant u$. Odtud aplikací monotonie f plyne $f(b) \leqslant f(u)$. Navíc $b \in B$ podle definice B znamená $b \leqslant f(b)$. Poslední dvě nerovnosti zapsány za sebou už jsou skutečně sugestivní: $b \leqslant f(b) \leqslant f(u)$. Tranzitivita uspořádání $\leqslant$ nyní dává $b \leqslant f(u)$. Protože b byl libovolně zvolený prvek B, je $f(u)$ horní závora B.

- Protože $f(u)$ je horní závora B a u je (jsouc supremem) ze všech takových nejmenší, máme $u \leqslant f(u)$. Aplikací monotonie f na tuto nerovnost ovšem dostáváme $f(u) \leqslant f(f(u))$, takže $f(u) \in B$ podle definice B. To ovšem znamená, že $f(u) \leqslant \sup B = u$. Máme tedy jak $u \leqslant f(u)$, tak i $f(u) \leqslant u$. Slabá antisymetrie $\leqslant$ tedy implikuje $u = f(u)$, a důkaz je hotov. □

3.9 Příklad. Nechť $f : [0, 1] \to [0, 1]$ je libovolná neklesající funkce (kde $[0, 1] \subseteq \mathbb{R}$ je uzavřený interval). Pak podle Věty o pevném bodě existuje $x \in [0, 1]$, pro nějž $f(x) = x$.

V tomto případě je pevný bod obzvlášť názorně představitelný, neboť je to právě takový bod, ve kterém se funkce dotýká diagonály čtverce $[0, 1] \times [0, 1]$ (viz obrázek).

Uvedené tvrzení pro funkci $f : [0, 1] \to [0, 1]$ není nijak zvlášť důležité a uvádím ho zde pouze pro zajímavost. Pozoruhodné je absencí předpokladu spojitosti funkce f: ve čtverci $[0, 1] \times [0, 1]$ se vám zkrátka nemůže podařit nakreslit graf neklesající funkce, který by neprotínal diagonálu. Naproti tomu pro důkaz Bolzanovy věty (která říká, že *spojitá* funkce na $[0, 1]$ taková, že $f(0) < 0 < f(1)$ má v nějakém bodě hodnotu 0) je předpoklad spojitosti zásadní. △

3.1.2 Důkaz Cantorovy-Bernsteinovy věty

V důkazu podstatným způsobem použijeme následující značení.

3.10 Značení. Je-li $f: A \to B$ funkce a $M \subseteq A$ je libovolná podmnožina, používáme následující značení:

$$f[M] := \{f(x) : x \in M\}.$$

3.11 Poznámka. Právě zavedené značení znamená, že $f[M]$ je množina sdružující všechny obrazy prvků M. Nejde tedy obecně o prvek B (prvky jsou jednotlivé hodnoty $f(x)$ pro $x \in A$), nýbrž o podmnožinu B, tj. $f[M] \subseteq B$. Speciálně tedy platí

$$f[\mathrm{dom}(f)] = \mathrm{rng}(f), \quad \text{to jest, chcete-li,} \quad f\big[\mathbb{D}_f\big] = \mathbb{H}_f.$$

Skuteční labužníci můžou dokonce použít pravdivý zápis (pro $M \subseteq A$)

$$f[M] = \mathrm{rng}\big(f|_M\big).$$

Můžeme si také všimnout, že libovlné funkci $f: A \to B$ odpovídá odvozená funkce $\hat{f}: \mathcal{P}(A) \to \mathcal{P}(B)$, která místo prvků A (resp. B) pracuje s podmnožinami A (resp. B) takto:

$$\text{Pro } U \in \mathcal{P}(A) \text{ položme} \quad \hat{f}(U) := f[U] \quad \in \mathcal{P}(B).$$

Je jasné, že vždy můžeme přejít o úroveň výš a dané funkci přiřadit tímto způsobem jistou funkci odvozenou. V opačném směru to obecně možné není, což lze nahlédnout dokázat celkem lehce se znalostí kardinálů.

Důkaz Věty 3.2. Mějme dány libovolné množiny A, B, které splňují předpoklady $A \preccurlyeq B$ a $B \preccurlyeq A$; máme najít bijekci A na B. Podle uvedených předpokladů existují prosté funkce $f: A \to B$ a $g: B \to A$. Víme, že $\mathrm{dom}(f) = A$ a $\mathrm{dom}(g) = B$, není ale žádný důvod se domnívat, že by jedna z funkcí byla surjektivní, ani věřit, že existuje nějaká souvislost mezi f a g. S jejich pomocí ale musíme zkonstruovat bijekci obou množin.

Začneme zavedením pomocného zobrazení $H: \mathcal{P}(A) \to \mathcal{P}(A)$, a to pro $U \in \mathcal{P}(A)$ takto:[1]

$$H(U) = A \setminus g\big[B \setminus f[U]\big].$$

Předpis pro H vypadá složitě, ale následující úsek důkazu nám ho pomůže celkem snadno pochopit. Náš cíl bude dokázat, že H je monotónní funkce na uspořádané množině $(\mathcal{P}(A), \subseteq)$. Buďte tedy dány $U, V \in \mathcal{P}(A)$ takové, že $U \subseteq V$. Následující sled odvození dokazuje žádanou

[1] Je $U \in \mathcal{P}(A)$, čili $U \subseteq A$. Přesto ale píšeme $H(U)$ místo $H[U]$, protože H bude zobrazení, které každé podmnožině množiny A přiřadí (jako svůj obraz) podmnožinu množiny B. Naproti tomu třeba f je zobrazení, které „působí na úrovni *prvků* A“, nikoliv podmnožin. Proto, když chci „do f dosadit množinu $U \subseteq A$“, musím použít Značení 3.10, tj. hranaté závorky místo kulatých (ty jsem u f oprávněn použít pouze na úrovni *prvků* A).

monotonii H a zároveň je z něj vidět, jak postupně z U utvoříme $H(U)$ (a totéž pro V):

$$
\begin{aligned}
U \subseteq V &\Rightarrow f[U] \subseteq f[V] \\
&\Rightarrow B \setminus f[U] \supseteq B \setminus f[V] \\
&\Rightarrow g\big[B \setminus f[U]\big] \supseteq g\big[B \setminus f[V]\big] \\
&\Rightarrow \underbrace{A \setminus g\big[B \setminus f[U]\big]}_{H(U)} \subseteq \underbrace{A \setminus g\big[B \setminus f[V]\big]}_{H(V)} \\
&\Rightarrow H(U) \subseteq H(V).
\end{aligned}
$$

Stručná zdůvodnění jednotlivých kroků: (1) Zobrazím-li (zobrazením f) menší množinu, dostanu méně obrazů. (2) Odečtu-li menší množinu, výsledek bude větší. (3) Obraz (při g) větší množiny je větší. (4) Odečtu-li větší množinu, výsledek bude menší. (5) Levá strana je přesně $H(U)$, pravá strana je $H(V)$. Celkem jsme tedy z $U \subseteq V$ odvodili $H(U) \subseteq H(V)$, což znamená, že H je monotónní, a to na uspořádané množině $(\mathcal{P}(A), \subseteq)$, o níž podle Věty 3.4 víme, že je to úplný svaz.

Podle Věty 3.8 má tedy funkce H nějaký pevný bod. Jinými slovy existuje $U \in \mathcal{P}(A)$ taková, že $H(U) = U$. $\square$