2. Teorie množin

Aby mohla matematika pomoci s popisem světa, musí mít struktury, které umožní zachytit různé aspekty toho, co zkoumá. V této kapitole si uvedeme ty úplně základní pojmy. Pojem množiny nám zhruba řečeno umožní zachytit situaci, kdy něco máme (popřípadě nemáme). K vystižení situace, kdy s našimi objekty něco provádíme (ubíráme, sesypáváme atd.) si zavedeme známé operace jako průnik, sjednocení a podobně. Po zevrubném prozkoumání světa množin si zavedeme další zásadní pojem, zobrazení.

Mnohé, možná většinu věcí z této kapitoly již student nejspíše někdy potkal. Využijeme proto této situace k prvnímu vážnějšímu ponoru do světa matematiky. Představíme čtenáři, jak se vytváří matematické teorie, procvičíme si důkazy a zkusíme také rozšířit rozsah naší představivosti. Díky tomu, že mnohá témata čtenář zná, bude se moci více věnovat vnímání matematického jazyka a postupů.

S Tato kapitola začíná základními věcmi, ale paradoxně právě u těch má čtenář někdy s důkazy problém, zejména pokud je tento způsob myšlení pro něj nový. Pro čtenáře, který se na to necítí, je proto naším doporučením číst tuto kapitolu spíš po povrchu, soustředit se na pochopení důležitých myšlenek a učení matematického jazyka, popřípadě si jen zlehka číst v lehkých důkazech označovaných jako rutinní, popř. poučné. Pro vniknutí do umění důkazu jsou nejlepší situace, kdy se pracuje s konkrétnějšími objekty, třeba důkaz prostoty nějakého zobrazení (viz kapitola 2b) či dokazování vlastností konkrétních relací (kapitola 3b). Až bude mít čtenář pocit, že už si s důkazy docela rozumí, může se k této kapitole zase vrátit a přečíst ji důkladněji.

2a. Množiny

Pro každého matematika představují množiny jeden ze základních vyjadřovacích prostředků. Teorie množin je ale zároveň samostatný obor matematiky, který studuje její základy, na kterých pak stojí ostatní matematické obory. Tuto hlubokou teorii zde dělat nebudeme, zaměříme se na zkoumání množin na spotřební úrovni.

Základním termínem je množina, ale právě proto, že nám chybí ty hluboké základy, tak si nebudeme schopni přesně specifikovat, co to vlastně je. Proto si namísto formální definice jen tak něco povíme.

Množina je neuspořádaný soubor objektů, které jsou přesně specifikovány. Tyto objekty se nazývají **prvky** dané množiny. Množina je těmito objekty jednoznačně dána, jinými slovy, pokud mají dvě množiny stejné prvky, pak je to tatáž množina.

By a **set** we mean an arbitrary collection of objects (called its **elements**).

Pokud jste to dobře pochopili (zejména to o shodnosti množin), tak už vás následující věc nepřekvapí:

Příklad 2a.a: Množina $\{b, a, a\}$ je stejná jako množina $\{b, a\}$, popřípadě množina $\{a, b\}$, protože mají stejné prvky. Jestliže se vás tedy někdo zeptá, kolik prvků má množina s pěti červenými kolečky, pak odpověď je jeden, leda že by každé to kolečko bylo nějak jiné.
△

Značení. Mějme množiny A, B. Značení $a \in A$ znamená, že objekt a je prvkem množiny A, naopak $a \notin A$ znamená, že objekt a není prvkem množiny A. Značení $A = B$ znamená, že jde o shodné množiny, naopak $A \neq B$ znamená, že množiny shodné nejsou, tedy nemají stejné prvky.

Množiny tradičně značíme velkými písmeny anglické abecedy, jejich prvky malými, pokud je to rozumně možné. Proč by to nemuselo být možné? Například $A = \{1, 2\}$ je množina, $B = \{13, 23\}$ je množina, ale lze z nich vytvořit další množinu: $M = \{\{1, 2\}, \{13, 23\}\}$. Množina M tedy má dva prvky, A a B, což jsou také množiny a už jsme je měli zapsané velkými písmeny. A M ještě může být strčeno do další množiny, nejde o nic výjimečného.

Množiny je možno zadat různými způsoby. Dva populární jsou výčtem prvků, třeba $M = \{1, 13, a, \diamond\}$, nebo značením zvaným anglicky „set builder“, kdy se nejprve odvoláme na nějakou větší známou množinu (universum) a pak uvedeme, které prvky z tohoto universa patří do naší množiny. Například množina všech sudých přirozených čísel se zapíše $M = \{x \in \mathbb{N};\ x \text{ sudé}\}$.

Čímž se dostáváme k nejznámějším universům, což jsou
- přirozená čísla $\mathbb{N} = \{1, 2, 3, \dots\}$; (natural numbers)
- celá čísla $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, \dots\}$; (integers)
- racionální čísla $\mathbb{Q} = \left\{\frac{p}{q};\ p \in \mathbb{Z} \wedge q \in \mathbb{N}\right\}$; (rational numbers)
- reálná čísla $\mathbb{R}$. (real numbers)

Používají se i různé modifikátory, malé plus či mínus omezuje znaménko, tedy třeba
$\mathbb{Z}^+ = \{n \in \mathbb{Z};\ n > 0\} = \mathbb{N}$ či $\mathbb{Q}^+ = \{x \in \mathbb{Q};\ x > 0\}$ nebo naopak $\mathbb{R}^- = \{x \in \mathbb{R};\ x < 0\}$,
malá nula přidá nulu, třeba $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ nebo $\mathbb{R}_0^+ = \{x \in \mathbb{R};\ x \geq 0\}$.

Nás budou zajímat hlavně první dvě množiny, protože diskrétní matematika v nich tráví většinu času. Naopak prakticky nebudeme pracovat s $\mathbb{R}$, o pár kapitol dále uvidíme, že těchto čísel je prostě příliš na to, aby je diskrétní matematika zvládla.

Velice důležitou množinou je prázdná množina čili množina bez prvků, $\emptyset = \{\}$.

Poznámka: Uděláme si malou exkurzi pro pokročilé a zvědavé. Intuitivní představa množin bývá taková, že si vymyslíme nějakou vlastnost p a ptáme se, pro které objekty je splněna. Pro usnadnění zápisu budeme psát $P(x)$, pokud objekt x tuto vlastnost splňuje. Když shromáždíme všechny objekty, které ji splňují, dostaneme množinu, zapsalo by se to $\{x;\ P(x)\}$.

Teď překvapení: Tohle nefunguje, i když je to přirozená představa a první teorie množin (za kterou děkujeme Cantorovi, cca polovina 19. století) byla takto vystavěna. Bohužel se na přelomu 19. a 20. století ukázalo, že to vede k průšvihům. Asi nejjednodušší a také nejznámější je Russelův paradox z roku cca 1901.

Začneme tímto: Existují množiny, které jsou svými vlastními prvky. Rozhodně to zní šíleně a dá velkou námahu si nějakou takovou představit, ale jde to. Třeba takto: Uvažujme vlastnost mít nekonečně mnoho prvků (přesná definice nekonečnosti přijde, ale snad máme nějakou představu už teď). Pokud by naše intuitivní představa o množinách byla správná, tak bychom pomocí této vlastnosti měli získat množinu M všech množin, které jsou nekonečné. Prázdná nebude, třeba $\mathbb{N} \in M$ nebo $\mathbb{R} \in M$. A teď to přijde: Toto M samotné má nekonečně mnoho prvků, protože určitě vymyslíme nekonečně mnoho nekonečně velkých množin, stačí třeba vzít $\mathbb{N}$ a postupně odebírat 1, 2, 3, ... , vznikají tak různé nekonečné množiny a všechny jsou v M. Proto podle definice $M \in M$, množina je svým vlastním prvkem. Takže stát se to může. Teď jsme připraveni na to hlavní.

Definujme množinu A jako množinu všech množin, které nejsou svými vlastními prvky, naším zápisem tedy $A = \{M;\ M \notin M\}$. Ta určitě obsahuje spoustu objektů, v zásadě většinu množin, které si běžně představujeme, třeba množina $\{13, 14\}$ určitě není svým prvkem a tudíž leží v A. Co platí o množině A? Kdyby byla svým vlastním prvkem, tedy $A \in A$, pak by nesplňovala podmínku z definice, proto by muselo platit $A \notin A$. Pak ale podmínku z definice splní, proto $A \in A$, pak ale ... Není tedy možné rozhodnout, zda A patří do A, což je pro teorii množin smrtící. Je to tzv. paradox, je z podobné líhně jako ten o pánovi, co prohlásí „Já teď lžu“.

Bylo tedy nutno přepracovat teorii množin, jmenovitě změnit způsob, kterým se množiny tvoří, aby se tím zakázaly určité nepříjemnosti. To se povedlo a už nějakých sto let máme uznávanou teorii množin, která těmito problémy netrpí. Základní finta je v tom, že se zakáže tvořit množiny pomocí vlastností jen tak z ničeho, vždy se musí pomocí vlastnosti vybírat z již existující množiny. Při práci s množinami se tedy obvykle pohybujeme v rámci nějaké ohromné množiny U zvané universum, zvolené tak, aby nám v ní nic nechybělo. Z jejích prvků pak tvoříme nové množiny povědomým způsobem: Vymyslíme podmínku P, která se vztahuje k prvkům z U, a definujeme $M = \{x \in U;\ P(x)\}$. Dá se ukázat, že když tvoříme množiny takto, tak už paradoxy nelze vyrobit.

Jsou tam ještě další komplikace, ale zde to budeme úspěšně ignorovat. Ukazuje se totiž, že problémy vyvstávají, jen když se člověk v množinách hrabe trochu hlouběji, při běžné „spotřební“ práci se na paradoxy nenarazí. Spousta lidí si proto vystačí s tou intuitivní představou, kterou jsme tuto kapitolu začali, říká se tomu naivní teorie množin a my se s ní spokojíme také.

△

Je čas představit si první definici. Připomínáme, že tradičně se definice píší jako implikace, ale míní se ekvivalence (viz úvodní kapitola o logice).

! **Definice.**
Nechť A, B jsou množiny. Řekneme, že A je **podmnožina** B, značeno $A \subseteq B$, jestliže jsou všechny prvky A také prvky B.
Řekneme, že A je **vlastní podmnožina** B, jestliže $A \subseteq B$, ale $A \neq B$.
Vztahu býti podmnožinou říkáme **inkluze**.

We say that a set A is a **subset** of a set B, denoted $A \subseteq B$, if all elements of A are also elements of B.
We say that A is a **proper subset** of B if $A \subseteq B$ but $A \neq B$.

Definice inkluze formálně: $A \subseteq B \iff [\forall a \in A\colon a \in B]$.

Na tento způsob zápisu byste si měli pomalu začít zvykat. Pokud si ještě nerozumíte s kvantifikátory, koukněte do první kapitoly.

Někteří autoři značí vlastnost býti vlastní podmnožinou jako $A \subset B$. Má to ale problém, protože jiní autoři používají z lenosti $A \subset B$ pro běžnou vlastnost inkluze (dokonce někdy i já, ale ne v této knize, na to jsem si dal pozor). Ve významu značení $\subset$ je tedy zmatek, proto jej tady zavádět nebudeme a spokojíme se se značením $A \subseteq B$, kterému rozumí všichni stejně.

Když matematici zavedou nový pojem či vlastnost, tak hned začnou přemýšlet, jak fungují a jak se chovají. V jistém smyslu se dá říci, že toto je jednou z hlavních náplní matematiky: Dozvídat se co nejvíce o různých pojmech. Pojmy se totiž definují, protože se zdají užitečné, a když známe jejich vlastnosti, tak nám to pomůže při práci s nimi, tak jako vám například při práci s algebraickými výrazy pomáhá znalost různých identit a pravidel (třeba že se dá krátit ve zlomku). Praktickým výstupem takových znalostí pak jsou různé metody na řešení problémů.

Začneme něčím snadným.

Fakt 2a.1.
Nechť A je libovolná množina. Pak platí následující:
(i) $A \subseteq A$;
(ii) $\emptyset \subseteq A$.

Teď si ukážeme náš první důkaz, proto bude poněkud podrobnější.

Důkaz (rutinní, poučný)**:** Normálně by se tento důkaz skládal ze slov „je to triviální“. Ukážeme, proč je to tak lehké.

(i): Pro každou množinu A máme dokázat tvrzení $A \subseteq A$.

Vezměme si tedy nějakou libovolnou množinu A. O této množině musíme dokázat, že $A \subseteq A$, což podle definice znamená $\forall a \in A$: $a \in A$. Jinými slovy, když si z ní vezmeme libovolný prvek a (viz ten kvantifikátor $\forall a$), tak je v A. To je ale triviálně pravda, všechno z A je v A, tudíž je důkaz hotov.

Zajímavý alternativní pohled na věc: To, co od A chceme, se dá přepsat do tvaru implikace:

$$\text{Pro libovolný objekt } x \text{ platí: } x \in A \implies x \in A.$$

Přeloženo do slov, jestliže je x z A, tak je z A. Tato implikace je samozřejmě pravdivá. Obecně se dá dokázat (třeba pravdivostní tabulkou, viz kapitola 1), že implikace $p \implies p$ je vždy pravdivá.

Pro libovolnou množinu A jsme tedy dokázali (aniž bychom věděli, jak vypadá), že $A \subseteq A$.

(ii): Nechť A je libovolná množina. Teď máme dokázat, že $\emptyset \subseteq A$, podle definice tedy chceme $\forall x \in \emptyset$: $x \in A$, což lze ještě přesněji vyjádřit slovy $\forall x$: $x \in \emptyset \implies x \in A$. V kapitole 1a jsme viděli, že takové tvrzení je pravdivé vždy, důkaz je hotov.

□

S **Poznámka:** Nebyly to typické důkazy, první byl triviální a druhý netypický, protože vlastně jeho podstata nebyla v práci s množinami, ale ve fungování logiky. Snadno se stane, že student má něco dokázat, ale nevidí, co vlastně přesně je třeba udělat. Velice často pomůže nesnažit se rovnou psát důkaz, ale nejprve si vyjasnit, jaká je vlastně situace. V typickém případě se podíváme na to, co máme dokázat a co máme k dispozici, a snažíme se to vyjádřit jinak. Často používáme definice, jak jsme to udělali výše, někdy už třeba máme za sebou nějakou teorii, která nám dovolí zkoumané vlastnosti vyjádřit pomocí jiných, o kterých už něco víme.

Někdy stačí jen formální úprava k tomu, aby náš mozek náhle uviděl, jak věci udělat. Proto když se zadrhneme, tak se může vyplatit, když si nějaký fakt zapíšeme jinak. Například to, že objekt a není v jisté množině A, lze zapsat $a \notin A$, $\neg(a \in A)$ či dokonce $a \in \overline{A}$. Může se stát, že jedno z těch vyjádření vyloženě zapadne do situace, zatímco ostatní by případný důkaz jen komplikovaly.

Následující výrok má velice příjemný důkaz, přirozený a snadný. Pokud chce student někde s důkazy začít, toto může být to správné místo.

△

!

Fakt 2a.2.
Nechť A, B, C jsou množiny. Jestliže $A \subseteq B$ a $B \subseteq C$, pak $A \subseteq C$.

Důkaz (rutinní, poučný)**:** Výrok má platit pro všechny trojice množin, proto si vezmeme libovolné množiny A, B, C a chceme pro ně ukázat pravdivost implikace

$$(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C.$$

Jako obvykle při důkazu implikace začneme tím, že považujeme její předpoklad za pravdivý, a musíme ukázat, že pak už bezpodmínečně dojdeme k závěru (viz kapitola 1b). V tomto případě tedy předpokládáme, že platí logická konjunkce $A \subseteq B \wedge B \subseteq C$, což znamená, že platí obě části, $A \subseteq B$ i $B \subseteq C$. Musíme ukázat, že pak také nutně platí $A \subseteq C$. Podle definice inkluze to znamená, že musíme ukázat, že pro libovolný prvek $a \in A$ platí i $a \in C$. Dejme se do toho.

Nechť $a \in A$ je libovolné. Podle našeho předpokladu, že $A \subseteq B$, pak také (podle definice inkluze) $a \in B$. Z toho podle předpokladu $B \subseteq C$ a definice inkluze zase dostaneme $a \in C$ a důkaz je hotov.

□

! **Poznámka o dokazování:** I tento důkaz by se v „normální“ knize odbyl slovem „triviální“, my jsme si na něm zopakovali logickou spojku „a“ a připomeneme si základy dokazování. Nejprve jsme si analýzou rozebrali, co vlastně máme dělat: Ukázat $a \in A \implies a \in C$. To jsme provedli přímým důkazem ve dvou krocích

$$a \in A \implies a \in B \implies a \in C.$$

Každý z těchto částečných kroků byl pečlivě odůvodněn odvolávkou buď na nějaký již akceptovaný fakt (zde definici vlastnosti býti podmnožinou) nebo na nějaký předpoklad, který jsme v té chvíli považovali za platný. U důkazu pokročilejších tvrzení se často také odvoláváme na již dokázaná tvrzení. V tom je podstata matematiky, pokaždé, když něco říkáme, tak to musíme mít podepřeno. V běžně psaných důkazech se ovšem detailní odvolávky vynechávají, protože se předpokládá, že si ty samozřejmější dokáže čtenář sám domyslet, komentují se jen kritické kroky. Až budete v dalších kapitolách číst stručnější důkazy, zkuste si rozmyslet, čím jsou podepřeny všechny ty „proto“, „tudíž“ a podobně, je to dobrý trénink. Až budete vy psát důkaz na písemce, tak je lepší ta odůvodnění napsat, jednak abyste si šplhli a ukázali, že víte, co děláte, druhak protože hlavně pro začátečníka je obtížné odhadnout, co se dá coby jasné vynechat.

△

! **Fakt 2a.3.**
Nechť A, B jsou množiny. Pak $A = B$ právě tehdy, když $A \subseteq B$ a $B \subseteq A$.

Toto je zrovna jedna z věcí, které asi čtenáři přijdou naprosto jasné, a právě proto patrně neví přesně, jak tohle vlastně dokázat. Budeme následovat výše zmíněné rady a začneme od základů, nejprve si vyjasníme strukturu problému a pak si jednotlivá tvrzení přeložíme do řeči jednodušších pojmů.

Důkaz (rutinní)**:** Vezměme dvě libovolné množiny A a B. Tvrzení, které o nich máme dokázat, je ekvivalence, což je totéž jako dvě implikace, tam i zpět. Máme tedy ukázat, že z faktu nalevo plyne fakt napravo a také naopak.

1) $\implies$: Předpokládejme, že $A = B$, což znamená, že tyto dvě množiny mají stejné prvky.

1a) Ukážeme, že pak $A \subseteq B$. Podle definice tedy máme ukázat, že $\forall a \in A$: $a \in B$. Nechť je $a \in A$ libovolné. Protože $A = B$, mají tyto množiny stejné prvky, tudíž $a \in A$ znamená také $a \in B$ a je to hotovo.

1b) Ukážeme, že pak i $B \subseteq A$. Vzhledem k symetrii situace půjde vlastně o stejný důkaz, jen se prohodí písmenka. Normálně bychom tedy v takové situaci napsali: „důkaz $B \subseteq A$ je obdobný.“ V rámci tréninku to zkusíme napsat: Nechť b je libovolný prvek z B. Protože A a B mají stejné prvky, pak také $b \in A$. Hotovo.

2) $\impliedby$: Předpokládejme, že $A \subseteq B$ a $B \subseteq A$. Potřebujeme dokázat, že pak $A = B$.

To je ale jasné. Všechny prvky z A jsou díky $A \subseteq B$ i v B a naopak všechny prvky z B jsou díky $B \subseteq A$ i v A. Množiny tedy mají shodné prvky. Důkaz je hotov.

□

Ta část 2) je asi nejtěžší, protože opravdu není jasné, co k tomu říct, když je to tak evidentní. Ukážeme ještě dva důkazy tohoto faktu v následující poznámce.

S **2a.4 Poznámka:** Vyzkoušíme si na implikaci

$$(A \subseteq B \wedge B \subseteq A) \implies A = B$$

nepřímý důkaz (viz kapitola 1b). Jinými slovy, budeme chtít dokázat její obměnu

$$\neg(A = B) \implies \neg(A \subseteq B \wedge B \subseteq A),$$

což se přepíše pomocí de Morganových zákonů (viz kapitola 1a) jako

$$A \neq B \implies [\neg(A \subseteq B) \vee \neg(B \subseteq A)]. \qquad (*)$$

Teď tuto implikaci dokážeme.

Důkaz: Předpokládejme tedy, že $A \neq B$. Rovnost množin je definována přes obecný kvantifikátor (všechny jejich prvky jsou sdíleny). Její negací je tedy tvrzení, že existuje prvek, který není sdílen (viz negace kvantifikátorů v kapitole 1a). Náš předpoklad $A \neq B$ tedy říká, že existuje nějaký prvek x, který je v jedné z těchto množin ale ne v druhé. Jsou dvě možnosti:

1) Jedna možnost je, že $x \in A$, ale $x \notin B$. To zapíšeme jako $\exists x \in A : \ x \notin B$, což podle právě probraných pravidel znamená

$$\exists x \in A\colon \neg(x \in B) \ \not\equiv \ \neg(\forall x \in A\colon x \in B).$$

Řečeno česky, není pravda, že všechny prvky z A jsou v B. To je negace vlastnosti $A \subseteq B$, čili A nemůže být podmnožinou B. Protože platí $\neg(A \subseteq B)$, platí i disjunkce $\neg(A \subseteq B) \vee \neg(B \subseteq A)$ (pro její pravdivost stačí, aby byla splněna některá ze složek). Pokud tedy nastane situace $x \in A$ ale $x \notin B$, pak je kýžená implikace $(*)$ dokázána.

2) Druhá možnost je, že $x \in B$, ale $x \notin A$. Stejným argumentem jako v 1) pak ukážeme, že neplatí $B \subseteq A$ a tudíž i v tomto případě je ona implikace $(*)$ pravdivá.

Žádný jiný případ už není možný, takže dokazovaná implikace (obměna) platí.

□

Všimněte si, že se nám důkaz rozvětvil na dvě možnosti. To se stává, je pak ale důležité v takové situaci probrat úplně všechny možnosti a pokaždé dojít ke správnému závěru, popřípadě ukázat, že ta či ona možnost v dané situaci vlastně nemůže nastat. Anglicky se tomuto říká „exhaustion argument" neboli „důkaz vyčerpáním", myslí se tím všech možností, ale často také čtenáře a nezřídka i autora.

Výraznou úsporou může být, pokud jsou některé situace obdobné a jejich případy by se řešily stejně, zejména užitečná je symetrie, například v našem důkazu se dají A a B zaměnit. V běžných důkazech se to využije tak, že si prostě jednu z možností vybereme, musí se to ale správně odůvodnit. Hned si to ukážeme.

Třetí rozšířený typ důkazu implikace je důkaz sporem (viz kapitola 1b), připomeneme si jej opět na naší oblíbené implikaci $(A \subseteq B \wedge B \subseteq A) \implies A = B$.

Důkaz: Předpokládejme tedy, že platí její předpoklady $A \subseteq B$ a $B \subseteq A$, ale neplatí závěr $A = B$. To znamená, že existuje nějaký bod x takový, že je v jedné množině a není v druhé. Protože je situace symetrická, můžeme předpokládat, že $x \in A$ a $x \notin B$. Ovšem z předpokladů $x \in A$ a $A \subseteq B$ také plyne, že $x \in B$. Prvek x tedy zároveň splňuje $x \notin B$ a $x \in B$, což je ve sporu. Důkaz implikace je hotov.

□

Tím končíme s důkazy, které byly sice většinou lehké, ale ukazovali jsme si na nich podrobně různé triky. Další důkazy budeme postupně dělat stručnější, ke konci této kapitoly už budou v zásadě psány standardním způsobem.
△

Definice.
Nechť A je množina. Definujeme **potenční množinu** A, značeno $P(A)$, jako množinu všech podmnožin A.

Příklad 2a.b: Jestliže $A = \{a, b\}$, pak $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
△

Jako rozcvičku si ukážeme jednu vlastnost, která je z matematického hlediska triviální, ale důkaz může být pro začátečníka poněkud drsný.

Fakt 2a.5.
Nechť A, B jsou množiny. Jestliže $A \subseteq B$, pak $P(A) \subseteq P(B)$.

Důkaz (rutinní)**:** Předpokládejme, že máme libovolné množiny A, B splňující $A \subseteq B$. Potřebujeme ukázat, že $P(A) \subseteq P(B)$, což podle definice znamená, že $\forall m \in P(A)$: $m \in P(B)$.

Zde je zásadní si rozmyslet, s jakými objekty vlastně pracujeme. Co jsou to ty m výše? $P(A)$ je množina všech podmnožin A, takže $m \in P(A)$ je vlastně nějaká podmnožina A. S tímto objektem tedy někdy pracujeme jako s prvkem (když mluvíme o $P(A)$ a $P(B)$) a jindy jako s množinou (když se budeme pohybovat v A, B). Pro začátečníka to může být zmatečné, ale důkaz je vlastně snadný, když si v tom člověk udělá v hlavě trochu pořádek, právě tak, jak jsme si to teď rozmysleli. Je čas na důkaz.

Vezměme tedy libovolný prvek m z $P(A)$. Podle definice $P(A)$ je m podmnožinou A, ale máme také předpoklad $A \subseteq B$, tudíž podle Faktu 2a.3 je $m \subseteq B$. Proto podle definice $P(B)$ platí $m \in P(B)$ a důkaz je hotov.

□

! Obvykle pracujeme s více množinami a všechny jsou schovány uprostřed jedné velké množiny, universa U, ze kterého při své práci nevyskočíme. V rámci tohoto universa pak množiny všelijak kombinujeme či vytváříme nové. Asi každý čtenář se již potkal se sjednocením množin (sesypeme všechny jejich prvky do jednoho pytlíčku), průnikem (to, co je množinám společné) a doplňkem (všechny prvky mimo). Teď si ukážeme formální definice, čtenář už by je měl být schopen plynule číst a překládat si je do srozumitelné představy.

! **Definice.**
Nechť A je množina v nějakém universu U. Definujem její **doplněk** vzhledem k U jako

$$A^c = \overline{A} = \{x \in U;\ x \notin A\}.$$

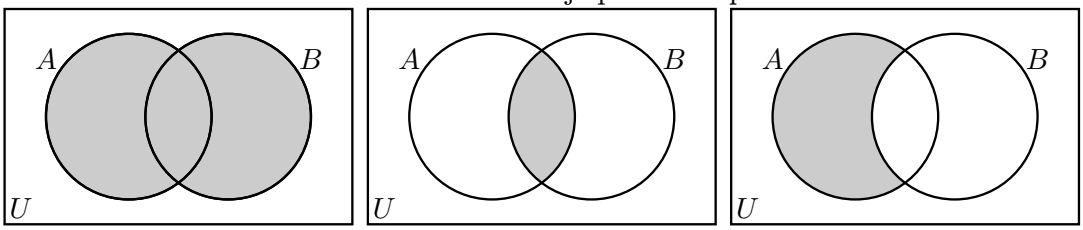
Let A be a set in a universe U. We define its **complement** (with respect to U) as the set $A^c = \overline{A}$ of all elements of U that are not in A.

! **Definice.**
Nechť A, B jsou množiny v nějakém universu U. Definujeme jejich
sjednocení: $A \cup B = \{x \in U;\ x \in A \vee x \in B\}$;
průnik: $A \cap B = \{x \in U;\ x \in A \wedge x \in B\}$;
rozdíl či **doplněk** B **v** A**:** $A - B = \{x \in U;\ x \in A \wedge x \notin B\}$;
kartézský součin: $A \times B = \{(a, b);\ a \in A \wedge b \in B\}$, zde (a, b) značí uspořádanou dvojici.

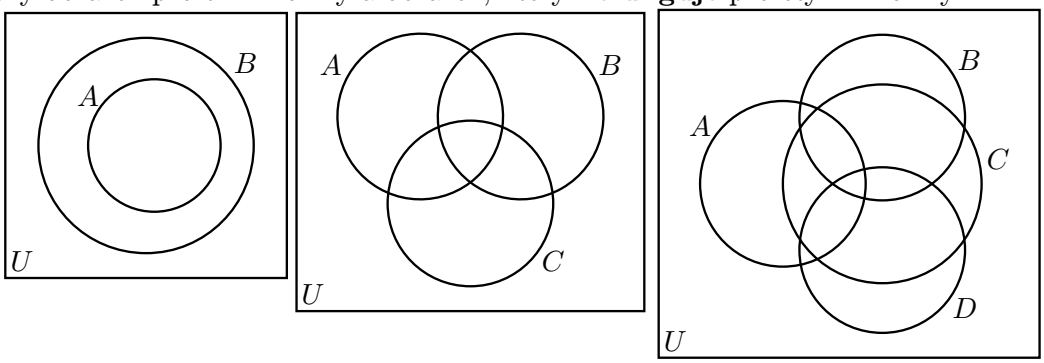
Anglickou verzi uděláme méně formální, ať si čtenář zvyká na jazyk.
Let A, B be sets in some universe U. We define their
union $A \cup B$ as the set of all elements that are in A or in B;
intersection $A \cap B$ as the set of all elements that are both in A and B;
difference $A - B$ as the set of all elements that are in A but not in B;
Cartesian product as the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Příklady asi moc nemají smysl, všichni to znají, ale budiž: Když třeba $A = \{1, 2, 13\}$ a $B = \{13, 23\}$, pak $A \cup B = \{1, 2, 13, 23\}$, $A \cap B = \{13\}$, $A - B = \{1, 2\}$ a také
$A \times B = \{(1, 13), (1, 23), (2, 13), (2, 23), (13, 13), (13, 23)\}$.
Co je doplněk A? To není jasné, protože jsme neřekli, v jakém universu pracujeme. Nabízí se třeba universum $\mathbb{N}$, pak je $\overline{A} = \{3, 4, \ldots, 11, 12, 14, 15, 16, \ldots\}$. Jenže můžeme vzít jiné U a pak bude $\overline{A}$ jiné. V zásadě se dá říct, že pokud nějaká situace vyžaduje, aby se dělal doplněk, tak už bývá z kontextu jasné i U, a pokud doplňky nepotřebujeme, tak nám v zásadě U nijak nechybí. Spousta lidí pracuje s množinami celá léta a ani neví, že jsou nějaká universa, i my jsme teď v pohodě vytvořili třeba $A \cup B$, aniž bychom znali U.

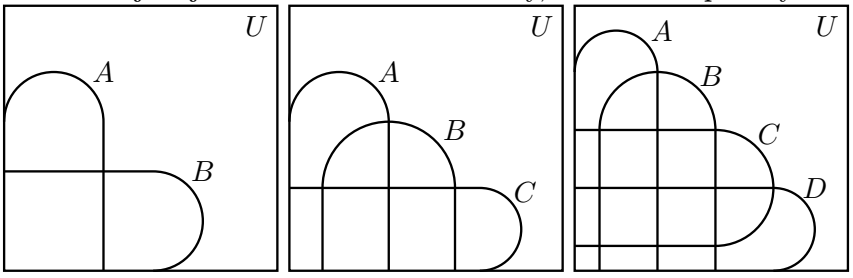
! Dobrým znázorněním vztahu mezi množinami jsou tzv. **Vennovy diagramy**. Následující obrázky ukazují standardní znázornění dvou množin a stínování v nich zobrazuje první tři operace z definice.



Někdy chceme obrázkem vyjádřit přímo určitou situaci. Následující obrázek ukazuje situaci, kdy $A \subseteq B$. Připojili jsme také klasický obrázek pro tři množiny a obrázek, který **nefunguje** pro čtyři množiny.



Proč nefunguje? Protože na něm není místo pro prvky, které jsou v A, B a D, ale nejsou v C, tedy chybí tam místo na vyznačení množiny $(A \cap B \cap D) - C$. Dá se dokázat, že nelze vytvořit obrázek ze čtyř kružnic, který by vyhovoval (jinými slovy, ať už nakreslíte čtyři kružnice jakkoliv, vždycky bude existovat určitý typ prvků, pro které ten obrázek nebude mít chlíveček). Co s tím? Jedna možnost je namísto jedné z kružnic použít klobásoid, což ale není moc estetické. Existují zajímavé alternativní obrázky, které už to pro čtyři množiny dokážou:



Tyhle obrázky to zase neumí pro pět množin, ale ještě mi to nikdy nechybělo.

! Uvedeme si teď vlastnosti operací. Rozhodně nemá smysl učit se pravidla z následujících tvrzení nazpaměť (až na pár výjimek), ani profesionální matematik by je nedokázal všechny vyjmenovat. Důležité je se nad nimi zamyslet, představit si různé situace a rozmyslet si, že by ta pravidla měla platit. Cílem je začít množinám rozumět, aby vám platnost těch pravidel přišla stejně přirozená jako platnost $7+5=5+7$. Když je pak člověk v situaci, kdy by nějaké to pravidlo potřeboval, tak se mu samo nabídne, jako se člověku nabízí třeba krácení ve zlomcích, aniž by o tom znal nějakou větu. Pro matematika je většina následujících tvrzení „jasná“, v jeho světě to tak prostě fungovat musí, stejně jako v našem světě když pustíme kámen, tak všichni víme, co se pak stane, nemusíme si na to pamatovat nějaké věty.

Pro získání této intuice je důležité si také rozmýšlet věci, které neplatí, aby člověk nepropadl přílišnému opimismu, jako třeba čtenář ví, že nelze napsat $\frac{1}{2+3}$ jako $\frac{1}{2}+\frac{1}{3}$. Podobně mnoho věci selhává pro množinové operace a o nejsvůdnějších by měl člověk vědět, asi nejzrádnější uvidíte za chvíli a ve cvičení 2a.2.

Přemýšlení nad pravidly je také dobrá příležitost si protrénovat logiku a důkazy.

Hned z definice operací dostaneme následující.

Fakt 2a.6.
Nechť A, B jsou množiny. Pak platí:
(i) $A \subseteq A \cup B$, $B \subseteq A \cup B$;
(ii) $A \cap B \subseteq A$, $A \cap B \subseteq B$.

Důkaz (rutinní)**:** (i): Dokážeme, že $A \subseteq A \cup B$. Nechť $x \in A$ je libovolné. Protože obecně je implikace $p \implies p \vee q$ pravdivá, tak z pravdivosti výroku $x \in A$ vyplývá i pravdivost výroku $x \in A \vee x \in B$ a tedy $x \in A \cup B$. Důkaz hotov.

Důkaz $B \subseteq A \cup B$ je stejný dle symetrie.

(ii): $A \cap B \subseteq A$: Nechť $x \in A \cap B$. Pak $x \in A \wedge x \in B$, proto tedy $x \in A$. Důkaz je hotov, druhé tvrzení plyne ze symetrie.

□

Všimněte si, že při důkazu (ii) jsme napsali jen „nechť $x \in A \cap B$“. Pokládá se za samozřejmé, že se v takové situaci bere x libovolné, tudíž se šetří místem a časem a to slovo se vynechává, i zde to budeme dělat. Pokud student předvádí důkaz u zkoušky, tak ať raději to „libovolné“ napíše, ať ukáže zkoušejícímu, že ví, co se děje.

Mimochodem, mohlo by se stát, že namísto inkluzí budou v těch vztazích rovnosti? A pokud ano, tak za jakých okolností? Matematici si pořád kladou takové zvědavé otázky, odpovědi na tyto dvě najdete ve cvičení 2a.1 (iii) a (iv).

! **Věta 2a.7.** (zákony pro počítání s množinami)
Nechť A, B, C jsou libovolné množiny z universa U. Pak platí následující:
(i) $A \cup \emptyset = A$, $A \cap U = A$; (zákony identity)
(ii) $A \cap \emptyset = \emptyset$, $A \cup U = U$; (zákony dominance)
(iii) $A \cup A = A$, $A \cap A = A$; (idempotence)
(iv) $\overline{\overline{A}} = A$; (zákon komplementu)
(v) $A \cup B = B \cup A$, $A \cap B = B \cap A$; (komutativní zákon)
(vi) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$; (asociativní zákon)
(vii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; (distributivní zákon)
(viii) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$; (De Morganovy zákony)
(ix) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$; (zákony absorbce)
(x) $A \cup \overline{A} = U$, $A \cap \overline{A} = \emptyset$. (zákony doplňku)

Doporučujeme, aby si čtenář postupně všechna pravidla prošel a pokaždé si začal kreslit Vennovy diagramy dané situace. Je velice užitečné zkusit si každou vlastnost vyvrátit, tedy nakreslit situaci, kdy neplatí. Samozřejmě se to nemůže podařit, ale naší intuici velice pomáhá, když se snažíme takovou protipříkladovou situaci vytvořit a ona se nám vždycky nějakým způsobem zvrtne, takže nakonec studovaná vlastnost platí.

Pokud si čtenář vlastnosti prošel, tak jistě zjistil, že hlavně těch prvních pět je opravdu jasných, ale pak jsou situace, které vyžadují hlubší zamyšlení a stojí za to si je pamatovat. Jde zejména o de Morganovy zákony a distributivní pravidlo („roznásobení závorky“), které dokonce funguje pro obě pozice operací (na rozdíl od násobení a sčítání, které si takto rozumí jen jedním způsobem).

Dokážeme to nejdůležitější, zbytek necháme na čtenáři, protože je to opravdu snadné.

Důkaz (rutinní, poučný)**:** (vii): Dokážeme první vztah, druhý je obdobný. Rovnost množin se nejčastěji dokazuje přes dvě inkluze, ty se pak dokazují podle definice, tedy implikace pro náležení prvků.

1) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$: Nechť $x \in A \cap (B \cup C)$. Pak $x \in A$ a $x \in B \cup C$. Druhý fakt nabízí dvě možnosti.

Jestliže $x \in B$, pak spolu s $a \in A$ dostaneme $x \in A \cap B$, proto $x \in (A \cap B) \cup (A \cap C)$.

Jestliže $x \in C$, pak symetricky dostaneme $x \in A \cap C$, proto $x \in (A \cap B) \cup (A \cap C)$.

Pokryli jsme všechny (obě) možnosti, důkaz je úplný.

V části 2) tento rozbor možností, které jsou v podstatě stejné, nahradíme odvolávkou na symetrii.

2) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$: Nechť $x \in (A \cap B) \cup (A \cap C)$. Pak x leží alespoň v jednom z těch průniků, díky symetrii můžeme předpokládat, že $x \in A \cap B$. Pak $x \in A$ a také $x \in B$. To druhé ale dává $x \in B \cup C$, tedy $x \in A \cap (B \cup C)$ a důkaz je hotov.

(viii): Nechť A, B, C jsou množiny.

1) Dokážeme, že $\overline{A \cup B} = \overline{A} \cap \overline{B}$, zase přes dvě inkluze.

1a) Nechť x je libovolný prvek z $\overline{A \cup B}$. To znamená, že $x \notin A \cup B$. Prvky $x \in A \cup B$ splňují $x \in A \vee x \in B$, prvky mimo tedy splňují negaci této vlastnosti, což je podle de Morganových zákonů pro formální logiku rovno

$$\neg(x \in A \vee x \in B) \;\models\; \neg(x \in A) \wedge \neg(x \in B) \;\models\; x \notin A \wedge x \notin B.$$

To znamená, že $x \in \overline{A} \wedge x \in \overline{B}$, tedy $x \in \overline{A} \cap \overline{B}$. Právě jsme dokázali, že $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

1b) Nechť naopak $x \in \overline{A} \cap \overline{B}$. Použijeme podobný postup jako v 1a), ale zapíšeme jej čistě formálně jako řetěz implikací.

$$\begin{aligned} x \in \overline{A} \cap \overline{B} &\implies x \in \overline{A} \wedge x \in \overline{B} \implies x \notin A \wedge x \notin B \implies \neg(x \in A) \wedge \neg(x \in B) \\ &\implies \neg(x \in A \vee x \in B) \implies \neg(x \in A \cup B) \implies x \in \overline{A \cup B}. \end{aligned}$$

Všimněte si, že všechny implikace platí i zpětně, tedy jsou to vlastně ekvivalence. To znamená, že části 1a) a 1b) šlo dokázat najednou. U snažších věcí lze někdy ekvivalenci dokázat přímo.

2) Teď dokážeme, že $\overline{A \cap B} = \overline{A} \cup \overline{B}$, tentokrát zkusíme jinou metodu. Jednak uděláme oba směry najednou, druhak zvolíme jinou formu zápisu. V předchozí části jsme pracovali s prvky, teď budeme pracovat s celými množinami a budeme upravovat podmínky, které je definují. Je asi zřejmé, že když v definici množiny podmínku příslušnosti nahradíme jinou, která je ekvivalentní (říká totéž), tak se dotyčná množina nezmění.

$$\begin{aligned} \overline{A \cap B} &= \{x \in U;\ x \notin A \cap B\} = \{x \in U;\ \neg(x \in A \cap B)\} = \{x \in U;\ \neg(x \in A \wedge x \in B)\} \\ &= \{x \in U;\ \neg(x \in A) \vee \neg(x \in B)\} = \{x \in U;\ x \notin A \vee x \notin B)\} = \{x \in U;\ x \in \overline{A} \vee x \in \overline{B}\} \\ &= \overline{A} \cup \overline{B}. \end{aligned}$$

□

Všechna právě probraná pravidla z Věty mají své prakticky stejně vypadající bratříčky ve formální logice, stačí namísto $\cap$ psát $\wedge$, místo $\cup$ se píše $\vee$, doplněk se nahradí negací, $\emptyset$ je F a podobně. Mezi množinovými a logickými operacemi je úzká souvislost, v důkazu výše to bylo také vidět, například de Morganovo pravidlo pro množiny jsme dokazovali pomocí de Morganova pravidla pro logické výrazy.

Poznámka: Někdy se v důkazu situace výrazně zjednoduší, pokud o prvku, se kterým pracujeme, víme něco navíc. Toho se dá dosáhnout například tím, že se hned na začátku prvky rozdělí do skupin podle nějakého kritéria a pak se důkaz dělá pro každou skupinu zvlášť. Někdy si toto rozdělení důkaz sám vynutí, i v důkazu výše je jedna rozdvojka.

Nejčastější dělení je podle toho, zda prvek leží či neleží v množinách z předpokladu, tedy v $A, B, C, \ldots$ Vznikají tak skupiny, jejichž počet rychle stoupá, pro dvě množiny jsou čtyři možnosti, pro tři množiny osm, pro čtyři 16 atd., v důkazu pak musíme probrat všechny skupiny, takže tento typ důkazu není zrovna nejpoužívanější. Často ale tuto metodu používáme v situacích, kdy jen chceme zjistit, zda nějaký množinový vztah platí či ne, pak se podíváme, co se děje pro typické zástupce různých skupin.

Jako příklad dokážeme rozborem pro typy prvků rovnost $\overline{A \cap B} = \overline{A} \cup \overline{B}$. Jsou čtyři možnosti, jaký vztah může nějaký prvek mít k množinám A, B.

a) Jestliže $x \in A$ a $x \in B$, pak i $x \in A \cap B$ a tudíž $x \notin \overline{A \cap B}$.

Pak ale také $x \notin \overline{A}$ a $x \notin \overline{B}$, tudíž $x \notin \overline{A} \cup \overline{B}$. Tyto prvky x tedy nejsou ani v množině nalevo, ani v množině napravo zkoumané rovnosti.

b) Jestliže je x takové, že $x \in A$ ale $x \notin B$, pak $x \notin A \cap B$, tudíž $x \in \overline{A \cap B}$.

Podle $x \in \overline{B}$ máme i $x \in \overline{A} \cup \overline{B}$. Tyto prvky x tedy jsou i v množině nalevo, i v množině napravo.

c) Ukažte sami, že prvky x splňující $x \notin A$ ale $x \in B$ jsou také v obou množinách, ukažte to i pro případ d), tj. prvky x splňující $x \notin A$ a $x \notin B$.

Proto jsou všechny typy prvků buď v obou zkoumaných množinách, nebo nejsou v žádné, ony množiny tedy mají stejné prvky a jsou si rovny.

Zdlouhavost takovýchto úvah lze zkrátit tabulkou. Ve sloupcích značíme množiny a v řádcích značíme pomocí 0 a 1, zda zkoumaný prvek v nich je nebo není. V záhlaví jsou dva sloupce, kterými si prvky vybíráme, tam musíme dostat všechny možné kombinace, takže tabulka pro dvě množiny bude mít 4 řádky. Tabulka našeho důkazu vypadá takto:

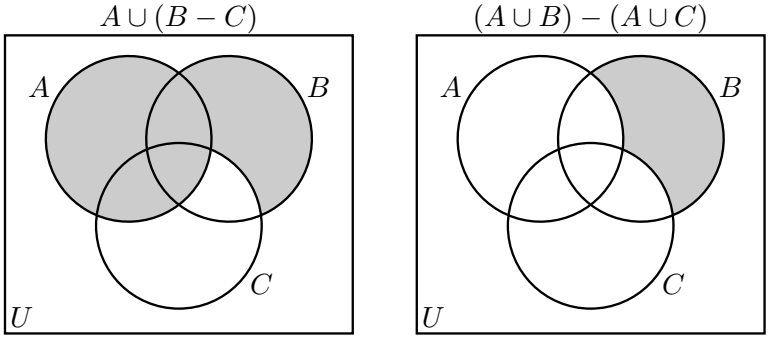
A	B	$A \cap B$	$\overline{A \cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cup \overline{B}$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Protože se sloupce zkoumaných množin shodují, jsou si tyto množiny rovny.
△

! Poznámka: Zatím jsme jen dokazovali, že něco platí. Může se ale stát, že nám někdo předhodí tvrzení, které není dobře, třeba toto:

Pro libovolné množiny A, B, C platí $A \cup (B - C) = (A \cup B) - (A \cup C)$.
(Je to pokus o distributivní zákon, zkusili jsme „roznásobit“ tu závorku.)

Jak zjistíme, zda má cenu to dokazovat? Jedna možnost je zakreslit si obě množiny ve Vennově diagramu.



Vidíme, že nejde o stejné objekty. Jak se tedy dokáže, že je dané tvrzení nepravdivé? Toto tvrzení je uvedeno obecným kvantifikátorem „pro všechny množiny“. K vyvrácení tedy stačí najít jediný protipříklad, kdy dané tvrzení selže (viz kapitola 1b). Obrázek nás inspiruje, stačí zvolit množiny tak, aby na nich byl vidět ten rozdíl v obrázku, neboli chceme mít prvek v místě, kde se obrázky liší. Zvolme tedy třeba $A = \{13\}$ a $B = C = \emptyset$, pak

$$A \cup (B - C) = \{13\} \cup \emptyset = \{13\}, \text{ zatímco } (A \cup B) - (A \cup C) = \{13\} - \{13\} = \emptyset.$$

Tento protipříklad tedy dokázal, že dané tvrzení neplatí.

Mimochodem, obrázek naznačuje, že by první množina měla vždy obsahovat tu druhou. A to je pravda, viz cvičení 2a.1 (ix).

Další možnost, jak najít protipříklad, je pomocí tabulky z poznámky výše. Pokud se sloupce zkoumaných množin neshodují, tak se podíváme na řádek, kde se liší, a vytvoříme takové množiny A, B, C ... , aby tuto situaci měly neprázdnou.
△

Když mají matematici operace pro dva objekty, tak se většinou nezastaví a chtějí je pro víc objektů. Ukážeme si standardní cestu, kterou k tomu dospívají. Začneme třemi množinami: Jak bychom vymysleli $A \cap B \cap C$? Protože dvě množiny pronikat umíme, nabízí se dělat tři postupně. Nejprve pronikneme $A \cap B$ a ten výsledek pak s C, formálně zapsáno to je $(A \cap B) \cap C$. To je zajímavý nápad, ale má zádrhel: Proč zrovna takto, proč nezačít třeba $B \cap C$, celkem pak $A \cap (B \cap C)$? V takové chvíli člověka zachrání hlavně asociativní zákon (což je moment, který se vyskytne opakovaně i v dalších kapitolách). Ten říká, že je jedno, které závorkování použijeme, takže nápad, který jsme měli, funguje docela dobře.

Jakmile umíme proniknout tři množiny, není důvod se zastavit a nepřidat množinu čtvrtou, můžeme třeba definovat $A \cap B \cap C \cap D$ jako $(A \cap B \cap C) \cap D$ a díky asociativitě zase víme, že to vyjde nastejno jako třeba $(A \cap B) \cap (C \cap D)$, což je také zajímavá možnost, protože používá jen průniky dvou množin.

Podobně pak uděláme průnik pěti, šesti, 50 atd. množin. Jak to pak ale zapsat pořádně? Nejjednodušší způsob je rekurzí či indukcí, což v zásadě znamená, že se na tu definici díváme od konce (viz ten příklad se čtyřmi

množinami):

$$\bigcap_{i=1}^{n+1} A_i = \Big(\bigcap_{i=1}^{n} A_i\Big) \cap A_{n+1}.$$

Toto je typ definice, který se používá často a zde na to máme speciální kapitolu 5a o indukci a rekurzi (berte to jako první vlaštovku či reklamu). Například chceme-li průnik pěti množin A_1 až A_5, tak vzorec s $n = 4$ říká, že nejprve musíme umět proniknout 4 množiny,

$$A_1 \cap \ldots \cap A_5 = (A_1 \cap \ldots \cap A_4) \cap A_5.$$

Na to podle stejného vzorce, ale s $n = 3$, zase potřebujeme umět proniknout 3 množiny $A_1 \cap A_2 \cap A_3$, odtud už se další iterací konečně dopracujeme k průniku dvou množin $A_1 \cap A_2$, který umíme, tak ho uděláme. Načež následuje „zpětný chod“ naším rozkladem: Výsledek $A_1 \cap A_2$ pronikneme s A_3 (průnik dvou množin umíme), tento výsledek s A_4, ten pak s A_5.

Tento způsob je klasický, spolehlivě zobecňuje asociativní operace na více objektů. Často se povede, že operace, která tak vnikne, má dokonce nějaký rozumný význam. Když si například člověk rozmyslí, které prvky jsou v množině $(A \cap B) \cap C$, tak zjistí, že to jsou přesně ty, které jsou zároveň ve všech třech množinách, podobně se to dá rozmyslet i pro více množin. Naše definice rekurzí tak zachovala hlavní smysl, průnik se ptá na to, co je společné. Podobně bychom mohli rekurzí definovat sjednocení pro více množin a zjistilo by se, že i tato operace funguje stejně jako ta pro dva, sesypává prvky z množin do jedné společné. Nabízí se tak možnost definovat operace pro mnoho množin najednou pomocí velice čitelné podmínky.

Definice.
Nechť $A_1, A_2, \ldots, A_n$ jsou množiny ve stejném universu U. Definujeme

$$\bigcup_{k=1}^{n} A_k = \{x \in U;\ \exists k \in \{1, 2, \ldots, n\} :\ x \in A_k\},$$

$$\bigcap_{k=1}^{n} A_k = \{x \in U;\ \forall k \in \{1, 2, \ldots, n\} :\ x \in A_k\},$$

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n);\ a_1 \in A_1 \wedge a_2 \in A_2 \wedge \ldots \wedge a_n \in A_n\}.$$

Jestliže jde o stejné množiny, tedy $A_i = A$ pro všechna i, pak značíme $A_1 \times A_2 \times \cdots \times A_n = A^n$.

Brzy uvidíme, že definice, kterou jsme nakonec zvolili, je výrazně vhodnější pro důkazy. Pokud bychom totiž operace zobecňovali na více objektů rekurzí, musely by všechny důkazy probíhat matematickou indukcí.

Adoptované definice mají ještě jednu výhodu, u průniku a sjednocení není vůbec důvod se omezovat na konečný počet množin. I když jich budeme mít nekonečně mnoho, pořád je možné se zeptat, zda existují prvky ležící úplně ve všech, popřípadě které prvky jsou v alespoň jedné.

Formálně se takové velké kolekce množin udělají tak, že se indexy k neberou z množin typu $\{1, 2, \ldots, n\}$, ale dovolí se jakákoliv množina indexů I, která může klidně být nekonečná. Jednoduchý příklad: Pro přirozené číslo i definujeme $A_i = \{i, i+1\}$, pak dostáváme nekonečný soubor dvouprvkových množin $\{A_i\}_{i \in \mathbb{N}}$, například $A_{13} = \{13, 14\}$, $A_{42} = \{42, 43\}$) atd.

! **Definice.**
Nechť A_i pro $i \in I$ jsou množiny ve stejném universu U, kde I je nějaká množina indexů. Definujeme

$$\bigcup_{i \in I} A_i = \{x \in U;\ \exists i \in I\colon x \in A_i\},$$

$$\bigcap_{i \in I} A_i = \{x \in U;\ \forall i \in I\colon x \in A_i\}.$$

! **Příklad 2a.c:** Uvažujme $A_i = \{i, i+1\}$ pro $i \in \mathbb{N}$. Nejprve se zamyslíme nad konečnými sjednoceními a průniky.

1) Jako inspiraci si všimneme, že $A_1 \cup A_2 = \{1, 2, 3\}$ a $A_1 \cup A_2 \cup A_3 = \{1, 2, 3, 4\}$, takže si tipneme, že pro $n \in \mathbb{N}$ je $\bigcup_{i=1}^{n} A_i = \{1, 2, 3, \ldots, n, n+1\}$. Důkaz:

$n+1 \in A_n$ a pro $i = 1, \ldots, n$ platí $i \in A_i$, proto $\{1, 2, 3, \ldots, n, n+1\} \subseteq \bigcup_{i=1}^{n} A_i$. Naopak pokud $j \in A_i$ pro nějaké $i = 1, \ldots, n$, tak určitě $i \leq j \leq i+1$, tedy $1 \leq j \leq n+1$. Proto $\bigcup_{i=1}^{n} A_i \subseteq \{1, 2, 3, \ldots, n, n+1\}$.

2) Podobně si vyzkoušíme $A_1 \cap A_2$, $A_1 \cap A_2 \cap A_3$ (zkoušíte to?), pak se zdá jasné, že

$$\bigcap_{i=1}^{n} A_i = \begin{cases} \{1,2\}, & n = 1; \\ \{2\}, & n = 2; \\ \emptyset, & n \geq 3. \end{cases}$$

Důkaz: Pokud $n \geq 3$, pak ten průnik obsahuje prvky společné mimo jiné množinám A_1 a A_3, tedy prvky z množiny $\{1,2\} \cap \{3,4\} = \emptyset$.

3) Teď se podíváme na nekonečné případy.

Protože každé $i \in \mathbb{N}$ leží alespoň v nějaké ze zúčastněných množin (konkrétně $i \in A_i$), dostáváme $\bigcup_{i\in\mathbb{N}} A_i = \mathbb{N}$.

Naopak každé číslo z $\mathbb{N}$ se s většinou našich množin míjí (určitě $i \notin A_j$ pro $j > i$), proto $\bigcap_{i=1}^{\infty} A_i = \emptyset$.

△

V příkladu jsme použili dva způsoby specifikace indexů, $\bigcap_{i\in\mathbb{N}}$ a $\bigcap_{i=1}^{\infty}$, jsou rovnocenné a můžete si vybrat. Pokud je I jasné z kontextu, tak jeho specifikaci někdy vynecháváme a píšeme jen $\bigcup A_i$ či $\bigcap A_i$.

Příklad 2a.d: Množina indexů může být opravdu veliká. Nechť $I = \mathbb{R}$. Pro libovolné reálné číslo r definujeme C_r jako množinu všech číslic, které se při zápisu r (v desítkové soustavě) použily. Například $C_{1.07} = \{0,1,7\}$, také víme, že $17/6 = 2.83333...$, proto $C_{17/6} = \{2,3,8\}$, a $C_\pi = \{0,1,2,3,4,5,6,7,8,9\}$. Dostáváme opravdu velký soubor množin $\{C_r\}$, ještě uvidíme, že je mnohem větší než ten z předchozího příkladu.

Protože je každá číslice použita v nějakém reálném čísle, je $\bigcup_{r\in\mathbb{R}} C_r = \{0,1,2,3,4,5,6,7,8,9\}$. Žádná cifra ale není ve všech číslech, proto $\bigcap_{r\in\mathbb{R}} C_r = \emptyset$.

△

Příklad 2a.e: Představme si, že I je množina všech molekul v mém těle (asi tedy bude konečná, ale neptejte se mě, kolik má prvků, ono se to i každou chvíli mění, raději do toho nebudeme vrtat).

Je-li i jedna taková molekula, pak M_i nechť je množina všech atomů, ze kterých se tato molekula skládá. Pak $\bigcup M_i$ je množina všech prvků, které jsou ve mne obsaženy, protože víme, že při tom sjednocování se ve výsledné množině opakované výskyty atomů ignorují a za každý typ atomu zůstane jen jeden zástupce.

Dobrá otázka je, jak vypadá $\bigcap M_i$. Možná tam bude uhlík, taky může být průnik prázdný, ale to je spíš otázka pro biology než matematiky.

△

Příklad 2a.f: Nechť $I = \mathbb{R}$. Pro $x \in I$ nechť L_x je množina všech lidí, která považuje x za své šťastné číslo. Pak $\bigcup L_x$ je množina všech číselně povědomých lidí a $\bigcap L_x$ je množina všech lidí, pro které je šťastné každé číslo.

△

Máme krásnou obecnou definici a teď ukážeme, že to hlavní se tím nezkazilo.

! **Věta 2a.8.** (de Morganovy zákony)
Nechť A_i pro $i \in I$ jsou množiny ve stejném universu U, kde I je nějaká množina indexů. Pak

$$\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A}_i \qquad \text{a} \qquad \overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A}_i.$$

Důkaz (rutinní, poučný)**:** Nejprve dokážeme první vztah, a to dlouze a komentovaně:

Prvek x leží v $\overline{\bigcup A_i}$ právě tehdy (podle definice doplňku), když neleží v $\bigcup A_i$, což je (podle definice sjednocení) právě tehdy, když není pravda, že existuje i, aby $x \in A_i$. Výraz $\neg(\exists i \in I\colon x \in A_i)$ je podle pravidel logiky totéž jako $\forall i \in I\colon \neg(x \in A_i)$, tedy x neleží v žádném A_i, což je (podle definice doplňku) právě tehdy, když leží ve všech $\overline{A}_i$, což je (podle definice průniku) právě tehdy, když leží v $\bigcap \overline{A}_i$.

Ukázali jsme, že $x \in \overline{\bigcup A_i} \iff x \in \bigcap \overline{A}_i$, čímž je rovnost těchto dvou množin dokázána.

Druhý vztah dokážeme v zásadě stejným důkazem, teď jej ale zapíšeme čistě symbolicky, abyste si procvičili překlad do lidštiny.

$$x \in \overline{\bigcap A_i} \iff x \notin \bigcap A_i \iff \neg\big(x \in \bigcap A_i\big) \iff \neg(\forall i \in I:\ x \in A_i)$$
$$\iff \exists i \in I:\ \neg(x \in A_i) \iff \exists i \in I:\ x \notin A_i \iff \exists i \in I:\ x \in \overline{A}_i \iff x \in \bigcup \overline{A}_i.$$

□

Ten druhý důkaz byl tedy opravdu úsporný, kdyby se tak psaly matematické knihy, tak by vážily čtvrtinu. Nevýhoda by byla, že by je nikdo nedokázal rozumně číst, ani matematici ne, protože i je by zdržoval překlad z matematičtiny do lidštiny, pro začátečníka by pak byly zcela nesrozumitelné. Klasické důkazy v knihách jsou tedy obvykle jakýmsi kompromisem mezi tím ukecaným a tím stručným výše.

Platí i distributivní zákon pro mnoho množin, viz cvičení 2a.5.

Poznámka: Všimněte si, že jsme nedefinovali množinový rozdíl pro více množin. Důvod je jednoduchý, odečítání není asociativní, tudíž nevíme, jak vlastně dělat $A - B - C$ (viz cvičení 2a.2 (ix)). Obdobně to ostatně funguje s čísly, umíme počítat $3 + 7 + 13$, ale co je $3/7/13$? Problém je právě v nedostatku asociativity, výrazy $(3/7)/13$ a $3/(7/13)$ nejsou stejné.
△

Na závěr ještě doplníme jednu definici.

! **Definice.**
Množiny A, B se nazývají **disjunktní**, jestliže $A \cap B = \emptyset$.

To je velice užitečný pojem, až budeme dělat kombinatoriku, tak se bez něj neobejdeme.

Zjímavá otázka: Má smysl definovat tento pojem i pro více množin? Šlo by to udělat a říct, že množiny A_i jsou disjunktní, pokud mají prázdný průnik. V praxi se to ale nepoužívá, protože se ukazuje, že by tato podmínka o množinách mnoho neřekla. Proč tomu tak je?

Představme si několik množin $A_1, \dots, A_n$. Pokud by náhodou platilo $A_1 \cap A_2 = \emptyset$, tak už automaticky také $\bigcap A_i = \emptyset$. To znamená, že nám pak informace $\bigcap A_i = \emptyset$ vlastně vůbec neříká o množinách $A_2, \dots, A_n$. Pro většinu aplikací je proto tato informace nedostatečná.

Pokud chceme vyjádřit, že nějaké množiny spolu nemají nic společného, pak většinou potřebujeme jinou frázi: Chce se, aby množiny A_i byly **po dvou disjunktní**, což znamená, že $A_i \cap A_j = \emptyset$ pro libovolné $i \neq j$. Tato podmínka odpovídá situaci, kterou si ve Vennově diagramu představíme jako zcela separátní kroužky.

! 2a.9 Reprezentace množin v počítačích

Nekonečně mnoho dat počítač nespolkne, takže už z principu budeme v počítačích pracovat s množinami konečnými. Existuje pak jednoduchý způsob, jak si je reprezentovat. Začneme tím, že vezmeme konečné universum a jeho prvky si očíslujeme, $U = \{u_1, \dots, u_n\}$. Každá podmnožina A tohoto universa se pak dá jednoduše zakódovat jako binární řetězec (číslo) délky n tak, že i-tá cifra je 1, pokud $u_i \in A$, jinak je to nula.

Například v universu $U = \{u_1 = 1, u_2 = 13, u_3 = a, u_4 = \diamond, u_5 = 23\}$ se množina $A = \{13, 23\}$ zakóduje jako 01001, popřípadě 10010, podle toho, jestli jsme si vybrali kódování (čtení řetězce) zprava doleva nebo naopak. V zásadě je to jedno, jen se pak toho kódování musíme už pořád držet `:-)`.

Jednou z velkých výhod této reprezentace je, že se pak krásně dělají množinové operace pomocí logických operací na bitech odpovídajících kódovacích řetězců. Sjednocení množin odpovídá logická disjunkce jednotlivých bitů, naopak průnik je přesně konjunkce neboli obyčejné binární násobení bitů. To jsou operace, které má počítač rád, takže je všechno v pohodě.

S 2a.10 Poznámka (jak psát a číst důkazy): Přichází cvičení a čtenář by měl začít psát důkazy. O stránce logické jsme již psali i v předchozí kapitole, zde se zaměříme na jedno pomocné hledisko. Chybně napsaný důkaz lze často odhalit i tím, že jej prostě nelze přečíst jako text. I matematický důkaz totiž musí dávat české věty (podmět, přísudek a tak podobně). Pro začátečníka je toto důležité zejména v situaci, kdy se rozhodne ušetřit čas použitím matematických symbolů.

Pořád platí, že když symboly zase nahradíme odpovídajícími slovy, musí vzniknout rozumný text. To se týká zejména symbolu $\implies$, který běžně používáme ve významu „z toho nalevo vyplývá to napravo“, neboli $A \implies B$ čteme například jako „platí A, proto také platí B“.

Zkusme si česky přečíst něco, co autor skripta potkal v písemce:

$\forall x \implies x > 2$.

Česky například „Pro každé x, z toho vyplývá, že $x > 2$“.

Člověk ani nemusí umět matematiku, aby jej napadlo, že je něco špatně. Je tedy dobré si po zapsání svůj argument zkusit říct slovy. Pokud to nefunguje, je někde problém, třeba jen v zápise.

Další úroveň, na které důkaz musí dávat smysl, je úroveň pojmová. Zacitujme opět z jedné písemky:

Protože $A \cap B$, musí být $A \subseteq B$.

Toto je implikace, tudíž by člověk čekal, že po slově „protože“ bude nějaký pravdivý fakt, ze kterého se pak něco dále dovodí. Jenže $A \cap B$ není fakt, není to něco, co může být pravda či nepravda. To je operace, jejímž výsledkem je nějaká množina. Dotyčná věta tedy nedává smysl již na úrovni pojmů, ani se nemusíme zamýšlet nad tím, co se říká v její druhé půlce. Kdyby tam ale bylo třeba „$A \cap B$ je něco“, tak už to je výrok (buď je to pravda nebo ne, podle toho, co je to „něco“) a věta není vykloubená (což ještě neznamená, že je celá implikace pravdivá, to je ta další a rozhodující úroveň, na které to musí fungovat.

Teď přijdou cvičení a jejich řešení jsou často psána vysoce kondenzovaně. Čtenář si tak může procvičit překlad těchto úvah do češtiny, mělo by to vždy rozumně jít.

△

Cvičení

Cvičení 2a.1 (rutinní^o, zkouškové*, dobré*, poučné$^+$)**:** Pravidel pro množinové operace je mnohem víc, než jsme uvedli v textu. Dokažte následující:

Nechť A, B, C jsou množiny v univerzu U. Pak platí:

(i)^o $A - B \subseteq A$;

(ii)$^{o*+}$ $A - B = A \cap \overline{B}$;

(iii)* $A \cap (B - A) = \emptyset$;

(iv)* $(A - B) \cap (B - C) = \emptyset$;

(v)* $(A - B) - C \subseteq A - C$;

(vi)$^{\star+}$ $A \cup (B - A) = A \cup B$;

(vii)$^{*+}$ $(A \cup B) - C = (A - C) \cup (B - C)$;

(viii)$^{*+}$ $A - (B \cup C) = (A - B) \cap (A - C)$;

(ix)$^{*+}$ $A - (B \cap C) = (A - B) \cup (A - C)$;

(x)$^{\star\star+}$ $A \cap (B - C) = (A \cap B) - (A \cap C)$;

(xi)$^{\star+}$ $A \subseteq B$ právě tehdy, když $\overline{B} \subseteq \overline{A}$;

(xii)$^{\star+}$ $A \subseteq B$ právě tehdy, když $A \cap B = A$;

(xiii)$^{\star+}$ $A \subseteq B$ právě tehdy, když $A \cup B = B$;

(xiv) $P(A) \subseteq P(B) \implies A \subseteq B$.

Poznámka: Všimněte si, že ve třech případech se jedná o distributivní zákon. Bod (vii) ukazuje, že $-$ umí roznásobit závorku se sjednocením zprava, ale v (viii) vidíme, že zleva už to nejde, tam je třeba vzorec upravit. Bod (ix) ukazuje, že $\cap$ umí roznásobit závorku s odčítáním, pro další kombinace operací se podívejte do následujícího cvičení.

Cvičení 2a.2 (poučné, zkouškové*, dobré*)**:** Rozhodněte, zda pro libovolné množiny A, B, C platí následující vztahy. Pak buď příslušný vztah dokažte, nebo dokažte, že neplatí.

V případě, že rovnost neplatí, rozmyslete si, jestli nebude platit alespoň nějaká inkluze, a tu dokažte.

Poznámka: Některé důkazy jsou dosti trikové, ale u všech příkladů byste měli být schopni určit, zda uvedená rovnost platí, popřípadě která inkluze platí. Dobré důkazy klidně vynechte. Mimochodem, v bodech (viii)-(xii) zkoumáme platnost různých verzí distributivního zákona.

(i)* $(A - B) \cup B = A$;

(ii)* $(A \cap B) \cup (A \cap \overline{B}) = A$;

(iii)* $(A - B) - C = (A - C) - B$.

(iv)** $(A - B) - C = A - (B - C)$;

(v)* $(A - B) \cup (B - C) = A - C$;

(vi)* $P(A \cap B) = P(A) \cap P(B)$;

(vii)* $P(A \cup B) = P(A) \cup P(B)$;

(viii)* $A \cup (B - C) = (A \cup B) - (A \cup C)$;

(ix)* $A - (B \cap C) = (A - B) \cap (A - C)$;

(x)* $A - (B \cup C) = (A - B) \cup (A - C)$;

(xi): $(A \cap B) - C = (A - C) \cap (B - C)$;

(xii): $(A \cup B) - C = (A - C) \cup (B - C)$;

(xiii)* $(A - B) - C = (A - C) - (B - C)$.

Cvičení 2a.3 (rutinní)**:** Nechť A, B, C, D jsou množiny. Platí $(A - B) - (C - D) = (A - C) - (B - D)$? Svou odpověď zdůvodněte.

Cvičení 2a.4 (poučné)**:** Uvažujme množinu indexů $I = \mathbb{N}$ a množiny M_i pro $i \in I$. Najděte výsledky operací $\bigcup_{i=1}^{n} M_i$, $\bigcup_{i=1}^{\infty} M_i$, $\bigcap_{i=1}^{n} M_i$ a $\bigcap_{i=1}^{\infty} M_i$, jestliže
(i) $M_i = \{1, 2, 3, ..., i\}$ pro $i \in \mathbb{N}$;
(ii) $M_i = \{i, i+1, i+2, \dots\}$ pro $i \in \mathbb{N}$.

Cvičení 2a.5 (poučné)**:** Nechť A a A_i pro $i \in I$ jsou množiny v universu U. Dokažte, že pak platí následující:
(i) $A \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I}(A \cap A_i)$;
(ii) $A \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I}(A \cup A_i)$.

Cvičení 2a.6 (poučné)**:** Uvažujme množinu indexů $I = \mathbb{R}^+ = (0, \infty)$ a množiny M_r pro $r \in I$. Najděte $\bigcup_{r\in I} M_r$ a $\bigcap_{r\in I} M_r$, jestliže
(i) $M_r = (-r, 13 + r)$;
(ii) $M_r = \langle -r, 13 + r\rangle$;
(iii) $M_r = (-r, r)$.

Cvičení 2a.7 (poučné)**:** Uvažujme množiny indexů $I = (0, 1)$ a $J = \langle 0, 1\rangle$. Najděte $\bigcup_{r\in I} M_r$ a $\bigcap_{r\in I} M_r$, $\bigcup_{r\in J} M_r$ a $\bigcap_{r\in J} M_r$, jestliže
(i) $M_r = (-r, 13 + r)$;
(ii) $M_r = \langle -r, 13 + r\rangle$.

Řešení:
2a.1: (i): $\forall x \in A - B$: $x \in A \wedge x \notin B \implies x \in A$.
(ii): Zkusíme oba směry najednou: $x \in A - B \iff x \in A \wedge x \notin B \iff x \in A \wedge x \in \overline{B} \iff A \cap \overline{B}$.
(iii): Sporem, existuje $x \in A \cap (B - A)$, pak $x \in A \wedge x \in (B - A) \implies x \in A \wedge (x \in B \wedge x \notin A) \implies x \in A \wedge x \notin A$, spor.
(iv): Sporem, existuje $x \in (A - B) \cap (B - C)$, pak $x \in (A - B) \wedge x \in (B - C) \implies$
$(x \in A \wedge x \notin B) \wedge (x \in B \wedge x \notin C) \implies x \in B \wedge x \notin B$, spor.
Nebo pomocí (ii): $(A - B) \cap (B - C) = (A \cap \overline{B}) \cap (B \cap \overline{C}) = A \cap (\overline{B} \cap B) \cap \overline{C} = A \cap \emptyset \cap \overline{C} = \emptyset$.
(v): $x \in (A - B) - C \implies (x \in A \wedge x \notin B) \wedge x \notin C \implies x \in A \wedge x \notin C \implies x \in A - C$.
Nebo pomocí (ii): $(A - B) - C = (A \cap \overline{B}) \cap \overline{C} = (A \cap \overline{C}) \cap \overline{B} \subseteq A \cap \overline{C} = A - C$.
(vi): Dokázat dvě inkluze. 1) $A \cup (B - A) \subseteq A \cup B$: $\forall x \in A \cup (B - A)$: $x \in A \vee x \in (B - A)$
$\implies x \in A \vee (x \in B \wedge x \notin A) \implies x \in A \vee x \in B \implies x \in A \cup B$.
2) $A \cup B \subseteq A \cup (B - A)$: $\forall x \in A \cup B$: $x \in A \vee x \in B$. Rozdělíme na případy. Pokud $x \in A$, pak $x \in A \cup (B - A)$. Pokud $x \in B$, tak zase dva případy. Jestliže $x \in B \wedge x \in A$, pak $x \in A$ a přejdeme na předchozí. Jestliže $x \in B \wedge x \notin A$, pak $x \in B - A \implies x \in A \cup (B - A)$.
Nebo pomocí (ii): $A \cup (B - A) = A \cup (B \cap \overline{A}) = (A \cup B) \cap (A \cup \overline{A}) = (A \cup B) \cap U = A \cup B$.
(vii): Zkusíme oba směry najednou pomocí distributivního zákona pro formální logiku: $x \in (A \cup B) - C \iff$
$(x \in A \vee x \in B) \wedge x \notin C \iff (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C) \iff x \in (A - C) \vee x \in (B - C) \iff$
$x \in (A - C) \cup (B - C)$.
Snažší varianta pomocí (ii): $(A \cup B) - C = (A \cup B) \cap \overline{C} = (A \cap \overline{C}) \cup (B \cap \overline{C}) = (A - C) \cup (B - C)$.
(viii): Zkusíme oba směry najednou pomocí distributivního zákona a deMorganova zákona pro formální logiku:
$A - (B \cup C) \iff x \in A \wedge \neg(x \in B \cup C) \iff x \in A \wedge \neg(x \in B \vee x \in C) \iff$
$x \in A \wedge \neg(x \in B) \wedge \neg(x \in C) \iff x \in A \wedge x \in A \wedge \neg(x \in B) \wedge \neg(x \in C) \iff$
$(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \iff x \in (A - B) \wedge x \in (A - C) \iff x \in (A - B) \cap (A - C)$.
Snažší varianta pomocí (ii) a deMorgana pro množiny:
$A - (B \cup C) = A \cap \overline{B \cup C} = A \cap \overline{B} \cap \overline{C} = A \cap A \cap \overline{B} \cap \overline{C} = (A \cap \overline{B}) \cap (A \cap \overline{C}) = (A - B) \cap (A - C)$.
(ix): Zkusíme oba směry najednou pomocí distributivního zákona a deMorganova zákona pro formální logiku:
$A - (B \cap C) \iff x \in A \wedge \neg(x \in B \cap C) \iff x \in A \wedge \neg(x \in B \wedge x \in C) \iff$
$x \in A \wedge (\neg(x \in B) \vee \neg(x \in C)) \iff (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \iff x \in (A - B) \vee x \in (A - C) \iff$
$(A - B) \cup (A - C)$.
Snažší varianta pomocí (ii) a deMorgana pro množiny:
$A - (B \cap C) = A \cap \overline{B \cap C} = A \cap (\overline{B} \cup \overline{C}) = (A \cap \overline{B}) \cup (A \cap \overline{C}) = (A - B) \cup (A - C)$.
(x): Tento důkaz je jedním směrem relativně snadný a používá distributivní zákon, těžší je najít směr opačný. Ukáže se, že ten snadný směr je vlastně ekvivalentní a funguje i naopak (rozmyslete si).

$x \in (A \cap B) - (A \cap C) \iff x \in A \cap B \wedge \neg(x \in A \cap C) \iff x \in A \cap B \wedge \neg(x \in A \wedge x \in C) \iff$
$(x \in A \wedge x \in B) \wedge (x \notin A \vee x \notin C) \iff [(x \in A \wedge x \in B) \wedge x \notin A] \vee [(x \in A \wedge x \in B) \wedge x \notin C] \iff$
$[x \in A \wedge x \notin A \wedge x \in B] \vee [x \in A \wedge (x \in B \wedge x \notin C)] \iff [F \wedge x \in B] \vee [x \in A \wedge x \in (B - C)] \iff$
$F \vee [x \in A \cap (B - C)] \iff x \in A \cap (B - C)$.
(xi): 1) Předpoklad $A \subseteq B$, chceme $\forall b \in \overline{B}$: $b \in \overline{A}$. Jedna možnost sporem: Nechť existuje $b \in \overline{B}$ takové, že $b \notin \overline{A}$. Pak $b \in A$, podle předpokladu $b \in B$. Takže $b \in \overline{B} \wedge b \in B$, spor.
Alternativa: Předpoklad říká $\forall x$: $x \in A \implies x \in B$. Přejdeme k ekvivalentní obměně: $\forall x$: $x \notin B \implies x \notin A$ neboli $\forall x$: $x \in \overline{B} \implies x \in \overline{A}$, přesně jak potřebujeme.
2) Předpoklad $\overline{B} \subseteq \overline{A}$, chceme $A \subseteq B$. Podle 1) plyne z předpokladu $\overline{\overline{A}} \subseteq \overline{\overline{B}}$, což je právě $A \subseteq B$.
(xii): 1) Předpoklad $A \subseteq B$, chceme $A \cap B = A$. Ukážeme dvě inkluze.
Důkaz $A \cap B \subseteq A$: $\forall x \in A \cap B$: $x \in A \wedge x \in B \implies x \in A$.
Důkaz $A \subseteq A \cap B$: $\forall a \in A$: $a \in B$ dle předpokladu. Proto $a \in A \wedge a \in B \implies a \in A \cap B$.
2) Předpoklad $A \cap B = A$, chceme $A \subseteq B$. Důkaz:
$\forall a \in A$: $a \in A \cap B$ dle předpokladu, proto $a \in A \wedge a \in B \implies a \in B$.
(xiii): 1) Předpoklad $A \subseteq B$, chceme $A \cup B = B$. Ukážeme dvě inkluze. Důkaz $A \cup B \subseteq B$:
$\forall x \in A \cup B$: $x \in A \vee x \in B$, ale předpoklad dává, že i v případě $a \in A$ je $a \in B$, proto každopádně $x \in B$.
Důkaz $B \subseteq A \cup B$: $\forall b \in B$: $a \in B \implies a \in A \wedge a \in B \implies a \in A \cup B$.
2) Předpoklad $A \cup B = B$, chceme $A \subseteq B$. Důkaz: $\forall a \in A$: $a \in A \cup B = B$ dle předpokladu, proto $a \in B$.
(xiv): Předpoklad říká, že prvky $P(A)$ jsou i prvky $P(B)$, zde je zásadní si uvědomit, že množina $P(A)$ má jako prvky podmnožiny A. Chceme ukázat, že prvky z A jsou v B:
$a \in A \implies \{a\} \subseteq A \implies \{a\} \in P(A) \implies \{a\} \in P(B) \implies \{a\} \subseteq B \implies a \in B$.
2a.2: (i): Protipříklad: třeba $A = \emptyset$, $B = \{13\}$. Platí ale $A \subseteq (A - B) \cup B$: Nechť $a \in A$ libovolné. Dvě možnosti: $x \in B$, pak $x \in (A - B) \cup B$, nebo $x \notin B$, pak $x \in A \wedge x \notin B \implies x \in (A - B) \implies x \in (A - B) \cup B$.
Formální důkaz: $x \in A \iff x \in A \wedge T \iff x \in A \wedge (x \notin B \vee x \in B) \iff$
$(x \in A \wedge x \notin B) \vee (x \in A \wedge x \in B) \implies x \in (A - B) \vee x \in B \implies x \in (A - B) \cup B$.
(ii): Platí. Dvě inkluze. $(A \cap B) \cup (A \cap \overline{B}) \subseteq A$: $x \in (A \cap B) \cup (A \cap \overline{B}) \implies x \in (A \cap B) \vee x \in (A \cap \overline{B}) \implies$
$x \in A \vee x \in A \implies x \in A$.
$A \subseteq (A \cap B) \cup (A \cap \overline{B})$: Nechť $x \in A$. Dvě možnosti. Pokud $x \in B$, pak $x \in A \wedge x \in B \implies x \in (A \cap B) \implies$
$x \in (A \cap B) \cup (A \cap \overline{B})$. Nebo $x \notin B$, pak $x \in A \wedge x \notin B \implies x \in (A \cap \overline{B}) \implies x \in (A \cap B) \cup (A \cap \overline{B})$.
(iii): Platí, důkaz obou směrů najednou: $x \in (A - B) - C \iff x \in (A - B) \wedge x \notin C \iff$
$(x \in A \wedge x \notin B) \wedge x \notin C \iff (x \in A \wedge x \notin C) \wedge x \notin B \iff x \in (A - C) \wedge x \notin B \iff x \in (A - C) - B$.
(iv) Protipříklad: $A = B = C = \{1\}$. Platí ale $(A - B) - C \subseteq A - (B - C)$ (důkaz dost trikový):
$x \in (A - B) - C \implies x \in (A - B) \wedge x \notin C \implies x \in A \wedge x \notin B \wedge x \notin C \implies x \in A \wedge x \notin B$
$\implies x \in A \wedge x \notin B \vee x \in C \implies x \in A \wedge \neg(x \in B \wedge x \notin C) \implies x \in A \wedge \neg[x \in (B - C)]$
$\implies x \in A \wedge x \notin (B - C) \implies x \in A - (B - C)$.
(v): Protipříklad: třeba $A = C = \emptyset$, $B = \{13\}$. Platí ale $A - C \subseteq (A - B) \cup (B - C)$: $x \in A - C \implies x \in A \wedge x \notin C$.
Dvě možnosti. Pokud $x \in B$, tak $x \in A \wedge x \in B \wedge x \notin C \implies x \in B \wedge x \notin C \implies x \in (B - C) \implies$
$x \in (A - B) \cup (B - C)$.
Nebo $x \notin B$, pak $x \in A \wedge x \notin B \wedge x \notin C \implies x \in A \wedge x \notin B \implies x \in (A - B) \implies x \in (A - B) \cup (B - C)$.
(vi): Platí, dokážeme dvě inkluze. 1) $P(A \cap B) \subseteq P(A) \cap P(B)$: Nechť $x \in P(A \cap B)$, pak x je vlastně podmnožina $A \cap B$. Proto $x \subseteq A \wedge x \subseteq B \implies x \in P(A) \wedge x \in P(B) \implies x \in P(A) \cap P(B)$.
2) $P(A) \cap P(B) \subseteq P(A \cap B)$: $x \in P(A) \cap P(B) \implies x \in P(A) \wedge x \in P(B) \implies x \subseteq A \wedge x \subseteq B \implies$
$x \subseteq A \cap B \implies x \in P(A \cap B)$.
(vii): Protipříklad: třeba $A = \{1, 2\}$, $B = \{3, 4\}$. Pak množina $M = \{2, 3\}$ leží v $P(A \cup B)$, ale není ani v $P(A)$, ani v $P(B)$, tedy není v jejich sjednocení. Platí ale $P(A) \cup P(B) \subseteq P(A \cup B)$:
$x \in P(A) \cup P(B) \implies x \in P(A) \vee x \in P(B) \implies x \subseteq A \vee x \subseteq B \implies x \subseteq A \cup B \implies x \in P(A \cup B)$.
(viii): Protipříklad: $A = \{13\}$, $B = C = \emptyset$. Platí ale $(A \cup B) - (A \cup C) \subseteq A \cup (B - C)$: $x \in (A \cup B) - (A \cup C) \iff$
$(x \in A \vee x \in B) \wedge \neg(x \in A \vee x \in C) \iff (x \in A \vee x \in B) \wedge (x \notin A \wedge x \notin C) \iff$
$(x \in A \wedge x \notin A \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C) \implies F \vee (x \in (B - C)) \iff x \in (B - C) \implies$
$x \in A \cup (B - C)$.
(ix): Protipříklad: $A = B = \{1\}$, $C = \emptyset$. Platí ale $(A - B) \cap (A - C) \subseteq A - (B \cap C)$: $x \in (A - B) \cap (A - C) \iff$
$x \in (A - B) \wedge x \in (A - C) \iff x \in A \wedge x \notin B \wedge x \in A \wedge x \notin C \iff x \in A \wedge (\neg x \in B \wedge \neg x \in C) \implies$
$x \in A \wedge (\neg x \in B \vee \neg x \in C) \iff x \in A \wedge \neg(x \in B \wedge x \in C) \iff$
$x \in A \wedge \neg(x \in B \cap C) \iff x \in A \wedge x \notin (B \cap C) \iff x \in A - (B \cap C)$.
(x): Protipříklad: $A = B = \{1\}$, $C = \emptyset$. Platí ale $A - (B \cup C) \subseteq (A - B) \cup (A - C)$: $x \in A - (B \cup C) \iff$
$x \in A \wedge x \notin (B \cup C) \iff x \in A \wedge \neg(x \in B \cup C) \iff x \in A \wedge \neg(x \in B \vee x \in C) \iff$
$x \in A \wedge x \notin B \wedge x \notin C) \iff (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \iff x \in (A - B) \wedge x \in (A - C) \implies$

$x \in (A-B) \vee x \in (A-C) \iff x \in (A-B) \cup (A-C)$.
(xi): Platí, zkusíme oba směry najednou, začneme od složitějšího: $x \in (A-C) \cap (B-C) \iff$
$x \in (A-C) \wedge x \in (B-C) \iff (x \in A \wedge x \notin C) \wedge (x \in B \wedge x \notin C) \iff x \in A \wedge x \notin C \wedge x \in B \wedge x \notin C \iff$
$x \in A \wedge x \in B \wedge x \notin C \iff x \in (A \cap B) \wedge x \notin C \iff x \in (A \cap B) - C$.
(xii): Platí, zkusíme oba směry najednou: $x \in (A \cup B) - C \iff x \in (A \cup B) \wedge x \notin C \iff$
$(x \in A \vee x \in B) \wedge x \notin C \iff (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C) \iff x \in (A-C) \vee x \in (B-C) \iff$
$x \in (A-C) \cup (B-C)$.
(xiii): Platí, zkusíme oba směry najednou, začneme od složitějšího: $x \in (A-C) - (B-C) \iff$
$x \in (A-C) \wedge x \notin (B-C) \iff (x \in A \wedge x \notin C) \wedge \neg(x \in B \wedge x \notin C) \iff (x \in A \wedge x \notin C) \wedge (x \notin B \vee x \in C) \iff$
$(x \in A \wedge x \notin C \wedge x \notin B) \vee (x \in A \wedge x \notin C \wedge x \in C) \iff (x \in A \wedge x \notin C \wedge x \notin B) \vee (x \in A \wedge F) \iff$
$(x \in A \wedge x \notin C \wedge x \notin B) \vee F \iff x \in A \wedge x \notin C \wedge x \notin B \iff (x \in A \wedge x \notin B) \wedge x \notin C \iff$
$(x \in (A-B) \wedge x \notin C \iff x \in (A-B) - C$.
2a.3: Neplatí, intuitivně vidíme, že vlevo odebíráme celé C, zatímco vpravo jen zmenšené C, na tomto pocitu zkusíme založit protipříklad: $A = C = D = \{13\}$, $B = \emptyset$.
2a.4: (i): $\{1, 2, 3, \dots, n\}$, $\mathbb{N}$, $\{1\}$, $\{1\}$.
(ii): $\mathbb{N}$, $\mathbb{N}$, $\{n, n+1, n+2, n+3, \dots\}$, $\emptyset$.
2a.5: (i): $x \in A \cap \bigcup_{i \in I} A_i \iff x \in A \wedge x \in \bigcup_{i \in I} A_i \iff x \in A \wedge \big(\exists i \in I\colon x \in A_i\big) \iff$
$\exists i \in I\colon (x \in A \wedge x \in A_i) \iff \exists i \in I\colon (x \in A \cap A_i) \iff x \in \bigcup_{i \in I} (A \cap A_i)$.
(ii): $x \in A \cup \bigcap_{i \in I} A_i \iff x \in A \vee x \in \bigcap_{i \in I} A_i \iff x \in A \vee \big(\forall i \in I\colon x \in A_i\big) \iff \forall i \in I\colon (x \in A \vee x \in A_i) \iff$
$\forall i \in I\colon (x \in A \cup A_i) \iff x \in \bigcap_{i \in I} (A \cup A_i)$.
2a.6: (i): $\mathbb{R}$, $\langle 0, 13\rangle$; (ii): $\mathbb{R}$, $\langle 0, 13\rangle$; (iii): $\mathbb{R}$, $\{0\}$.
2a.7: (i): $(-1, 14)$, $\langle 0, 13\rangle$, $(-1, 14)$, $(0, 13)$; (ii): $(-1, 14)$, $\langle 0, 13\rangle$, $\langle -1, 14\rangle$, $\langle 0, 13\rangle$.

2b. Zobrazení

Z kapitoly 2a známe pojem množiny, který nám v zásadě umožní vyjádřit to, že něco máme či nemáme. Často jsme ale v situaci, že máme nějaké objekty a mezi těmito objekty existují určité vztahy. Abychom tuto situaci mohli zkoumat, potřebujeme matematickou strukturu, která ony vztahy dokáže zachytit. Takové struktury existují, dokonce je jich více, aby dokázaly správně zachytit různé typy vztahů.

Zde se soustředíme na vztah, který má podobu jednoduchého přiřazení. Například každý člověk má rodné číslo. Matematicky to vidíme tak, že máme množinu lidí A a množinu čísel B a každému člověku z množiny A přiřadíme právě jedno číslo z množiny B. Tím vzniká vztah. Podobně funguje třeba přiřazení, které každému místu na zemi dává souřadnici GPS, či přiřazení, které každému konkrétnímu zvířeti (savci) přiřadí jeho pohlaví.

Tím se dostáváme k pojmu zobrazení, což je jeden ze základních matematických nástrojů. Všimněme si, že tento pojem nebude schopen obsáhnout například situaci, která každému žákovi přiřadí učitele, který jej učí, protože takových učitelů je více. My bychom samozřejmě mohli definici zobrazení udělat tak, aby umožňovala přiřazovat více objektů, ale tím by vznikl pojem, který se chová úplně jinak, na takovéto situace máme jiné nástroje.

Student se s pojmem podobným zobrazení již setkal, když pracoval s funkcemi. Tato zkušenost mu zde pomůže, ale neměl by na ni spoléhat až příliš. Hodně středoškoláků si ze školy odnáší představu, že funkce je vzoreček, a právě na toto je třeba rychle zapomenout. Mnohem lepší je dívat se na funkci jako na černou skříňku, které podstrčíme číslo a ona na oplátku jiné vydá. Když máme velké štěstí, tak se tento proces dá vyjádřit vzorečkem, ale rozhodně se na to nedá spoléhat.

Jednoduchý příklad pro čtenáře, pro které je to nové: Definujme funkci f následovně. Jestliže je reálné číslo x vyjádřitelné jako desetinné číslo s konečným rozvojem, pak je hodnota $f(x)$ dáno jako ta cifra, která se v jeho zápise vyskytuje nejčastěji; pokud by byla plichta, bere se nejmenší taková cifra. Pokud se x nedá vyjádřit pomocí konečného desetinného rozvoje, pak definujeme $f(x) = 0$. Touto definicí je f definováno pro všechna reálná čísla, třeba $f(146824834) = 4$, $f(714.397721) = 7$, $f(0.333) = 3$, naopak $f(\pi) = 0$ či třeba $f\left(\frac{1}{3}\right) = 0$. Je to naprosto normální funkce, jen ji nelze vyjádřit vzorečkem.

Smiřme se tedy s tím, že funkce je jakékoliv posílátko, které bere čísla a posílá je na jiná čísla. Jak ale takovou funkci reprezentovat matematicky, když nemůžeme spoléhat na vzoreček? Nejjednodušší je představit si, že je funkce dána množinou uspořádaných párů (počáteční bod,cílový bod), což vlastně přesně odpovídá grafu. Tento způsob nás vrací zpět k množinám, což je objekt, se kterým umíme pracovat, je to tedy perspektivní představa.

Když se na funkce podíváme tímto způsobem, hned se nabídne nápad, že by se nemusela posílat jen čísla, ale i jiné objekty, můžeme si klidně představit třeba černou skříňku, které dáváme písmenka a ona na oplátku vydává třeba různá lízátka. I fungování takovéto skříňky by šlo (přinejmenším teoreticky) zachytit jako množinu dvojic (písmenko,lízátko). Tím se dostáváme k obecné definici.

Definice.
Nechť A, B jsou neprázdné množiny. Definujeme **zobrazení** z A do B jako libovolnou podmnožinu T množiny $A \times B$ splňující

$$\forall a \in A\ \exists! b \in B\colon (a,b) \in T.$$

Fakt $(a,b) \in T$ značíme $T(a) = b$.
Množina A je **definiční obor** T, značeno $D(T)$, množina B je cílová množina T. Definujeme také **obor hodnot** T jako

$$R(T) = \{b \in B;\ \exists a \in A\colon T(a) = b\} = \{T(a);\ a \in A\}.$$

By a **mapping** we mean any subset T of $A \times B$ satisfying the following condition: For every $a \in A$ there is exactly one $b \in B$ such that $(a,b) \in T$. We denote this $T(a) = b$. The set A is called the **domain** of T, denoted $D(T)$, and the set B is called the **codomain** of T. We also define the **range** of T as $R(T) = \{T(a);\ a \in A\}$.

Připomínáme, že $\exists!$ čteme „existuje právě jedno“ (viz kapitola 1a), tedy definice opravdu vyžaduje, aby posílátko neposílalo jeden vstupní objekt na více míst. Tuto podstatu zobrazení coby posílátka dobře vystihuje ono alternativní značení $T(a) = b$, používá se také (řídčeji) $T\colon a \mapsto b$. Fakt, že T je zobrazení z A do B, pak často značíme jako $T\colon A \mapsto B$.

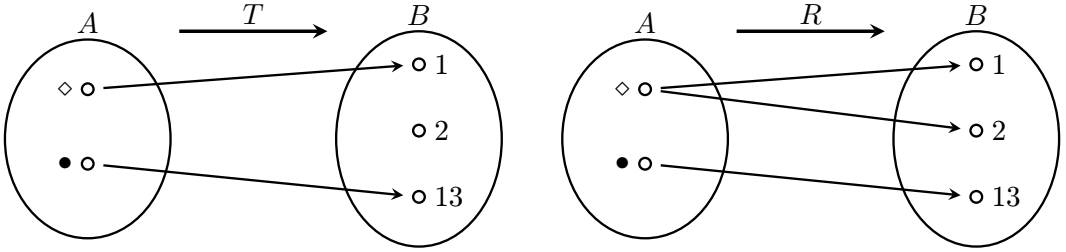
Poznamenejme, že zápis $T(a) = b$ je sice intuitivně příjemný, ale je třeba si uvědomit, že se tím rozhodně nenaznačuje, že by se a dosazovalo do nějakého vzorečku. Je to jen sugestivní zkratka pro fakt, že dvojice (a,b) leží v T. Práce se zápisem $T(a) = b$ je často příjemná, ale jsou chvíle (zejména v některých důkazech), kdy nezbývá než přejít ke skutečnému významu a používat značení $(a,b) \in T$.

Příklad 2b.a: Uvažujme množiny $A = \{\diamond, \bullet\}$ a $B = \{1, 2, 13\}$. Pak $\widehat{R} = \{(\diamond, 13)\}$ není zobrazení $A \mapsto B$, protože prvku $a = \bullet$ není nic přiřazeno. Také $R = \{(\diamond, 13), (\bullet, 1), (\diamond, 2)\}$ není zobrazení, protože prvku $a = \diamond$ jsou přiřazeny dvě různá b.

Jak se dá čekat, teď přijde zobrazení, třeba $T = \{(\diamond, 1), (\bullet, 13)\}$. Toto je správný formální zápis podle definice, ale máme k dispozici i možná přirozenější zápis ve formě výčtu $T(\diamond) = 1$, $T(\bullet) = 13$.

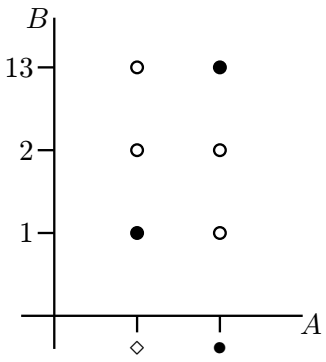
Toto zobrazení má definiční obor $D(T) = A$ a obor hodnot $R(T) = \{1, 13\}$.
△

Jak si takové zobrazení můžeme znázornit? Každému a je přiřazeno jediné b, toto posílání $a \mapsto b$ se přirozeně zachytí šipkami. Ukážeme obrázek pro naše T a také pro R z příkladu 2b.a (R sice není zobrazení, ale jak uvidíme v kapitole o relacích, tyto obrázky se nedělají jen pro zobrazení).



Takový obrázek je velice užitečný, například obor hodnot v něm vidíme jako všechny body z B, do kterých vede šipka. Hned také vidíme, kdy nějaká podmnožina $A \times B$ není zobrazení, buď pro ni nějaké a nemá šipku žádnou, nebo jich má více (viz R).

Alternativní možnost znázornění je vyjít z definice, tedy vnímat T jako nějakou podmnožinu kartézského součinu $A \times B$, který si (přinejmenším u konečných množin) tradičně znázorňujeme jako obdélníkovou síť bodů. V ní zvýrazníme dvojice ležící v T.



Tento obrázek se u diskrétních příkladů (konečné množiny a podobně) moc nepoužívá, ale velmi užitečný začne být, když $A = \mathbb{R}$, tak jej asi čtenář zná. Pak většinou mluvíme o **funkcích**. Někteří autoři používají název funkce i pro obecná zobrazení, jiní si jej rezervují jen pro zobrazení, jejichž definiční obor je v $\mathbb{R}$, popřípadě v $\mathbb{Z}$. Zde se držíme druhého způsobu, takže když pracujeme s množinami, budeme mluvit o zobrazení a upřednostňovat ten šipkový obrázek.

Příklad 2b.b: Uvažujme A coby množinu všech studentů a $B = \mathbb{R}$. Definujeme zobrazení $T\colon A \mapsto B$ předpisem, že pro konkrétní $a \in A$ udává $T(a)$ studijní průměr studenta a k určitému pevně zvolenému dni. Pak by T mělo být zobrazení.
△

Příklad 2b.c: Uvažujme A coby množinu všech studentů a B množinu všech předmětů. Jestliže definujeme T jako množinu všech dvojic $(a, b) \in A \times B$ takových, že student a si v tomto semestru zapsal kurs b, pak to téměř určitě nebude zobrazení, protože se nejspíše najde nějaký sabotující student a, který si zapsal více než jeden kurs, díky čemuž se toto a vyskytne v množině T ve více dvojicích a poruší tak podmínku z definice zobrazení.
Takovéto objekty zkoumáme v kapitole 3.
Pro určité množiny studentů by to ale zobrazení být mohlo, takže obecně se nedá říct nic.
△

Jakmile umíme posílat někam prvky, tak už umíme posílat i celé množiny, prostě je pošleme po jednotlivých prvcích. Můžeme si také vzít nějaký objekt v cílové množině a zeptat se, kdo všechno je na něj poslán.

Definice.
Nechť $T\colon A \mapsto B$ je zobrazení. Pro $M \subseteq A$ definujeme **obraz** M jako

$$T[M] = \{b \in B;\ \exists a \in M : T(a) = b\} = \{T(a);\ a \in M\}.$$

Pro $N \subseteq B$ definujeme **vzor** N jako

$$T^{-1}[N] = \{a \in A;\ T(a) \in N\}.$$

Pak máme třeba $R(T) = T[D(T)]$, evidentně vždy $T^{-1}[B] = A$. Značení T^{-1} pro vzor se může plést se značením pro inverzní zobrazení (viz níže), vzor množiny se pozná podle hranaté závorky. Hledání vzoru ve smyslu množiny se dá udělat vždycky. Vrátíme-li se k příkladu 2b.a, tak $T^{-1}[\{1\}] = T^{-1}[\{1, 2\}] = \{\diamond\}$, $T^{-1}[\{2\}] = \emptyset$.

Kdy se dvě zobrazení rovnají? Není to tak jednoduché, jak to vypadá na první pohled. U funkcí je mnohý čtenář zvyklý, že se rovnají, pokud jsou dány stejným vzorečkem, ale jsou v tom tři háčky. Za prvé, tentýž vzoreček se dá vyjádřit více způsoby a čtenáře možná překvapí, že obecně neexistuje způsob, jak spolehlivě poznat, zda dva vzorečky dávají totéž. Za druhé, my už navíc víme, že na existenci vzorečků nelze spoléhat, takže se spíš musíme zaměřit na to, co zobrazení opravdu dělají, tedy kam prvky posílají. A za třetí, dokonce i kdyby byly dvě zobrazení dány stejnými vzorci, tak ještě nemusí být stejná, pokud nepracují se stejnými výchozími a cílovými množinami. Brzy totiž uvidíme, že u zobrazení stačí změnit jednu z množin (aniž bychom měnili šipky samotné) a už tím můžeme změnit jeho vlastnosti, vznikne tím tedy vlastně jiné zobrazení. Tím se dostáváme k následující definici.

Definice.
Nechť $T\colon A \mapsto B$ a $S\colon C \mapsto D$ jsou zobrazení. Řekneme, že jsou si rovna, značeno $T = S$, jestliže $A = C$, $B = D$ a platí $\forall a \in A\colon T(a) = S(a)$.

Jinak řečeno, všechny tři symboly v obrázku „$T\colon A \mapsto B$“ jsou důležité.
My jsme ovšem definovali zobrazení jako určité množiny dvojic. Pokud se k tomuto pohledu vrátíme, tak se celý problém rovnosti poněkud zjednoduší: Zobrazení T, S jsou si rovna právě tehdy, pokud $C = D$ a zobrazení jsou si rovna coby množiny dvojic.

Zobrazení a operace.
Nejjednodušší operací je proces, kdy se omezíme z původní množiny A jen na nějakou její podmnožinu. To je vysoce užitečný nástroj, například v případech, kdy se nám nelíbí, co zobrazení na jisté části množiny A dělá, a situace nám umožňuje dotyčnou část ignorovat. Formálně to funguje takto.

Definice.
Nechť $T\colon A \mapsto B$ je zobrazení, nechť $M \subseteq A$. Definujeme **restrikci** zobrazení T na M, značeno $T|_M$, jako zobrazení z M do B definované

$$T|_M(a) = T(a) \text{ pro } a \in M.$$

Například T z příkladu 2b.a může být omezeno na podmnožinu $M = \{\diamond\}$, vznikne pak zobrazení $T|_M\colon M \mapsto B$ definované $T(\diamond) = 1$.

Vrátíme-li se k definici zobrazení, tedy nahlížíme-li na něj jako na nějakou množinu dvojic z $A \times B$, pak nás zajímají jen ty dvojice, které mají první souřadnici z M, proto $T|_M = T \cap (M \times B)$. Není to nic zásadního, ale je

dobré umět si takovéto věci rozmyslet. V zásadě ale se zobrazeními jako s množinami pracujeme jen výjimečně, protože ten jazyk pro ně není úplně nejvhodnější, jde přeci jen o velice speciální množiny.

U zobrazení se nejvíce pracuje s operací skládání.

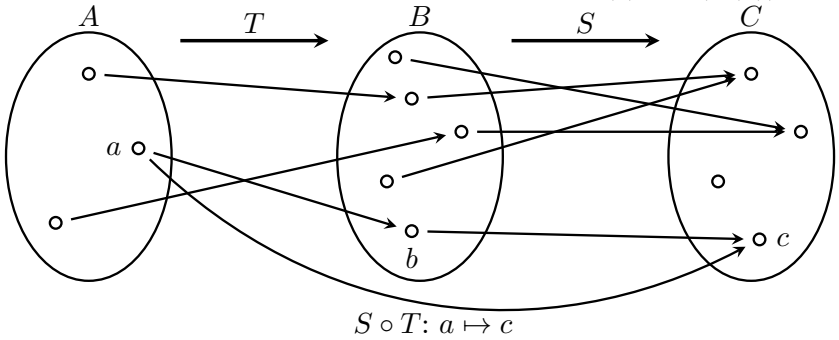
! **Definice.**
Nechť $T\colon A \mapsto B$ a $S\colon B \mapsto C$ jsou zobrazení. Definujeme jejich **složené zobrazení** či **kompozici** $S \circ T\colon A \mapsto C$ předpisem

$$(S \circ T) : a \mapsto S(T(a)) \text{ pro } \ a \in A.$$

Značíme také $S \circ T = S(T)$.

Consider mappings $T\colon A \mapsto B$ and $S\colon B \mapsto C$. We define their **composition** as the mapping $S \circ T\colon A \mapsto C$ defined by $(S \circ T)(a) = S(T(a))$ for $a \in A$.

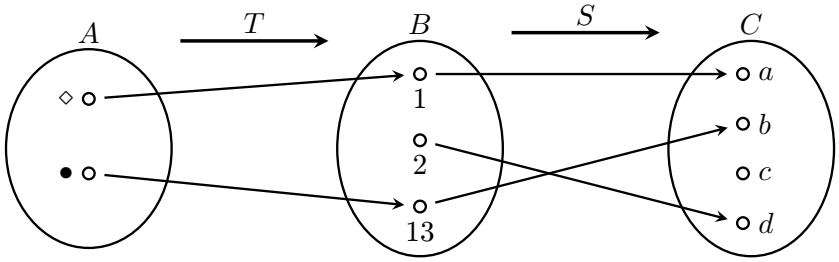
Obrázek naznačuje, oč zde jde. Zobrazení T posílá $a \in A$ na nějaké $b \in B$, ale situace je tak pěkně nastavená, že toto $b = T(a)$ lze poslat dále pomocí zobrazení S na nějaký prvek $S(b) = S(T(a))$.



Když se u každého takového dvoukroku podíváme jen na výchozí a cílový bod (tedy vynecháme prostředníka), dostáváme zobrazení $S \circ T :\ A \mapsto C$.

Všimněte si, že když chceme $S \circ T$ použít, tak nejdříve aplikujeme na výchozí prvek zobrazení T a na ten výsledek pak teprve S. Jinými slovy, složení $S \circ T$ se čte zprava doleva. To je poněkud nezvyklé, ale kdysi se tak matematici dohodli, protože jim přišlo, že to pěkně ladí s běžným funkčním zápisem. Když aplikujeme T na a, dostaneme $T(a)$. Tohle pak chceme dosadit do S, čili děláme $S(T(a))$, takže T je jako první, ale vpravo.

! **Příklad 2b.d:** Uvažujme naše známé T z příkladu 2b.a a také zobrazení S z B do $C = \{a, b, c, d\}$ dané $S(1) = a$, $S(2) = d$, $S(13) = b$. Zkusíme je složit.



Vidíme, že opravdu dostáváme zobrazení z A do C, které posílá $\diamond \mapsto a$ a $\bullet \mapsto b$. Ověříme si to první podle definice: $(S \circ T)(\diamond) = S(T(\diamond)) = S(1) = a$.

Je vidět, že $S(2)$ je pro složené zobrazení irelevantní.

△

Poznámka: Vidíme, že nápad s navazováním funguje vždy, když je možné hodnoty T dosadit do S. Skládání lze tedy zavést obecněji pro libovolná zobrazení T, S splňující $R(T) \subseteq D(S)$. Proč jsme tedy neudělali obecnější definici, která pracuje se zobrazeními $T :\ A \mapsto B$ a $S :\ C \mapsto D$ splňujícími $B \subseteq C$? Protože ta naše je jednodušší a bude se nám s ní dále trochu lépe pracovat, přičemž jsme nic neztratili.

Pokud jsme totiž v oné obecnější situaci, tak nás při skládání stejně nezajímá, so S dělá s prvky, do kterých se T nedostane. Jinými slovy, vždy se můžeme omezit na restrikci $S|_B :\ B \mapsto D$ a pak už můžeme použít naši definici.

Poznámka: zkusme udělat výjimku a vrátit se ještě k množinovému přístupu k zobrazení. Jestliže bychom chtěli s T a S pracovat podle definice, tedy jako s dvojicemi prvků, jak bude vypadat definice složeného zobrazení? Musíme specifikovat, které dvojice prvků jej tvoří, rozmyslete si, že to dopadne takto:

$$S \circ T = \{(a,c) \in A \times C;\ \exists b \in B :\ (a,b) \in T \wedge (b,c) \in S\}.$$

Jako obvykle se nám bude se zobrazeními a skládáním lépe pracovat, pokud budeme umět dělat nějaké zaručeně správné „úpravy“, jinými slovy nás zajímá, jaká pravidla pro tuto operaci platí.

Už z principu je jasné, že skládání nemůže být komutativní, protože například v tom našem příkladě pořadí $T \circ S$ vůbec nemá smysl. Když se podíváme, jak by zobrazení za sebou šla: S: $B \mapsto C$, T: $A \mapsto B$, tak vidíme, že zobrazení T vůbec není schopno akceptovat výsledky S jako svůj vstup. To je tedy principiální problém.

Jsou ovšem situace, kdy při obrácení pořadí se množiny správně navážou, například pokud používáme stále stejnou množinu. Ani pak ale není komutativita zaručena.

Příklad 2b.e: Uvažujme množinu $B = \{1, 2, 13\}$ a zobrazení U, V: $B \mapsto B$ definovaná takto:

U: $1 \mapsto 1$, $2 \mapsto 13$, $13 \mapsto 1$.

V: $1 \mapsto 2$, $2 \mapsto 13$, $13 \mapsto 1$.

Pak zobrazení $V \circ U$ posílá $1 \mapsto V(U(1)) = V(1) = 2$, zatímco $U \circ V$ posílá $1 \mapsto U(V(1)) = U(2) = 13$. Neplatí tedy $V \circ U = U \circ V$.

△

! **Příklad 2b.f:** Vraťme se teď k tomu, co student dobře zná, reálným funkcím. Uvažujme funkce $f(x) = x^2$ a $g(x) = x + 13$, obě jsou vlastně zobrazení $\mathbb{R} \mapsto \mathbb{R}$ a můžeme je tedy složit v libovolném pořadí. Složení $g \circ f$ posílá

$$x \mapsto g(f(x)) = g(x^2) = x^2 + 13,$$

nahradili jsme nejprve $f(x)$ příslušnou hodnotou a pak jsme tento výsledek použili jako vstupní hodnotu pro g. Můžeme začít i vyhodnocením g a dopadne to stejně,

$$x \mapsto g(f(x)) = f(x) + 13 = x^2 + 13.$$

Každopádně $(g \circ f)(x) = x^2 + 13$. Rozmyslete si, že v opačném pořadí skládání dostaneme $(f \circ g)(x) = (x + 13)^2$, značeno také $f(g)(x) = (x + 13)^2$. Zase vidíme, že změnou pořadí skládání dostáváme jinou funkci.

△

Popravdě řečeno, komutativita je sice příjemná, ale až tak zásadní není, takže její selhání tolik nevadí. Mnohem více nám záleží na asociativitě a tam máme štěstí.

! **Věta 2b.1.**
Nechť T: $A \mapsto B$, S: $B \mapsto C$ a R: $C \mapsto D$ jsou zobrazení. Pak platí $(R \circ S) \circ T = R \circ (S \circ T)$.

Důkaz (rutinní)**:** Nejprve si rozmyslíme, že $(R \circ S) \circ T$ a $R \circ (S \circ T)$ jsou obojí zobrazení z A do D (nakreslete si obrázek), takže se shodují výchozí a cílové množiny. Teď ukážeme, že obě zobrazení dávají stejné hodnoty na prvcích z A.

Vezměme libovolné $a \in A$. Zobrazení $(R \circ S) \circ T$ vzniká jako složení T a $R \circ S$. Podle definice se tedy a nejprve dosazuje do T a výsledný prvek pak do $R \circ S$. Dostáváme $(R \circ S)[T(a)]$ a podle definice skládání si rozmyslíme, jak složené zobrazení $R \circ S$ působí na prvek $T(a)$.

$$a \mapsto (R \circ S)[T(a)] = R(S[T(a)]) = R(S(T(a))).$$

Použili jsme hranaté závorky, abychom vizuálně oddělili úrovně, na kterých se používá definice, ale různé typy závorek jsou samozřejmě pořád jen závorky.

Stejně rozebereme $R \circ (S \circ T)$, podle definice se má R aplikovat na složení $(S \circ T)[a]$, což si pak přepíšeme pomocí definice:

$$a \mapsto R[(S \circ T)(a)] = R[S(T(a))] = R(S(T(a))),$$

tedy hodnoty jsou stejné.

□

Už jsme viděli v kapitole 2a, že asociativita nám umožňuje rozšířit definici operace indukcí ze dvou prvků na libovolný konečný počet, tedy nejprve ze dvou na tři předpisem $R_3 \circ R_2 \circ R_1 = R_3 \circ (R_2 \circ R_1)$, odtud pak na čtyři předpisem $R_4 \circ R_3 \circ R_2 \circ R_1 = R_4 \circ (R_3 \circ R_2 \circ R_1)$ a tak dále. Obecně se to dělá indukcí/rekurzí (viz kapitola 5):

Definice.
Nechť $n \in \mathbb{N}$, $n \geq 2$. Uvažujme množiny $A_1, \ldots, A_n, A_{n+1}, A_{n+2}$ a zobrazení T_i: $A_i \mapsto A_{i+1}$ pro $i = 1, \ldots, n+1$. Jejich složení definujeme vzorcem

$$T_{n+1} \circ T_n \circ T_{n-1} \circ \cdots \circ T_1 = T_{n+1} \circ (T_n \circ T_{n-1} \circ \cdots \circ T_1).$$

Je to zase lehké, při pohledu na obrázky výše člověka napadne, že by klidně těch zobrazení mohl za sebe navázat hodně a pak ignorovat vše uprostřed.

Zajímavé to začne být, když se podobné hrátky dělají jen s jedním zobrazením, které zřetězíme. Aby ale $T \circ T$ fungovalo, musí být cílová množina T podmnožinou jeho definičního oboru, nejčastěji jsou rovnou stejné a máme po starostech. Výraz $T \circ T \circ \cdots \circ T$ se pak nazývá mocnina, inspirace násobením je evidentní. Uděláme si na to speciální definici.

Definice.
Nechť T: $A \mapsto A$ je zobrazení, $n \in \mathbb{N}_0$. Pak definujeme **n-tou mocninu** T značenou T^n takto:
- definujeme $T^1 = T$;
- pro $n \geq 1$ definujeme $T^{n+1} = T \circ T^n$;
- definujeme T^0 jako zobrazení i_A: $A \mapsto A$ definované předpisem $\forall a \in A$: $i_A(a) = a$.
  Tomuto zobrazení říkáme **identita** nebo **identické zobrazení** na A.

Příklad 2b.g: Jak toto funguje u funkcí? Uvažujme $f(x) = x^3$ coby zobrazení $\mathbb{R} \mapsto \mathbb{R}$. Pak $f^0(x) = x$, je to identické zobrazení posílající každé číslo na sebe, snadné je i $f^1(x) = f(x) = x^3$. Dále máme $f^2(x) = f(f(x)) = (x^3)^3 = x^9$, $f^3(x) = f(f^2(x)) = f(x^9) = (x^9)^3 = x^{27}$, $f^4(x) = f(f^3(x)) = (x^{27})^3 = x^{81}$ atd.

Rozmyslete si, že pro $g(x) = \sin(x)$ bude $g^2(x) = \sin(\sin(x))$, $g^3(x) = \sin(\sin(\sin(x)))$ atd.

Zde narážíme na jednu nepříjemnost. U funkcí totiž také máme operace na výchozím prostoru $\mathbb{R}$ (sčítání, násobení) a od nich odvozené operace s funkcemi (funkce vzájemně sčítáme, násobíme atd.). Pak také interpretujeme f^k jako součin $f \cdot f \cdots f$, například $f^2(x) = f(x) \cdot f(x) = x^3 \cdot x^3 = x^6$, $f^3(x) = f(x) \cdot f(x) \cdot f(x) = x^3 \cdot x^3 \cdot x^3 = x^9$ atd., také $f^0(x) = (x^3)^0 = 1$. Podobně máme v tomto smyslu $g^k(x) = \sin^k(x)$. Evidentně dostáváme jiné výsledky než v předchozím odstavci, ale značení je stejné. To je vysoce nepříjemné, ale naštěstí méně, než by se zdálo. V analýze hodně pracujeme s operacemi na reálných číslech a nejsme zvyklí opakovaně skládat funkce se sebou, takže tam f^k automaticky bereme jako opakované násobení. Zde nás naopak při práci se zobrazením T: $A \mapsto B$ vůbec nezajímá, co si množiny A a B dělají, často ani žádné své operace nemají (množina lidí atd.), takže T^k vždy znamená opakované skládání.

Na tento rozpor narazíme v silnější podobě u inverzních funkcí, naštěstí nás v této knize trápit nebude.
△

Příklad 2b.h: Vraťme se k příkladu se zobrazeními U, V na množině $B = \{1, 2, 13\}$. Pak máme následující:

$U^1 = U$: $1 \mapsto 1$, $2 \mapsto 13$, $13 \mapsto 1$.

$U^2 = U \circ U$: $1 \mapsto 1 \mapsto 1$, $2 \mapsto 13 \mapsto 1$, $13 \mapsto 1 \mapsto 1$, tedy $U^2(b) = 1$ pro všechna $b \in B$.

$U^3 = U \circ U^2$: $1 \mapsto 1 \mapsto 1$, $2 \mapsto 1 \mapsto 1$, $13 \mapsto 1 \mapsto 1$, tedy $U^3 = U^2$. Rozmyslete si, že u tohoto zobrazení jsou všechny další mocniny stejné, posílají všechno z B do 1.

$V^1 = V$: $1 \mapsto 2$, $2 \mapsto 13$, $13 \mapsto 1$.

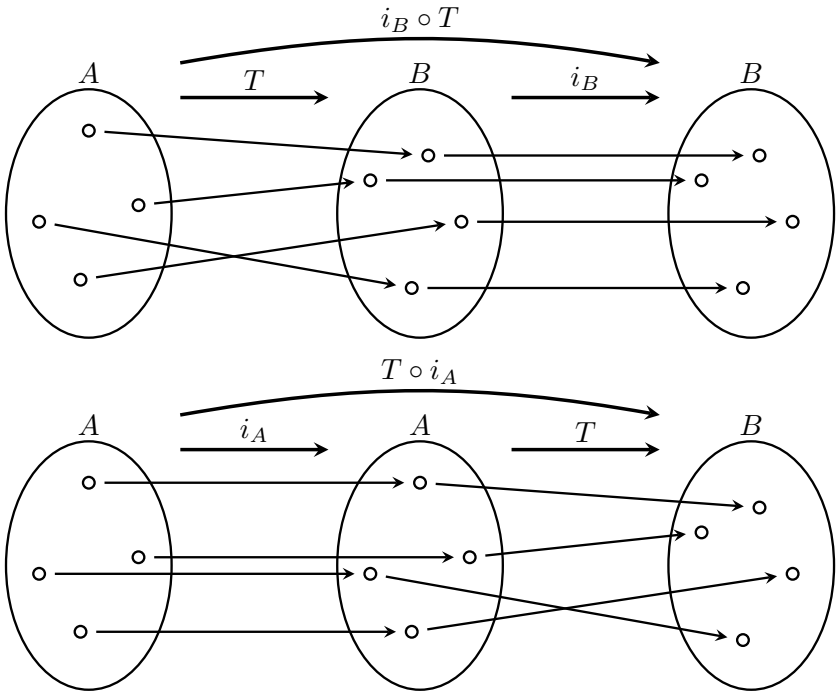
$V^2 = V \circ V$: $1 \mapsto 2 \mapsto 13$, $2 \mapsto 13 \mapsto 1$, $13 \mapsto 1 \mapsto 2$, tedy V^2: $1 \mapsto 13$, $2 \mapsto 1$, $13 \mapsto 2$.

$V^3 = V \circ V^2$: $1 \mapsto 13 \mapsto 1$, $2 \mapsto 1 \mapsto 2$, $13 \mapsto 2 \mapsto 13$. Takže vlastně $V^3 = i_B$ je identické zobrazení na B. Rozmyslete si, že $V^4 = V$, $V^5 = V^2$, $V^6 = i_B$, $V^7 = V$, $V^8 = V^2$, $V^9 = i_B$ atd.
△

Poslední pozorování už plyne obecně z rovnosti $V^3 = i_B$ a následujícího faktu:

Fakt 2b.2.
Nechť T: $A \mapsto B$ je zobrazení. Pak $i_B \circ T = T$ a $T \circ i_A = T$.

Tohle by mělo být jasné, když si člověk představí správný obrázek.



Z obrázku je také jasné, proč je v jednom vzorci potřeba i_A a v druhém i_B.

Důkaz (rutinní)**:** Nejprve dokážeme, že $i_B \circ T = T$. Protože $T\colon A \mapsto B$ a $i_B\colon B \mapsto B$, množiny správně navazují a toto skládání má smysl. Ukážeme, že zobrazení $i_B \circ T$ dělá totéž co T. Nechť $a \in A$. Pak

$$(i_B \circ T)(a) = i_B(T(a)) = T(a),$$

protože $T(a)$ je prvek z B a zobrazení i_B takové prvky nechává, jak jsou.

Podobně dokážeme druhou rovnost.

□

Velice zajímavé je, když si vezmeme zobrazení $T\colon A \mapsto A$. Rovnosti pak dají $i_A \circ T = T \circ i_A = T$. To znamená, že zobrazení i_A se chová vůči skládání jako číslo 1 při násobení čísel. Dají se dokonce (relativně snadno pomocí asociativity) dokázat i pravidla $T^m \circ T^n = T^{m+n}$ a $(T^m)^n = T^{mn}$. Ještě se k tomu vrátíme v kapitole o binárních operacích, teď si od násobení čísel vypůjčíme inspiraci, jmenovitě to, že se k číslům x pokoušíme hledat čísla $\frac{1}{x}$ tak, aby $x \cdot \frac{1}{x} = 1$.

! **Definice.**
Nechť $T\colon A \mapsto B$ je zobrazení. Řekneme, že zobrazení $S\colon B \mapsto A$ je **inverzní** k T, jestliže $S \circ T = i_A$ a $T \circ S = i_B$. Pokud takové zobrazení existuje, tak řekneme, že T je **invertibilní**, a inverzní zobrazení značíme T^{-1}.

Let $T\colon A \mapsto B$ be a mapping. We say that a mapping $S\colon B \mapsto A$ is an **inverse mapping** of T if it satisfies $S \circ T = i_A$ a $T \circ S = i_B$. If such a mapping exists, then we denote it T^{-1} and say that T is **invertible**.

Co ta definice vlastně požaduje? Máme tam rovnosti dvou zobrazení, což znamená, že se chovají stejně, když do nich dosazujeme prvky. Pro začátek si vždy rozmyslíme, jaké prvky:

Máme $T\colon A \mapsto B$ a $S\colon B \mapsto A$, proto $S \circ T$ jde z A do A. Má tedy smysl jej porovnávat s i_A, které jde také z A do A. Porovnání děláme dosazováním prvků z A, takže rovnost $S \circ T = i_A$ ve skutečnosti znamená, že

$$S(T(a)) = a \quad \text{pro všechna } a \in A. \qquad (1)$$

Podobně si rozmyslíme, že $T \circ S$ jde z B do B, a vidíme, že rovnost z definice je ekvivalentní rovnosti

$$T(S(b)) = b \quad \text{pro všechna } b \in B. \qquad (2)$$

Definici je tedy alternativně možno formulovat prostřednictvím podmínek (1) a (2), bez použití zobrazení identity, mnoho autorů to tak dělá.

Lidově řečeno, podmínky (1) a (2) nám říkají, že se zobrazení T a S „navzájem zkrátí“, pokud se ve skládání objeví vedle sebe. Čtenář to už nejspíše viděl, například funkce $\ln(x)$ a e^x jsou navzájem inverzní, tudíž platí $e^{\ln(x)} = x$ pro $x > 0$ a $\ln(e^x) = x$ pro $x \in \mathbb{R}$.

Příklad 2b.i: Vraťme se k zobrazení $V\colon 1 \mapsto 2,\ 2 \mapsto 13,\ 13 \mapsto 1$ z příkladu 2b.e.

Tvrdíme, že zobrazení $W\colon 1 \mapsto 13,\ 2 \mapsto 1,\ 13 \mapsto 2$ je inverzní k zobrazení V. Dokážeme to dosazením, přesně jak jsme si to teď rozmysleli.

$W \circ V$: $1 \mapsto 2 \mapsto 1$, $2 \mapsto 13 \mapsto 2$, $13 \mapsto 1 \mapsto 13$. Ano, vidíme, že toto složené zobrazení je identita.
$V \circ W$: $1 \mapsto 13 \mapsto 1$, $2 \mapsto 1 \mapsto 2$, $13 \mapsto 2 \mapsto 13$. A zase máme identitu. Takže $W = V^{-1}$.
△

Příklad 2b.j (pokračování 2b.a)**:** Teď si zase připomeneme zobrazení T z množiny $A = \{\diamond, \bullet\}$ do $B = \{1, 2, 13\}$ definované předpisem $T(\diamond) = 1$, $T(\bullet) = 13$. Definujme $\widehat{T}$: $B \mapsto A$ předpisem $\widehat{T}(1) = \diamond$, $\widehat{T}(2) = \bullet$, $\widehat{T}(13) = \bullet$.

Pak $\widehat{T} \circ T$ jde z A do A a dělá $\widehat{T}(T(\diamond)) = \widehat{T}(1) = \diamond$ a $\widehat{T}(T(\bullet)) = \widehat{T}(13) = \bullet$, tedy $\widehat{T} \circ T = i_A$.

To vypadá nadějně. Bohužel ale $T(\widehat{T}(2)) = T(\bullet) = 13$ a jsme v háji, zobrazení $T \circ \widehat{T}$ neposílá $2 \mapsto 2$ a tím pádem to není i_B, proto také $\widehat{T}$ není inverzní zobrazení k T.
△

Vidíme, že v definici opravdu potřebujeme mít obě rovnosti.

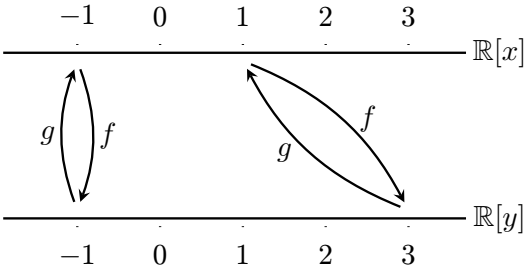
Příklad 2b.k: Uvažujme funkci $f(x) = 2x + 1$. Standardní algoritmus na hledání inverzní funkce funguje tak, že rovnost $y = 2x + 1$ vyřešíme pro x, dostáváme tak vzorec $g(y) = \frac{1}{2}(y - 1)$. Dokážeme, že jsme opravdu dostali inverzní funkci:

$$x \in \mathbb{R} \implies g(f(x)) = g(2x + 1) = \tfrac{1}{2}([2x + 1] - 1) = x,$$
$$y \in \mathbb{R} \implies f(g(y)) = f\big(\tfrac{1}{2}(y - 1)\big) = 2 \cdot \tfrac{1}{2}(y - 1) + 1 = y.$$

Potvrzeno, $g \circ f = I_{\mathbb{R}}$ a $f \circ g = I_{\mathbb{R}}$, tedy g je inverzní zobrazení k f.

Jak bychom to zapsali? Zase máme problém, z hlediska teorie zobrazení píšeme $g = f^{-1}$, ale u reálných funkcí f^{-1} znamená $\frac{1}{f}$, což je $x \mapsto \frac{1}{2x+1}$ neboli úplně jiná funkce než g. Někteří autoři proto používají značení f_{-1} pro inverzní funkci.

Poznamenejme ještě jednu věc, na mnohých středních školách se studenti učí přejít u inverzní funkce zase k proměnné x, tedy psali by $g(x) = \frac{1}{2}(x - 1)$. To ale není moc dobrý nápad, jednak to není třeba a druhak to dokonce posílá špatný vzkaz. My totiž pracujeme s dvěma kopiemi množiny reálných čísel, v jedné používáme pro prvky x a v druhé y.

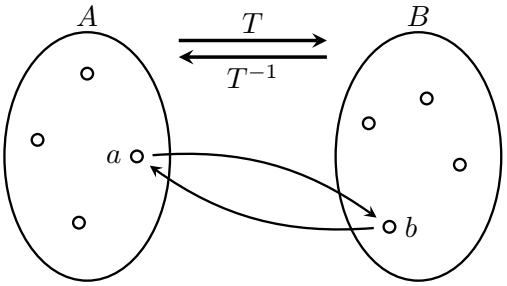


Jak vidíme, funkce g vůbec neumí s prvky x pracovat, protože má jako výchozí množinu úplně jiný svět. Nemá tedy smysl jí tyto proměnné podsouvat, naopak dosazováním y čtenáři jasně sdělujeme, jak tato funkce funguje.
△

Teď se zamyslíme, jak vlastně takové inverzní zobrazení funguje, zároveň tím vyřešíme jeden problém, který se objevil v definici. Tam jsme si pro inverzní zobrazení zavedli značení T^{-1}, ale co když je jich víc? Někteří autoři proto toto značení zavedou až později, když je jasné, jaká je situace.

Jaká tedy je? Obrázek výše silně napovídá, podívejme se na to obecně. Prvek $a \in A$ je zobrazením T někam poslán, jmenovitě na prvek $T(a) = b$. Aby pro zobrazení S platila rovnost $S(T(a)) = a$, tak S musí vrátit b zpět na a.

Zdá se, že T^{-1} má přesně stejné šipky jako T, jen jdou opačným směrem, což mimochodem souhlasí s předchozími třemi příklady. Také to ukazuje, že inverzní zobrazení nemá na výběr, jak jít.



Potvrdíme si to oficiálně.

Fakt 2b.3.
Nechť T: $A \mapsto B$ je invertibilní zobrazení. Pak $T^{-1}(b) = a$ právě tehdy, když $T(a) = b$.

Důkaz: Je to ekvivalence, musíme dokázat implikace oběma směry.

1) $\Longrightarrow$: Předpokládejme, že $T^{-1}(b) = a$. Je to tedy prvek z A, proto na něj můžeme aplikovat zobrazení T: $T(a) = T(T^{-1}(b))$. Jenže napravo máme $T \circ T^{-1} = i_B$, proto dostáváme $T(a) = b$.

2) $\Longleftarrow$: Předpokládejme, že $T(a) = b$. Toto je prvek z B, můžeme na něj aplikovat T^{-1}: $T^{-1}(b) = T^{-1}(T(a))$. Jenže napravo máme $T^{-1} \circ T = i_A$, proto $T^{-1}(b) = a$.

□

Důsledek 2b.4.
Nechť T: $A \mapsto B$ je zobrazení. Jestliže je invertibilní, tak je jeho inverzní zobrazení T^{-1} dáno jednoznačně.

Teď si všichni matematici oddechli, definice inverzního zobrazení byla korektní.

Coby cvičení matematické představivosti se ještě jednou podíváme na zobrazení jako na množinu dvojic. Právě jsme zjistili, že jestliže je nějaké zobrazení $T \subseteq A \times B$ invertibilní, pak

$$T^{-1} = \{(b,a) \in B \times A;\ (a,b) \in T\}.$$

Z představy otáčení šipek lze snadno odvodit základní pozorování o inverzních zobrazeních. Začneme něčím jednoduchým. Jestliže je T invertibilní, tak umíme otočit šipky a dostaneme tím nové zobrazení. Nic by nám pak nemělo bránit v novém otočení šipek a dostaneme zase zpět to původní zobrazení. Teď to řekneme matematicky.

! **Fakt 2b.5.**
Nechť T: $A \mapsto B$ je zobrazení. Jestliže je T invertibilní, tak je i T^{-1} invertibilní a $(T^{-1})^{-1} = T$.

Důkaz (poučný)**:** Předpokládejme, že T je invertibilní, takže máme T^{-1}: $B \mapsto A$. Potřebujeme ukázat, že je nějaké zobrazení S, které jde naopak než T^{-1}, tedy $A \mapsto B$, a splňuje $T^{-1} \circ S = i_A$ a $S \circ T^{-1} = i_B$. Zobrazení T opravdu jde $A \mapsto B$ a když jej dosadíme do těch rovností místo S, tak dostaneme $T \circ T^{-1} = i_A$ a $T^{-1} \circ T = i_B$, což určitě platí, protože je T^{-1} je inverzní k T. T tedy splňuje požadavky na S, je to $(T^{-1})^{-1}$.

□

Umíme dělat inverzi a také umíme skládat, jak to jde dohromady?

! **Věta 2b.6.**
Nechť T: $A \mapsto B$ a S: $B \mapsto C$ jsou zobrazení. Jestliže jsou invertibilní, tak je i $S \circ T$ invertibilní a navíc platí $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$.

Ten vzorec je opravdu zajímavý, protože obrací pořadí. To je u inverzních pojmů normální (viz Věta 8a.9), podívejme se, že to ani jinak nejde. Daná zobrazení jdou $A \xrightarrow{T} B \xrightarrow{S} C$ a když složíme, dostaneme $S \circ T$: $A \mapsto C$. Případné inverzní zobrazení k němu tedy musí jít $C \mapsto A$. Abychom vyšli z C, musíme začít s S^{-1}, protože T^{-1} začíná v množině B. Tím jsme inspirováni k opačnému pořadí a ověříme, že to opravdu dopadne dle očekávání: Máme „řetízek“ $C \xrightarrow{S^{-1}} B \xrightarrow{T^{-1}} A$, čili $T^{-1} \circ S^{-1}$ jde $C \mapsto A$, přesně jak potřebujeme. Ukázali jsme, že z hlediska množin má všechno ten správný smysl, ale to na rovnost $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$ nestačí. Ještě se musíme podívat, kam se posílají jednotlivé prvky.

Důkaz (rutinní, poučný)**:** Předpokládejme, že T a S jsou invertibilní. Potřebujeme dokázat, že existuje zobrazení inverzní k $S \circ T$, tedy zobrazení U: $C \mapsto A$ splňující $U \circ (S \circ T) = i_A$ a $(S \circ T) \circ U = i_C$. Takže jedno takové najdeme, ukážeme, že $U = T^{-1} \circ S^{-1}$ funguje. Už jsme si rozmysleli, že jde $C \mapsto A$, a opakovanou aplikací asociativního zákona, Faktu 2b.2 a vlastnosti inverzní funkce dostaneme

$$(T^{-1} \circ S^{-1}) \circ (S \circ T) = T^{-1} \circ (S^{-1} \circ S) \circ T = T^{-1} \circ i_B \circ T = T^{-1} \circ (i_B \circ T) = T^{-1} \circ T = i_A,$$
$$(S \circ T) \circ (T^{-1} \circ S^{-1}) = S \circ (T \circ T^{-1}) \circ S^{-1} = S \circ i_B \circ S^{-1} = S \circ (i_B \circ S^{-1}) = S \circ S^{-1} = i_C.$$

□

Toto tvrzení snadno zobecníme pro vícenásobné skládání.

Věta 2b.7.
(i) Nechť $n \in \mathbb{N}$, $n \geq 2$. Uvažujme množiny $A_1, \ldots, A_n, A_{n+1}$ a zobrazení T_i: $A_i \mapsto A_{i+1}$ pro $i = 1, \ldots, n$. Jestliže jsou všechna tato zobrazení invertibilní, pak je invertibilní i složené zobrazení $T_n \circ \cdots \circ T_1$ a

$$(T_n \circ \cdots \circ T_1)^{-1} = T_1^{-1} \circ \cdots \circ T_n^{-1}.$$

(ii) Nechť je T: $A \mapsto A$ invertibilní, $n \in \mathbb{N}_0$. Pak je i T^n invertibilní a $(T^n)^{-1} = (T^{-1})^n$.

Důkaz se dělá indukcí, necháme jej do příslušné kapitoly jako cvičení (viz cvičení 5a.8), protože je rutinní. Mimochodem, ten druhý vztah vlastně známe z reálných čísel, $\frac{1}{x^n} = \left(\frac{1}{x}\right)^n$.

Poznámka (pokročilá): Pro invertibilní zobrazení je možné definovat mocninu i pro záporné exponenty vzorcem $T^{-n} = (T^{-1})^n$. Máme pak pro invertibilní zobrazení T definováno T^n pro všechna $n \in \mathbb{Z}$, podobně

jako máme pro nenulová čísla x definováno x^n pro všechna $n \in \mathbb{Z}$. Dá se ukázat (není to těžké, ale dlouhé a nudné), že jsme tím rozšířením na záporné exponenty nepokazili pěkné vlastnosti původní mocniny, například pořád platí $T^m \circ T^n = T^{m+n}$ a $(T^m)^n = T^{mn}$, tentokráte ovšem pro libovolná celá čísla m, n.

Teď se vraťme k tomu, že inverzní zobrazení prostě jen obrací šipky. Tím se ovšem dostáváme k problému, že ne všechna zobrazení jsou invertibilní (ostatně ani $\frac{1}{x}$ nenajdeme pro všechna čísla x). Vidíme dva zádrhele, které by nás mohly při pokusu o obrácení šipek potkat. Pokud by se dvě šipky zobrazení T sbíhaly v jednom bodě, pak nevíme, kterou z nich si vybrat pro cestu zpět. A kdyby u nějakého prvku z B šipka chyběla, pak zase nevíme, kam jej zpětně poslat (přesně toto nás postihlo v příkladu 2b.j). Zavedeme si vlastnosti, které přesně toto popíšou.

! **Definice.**
Nechť $T\colon A \mapsto B$ je zobrazení.
Řekneme, že T je **prosté** či **injektivní**, jestliže

$$\forall x, y \in A\colon [x \neq y \implies T(x) \neq T(y)].$$

Řekneme, že T je **na** či **surjektivní**, jestliže $R(T) = B$.
Řekneme, že T je **vzájemně jednoznačné** či **bijekce**, jestliže je prosté a na.

A mapping $T\colon A \mapsto B$ is called **one-to-one** (often denoted **1-1**) or **injective**, if for all distinct elements $x \neq y \in A$ one has $T(x) \neq T(y)$. It is called **onto** or **surjective** if $R(T) = B$. If it is both 1-1 and onto, then we call it a **bijection**.

Podmínka $R(T) = B$ se dá také napsat $T[A] = B$ nebo podrobněji

$$\forall b \in B\ \exists a \in A\colon T(a) = b$$

a znamená, že ke každému prvku v cílové množině B vede alespoň jedna šipka. Každé zobrazení identita i_A je automaticky na, z ostatních příkladů v této kapitole jsou na jen V, $f(x) = 2x + 1$ a jeho inverze g.

Podmínka pro prostotu zase říká, že se žádné šipky zčínající v různých místech nemohou sejít v jednom bodě. Když si projdeme naše příklady, tak těch prostých je docela dost: T, S, V, $f(x) = 2x + 1$ a jeho inverze a automaticky každá i_A. Příklad U není prostý, protože prvky $x = 1$ a $x = 13$ splňují předpoklad implikace z definice ($x \neq y$), ale nesplňují její závěr ($U(x) = 1 = U(13)$), tudíž je implikace nepravdivá a U tedy není prosté.

Protože pracovat se vztahem $\neq$ je nepříjemné, mnoho autorů (možná i většina) raději používá v definici obměnu té původní implikace, podmínka prostoty se dá také napsat

$$\forall x, y \in A\colon [T(x) = T(y) \implies x = y]. \qquad \text{(I)}$$

V praxi prostotu daného zobrazení T zkoumáme tak, že začneme s rovností $T(x) = T(y)$ a řešíme to jako rovnici, což je mnohem pohodlnější. Většinou to tak budeme dělat i zde.

Co se týče bijekce, mezi příklady máme bijekci V, funkci $f(x) = 2x + 1$ a její inverzi a pro libovolnou množinu A je identita i_A samozřejmě také bijekce. Dá se říct, že bijekce jsou z pohledu teorie množin nejlepší zobrazení.

Zde jak vidno používáme kratšího slova „bijekce“, které postupně začíná být bráno na milost, název „vzájemně jednoznačné“ je tradičnější a pěknější, nicméně delší.

Před chvílí jsme si rozmysleli, že při obrácení šipek nám vadí situace, když se u T šipky sbíhají nebo nedojdou všude. To první nám zakáže prostota, to druhé surjektivita, takže následující tvrzení by nemělo překvapit.

! **Věta 2b.8.**
Nechť $T\colon A \mapsto B$ je zobrazení. Je invertibilní právě tehdy, když je to bijekce.

Důkaz (poučný)**:** 1) $\implies$: Předpokládejme, že T je invertibilní.

Nejprve ukážeme, že T je prosté, pomocí obměny (I). Vezměme prevky $x, y \in A$ takové, že $T(x) = T(y)$. Dosadíme do zobrazení T^{-1} (máme ho k dispozici, T je invertibilní), stejný vstup musí dát stejný výsledek, proto dostaneme $T^{-1}(T(x)) = T^{-1}(T(y))$ a tedy $x = y$. Prostota je dokázána.

Teď ukážeme, že je na. Nechť $b \in B$. Potřebujeme najít nějaký jeho vzor. Definujme $a = T^{-1}(b)$. Pak $a \in A$ a $T(a) = T(T^{-1}(b)) = b$. Surjektivita je dokázána.

2) $\impliedby$: Předpokládejme, že T je bijekce. Ukážeme, že je invertibilní. Nejprve definujeme zobrazení $S\colon B \mapsto A$. Nechť $b \in B$. Protože T je na, tak určitě existuje nějaké a takové, že $T(a) = b$, a protože je T prosté, tak je to jediný takový prvek. Můžeme tedy definovat $S(b) = a$.

Dokážeme, že $S = T^{-1}$.

Nechť $b \in B$. Pak $S(b)$ je prvek a splňující $T(a) = b$, proto $T(S(b)) = T(a) = b$.

Nechť $a \in A$. Potřebujeme vědět, co je $S(T(a))$. Hodnota S v bodě $b = T(a)$ je definovaná jako nějaký prvek $x \in A$ takový, že $T(x) = b$. Jedním z takových prvků je a, ten to určitě splní, a díky prostotě T je také jediný takový. Proto jsme při definici S použili $S(b) = a$, tedy $S(T(a)) = a$. Důkaz je hotov.

□

Příklad 2b.l: Uvažujme zobrazení T z množiny občanů ČR do množiny desetimístných čísel definované tak, že $T(x)$ je dáno jako rodné číslo člověka x. Určitě není na, například není možné se narodit ve třináctém měsíci, tudíž desetimístná čísla začínající xx13 nebudou dosažitelná pomocí T. Dobrá otázka je, zda je toto zobrazení prosté. Skutečnost je taková, že my chceme, aby bylo prosté, dlouho jsme si to i mysleli, ale v devadesátých letech se ukázalo, že občas někdo někde něco spletl a toto zobrazení prosté nebylo. Úřady se to snažily napravit, ale kdo ví.
△

Příklad 2b.m: Prozkoumáme prostotu a surjektivitu pro několik funkcí coby zobrazení $\mathbb{R} \mapsto \mathbb{R}$.

a) $f(x) = x^3 - x$. Není problém si načrtnout graf této funkce, začíná v levém dolním rohu (utíká do mínus nekonečna), při své cestě nahoru protne osu x v bodě -1, pak se otočí a zase jede dolů, protne osu v počátku, pak se zase otočí nahoru a uteče do nekonečna, protínaje osu x v bodě 1. Vidíme, že tato funkce dokáže nabýt libovolné reálné hodnoty, je tedy na. Zároveň také vidíme, že není prostá, protože například $f(0) = 0$ a také $f(1) = 0$, takže se nám sešly šipky $0 \mapsto 0$ a $1 \mapsto 0$.

b) $f(x) = 2x - 1$. Tato funkce je prostá. Důkaz: použijeme alternativní podmínku (I).

Vezměme tedy libovolné $x, y \in \mathbb{R}$ takové, že $f(x) = f(y)$. Pak $2x - 1 = 2y - 1$, odsud hravě dostaneme $x = y$ a důkaz je hotov.

Tato funkce je také na. Důkaz: Nechť y je nějaký prvek z cílové množiny $\mathbb{R}$. Tvrdíme, že existuje jisté x_0 splňující $f(x_0) = y$. Toto tvrzení dokážeme tak, že takové x_0 najdeme. Chceme, aby $f(x_0) = y$, tedy aby $2x_0 - 1 = y$. Odtud $x_0 = \frac{y+1}{2}$. To je určitě reálné číslo, ještě potvrdíme, že splňuje požadavek:

$$f(x_0) = 2x_0 - 1 = 2\tfrac{y+1}{2} - 1 = y.$$

Pro dané y jsme tedy našli $x_0 \in \mathbb{R}$ takové, že $f(x_0) = y$, tudíž je f na.

Toto f je proto bijekce. Všimněte si, že jsme právě ukázali, že pro libovolné $y \in \mathbb{R}$ najdeme $x = \frac{1}{2}(y + 1)$ tak, aby $f(x) = y$. Našli jsme tedy vzorec obracející šipky neboli vzorec pro f_{-1} (viz příklad výše).

c) $f(x) = \operatorname{arctg}(x)$. Znalosti z analýzy ukazují, že tato funkce je prostá, ale není na.

d) $f(x) = x^2 + 1$. Grafem je klasická parabola obrácená nahoru a posunutá nahoru o 1, tato funkce tedy rozhodně není na a není ani prostá.

Důkaz, že není na: Protože vždy platí $x^2 \geq 0$, je i $f(x) \geq 1$. Nelze tedy nalézt $x \in \mathbb{R}$ takové, aby $f(x) = -13$.

Důkaz, že není prostá: Protipříkladem je třeba $f(-1) = 2 = f(1)$.

Poznámka: Co kdybychom prostotu zkoumali tradičním způsobem, tedy testováním podmínky (I)? Vyšli bychom z rovnosti $f(x) = f(y)$ neboli $x^2 + 1 = y^2 + 1$, odtud pak $x^2 = y^2$. Z tohoto ale neumíme přejít k $x = y$, což ještě nemusí nic znamenat (třeba jen nejsme dost šikovní), ale je to znamení, že máme zpozornět. Pokud si dále všimneme, že z $x^2 = y^2$ vyplývá $y = \pm x$, tak nás to navede k protipříkladu k prostotě.
△

S 2b.9 Jak na vlastnosti funkcí

Tento příklad ukazuje nejčastější způsob zkoumání prostoty a surjektivity. Dostane-li student k prozkoumání nějaké zobrazení T, tak se není třeba bát toho, že je třeba na první pohled komplikované, stačí se držet definice (či její obměny):

1. Chceme-li určit, zda je T **prosté**, tak si vezmeme dva libovolné prvky $x, y \in A$ (tedy obecné prvky, nemůžeme si vybrat dva pěkné konkrétní) a napíšeme si rovnici $T(x) = T(y)$. Dosadíme z definice zobrazení T do obou stran a dostaneme rovnici, ze které se pokusíme odvodit informaci o vztahu x a y. Tento obecný začátek většinou silně napoví, jak dál.

Je-li například T: $\mathbb{N}^3 \mapsto \mathbb{N}^2$ dáno $T(r, s, t) = (r^3, s^t)$, pak prvky $x, y \in A$ jsou vlastně oba třísložkové vektory, tedy třeba $x = (r, s, t)$ a $y = (u, v, w)$ pro nějaké neznámé $r, s, t, u, v, w \in \mathbb{N}$. Základní rovnice pak dává

$$T(r, s, t) = T(u, v, w) \implies (r^3, s^t) = (u^3, v^w)$$

a je třeba se rozmyslet, co dál. Rovnost vektorů znamená rovnost souřadnic, máme tedy $r^3 = u^3$ a $s^t = v^w$. Dá se z toho něco odvodit? Třetí mocnina je prostá funkce, proto z první rovnice vyjde $r = u$. U druhé rovnice ale nic tak očividného není, takže v takovém případě je dobré začít experimenovat, zkoušet různá čísla a vzpomínat na předchozí zkušenosti. Zde se rychle ukáže, že dvojic dávajících stejnou mocninu může být víc, třeba $3^4 = 9^2$. To

ukazuje, že dané zobrazení nebude prosté, a máme i protipříklad na prostotu: $T(1,3,4) = (1,81) = T(1,9,2)$, ale neplatí $(1,3,4) = (1,9,2)$. T tedy není prosté.

Někdy ovšem z rovnice $T(x) = T(y)$ dokážeme odvodit $x = y$ (což může klidně znamenat rovnost vektorů neboli rovnost složek), pak bude zobrazení prosté.

2. Chceme-li určit, zda je T **na**, tak si vezmeme libovolný prvek $y \in B$ (z cílového prostoru) a zkusíme k němu najít $x \in A$ takové, aby $T(x) = y$. Pokud takto začneme a pak dosadíme konkrétní T, navede nás to obvykle na správnou cestu. Rovnost $T(x) = y$ je v zásadě rovnice, kterou se snažíme vyřešit pro x, což je trochu komplikováno tím, že vlastně y neznáme, potřebujeme to udělat obecně, pro všechna y. Pokud se to povede, pak je zobrazení na.

U našeho příkladu vybíráme y z cílového prostoru $\mathbb{N}^2$, je to tedy nějaký vektor, třeba $y = (u, v)$, přičemž u, v neznáme, jde o nějaká libovolná čísla z $\mathbb{N}$. Ptáme se, zda existuje $x \in A$ neboli zda existují $r, s, t \in \mathbb{N}$ tak, aby $T(r, s, t) = (u, v)$. Tento obecný začátek nám dává rovnice $r^3 = u$, $s^t = v$ a my se ptáme, zda jsou řešitelné pro r, s, t, přesněji řečeno, zda vždy dokážeme najít r, s, t tak, aby to fungovalo (problém nemusí mít jediné řešení, to nás ale nezajímá).

U rovnice $s^t = v$ si všimneme, že řešení určitě má bez ohledu na volbu v, stačí prostě vzít $s = v$ a $t = 1$. To je dobrý začátek, pomocí T a vektoru z A dokážeme dostat do libovolné druhé souřadnice. Teď se podíváme na tu první: Existuje určitě nějaké $r \in \mathbb{N}$ takové, aby $r^3 = u$? Protože u je libovolné, zkušený student hned tuší, že je zle, protože například třetí odmocnina z 2 existuje, ale není to celé číslo. Takže nenajdeme $r \in \mathbb{N}$ takové, aby $r^3 = 2$, tím pádem ani nelze najít $(r, s, t) \in \mathbb{N}^3$ tak, aby $T(r, s, t) = (2, v)$. Zobrazení T proto není na.

Tyto postupy fungují spolehlivě (viz první cvičení v této kapitole), nicméně jsou situace, kdy je lepší hledat alternativu. U prostoty je někdy lépe vidět přímo vlastnost z definice, tedy doloží se, že když $x \neq y$, pak určitě $T(x) \neq T(y)$, ale to je vzácné.

Někdy se dá také prostota či surjektivita získat mnohem snadněji nepřímo, pomocí vlastností již prozkoumaného zobrazení, od kterého nějakým trikem přejdeme k tomu, které zkoumáme. Dobrou ukázkou jsou poslední cvičení této kapitoly.

V mnoha příkladech (zejména při práci s funkcemi) je lepší zkoumat prostotu pomocí metod matematické analýzy, ale to je jiná pohádka.

△

Vraťme se k teorii, začneme zkoumat chování nových pojmů. Jak si naše tři vlastnosti rozumí se skládáním?

Fakt 2b.10.
Nechť $T\colon A \mapsto B$ a $S\colon B \mapsto C$ jsou zobrazení. Pak platí:
(i) Jestliže jsou T a S prosté, tak je $S \circ T$ prosté.
(ii) Jestliže jsou T a S na, tak je $S \circ T$ na.
(iii) Jestliže jsou T a S bijekce, tak je $S \circ T$ bijekce.

Důkaz (poučný)**:** (i): Prostotu dokážem pomocí obměny (I) aplikované na $S \circ T$.

Nechť $x, y \in A$ splňují $(S \circ T)(x) = (S \circ T)(y)$. To se dá napsat jako $S[T(x)] = S[T(y)]$, je to tedy S aplikované na nějaké dva body. Protože je S prosté, tak odtud nutně $T(x) = T(y)$. A protože je T prosté, tak $x = y$. Prostota je dokázána.

(ii): Dokážeme podle definice, že $S \circ T$ je na. Nechť $c \in C$. Protože je S na, musí existovat $b \in B$ takové, že $S(b) = c$. Protože T je na, musí existovat $a \in A$ takové, že $T(a) = b$. Našli jsme a takové, že $(S \circ T)(a) = S(T(a)) = S(b) = c$.

(iii): Jestliže jsou T a S bijekce, tak jsou prosté, a tudíž podle (i) je i $S \circ T$ prosté.

Jestliže jsou T a S bijekce, tak jsou na, a tudíž podle (ii) je i $S \circ T$ na. Takže $S \circ T$ je bijekce.

(Všimněte si, jak jsme pěkně využili již udělané práce. To je pro matematiku typické.)

Alternativa: Jestliže jsou T a S bijekce, tak jsou dle Věty 2b.8 invertibilní, tudíž dle Věty 2b.6 je i $S \circ T$ invertibilní, tudíž bijekce.

□

Stručně řečeno, skládání nepokazí dobré vlastnosti (bude se nám to hodit v příští kapitole). Jako obvykle se tento výsledek dá zobecnit na skládání více zobrazení. Může skládání vylepšit špatné vlastnosti? Někdy ano, někdy ne, podívejte se na cvičení 2b.10. Tuto otázku lze ekvivalentně položit i jinak: Víme-li, že $S \circ T$ má nějakou vlastnost, musí ji mít nutně i složky S a T? Cvičení odpoví.

Fakt 2b.11.
Jestliže je zobrazení T bijekce, tak T^{-1} existuje a je to také bijekce.

Toto okamžitě plyne z Věty 2b.8 a Faktu 2b.5.

Rozeberme si trochu situaci. Když jsme si hráli s našimi příklady, tak nás mohlo napadnout, že S z příkladu 2b.d nemůže být na už z principu, protože má jen tři šipky (B má jen tři prvky), ale cílová množina má 4 prvky, tudíž je nelze všechny pokrýt.

Podobně se dá rozmyslet, že když posíláme šipky a cílový prostor má méně prvků, než je šipek, tak se musí nějaké šipky potkat a je po prostotě. Shrneme si to oficiálně.

Fakt 2b.12.
Nechť $T\colon A \mapsto B$ je zobrazení a A, B mají konečně mnoho prvků.
(i) Jestliže má B více prvků než A, pak T nemůže být na.
(ii) Jestliže má A více prvků než B, pak T nemůže být prosté.
(iii) Jestliže A a B nemají stejně prvků, pak T nemůže být bijekce.

Dokazovat to nebudeme, protože bychom museli hlouběji do teorie množin (například jsme zatím ani nedefinovali, co je to počet prvků množiny). Naštěstí tento fakt nebudeme v dalších důkazech používat, takže vynecháním jeho důkazu nevznikne díra v základech toho, co tu v dalších kapitolách vystavíme.

Všimněte si, že všechna tato tvrzení jsou zjevně jen implikace. Když se například v (i) podíváme na situaci, kdy je u nějakého zobrazení splněn závěr implikace (T není na), tak nelze s jistotou tvrdit, že počty prvků množin splňují předpoklad. Klidně se totiž mohlo stát, že množiny A, B vyšly tomu zobrazení vstříc a B má nejvýše tolik prvků jako A, ale dotyčné zobrazení svou šanci nevyužilo a vyplýtvalo šipky tím, že jich spoustu poslalo do jednoho prvku.

U tvrzení (iii) je zajímavá i obměna:
(iii)* Jestliže je T bijekce, tak mají A a B stejný počet prvků.
Toto bude výchozí bod pro další kapitolu, stejně jako obměna tvrzení (ii).

I (iii)* je obecně jen implikace, tedy z rovnosti počtu prvků dvou množin nelze automaticky prohlásit všechna zobrazení mezi nim za bijekce, nicméně něco zajímavého se o této situaci říct dá. Uvažujme tedy dvě množiny A, B se shodným (konečným) počtem prvků (nakreslete si obrázek). Co se může stát nějakému zobrazení $T: A \mapsto B$? Pokud T není prosté, tak se nějaké šipky spojí, pak ale chybí v cílové oblasti a nedojde k jejímu pokrytí, T nebude na. Pokud naopak začneme předpokladem, že T není na, tak vlastně T leze do menší množiny a nemůže být prosté.

Fakt 2b.13.
Nechť $T\colon A \mapsto B$ je zobrazení, předpokládejme, že A a B mají stejný konečný počet prvků. Pak je T prosté právě tehdy, když je T na.

Toto je někdy velice užitečné, protože nám to ušetří polovinu práce s dokazováním bijekce.

! Existují situace, kdy máme zobrazení a potřebujeme pracovat s opačnými šipkami, ale nejde to, protože T není prosté. Někdy se dá tento problém obejít tak, že „vyhodíme“ prvky, které nám prostotu kazí, neboli omezíme se na množinu takovou, že už je na ní T prosté.

Je to vlastně něco, co čtenář patrně zná ze střední školy. Funkce (zobrazení) $f\colon \mathbb{R} \mapsto \mathbb{R}$ definovaná jako $f(x) = x^2$ není prostá ani náhodou, třeba $f(-13) = 169 = f(13)$ je protipříklad, ale rádi bychom používali opačné šipky (odmocňovali). To se vyřeší tak, že se namísto f uvažuje její restrikce na množinu $\{x \in \mathbb{R};\ x \geq 0\}$. Na této množině je už f prostá a vesele inverzníme.

Při definici rovnosti zobrazení jsme zmínili, že změnami množin se mohou podstatně změnit vlastnosti zobrazení. Právě jsme viděli, jak se dá „vyrobit“ prostota tím, že z definičního oboru odstraníme zlobivce. S ještě menším úsilím „vyrobíme“ surjektivitu. Mějme nějaké zobrazení $T\colon A \mapsto B$, které není na. To znamená, že v B jsou prvky, do kterých se T nedostane. Jenže ono se dostane do všech prvků z $R(T)$, tak je to ostatně definováno, tudíž když se na T podíváme jako na zobrazení z A do $R(T)$, tak už je na. Takže $T\colon A \mapsto B$ a $T\colon A \mapsto R(T)$ nemohou být z hlediska teorie stejná zobrazení, protože mají jiné vlastnosti, i když jsme vlastně T samotné vůbec nemodifikovali, pořád posílá stejné prvky stejným způsobem.

Tento trik je v některých situacích velice užitečný. Vyplývá z něj totiž následující:

- Jestliže je $T\colon A \mapsto B$ prosté, pak je $T\colon A \mapsto R(T)$ bijekce, takže například máme i její inverzi $T^{-1}\colon R(T) \mapsto A$.

Teď si ukážeme dvě funkce, které jsou v computer science docela důležité.

Definice.
Definujme následující funkce na $\mathbb{R}$:

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z};\ n \leq x\}; \qquad \text{(zaokrouhlení dolů)}$$
$$\lceil x \rceil = \min\{n \in \mathbb{Z};\ n \geq x\}. \qquad \text{(zaokrouhlení nahoru)}$$

Význam je doufejme zjevný. Například $\lfloor x \rfloor$ je největší celé číslo, které se najde „pod“ x. Pokud je tedy x celé, tak tím největším celým číslem ne větším než x je samozřejmě přímo to x. Kdyby ale x celé nebylo, tak se při procházení celými čísly směrem nahoru zarazíme dřív, než k x dojdeme, jmenovitě u kladných čísel se zarazíme přesně u toho, co vidíme před desetinnou čárkou. U záporných čísel je to drobet jiné, protože na záporné části osy pořád přicházíme k x s celými čísly zleva, od menších, čtenář si teď zkusí namalovat reálnou osu a rozmyslet si, co se pak děje. Při jednom si také rozmyslí, jak funguje $\lceil x \rceil$.

Takže například $\lfloor 13 \rfloor = 13$ a $\lceil 13 \rceil = 13$, $\lfloor -13 \rfloor = -13$ a $\lceil -13 \rceil = -13$, $\lfloor 13.23 \rfloor = 13$ a $\lceil 13.23 \rceil = 14$, ale také $\lfloor -13.23 \rfloor = -14$ a $\lceil -13.23 \rceil = -13$. Opravdu to tedy zaokrouhluje dolů, tedy k menším číslům, a nahoru, tedy k větší k číslům, a to nikoliv v absolutní hodnotě, ale doleva a doprava na reálné ose.

Anglicky se těmto funkcím říká **floor** (podlaha) a **ceiling** (strop).

Bývá dobré si tu definici rozmyslet více způsoby, protože člověk to pak lépe vidí. $\lfloor x \rfloor$ je celé číslo, které má určité speciální vlastnosti. Podle čeho poznáme, že zrovna jedno konkrétní celé číslo je $\lfloor x \rfloor$?

Fakt 2b.14.
Nechť $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Pak platí:
(i) $\lfloor x \rfloor = n \iff n \leq x < n+1$.
(ii) $\lceil x \rceil = n \iff n-1 < x \leq n$.
(iii) $\lfloor x \rfloor = n \iff x-1 < n \leq x$.
(iv) $\lceil x \rceil = n \iff x \leq n < x+1$.
(v) $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.

Důkaz (pro úplnost)**:** (i): $\Longrightarrow$: Předpokládejme, že $n = \lfloor x \rfloor$. Pak $n = \max\{m \in \mathbb{Z};\ m \leq x\}$. To mimo jiné znamená, že n v té množině leží, tudíž $n \leq x$. Protože je to ale maximální celé takové číslo, tak už v ní $n+1$ neleží, proto $n + 1 > x$.

$\Longleftarrow$: Předpokládejme, že celé číslo n splňuje $n \leq x < n+1$. Pak toto n leží v množině $\{m \in \mathbb{Z};\ m \leq x\}$. Z nerovnosti $x < n+1$ ale vidíme, že $n+1$ už v této množině neleží, proto je n největší číslo z této množiny, a tedy $n = \lfloor x \rfloor$.

(ii) se dokazuje podobně.

(iii): $\Longrightarrow$: Jestliže je $n = \lfloor x \rfloor$, pak podle (i) je $n \leq x$ a také $x < n - 1$, což je $x - 1 < n$.

$\Longleftarrow$: Nechť celé číslo n splňuje $x - 1 < n \leq x$. Z levé nerovnosti máme $x < n + 1$, proto $n \leq x < n + 1$ a podle (i) je $n = \lfloor x \rfloor$. Důkaz (iv) je podobný.

(v): Plyne z (i) až (iv), stačí do vztahů na pravých stranách dosadit namísto n příslušnou funkci.

□

Ukážeme si ještě jiný způsob, jak poznat, že nějaké číslo n je jedna z těch dvou funkcí.

Fakt 2b.15.
Nechť $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Pak platí:
(i) $n = \lfloor x \rfloor$ právě tehdy, když existuje ε splňující $0 \leq \varepsilon < 1$ a $x = n + \varepsilon$.
(ii) $n = \lceil x \rceil$ právě tehdy, když existuje ε splňující $0 \leq \varepsilon < 1$ a $x = n - \varepsilon$.

Důkaz (pro úplnost)**:** (i): 1) $\Longrightarrow$: Definujme $\varepsilon = x - \lfloor x \rfloor = x - n$. Pak $x = n + \varepsilon$ a podle (i) z předchozího Faktu pak $0 \leq \varepsilon < 1$.

2) $\Longleftarrow$: Předpokládejme, že $x = n + \varepsilon$ a $0 \leq \varepsilon < 1$. Pak $n \leq x$ a z $\varepsilon < 1$ máme $x < n + 1$, tudíž je splněna podmínka v (i) předchozího Faktu a $n = \lfloor x \rfloor$.

Důkaz (ii) je obdobný.

□

Někteří autoři definují $\lfloor x \rfloor$ a $\lceil x \rceil$ pomocí podmínek z tohoto faktu.

Jak už jsme viděli, matematici se rádi ptají na pravidla, která by mohla platit, protože se pak lépe pracuje. Například by se mohly hodit vzorečky typu $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ či podobné pravidlo pro násobení, ale zrovna tohle nefunguje (viz cvičení níže). Zato platí desítky různých speciálních vzorečků. Alternativní definice z Faktu 2b.14 nám snadno dají následující identity.

Fakt 2b.16.
Nechť $x \in \mathbb{R}$. Pak platí:
(i) $\lfloor -x \rfloor = -\lceil x \rceil$.
(ii) $\lceil -x \rceil = -\lfloor x \rfloor$.
(iii) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ pro všechna $n \in \mathbb{Z}$.
(iv) $\lceil x + n \rceil = \lceil x \rceil + n$ pro všechna $n \in \mathbb{Z}$.

Důkaz (rutinní)**:** (i): Nechť $n = \lceil x \rceil$. Pak podle Faktu 2b.14 (ii) platí $n - 1 < x \leq n$. Potom také platí $-n + 1 > x \geq -n$, tedy $(-n) \leq x < (-n) + 1$ a podle Faktu 2b.14 (i) je $-n = \lfloor x \rfloor$.

Důkaz (ii) je podobný.

(iii): Označme si $m = \lfloor x \rfloor$. Pak podle Faktu 2b.14 (i) je $m \leq x < m + 1$. Pak $m + n$ je celé číslo splňující $m + n \leq x + n < m + n + 1$, tudíž podle Faktu 2b.14 (i) je $m + n = \lfloor x + n \rfloor$.

Důkaz (iv) je obdobný.

□

Charakterizace z Faktu 2b.15 se zase hodí při důkazu této identity.

Fakt 2b.17.
Pro každé $x \in \mathbb{R}$ platí $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Důkaz (poučný)**:** Označme $x = \lfloor x \rfloor + \varepsilon$. Rozebereme dva případy.

A) Předpokládejme, že $\varepsilon < \frac{1}{2}$. Pak máme i $x + \frac{1}{2} = \lfloor x \rfloor + \left(\varepsilon + \frac{1}{2}\right)$ a $0 \leq \varepsilon + \frac{1}{2} < 1$, proto podle Faktu 2b.15 (ii) platí $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor$.

Dále také máme $2x = 2\lfloor x \rfloor + (2\varepsilon)$ a $0 \leq 2\varepsilon < 1$, proto podle Faktu 2b.15 (ii) platí $\lfloor 2x \rfloor = 2\lfloor x \rfloor$. Dáme to dohromady:

$$\lfloor 2x \rfloor = 2\lfloor x \rfloor = \lfloor x \rfloor + \lfloor x \rfloor = \lfloor x \rfloor + \lfloor x + \tfrac{1}{2} \rfloor.$$

B) Druhá (a poslední) možnost je, že $\frac{1}{2} \leq \varepsilon < 1$. Pak $0 \leq \varepsilon - \frac{1}{2} < 1$. Také máme $x + \frac{1}{2} = (\lfloor x \rfloor + \varepsilon) + \frac{1}{2} = (\lfloor x \rfloor + 1) + \left(\varepsilon - \frac{1}{2}\right)$, proto podle Faktu 2b.15 (ii) platí $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor + 1$.

Z předpokladu $\frac{1}{2} \leq \varepsilon < 1$ také vidíme, že $1 \leq 2\varepsilon < 2$, tedy $0 \leq 2\varepsilon - 1 < 1$. Také máme $2x = 2\lfloor x \rfloor + 2\varepsilon = (2\lfloor x \rfloor + 1) + (2\varepsilon - 1)$, proto podle Faktu 2b.15 (ii) platí $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$. Dáme to dohromady:

$$\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1 = \lfloor x \rfloor + (\lfloor x \rfloor + 1) = \lfloor x \rfloor + \lfloor x + \tfrac{1}{2} \rfloor.$$

□

Ukážeme si teď jednu aplikaci, další se budou tu a tam objevovat, viz třeba příklad 6a.b nebo Fakt 11b.6.

Příklad 2b.n: Máte flashku o velikosti 12GB. Kolik filmů o velikosti 700MB si na ni dokážete stáhnout?
Odpověď: $\left\lfloor \frac{12 \cdot 1024}{700} \right\rfloor = 17$.
△

Cvičení

Cvičení 2b.1: Který z následujících předpisů definuje zobrazení z množiny všech binárních řetězců do množiny celých čísel?
(i) $T(r)$ je počet bitů 1 v r; (ii) $T(r)$ je pozice prvního výskytu bitu 0 v r.

Cvičení 2b.2 (rutinní)**:** Pro následující zobrazení určete jejich definiční obor a obor hodnot.
(i) Zobrazení přiřazuje každému nezápornému celému číslu jeho poslední číslici.
(ii) Zobrazení přiřazuje každému přirozenému číslu následující číslo.
(iii) Zobrazení přiřazuje každému binárnímu řetězci jeho délku.
(iv) Zobrazení přiřazuje každému binárnímu řetězci počet skupin „01“ v něm.
(v) Zobrazení přiřazuje každému binárnímu řetězci počet jedniček mínus počet nul v něm.
(vi) Zobrazení přiřazuje každému celému číslo nejmenší čtverec, tj. číslo typu k^2, který není menší než ono.
(vii) Zobrazení dává maximum ze dvou reálných čísel.

Cvičení 2b.3: Zobrazení T přiřazuje každému studentovi jeho studijní průměr a zobrazení S přiřazuje k jednotlivým studijním průměrům stipendia. Co je zobrazení $S \circ T$?

Cvičení 2b.4 (rutinní, poučné)**:** Pro následující dvojice funkcí $f, g\colon \mathbb{R} \mapsto \mathbb{R}$ najděte $g \circ f$ a $f \circ g$:
(i) $f(x) = \sin(x)$, $g(x) = \pi x$;
(ii) $f(x) = x$, $g(x) = e^x$;
(iii) $f(x) = x^2$, $g(x) = 13$;
(iv) $f(x) = 1 + x^2$, $g(x) = 1 + x^2$;
(v) $f(x) = x^3 - 1$, $g(x) = \sqrt[3]{x+1}$;
(vi) $f(x) = e^x$, $g(x) = \ln(|x|)$ pro $x \neq 0$ a $g(0) = 0$;
(vii) $f(x) = 1 - x$, $g(x) = 1 - x$;
(viii) $f(x) = 1 + x$, $g(x) = 1 + x$.

Cvičení 2b.5 (poučné)**:** Pro následující dvojice funkcí $f, g\colon \mathbb{Z} \mapsto \mathbb{Z}$ rozhodněte, zda číslo 13 leží v oboru hodnot složené funkce $g \circ f$:
(i) $f(x) = x^2 + 2$, $g(x) = 2x + 1$;
(ii) $f(x) = x^3 + 4$, $g(x) = 2x - 11$;
(iii) $f(x) = x^3 - 1$, $g(x) = 13x$.

Cvičení 2b.6 (poučné)**:** Nechť $f(x) = ax + b$, $g(x) = cx + d$. Pro která a, b, c, d platí, že $f \circ g = g \circ f$?

Cvičení 2b.7 (rutinní, zkouškové, dobré*)**:** Jsou následující funkce prosté a na? Svou odpověď dokažte.
(i) $f(n) = n + 1$ ze $\mathbb{Z}$ do $\mathbb{Z}$;
(ii) $f(n) = n + 1$ z $\mathbb{N}$ do $\mathbb{N}$;
(iii) $f(n) = 13n$ ze $\mathbb{Z}$ do $\mathbb{Z}$;
(iv) $f(x) = 13x$ z $\mathbb{Q}$ do $\mathbb{Q}$;
(v) $f(n) = n^3$ ze $\mathbb{Z}$ do $\mathbb{Z}$;
(vi) $f(x) = x^3$ z $\mathbb{R}$ do $\mathbb{R}$;
(vii) $f(n) = n^2 + 1$ ze $\mathbb{Z}$ do $\mathbb{Z}$;
(viii) $f(n) = \left\lfloor \frac{n}{2} \right\rfloor$ ze $\mathbb{Z}$ do $\mathbb{Z}$;
(ix) $f(n) = (-1)^n n$ z $\mathbb{N}_0$ do $\mathbb{Z}$;
(x)* $f(n) = (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor$ z $\mathbb{N}_0$ do $\mathbb{Z}$;
(xi) $f(n) = (n + 1, 2n)$ z $\mathbb{N}$ do $\mathbb{N} \times \mathbb{N}$;
(xii) $f(n) = (n^2, n^2 + 2n)$ ze $\mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
(xiii) $f(m, n) = (m^2, mn)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
(xiv) $f(x, y) = (x + y, x - y)$ z $\mathbb{Q} \times \mathbb{Q}$ do $\mathbb{Q} \times \mathbb{Q}$;
(xv) $f(m, n) = (m + n, m - n)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
(xvi) $f(m, n) = 2m - n$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$;
(xvii)* $f(m, n) = m^2 - n^2$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$;
(xviii) $f(m, n) = m + n + 13$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$;
(xix) $f(m, n) = m - n$ z $\mathbb{N}_0 \times \mathbb{N}$ do $\mathbb{Z}$.

Cvičení 2b.8 (poučné, dobré)**:** Uvažujte zobrazení $T : \mathbb{N} \mapsto \mathbb{N}$ definované takto: $T(n) = \begin{cases} \frac{1}{2}n, & n \text{ sudé;} \\ 3n + 1, & n \text{ liché.} \end{cases}$
Rozhodněte, zda je toto zobrazení bijekce $\mathbb{N}$ na $\mathbb{N}$.
Poznámka: Vezměte si nějaké přirozené číslo n, dosaďte do T, pak ten výsledek zase strčte do T a tak dále, dokud nedostanete 1. Povedlo se to? Zkuste začít jiným číslem. A zase jiným. Co si o tom myslíte? Viz poznámka 5a.7.

Cvičení 2b.9 (poučné, dobré)**:** Ukažte příklady funkcí z $\mathbb{N}$ do $\mathbb{N}$ (tedy vymyslete vzorečky), které by pokryly všechny kombinace vlastností prostoty a na (každá z nich má dvě možnosti, platí/neplatí, celkem tedy čtyři možné kombinace těchto vlastností).
Vymyslete čtyři obdobné funkce ze $\mathbb{Z}$ do $\mathbb{N}$.

Cvičení 2b.10 (poučné, dobré, zkouškové)**:** Nechť $T\colon A \mapsto B$ a $S\colon B \mapsto C$ jsou zobrazení. Rozhodněte, zda následující implikace platí, ty pravdivé dokažte, ty nepravdivé vyvraťte protipříkladem.
U všech implikací napište i její obměnu.
(i) Jestliže T není prosté, tak $S \circ T$ není prosté.
(ii) Jestliže S není prosté, tak $S \circ T$ není prosté.
(iii) Jestliže T není na, tak $S \circ T$ není na.
(iv) Jestliže S není na, tak $S \circ T$ není na.
(v) Jestliže T není bijekce, tak $S \circ T$ není bijekce.
(vi) Jestliže S není bijekce, tak $S \circ T$ není bijekce.

Cvičení 2b.11 (poučné, zkouškové, dobré*)**:** Nechť $T\colon A \mapsto B$ je zobrazení, $M, N \subseteq A$. Dokažte, že pak platí:
(i) $T[M \cup N] = T[M] \cup T[N]$;
(ii) $T[M \cap N] \subseteq T[M] \cap T[N]$.
(iii)* Je-li T prosté, pak $T[M \cap N] = T[M] \cap T[N]$.
(iv) Ukažte, že obecně $T[M \cap N] = T[M] \cap T[N]$ neplatí.

Cvičení 2b.12 (poučné, dobré)**:** Nechť U je universum. Pro $M \subseteq U$ definujme tzv. **charakteristickou funkci** M jako

$$\chi_M(x) = \begin{cases} 1, & x \in M; \\ 0, & x \notin M. \end{cases}$$

Také se jí říká indikátorová funkce, protože jedničkami indikuje, které body z U jsou v M. Dokážte následující:
(i) Pro libovolné $M \subseteq U$: $\chi_{\overline{M}} = 1 - \chi_M$.
(ii) Pro libovolné $M, N \subseteq U$: $\chi_{M\cap N} = \chi_M \cdot \chi_N$.
(iii) Pro libovolné $M, N \subseteq U$: $\chi_{M\cup N} = \chi_M + \chi_N - \chi_{M\cap N}$.

Cvičení 2b.13 (rutinní)**:** Kolik bajtů (bytes) je třeba na zakódování informace v délce 4/10/500/3000 bitů (bits)?

Cvičení 2b.14 (dobré)**:** Nechť $a < b \in \mathbb{R}$.
(i) Kolik celých čísel se nachází v intervalu $\langle a, b\rangle$?
(ii) Kolik celých čísel se nachází v intervalu (a, b)?

Cvičení 2b.15 (poučné)**:** Dokažte, že pro $x \in \mathbb{R}$ platí $\lceil x\rceil - \lfloor x\rfloor = \begin{cases} 1, & x \notin \mathbb{Z}; \\ 0, & x \in \mathbb{Z}. \end{cases}$

Cvičení 2b.16 (poučné)**:** Dokažte, že pro $n \in \mathbb{Z}$ platí $\lfloor n/2\rfloor = \begin{cases} n/2, & n \text{ sudé}; \\ (n-1)/2, & n \text{ liché}. \end{cases}$

Cvičení 2b.17 (dobré)**:** Načrtněte grafy funkcí $f_1(x) = \lfloor 2x\rfloor$, $f_2(x) = \lfloor x/2\rfloor$, $f_3(x) = \lfloor x\rfloor + \lfloor x/2\rfloor$, $f_4(x) = \lceil x\rceil + \lfloor x/2\rfloor$, $f_5(x) = \lceil 2\lfloor x/2\rfloor + \frac{1}{2}\rceil$ a $f_6(x) = \lceil x - 2\rceil + \lfloor x + 2\rfloor$.

Cvičení 2b.18 (dobré)**:** Dokažte, že pro všechna $n \in \mathbb{Z}$ platí:
(i) $\lfloor\lfloor n/2\rfloor/2\rfloor = \lfloor n/4\rfloor$;
(ii) $\lfloor n/2\rfloor \cdot \lceil n/2\rceil = \lfloor n^2/4\rfloor$.

Cvičení 2b.19 (poučné, dobré)**:** Dokažte či vyvraťte následující tvrzení:
(i) $\forall x \in \mathbb{R}$: $\lfloor 2x\rfloor = 2\lfloor x\rfloor$.
(ii) $\forall x, y \in \mathbb{R}$: $\lfloor x + y\rfloor = \lfloor x\rfloor + \lfloor y\rfloor$.
(iii) $\forall x, y \in \mathbb{R}$: $\lceil x + y\rceil = \lceil x\rceil + \lceil y\rceil$.
(iv) $\forall x, y \in \mathbb{R}$: $\lceil x\rceil + \lceil y\rceil - \lceil x + y\rceil$ je 0 nebo 1.
(v) $\forall x, y \in \mathbb{R}$: $\lceil xy\rceil = \lceil x\rceil \cdot \lceil y\rceil$.
(vi) $\forall x, y \in \mathbb{R}$: $\lfloor xy\rfloor = \lfloor x\rfloor \cdot \lfloor y\rfloor$.
(vii) $\forall x \in \mathbb{R}$: $\lfloor\lceil x\rceil\rfloor = \lceil x\rceil$.
(viii) $\forall x \in \mathbb{R}$: $\lceil\lfloor x\rfloor\rceil = \lfloor x\rfloor$.
(ix) $\forall x \in \mathbb{R}$: $\lfloor\sqrt{\lceil x\rceil}\rfloor = \lfloor\sqrt{x}\rfloor$.
(x) $\forall x \in \mathbb{R}$: $\lfloor\sqrt{\lfloor x\rfloor}\rfloor = \lfloor\sqrt{x}\rfloor$.
(xi) $\forall x \in \mathbb{R}$: $\lceil\sqrt{\lceil x\rceil}\,\rceil = \lceil\sqrt{x}\,\rceil$.

Řešení:
2b.1: (i): ano. (ii): Co když je r prázdný, co když neobsahuje 0?
2b.2: (i): $D(T) = \mathbb{N}_0$, $R(T) = \{0, 1, 2 \dots, 8, 9\}$. (ii): $D(T) = \mathbb{N}$, $R(T) = \{2, 3, 4, \dots\} = \mathbb{N} - \{1\}$. (iii): $D(T)$ je množina konečných binárních řetězců, $R(T) = \mathbb{N}_0$. (iv): $D(T)$ je množina konečných binárních řetězců, $R(T) = \mathbb{N}_0$. (v): $D(T)$ je množina konečných binárních řetězců, $R(T) = \mathbb{Z}$. (vi): $D(T) = \mathbb{Z}$, $R(T) = \mathbb{N}_0$. (vii): $D(T) = \mathbb{R} \times \mathbb{R}$, $R(T) = \mathbb{R}$.
2b.3: Přiřazuje studentovi jeho stipendium.
2b.4: (i): $(g \circ f)(x) = g(f(x)) = \pi \sin(x)$, $(f \circ g)(x) = f(g(x)) = \sin(\pi x)$. (ii): $(g \circ f)(x) = g(f(x)) = e^x$, $(f \circ g)(x) = f(g(x)) = e^x$. (iii): $(g \circ f)(x) = g(f(x)) = 13$ (cokoliv dosazené do konstantní funkce je ta konstanta), $(f \circ g)(x) = f(g(x)) = 13^2$. (iv): $(g \circ f)(x) = g(f(x)) = 1 + (1 + x^2)^2$, $(f \circ g)(x) = f(g(x)) = 1 + (1 + x^2)^2$, je to vlastně f^2 (ve smyslu skládání zobrazení, ne ve smyslu násobení funkcí, pozor). (v): $(g \circ f)(x) = g(f(x)) = x$, $(f \circ g)(x) = f(g(x)) = x$, máme $g = f^{-1}$ a $f = g^{-1}$. (vi): $(g \circ f)(x) = g(f(x)) = x$ neboť $e^x > 0$ a tedy $g(f(x)) = \ln(|e^x|) = \ln(e^x) = x$, $(f \circ g)(x) = f(g(x)) = |x|$ pro $x \neq 0$ (takže není $g = f^{-1}$) a $(f \circ g)(0) = 1$. (vii): $(g\circ f)(x) = g(f(x)) = x$, $(f\circ g)(x) = f(g(x)) = x$, máme $g = f^{-1}$ neboli $f = f^{-1}$. (viii): $(g\circ f)(x) = g(f(x)) = x+2$, $(f \circ g)(x) = f(g(x)) = x + 2 = f^2(x)$.
2b.5: Hledáme $x \in \mathbb{Z}$ tak, aby $x \overset{f}{\mapsto} y \overset{g}{\mapsto} 13$. Nejprve y, pak x.
(i): $2y + 1 = 13 \implies y = 6$, $x^2 + 2 = 6 \implies x = \pm 2$. Ano, $g(f)(\pm 2) = 13$, proto $13 \in R(g \circ f)$.

(ii): $2y-11=13 \implies y=12$, $x^3+4=12 \implies x=2$. Ano, $g(f)(2)=13$, proto $13 \in R(g\circ f)$.
(iii): $13y=13 \implies y=1$, $x^3-1=1 \implies x^3=2$ nemá řešení ze $\mathbb{Z}$. Proto $13 \notin R(g\circ f)$.
2b.6: Musí platit $ad+b=bc+d$ neboli $b(c-1)=d(a-1)$.
2b.7: (i): Je prosté: $T(x)=T(y) \implies x+1=y+1 \implies x=y$. Je na: $y\in\mathbb{Z} \implies \exists x=y-1\in\mathbb{Z}$: $T(x)=T(y-1)=(y-1)+1=y$.
(ii): Je prosté: $T(x)=T(y) \implies x+1=y+1 \implies x=y$. Není na: neexistuje $x\in\mathbb{N}$ aby $x+1=1$, proto $1\notin R(T)$.
(iii): Je prosté: $T(x)=T(y) \implies 13x=13y \implies x=y$. Není na: neexistuje $x\in\mathbb{Z}$ aby $13x=23$, proto $23\notin R(T)$.
(iv): Je prosté: $T(x)=T(y) \implies 13x=13y \implies x=y$. Je na: $y\in\mathbb{Q} \implies \exists x=\frac{1}{13}y\in\mathbb{Q}$: $T(x)=T\left(\frac{y}{13}\right)=13\cdot\frac{y}{13}=y$.
(v): Je prosté: $T(x)=T(y) \implies x^3=y^3 \implies x=y$. Není na: neexistuje $x\in\mathbb{Z}$ aby $x^3=2$, proto $2\notin R(T)$.
(vi): Je prosté: $T(x)=T(y) \implies x^3=y^3 \implies x=y$. Je na: $y\in\mathbb{R} \implies \exists x=\sqrt[3]{y}\in\mathbb{R}$: $T(x)=T\left(\sqrt[3]{y}\right)=\left(\sqrt[3]{y}\right)^3=y$.
(vii): Není prosté, třeba $T(1)=T(-1)$. Není na: neexistuje $x\in\mathbb{Z}$ aby $x^2+1=0$, proto $0\notin R(T)$.
(viii): Není prosté, třeba $T(2)=T(3)$. Je na: $y\in\mathbb{Z} \implies \exists x=2y\in\mathbb{Z}$: $T(x)=T(2y)=\lfloor y\rfloor=y$.
(ix): Je prosté: $T(x)=T(y) \implies (-1)^x x=(-1)^y y \implies |(-1)^x x|=|(-1)^y y| \implies |x|=|y|$. Pak také $(-1)^x=(-1)^y$, tedy z $(-1)^x x=(-1)^y y$ je $x=y$. Není na: neexistuje $x\in\mathbb{Z}$ aby $(-1)^x x=1$, proto $1\notin R(T)$.
(x): Je prosté: $T(x)=T(y)$ pak musí mít $T(x),T(y)$ stejné znaménko, proto mají x,y stejnou paritu, tedy $y=x+2k$. Platí také $|T(x)|=|T(y)|$ a tedy $\left\lfloor\frac{x+1}{2}\right\rfloor=\left\lfloor\frac{y+1}{2}\right\rfloor$, tedy $\left\lfloor\frac{x+1}{2}\right\rfloor=\left\lfloor\frac{x+1}{2}+k\right\rfloor=k+\left\lfloor\frac{x+1}{2}\right\rfloor$, proto $k=0$ a $x=y$.
Je na: Nechť $y\in\mathbb{Z}$. Pokud $y\geq 0$, pak existuje $x=2y\in\mathbb{N}_0$ a $T(x)=1\cdot\left\lfloor y+\frac{1}{2}\right\rfloor=y+\left\lfloor\frac{1}{2}\right\rfloor=y$.
Pokud $y<0$, pak $-2y\geq 2$ a existuje $x=-2y-1\in\mathbb{N}_0$ takové, že $T(x)=(-1)\cdot\lfloor -y\rfloor=y$.
(xi): Je prosté: $T(x)=T(y) \implies (x+1,2x)=(y+1,2y) \implies 2x=2y \implies x=y$. Není na: neexistuje $x\in\mathbb{Z}$ aby $x+1=1$ a $2x=1$, proto $(1,1)\notin R(T)$.
(xii): Je prosté: $T(x)=T(y) \implies (x^2,x^2+2x)=(y^2,y^2+2y) \implies x^2=y^2\wedge x^2+2x=y^2+2y$
$\implies 2x=2y \implies x=y$. Není na: neexistuje $x\in\mathbb{Z}$ aby $x^2=0$ a $x^2+2x=1$, proto $(0,1)\notin R(T)$.
(xiii): Není prosté, třeba $T(2,1)=(4,2)=T(-2,-1)$. Není na: neexistují $x,y\in\mathbb{Z}$ aby $x^2=0$ a $xy=1$, proto $(0,1)\notin R(T)$.
(xiv): Je prosté: $T(x,y)=T(u,v) \implies (x+y,x-y)=(u+v,u-v) \implies x+y=u+v\wedge x-y=u-v$, sečteme: $2x=2u \implies x=u$, odečteme: $2y=2v \implies y=v$, proto $(x,y)=(u,v)$.
Je na: $(u,v)\in\mathbb{Q}^2 \implies \exists x=\frac{1}{2}(u+v), y=\frac{1}{2}(u-v)\in\mathbb{Q}$ a $T(x,y)=(u,v)$.
(xv): Je prosté: $T(x,y)=T(u,v) \implies (x+y,x-y)=(u+v,u-v) \implies x+y=u+v\wedge x-y=u-v$, sečteme: $2x=2u \implies x=u$, odečteme: $2y=2v \implies y=v$, proto $(x,y)=(u,v)$.
Není na: Soustava $x+y=1$, $x-y=0$ nemá řešení v $\mathbb{Z}$, proto $(1,0)\notin R(T)$.
(xvi): Není prosté, třeba $T(1,2)=0=T(0,0)$. Je na: $z\in\mathbb{Z} \implies \exists x=0, y=-z\in\mathbb{Z}$ a $T(x,y)=z$.
(xvii): Není prosté, třeba $T(1,1)=0=T(0,0)$. Na: To je moc dobrá otázka. Existují celá čísla m,n tak, aby třeba $m^2-n^2=2$? Kupodivu ne. Omezíme se na nezáporná m,n. Aby vyšel výsledek kladný, musí být $m>n$, takže $m\geq n+1$ a proto $m^2-n^2\geq(n+1)^2-n^2=2n+1$. Kdyby $n=0$, vyjde z rovnice $m^2-n^2=2$ neřešitelné $m^2=2$, a pro $n\geq 1$ je $m^2-n^2\geq 3$. Takže nic.
(xviii): Není prosté, třeba $T(1,-1)=13=T(-1,1)$. Je na: $z\in\mathbb{Z} \implies \exists x=z, y=-13\in\mathbb{Z}$ a $T(x,y)=z$.
(xix): Není prosté, třeba $T(1,1)=0=T(2,2)$.
Je na: Nechť $z\in\mathbb{Z}$. Pokud $z\geq 0$, pak existuje $x=y, y=0\in\mathbb{N}_0$ a $T(x,y)=z$. Pokud $z<0$, pak existuje $x=0, y=-z\in\mathbb{N}_0$ a $T(x,y)=z$.
2b.8: Není prosté, protože $T(1)=4=T(8)$. Je na, pro $y\in\mathbb{N}$ existuje $x=2y\in\mathbb{N}$ takové, že $T(x)=y$.
2b.9: $T(n)=n$ je prosté a na; $T(n)=2n$ je prosté ale není na; $T(n)=n-1$ pro $n\geq 2$, $T(1)=1$ není prosté a je na, $T(n)=(n-3)^2+2$ není prosté ani na.
$T(n)=\begin{cases}2n+1; & n\geq 0;\\ -2n; & n<0\end{cases}$ je prosté a na; $T(n)=\begin{cases}2n+3; & n\geq 0;\\ -2n; & n<0\end{cases}$ je prosté a není na; $T(n)=|n|+1$ není prosté a je na, $T(n)=n^2+1$ není prosté ani na.
2b.10: Obměny: (i) Jestliže je $S\circ T$ prosté, tak je T prosté. (ii) Jestliže je $S\circ T$ prosté, tak je S prosté.
(iii) Jestliže je $S\circ T$ na, tak je T na. (iv) Jestliže je $S\circ T$ na, tak je S na.
(v) Jestliže je $S\circ T$ bijekce, tak je T bijekce. (vi) Jestliže je $S\circ T$ bijekce, tak je S bijekce.
(i): Platí, T není prosté $\implies \exists x\neq y\in A$: $T(x)=T(y)$, pak $S(T(x))=S(T(y))$ neboli $(S\circ T)(x)=(S\circ T)(y)$.
(ii), (iii), (v), (vi): nepravda. Třeba $A=\{1\}$, $B=\{a,b\}$, $C=\{\alpha\}$. Nechť T: $1\mapsto a$, S: $a,b\mapsto\alpha$. Pak T není na, S není prosté, ale $S\circ T$ je bijekce.

(iv): Platí, dokážeme tu obměnu. Zvolme $c \in C$ libovolné. Protože $S \circ T$ je na, $\exists a \in A$: $(S \circ T)(a) = c$ neboli $S(T(a)) = c$. Označme $b = T(a) \in B$, pak $S(b) = c$. Tedy $\forall c \in C$ najdeme $b \in B$ aby $S(b) = c$, tedy S je na.

2b.11: (i): $y \in T[M \cup N] \iff \exists x \in M \cup N\colon T(x) = y \iff (\exists x_1 \in M\colon T(x_1) = y) \vee (\exists x_2 \in N\colon T(x_2) = y) \iff y \in T[M] \vee y \in T[N] \iff y \in T[M] \cup T[N]$.

(ii): $y \in T[M \cap N] \iff \exists x \in M \cap N\colon T(x) = y \implies (\exists x_1 \in M\colon T(x_1) = y) \wedge (\exists x_2 \in N\colon T(x_2) = y) \iff$

$\iff y \in T[M] \wedge y \in T[N] \iff y \in T[M] \cap T[N]$.

(iii): $y \in T[M] \cap T[N] \iff y \in T[M] \wedge y \in T[N] \iff (\exists x_1 \in M\colon T(x_1) = y) \wedge (\exists x_2 \in N\colon T(x_2) = y)$. protože je T prosté, musí nutně být $x_1 = x_2$, označme $x = x_1 = x_2$ a vidíme, že $x \in M \cap N$, proto $x \in M \cap N$ a $T(x) = y$, tedy $y \in T[M \cap N]$.

(iv): $A = \{1, 2, 3\}$, $B = \{a, b\}$, $M = \{1, 2\}$, $N = \{2, 3\}$, $T(2) = b$, $T(1) = T(3) = a$.

2b.12: (i): $\chi_{\overline{M}}(x) = 1 \iff x \in \overline{M} \iff x \notin M \iff \chi_M(x) = 0 \iff (1 - \chi_M)(x) = 1$, podobně $\chi_{\overline{M}}(x) = 0 \iff (1 - \chi_M)(x) = 0$, tato dvě zobrazení tedy mají stejné hodnoty. Druhou ekvivalenci není třeba dokazovat, protože obě funkce mají jen dvě možné hodnoty, 0 a 1, jestliže tedy nabývají jedničky ve stejných případech, pak nabývají i nuly ve stejných případech (těch ostatních).

(ii): $\chi_{M \cap N}(x) = 1 \iff x \in M \cap N \iff x \in M \wedge x \in N \iff \chi_M(x) = 1 \wedge \chi_N(x) = 1 \iff (\chi_M \cdot \chi_N)(x) = 1$. Poslední ekvivalence plyne z toho, že χ_X může být jen 0 nebo 1.

(iii): Důkaz se nejlépe dělá rozborem podle příslušnosti x k množinám. 1) Jestliže $x \in M \cap N$, pak $\chi_{M \cup N}(x) = 1$ a $(\chi_M + \chi_N - \chi_{M \cap N})(x) = 1 + 1 - 1 = 1$. 2) Jestliže $x \in M$, $x \notin N$, pak $\chi_{M \cup N}(x) = 1$ a $(\chi_M + \chi_N - \chi_{M \cap N})(x) = 1 + 0 - 0 = 1$. 3) Jestliže $x \in N$, $x \notin M$, pak $\chi_{M \cup N}(x) = 1$ a $(\chi_M + \chi_N - \chi_{M \cap N})(x) = 0 + 1 - 0 = 1$. 4) Jestliže $x \notin M$, $x \notin N$, pak $\chi_{M \cup N}(x) = 0$ a $(\chi_M + \chi_N - \chi_{M \cap N})(x) = 0 + 0 - 0 = 0$.

Tyto dvě funkce tedy mají vždy stejné hodnoty.

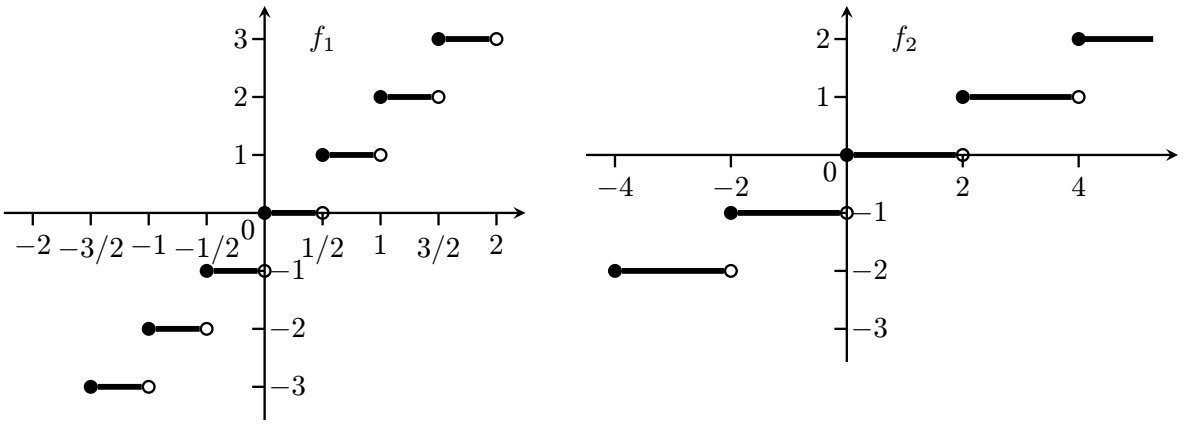
2b.13: 1 byte je 8 bits, takže: $\lceil \frac{4}{8} \rceil = 1$, $\lceil \frac{10}{8} \rceil = 2$, $\lceil \frac{500}{8} \rceil = 63$, $\lceil \frac{3000}{8} \rceil = 375$.

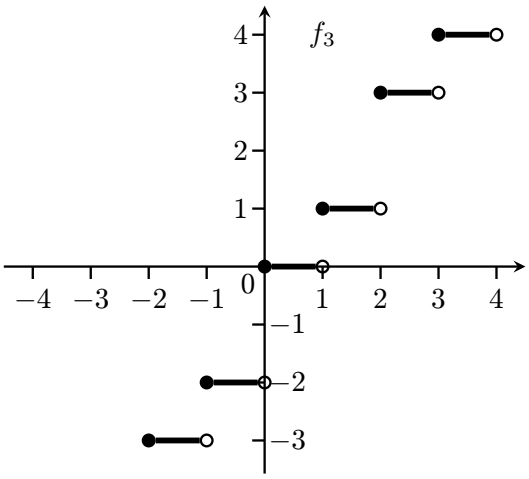
2b.14: Toto chce hodně experimentovat se zaokrouhlováním. (i): $\lfloor b \rfloor - \lceil a \rceil + 1$; (ii): $\lceil b \rceil - \lfloor a \rfloor - 1$.

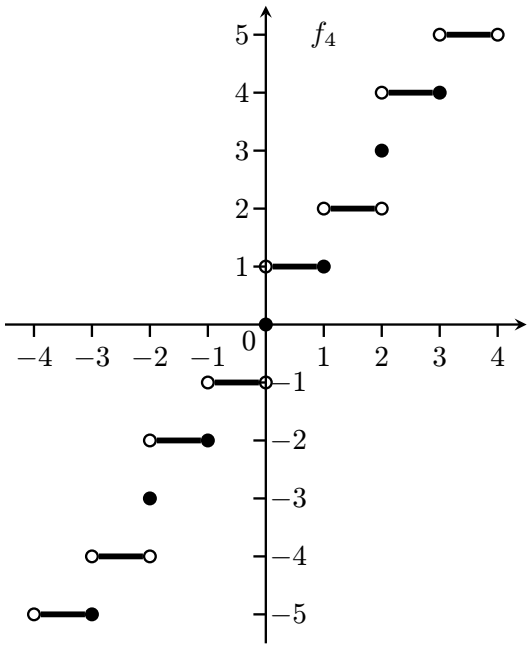
2b.15: Nechť $x = n + r$, kde $r \in \langle 0.1)$. Jestliže $r = 0$, pak $\lfloor x \rfloor = \lceil x \rceil = n$, jinak $\lfloor x \rfloor = n$ a $\lceil x \rceil = n + 1$.

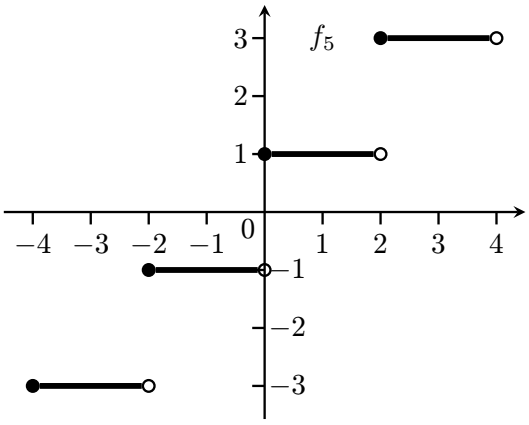
2b.16: Je-li n sudé, pak $n = 2k$ pro $k \in \mathbb{Z}$ a proto $\lfloor \frac{n}{2} \rfloor = \lfloor k \rfloor = k = \frac{n}{2}$. Je-li n liché, pak $n = 2k + 1$ pro $k \in \mathbb{Z}$ a proto $\lfloor \frac{n}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = k = \frac{n-1}{2}$.

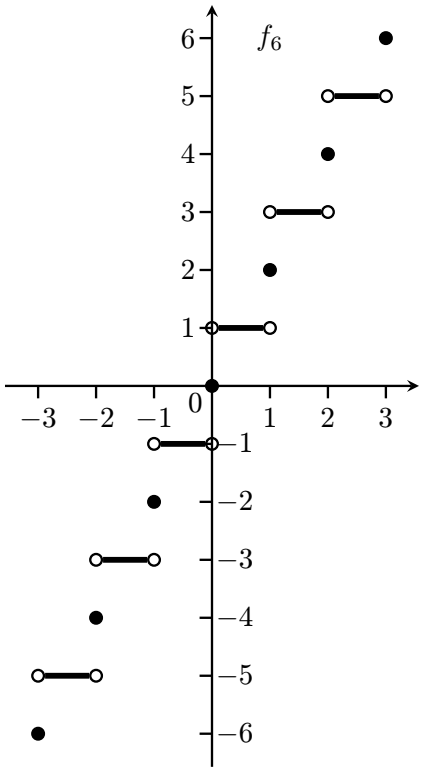
2b.17:











2b.18: (i): Nechť $n = 4k + r$ pro $k \in \mathbb{Z}$ a $r = 0, 1, 2, 3$. Pak $\lfloor \frac{r}{2} \rfloor$ je 0 nebo 1, tedy $\lfloor \frac{1}{2} \lfloor \frac{r}{2} \rfloor \rfloor = 0$ a proto $\lfloor \frac{1}{2} \lfloor \frac{n}{2} \rfloor \rfloor = \lfloor \frac{1}{2} \lfloor 2k + \frac{r}{2} \rfloor \rfloor = \lfloor k + \frac{1}{2} \lfloor \frac{r}{2} \rfloor \rfloor = k + \lfloor \frac{1}{2} \lfloor \frac{r}{2} \rfloor \rfloor = k = \lfloor \frac{n}{4} \rfloor$.
(ii): Nechť $n = 2k + r$, kde $k \in \mathbb{Z}$ a $r = 0, 1$. Pak $\lfloor \frac{n}{2} \rfloor = k$ a $\lceil \frac{n}{2} \rceil = k + r$, proto $\lfloor \frac{n}{2} \rfloor \cdot \lfloor \frac{n}{2} \rfloor = k(k + r)$, zatimco $\lfloor \frac{n^2}{4} \rfloor = \lfloor \frac{4k^2+4kr+r^2}{4} \rfloor = k^2 + kr + \lfloor \frac{r^2}{4} \rfloor = k^2 + kr = k(k + r)$.
2b.19: (i): Neplatí, třeba: $\lfloor 2 \cdot 0.7 \rfloor = 1$, ale $2\lfloor 0.7 \rfloor = 0$.
(ii): Neplatí, třeba $\lfloor 0.5 + 0.5 \rfloor = 1$, ale $\lfloor 0.5 \rfloor + \lfloor 0.5 \rfloor = 0$.
(iii): Neplatí, třeba $\lceil 0.4 + 0.4 \rceil = 1$, ale $\lceil 0.4 \rceil + \lceil 0.4 \rceil = 2$.
(iv): Platí, případy: pokud $x, y \in \mathbb{Z}$, pak evidentně vyjde 0. Pokud $x \in \mathbb{Z}$ a $y \notin \mathbb{Z}$, pak $x = n+r$ a $x+y = x+y+r$, kde $n \in \mathbb{Z}$, $n + y \in \mathbb{Z}$ a $0 < r < 1$, proto $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil = n + 1 + y - (n + y + 1) = 0$. Zbývá případ $x, y \notin \mathbb{Z}$, tedy $x = n + r$, $y = m + s$, kde $m, n \in \mathbb{Z}$ a $0 < r, s < 1$. Dva případy. Pokud $r + s > 1$, pak $\lceil x \rceil + \lceil y \rceil - \lceil x+y \rceil = n+1+y+1-(n+y+2) = 0$. Pokud $r+s \leq 1$, pak $\lceil x \rceil + \lceil y \rceil - \lceil x+y \rceil = n+1+y+1-(n+y+1) = 1$.
(v): Neplatí, třeba $\lceil 1.1 \cdot 1.1 \rceil = \lceil 1.21 \rceil = 2$, ale $\lceil 1.1 \rceil \cdot \lceil 1.1 \rceil = 2 \cdot 2 = 4$.
(vi): Neplatí, třeba $\lfloor 4 \cdot 0.5 \rfloor = \lfloor 2 \rfloor = 2$, ale $\lfloor 4 \rfloor \cdot \lfloor 0.5 \rfloor = 4 \cdot 0 = 0$.
(vii) a (viii): Platí, protože $\lfloor x \rfloor \in \mathbb{Z}$ a $\lfloor x \rfloor \in \mathbb{Z}$, takže aplikace dalšího zaokrouhlení již nic neovlivní.
(ix): Neplatí, nechť $x = 1.9^2 = 3.61$, pak $\lfloor \sqrt{\lceil x \rceil} \rfloor = 2$, ale $\lfloor \sqrt{x} \rfloor = 1$.

(x): Platí. Pro $x \geq 0$ nechť $n \in \mathbb{N}_0$ je číslo takové, že $n^2 \leq x < (n+1)^2$. Pak $n \leq \sqrt{x} < n+1$, proto $\lfloor \sqrt{x} \rfloor = n$. Jelikož $n^2 \in \mathbb{Z}$, bude i $n^2 \leq \lfloor x \rfloor < (n+1)^2$ a tedy $n \leq \sqrt{\lfloor x \rfloor} < n+1$, proto i $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = n$.
(xi): Platí, důkaz jako v (xi), pro dané $x \geq 0$ se vybere $n \in \mathbb{N}$ tak, aby $(n-1)^2 < x \leq n^2$.

2c. Mohutnost množin

V předchozí sekci jsme si intuitivně rozmysleli, že pokud máme konečné množiny s různým počtem prvků, tak mezi nimi nedokážeme udělat bijekci, viz Fakt 2b.12 (iii). Naopak pokud máme dvě konečné množiny se stejným počtem prvků, tak mezi nimi bijekci udělat dokážeme (stačí si prvky v obou množinách očíslovat a poslat první na první, druhý na druhý atd.) Tato pozorování se stanou východiskem pro porovnávání velikostí množin obecně.

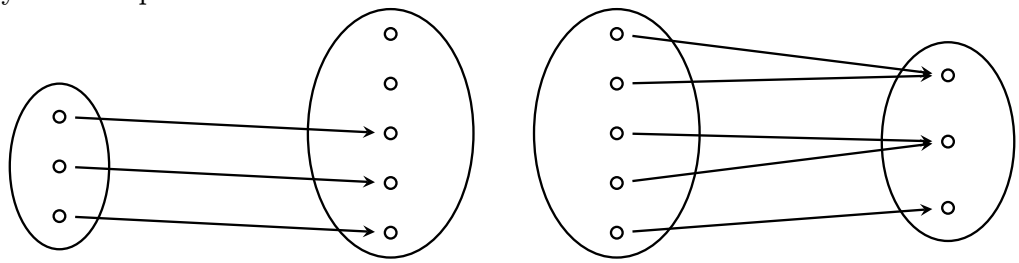
! **Definice.**
Řekneme, že množiny A, B mají stejnou **mohutnost**, značeno $|A| = |B|$, jestliže existuje bijekce z A na B.
Řekneme, že mohutnost množiny A je menší nebo rovna mohutnosti množiny B, značeno $|A| \leq |B|$ nebo $|B| \geq |A|$, jestliže existuje prosté zobrazení z A do B.

We say that two sets A, B have the same **cardinality**, denoted $|A| = |B|$, if there exists a bijection from one onto the other.

We say that cardinality of A is less then or equal to cardinality of B, denoted $|A| \leq |B|$, if there exists a 1-1 mapping from A to B.

Odpovídá i druhá definice naší intuici pro konečné množiny?

Předpokládejme, že máme prosté zobrazení $T\colon A \mapsto B$. Pak je $T\colon A \mapsto R(T)$ bijekce, tudíž mají A a $R(T)$ stejnou mohutnost (šipky se nesbíhají, to zní rozumně). A protože $R(T) \subseteq B$, tak je přirozené, že pak považujeme B za větší (případně stejně velké) ve srovnání s A, přesně toto konec konců říká obměna tvrzení (ii) z Faktu 2b.12. A naopak, přinejmenším u konečných množin má člověk pocit, že by z menší dokázal posílat šipky do větší tak, aby se nesbíhaly, a vyrobit tak prosté zobrazení.



Obrázek napravo naznačuje ještě jeden způsob, jak poznat tu větší množinu ze dvou, vycházíme zde z obměny tvrzení (i) z Faktu 2b.12. Formálně:

Fakt 2c.1.
Nechť A, B jsou množiny.
$|A| \leq |B|$ právě tehdy, když existuje zobrazení $T\colon B \mapsto A$, které je na.

Toto se občas hodí, ale většinou je výrazně snadnější pracovat s prostými zobrazeními jako v definici.

Poznamenejme, že existuje ještě alternativní a velmi rozšířené značení pro porovnávání mohutnosti. Někteří autoři píšou místo $|A| \leq |B|$ zápis $A \preceq B$ a místo $|A| = |B|$ píšou $A \sim B$, popřípadě $A \approx B$. Sám nemám jasnou preferenci, možná mírně k tomuto alternativnímu značení, ale v této knize používáme symbol $\preceq$ pro relaci částečného uspořádání, tak jsem pro mohutnost zvolil verzi s $|A|$.

Teď dokážeme několik jednoduchých vlastností, které nás ubezpečí, že se nové pojmy chovají tak, jak bychom rádi.

Fakt 2c.2.
Nechť A je množina.
(i) $|A| = |A|$ a $|A| \leq |A|$.
(ii) Jestliže $B \subseteq A$, pak $|B| \leq |A|$.
(iii) $|A| = |B|$ právě tehdy, když $|B| = |A|$.

Důkaz (rutinní)**:** (i): Uvažujme identitu i_A: $A \mapsto A$ (viz mocniny T^n). Toto zobrazení je bijekce, tudíž je $|A| = |A|$, a je i prosté, proto $|A| \leq |A|$.

(ii): Zobrazení i_B: $B \mapsto B$ lze považovat také za zobrazení i_B: $B \mapsto A$. Tím, že se do cílové množiny přidaly prvky navíc, jsme nemohli změnit prostotu i_B (pořád posílá stejné prvky stejným způsobem), podle definice tedy $|B| \leq |A|$.

(iii): Jestliže $|A| = |B|$, pak existuje bijekce T: $A \mapsto B$. Inverzní zobrazení T^{-1} dává bijekci z B na A, tedy $|B| = |A|$. Opačný směr plyne ze symetrie.

□

Čtenáři se tato tvrzení (stejně jako mnohá další) mohou zdát samozřejmá, ale samozřejmá jsou jen pro intuitivní pojem „velikosti množiny“ tak, jak jej zná z běžného života. Zde máme „mohutnost“ definovanou pomocí zobrazení, takže platnost oněch „jasných“ věcí není automatická a je třeba je ověřit pomocí definice. Protože jsme pojem mohutnosti vymysleli dobře, budou ty běžné věci v běžných situacích fungovat, ale občas to dá překvapivě hodně práce a někdy ty jasné věci nebudou fungovat vůbec (to je reklama na zbytek kapitoly).

S mohutností (tedy porovnávání množin dle velikosti) se pracuje podobně jako s porovnáváním čísel podle velikosti $|x| \leq |y|$ a $|x| = |y|$, následující tvrzení ukážou, že tyto vztahy mají podobné vlastnosti.

Fakt 2c.3.
Nechť A, B, C jsou množiny.
(i) Jestliže $|A| \leq |B|$ a $|B| \leq |C|$, pak $|A| \leq |C|$.
(ii) Jestliže $|A| \leq |B|$ a $|B| = |C|$, pak $|A| \leq |C|$.
Jestliže $|A| = |B|$ a $|B| \leq |C|$, pak $|A| \leq |C|$.
(iii) Jestliže $|A| = |B|$ a $|B| = |C|$, pak $|A| = |C|$.

Důkaz (rutinní, poučný)**:** (i): Z předpokladu $|A| \leq |B|$ dostáváme existenci zobrazení T: $A \mapsto B$, které je prosté. Podobně z předpokladu $|B| \leq |C|$ dostaneme prosté zobrazení S: $B \mapsto C$. Podle Faktu 2b.10 (i) je i složené zobrazení $S \circ T$: $A \mapsto C$ prosté, proto podle definice je $|A| \leq |C|$.

(ii): Teď se začne prostým zobrazením a bijekcí, ale ta je také prostá, tudiž máme dvě prostá zobrazení a dál je to jako v (i).

(iii): Stejný důkaz, jen se použije Fakt 2b.10 (iii).

Na tento důkaz už byste opravdu měli přijít sami.

□

Fakt 2c.4.
Nechť A, B jsou množiny.
Jestliže $|A| = |B|$, pak $|A| \leq |B|$ a $|B| \leq |A|$.

Důkaz (rutinní)**:** Jestliže $|A| = |B|$, pak existuje bijekce T: $A \mapsto B$. Tato bijekce je i prostá, proto $|A| \leq |B|$, a je na, tedy $|A| \geq |B|$.

□

Platí to i naopak? Ano, ale už to není tak lehké, což je vidět například z toho, že je to věta a navíc pojmenovaná po třech lidech, kteří se na ni museli dát dohromady.

! **Věta 2c.5.** (Cantor-Bernstein-Schroeder)
Nechť A, B jsou množiny. Jestliže $|A| \leq |B|$ a $|B| \leq |A|$, pak $|A| = |B|$.

Důkaz je těžký, je totiž třeba ze dvou prostých zobrazení $A \mapsto B$ a $B \mapsto A$ vyrobit bijekci. Zvědavci a puntičkáři mohou zkusit prakticky jakoukoliv tlustší knihu o teorii množin či Wikipedii. Každopádně je to věta zajímavá nejen z hlediska teoretického, ale i z hlediska praktického. Vyrábět bijekce je totiž často výrazně obtížnější než vyrobit prostá zobrazení, která potřebujeme k důkazu oněch dvou „nerovností“.

Vidíme, že porovnávání mohutnosti se opravdu silně podobá rovnosti a nerovnosti, pro další užitečné vlastnosti se podívejte na cvičení 2c.1. Zavedeme ještě jedno značení, které nám občas zjednoduší práci.

Definice.
Nechť A, B jsou množiny. Řekneme, že mohutnost A je **striktně (ostře) menší** než mohutnost B, značeno $|A| < |B|$, jestliže $|A| \leq |B|$, ale neplatí $|A| = |B|$.
Zavedeme také značení $|A| \neq |B|$ pro případ, kdy neplatí $|A| = |B|$.

Teď si v mohutnostech množin uděláme pořádek.

! **Definice.**
Množina A se nazve **konečná**, jestliže $A = \emptyset$ (pak píšeme $|A| = 0$) nebo existuje takové $m \in \mathbb{N}$, aby platilo $|A| = |\{1, 2, \dots, m\}|$, pak píšeme $|A| = m$.
Jinak se množina nazve **nekonečná**.
Množina A se nazve **spočetná**, jestliže má stejnou mohutnost jako množina $\mathbb{N}$.
Množina A se nazve **nespočetná**, jestliže je nekonečná, ale není spočetná.

We say that a set A is **finite** if either $A = \emptyset$, then we write $|A| = 0$, or if there exists $m \in \mathbb{N}$ such that $|A| = |\{1, 2, \dots, m\}|$, then we write $|A| = m$. Otherwise we say that A is **infinite**. We say that A is **countable** if $|A| = |\mathbb{N}|$. We say that A is **uncountable** if it is infinite but not countable.

Poznámka: Někteří autoři rozumí pod pojmem „spočetná“ podmínku $|A| \leq |\mathbb{N}|$, z pohledu diskrétní matematiky to docela dává smysl, protože právě s těmito množinami se dobře pracuje například indukcí. My zde volíme obvyklejší názvosloví (spočetná znamená $|A| = |\mathbb{N}|$), podmínku $|A| \leq |\mathbb{N}|$ umíme vyjádřit slovy „A je nejvýše spočetná“. Praktický dopad nejednoznačnosti v terminologii je, že až se budete s někým o spočetnosti bavit, tak se nejprve domluvte, co tím vlastně myslíte.
△

Příklad 2c.a: $|\{a, b, a\}| = 2$, $|\emptyset| = 0$. Množina $\mathbb{N}$ je nekonečná a spočetná. Množina $\mathbb{R}$ je nekonečná, ale zatím nevíme, jestli je spočetná.
△

Poučná poznámka. Čtenáře možná překvapí, že si v zásadě můžeme definice dělat, jak chceme. Můžeme třeba zadefinovat, že konečné množiny jsou ty, které obsahují číslo 13, ostatní množiny jsou pak nekonečné. Z čistě logického hlediska by to nebylo špatně, jenže nový pojem velikosti by měl divné vlastnosti (například sjednocením konečné a nekonečné množiny bychom dostali konečnou). To v zásadě nevadí, matematici rádi vymýšlejí podivné světy a pak zkoumají, co tam vlastně platí a co ne, jenže my matematiku vytváříme také proto, aby byla užitečná, a moje alternativní definice velikosti množin je na pytel. Kdybych tu definici vážně navrhnul, matematici by se mi hlasitě smáli.

Když matematici nové pojmy vymýšlejí, tak se přitom řídí několika zásadami. Jako druhou věc po definici chtějí, aby ten nový pojem k něčemu byl. Často se jedná o pojem inspirovaný naší intuicí či zkušeností, pak se také chce, aby ten pojem s naší intuicí souhlasil. Naše diskuse a faktíky výše i níže doufejme přesvědčí čtenáře, že zde zavedený pojem mohutnosti opravdu funguje tak, jak bychom chtěli. Třeba jsme dokázali, že když je A „menší“ než B a B „menší“ než C, tak je nutně A „menší“ než C. Kdyby to náš pojem velikosti množin nesplňoval, tak bychom měli silné podezření, že jsme naši definici nevymysleli zrovna nejlépe.

Ovšem to první, co matematici při vytváření definice žádají, je její správnost logická. Říká se tomu, že se chce, aby „definice měla smysl“, což mimo jiné znamená, že musí umět rozhodnout. Například to, zda $|A| = |B|$, je jasné, prostě buď nějaká bijekce je, nebo není. U naší definice konečných a jiných množin to ovšem jasné není, čímž se konečně dostáváme k tématu této poznámky. Je velikost množiny touto definicí jasně dána? Máme například množinu A, která je bijekcí spojena s množinou $\{1, 2, 3\}$, tudíž podle definice $|A| = 3$. Mohlo by se stát, že by také existovala bijekce z A na $\{1, 2, 3, 4\}$? To by bylo velice nemilé, protože pak by také $|A| = 4$ a my rozhodně nechceme, aby jedna množina mohla mít více velikostí.

Podle Faktu 2c.3 (iii) by pak ale platilo $|\{1, 2, 3\}| = |\{1, 2, 3, 4\}|$, což nevypadá moc pravděpodobně. Abychom ukázali, že naše definice funguje rozumně, musíme dokázat, že nelze vytvořit bijekci mezi $\{1, 2, 3\}$ a $\{1, 2, 3, 4\}$, podobně o dalších vzorových množinách rozdílných velikostí. To je ale spíš téma pro teorii množin, necháme to odborníkům a spokojíme se s konstatováním, že to ověřili a nepřístojnosti se nekonají.

Podobně si necháme dokázat, že ani množina $\mathbb{N}$ se nedá bijekcí spojit s množinami typu $\{1, \dots, n\}$, čímž se potvrdí, že nejde o množinu konečnou (to jsme si oddechli). V definici je tedy vše v pořádku.
△

Teď se postupně podíváme na jednotlivé typy mohutností. Začneme množinami konečnými a ukážeme, že věci fungují tak, jak bychom čekali. Nejprve zkusíme (snadným) tvrzením čtenáře přesvědčit, že definice opravdu správně vystihla, co konečné množiny jsou.

Fakt 2c.6.
(i) Nechť A je konečná množina, $|A| = n$. Pak ji lze zapsat jako $A = \{a_1, a_2, \dots, a_n\}$, kde a_k jsou navzájem různé prvky.
(ii) Je-li naopak $A = \{a_1, a_2, \dots, a_n\}$, kde a_k jsou navzájem různé prvky, pak A je konečná a $|A| = n$.

Důkaz (poučný)**:** (i): Protože je to množina konečná, existuje bijekce T z nějaké množiny $\{1, 2, \dots, n\}$ na A. Definujme $a_k = T(k)$, pak z prostoty vyplývá, že jsou to navzájem různé prvky A, a ze surjektivity T vyplývá, že $A = \{a_1, a_2, \dots, a_n\}$.

(ii): Jestliže $A = \{a_1, \dots, a_n\}$, pak stačí definovat $T(a_k) = k$. To bude určitě zobrazení z A na $\{1, \dots, n\}$ a prosté je také: Jestliže jsou $x \neq y \in A$, pak existují indexy k, l takové, že $x = a_k$ a $y = a_l$. Protože $x \neq y$, musí být i $k \neq l$ a tedy $T(x) \neq T(y)$.

□

Následující věta ukazuje, že se pojmy spojené s konečnými množinami chovají v souladu s naší intuicí. Poznamenejme, že důkaz je snadný, ale dlouhý, protože je třeba hlídat spoustu věcí. Pro čtenáře může být zajímavé si důkaz číst a přitom si kreslit odpovídající obrázky.

! **Věta 2c.7.**
(i) Jestliže je A konečná množina, pak je i každá její podmnožina B konečná a platí $|B| \leq |A|$.
Je-li navíc B podmnožina vlastní, pak $|B| < |A|$.
(ii) Nechť A, B jsou konečné množiny. Pak je i $A \cup B$ konečná a platí $|A \cup B| \leq |A| + |B|$.
Jsou-li navíc A, B disjunktní, pak $|A \cup B| = |A| + |B|$.
(iii) Nechť A, B jsou konečné množiny. Pak je $A \times B$ konečná a platí $|A \times B| = |A| \cdot |B|$.

U (i) je zajímavá i obměna, viz cvičení 2c.5.

Důkaz (poučný, asi drsný)**:** Důkaz (i) spíš jen naznačíme. Nechť A je konečná množina. Podle definice tedy existuje $m \in \mathbb{N}$ a bijekce T z A na $\{1, \dots, m\}$. Začneme následující situací. Nechť a je libovolný prvek A a uvažujme množinu $A' = A - \{a\}$. Chceme dokázat, že je konečná a má menší mohutnost než A. Kdyby náhodou $T(a) = m$, pak je restrikce $T|_{A'}$ bijekcí z A' na $\{1, \dots, m-1\}$, což dokazuje, že A' je konečná a $|A'| = m - 1 < |A|$.

Zbývá rozebrat situaci, když $T(a) = n < m$. Protože je T na, musí existovat jiný prvek $b \in A$ takový, že $T(b) = m$. Vytvoříme nové zobrazení tak, že tyto dvě šipky prohodíme. Formálně to uděláme tak, že definujeme

$$S(x) = \begin{cases} T(x), & x \in A' - \{b\}; \\ n, & x = b. \end{cases}$$

Protože si S vybírá své hodnoty z hodnot T, dostali jsme zobrazení z A' do $\{1, \dots, m\}$, ale hodnotě m jsme se také vyhnuli, takže zobrazení S jde vlastně do množiny $\{1, \dots, m-1\}$.

Je prosté? Nechť $x \neq y \in A'$. Jestliže se ani jeden z x, y nerovná b, pak $S(x) = T(x)$ a $S(y) = T(y)$; ale T bylo prosté, proto $S(x) \neq S(y)$. Druhá možnost je, že jeden z nich je b, podle symetrie můžeme předpokládat, že třeba $x = b$ a $y \neq b$. Pak $S(x) = n$, mohlo by být i $S(y) = n$? Protože $y \neq b$, tak $S(y) = T(y)$, a jediný prvek z A, který dá po dosazení do T hodnotu n, byl a, ale ten v A' není a proto $y \neq a$, tedy i $S(y) \neq n$.

Takže T je prosté z A do $\{1, \dots, m-1\}$, proto $|A'| \leq m - 1 < |A|$.

Ukázali jsme, že se mohutnost konečné množiny při odebrání prvku zmenší, z toho už (i) vyplyne.

(ii): Nejprve dokážeme případ, kdy jsou A a B disjunktní. Podle předpkladu jsou konečné, tedy existují čísla $m, n \in \mathbb{N}$ a bijekce R: $A \mapsto \{1, \dots, m\}$ a S: $A \mapsto \{1, \dots, n\}$.

Definujme zobrazení T na množině $A \cup B$ takto:

$$T(x) = \begin{cases} R(x), & x \in A; \\ S(x) + m, & x \in B. \end{cases}$$

Obrázkem: Jako bychom posunuli cíle šipek vedoucích z B do $\mathbb{N}$ nahoru o m, čímž na začátku $\mathbb{N}$ vzniklo přesně m volných míst pro původní (neposunuté) šipky z A.

Tato definice má smysl, protože každý prvek x padne přesně do jedné z těch kategorií (A či B), u žádného nemůže být spor mezi dvěma různými možnostmi—tady právě silně používáme toho, že jde o množiny disjunktní.

Tvrdíme, že jde o bijekci z $A \cup B$ na $\{1, \dots, m+n\}$.

Nejprve ukážeme, že nevyskočí pryč. Vezměme $x \in A \cup B$. Jestliže $x \in A$, pak $T(x) = R(x) \leq m \leq m + n$. Jestliže $x \in B$, pak $T(x) = S(x) + m \leq n + m$. Zobrazení T tedy opravdu jde do cílové množiny. Je na?

Nechť $k \in \{1, \dots, m+n\}$. Jsou dvě možnosti. Pokud je $k \leq m$, pak díky tomu, že je R na, dostaneme $a \in A$ takové, že $T(a) = k$. Pak ovšem $a \in A \cup B$ a $T(a) = R(a) = k$.

Pokud je $k > m$, pak $1 \leq k - m \leq n$ a S bylo také na, tudíž existuje $b \in B$ splňující $S(b) = k - m$. Pak $b \in A \cup B$ a $T(b) = S(b) + m = (k - m) + m = k$. Surjektivita T je dokázána.

Je T prosté? Vezměme $x \neq y \in A \cup B$. Jestliže obě splňují $x, y \in A$, pak $T(x) = R(x)$ a $T(y) = R(y)$. Protože R bylo prosté, musí být $T(x) \neq T(y)$.

Jestliže jsou oba prvky v B, pak podobně $S(x) \neq S(y)$ a proto $S(x) + m \neq S(y) + m$, tedy $T(x) \neq T(y)$.

Zbývá situace, že jeden prvek je z A a druhý z B, podle symetrie situace můžeme předpokládat, že $x \in A$ a $y \in B$. Pak ale $T(x) = R(x) \leq m$, zatímco $T(y) = S(y) + m > m$. Tudíž zase $T(x) \neq T(y)$ a všechny možnosti jsme vyčerpali. T je prosté.

Ukázali jsme, že existuje bijekce z $A \cup B$ na $\{1, \ldots, m + n\}$. Proto je podle definice množina $A \cup B$ konečná a $|A \cup B| = m + n = |A| + |B|$.

Zbývá ukázat, že platí to obecné tvrzení pro A a B libovolné. To se udělá následujícím trikem.

Uvažujme množinu $B' = B - A$ (vyhodíme z B společné prvky s A, pokud nějaké jsou). Pak $B' \subseteq B$, proto je to podle (i) konečná množina a platí $|B'| \leq |B|$. Navíc jsou A a B' disjunktní, proto podle právě dokázaného je i $A \cup B'$ konečná a platí $|A \cup B'| = |A| + |B'|$.

Platí také $A \cup B = A \cup B'$ (viz cvičení 2a.1 (vi), když tak si nakreslete Vennův diagram), proto máme

$$|A \cup B| = |A \cup B'| = |A| + |B'| \leq |A| + |B|.$$

(iii): Protože je A konečná množina, můžeme ji napsat jako $\{a_1, \ldots, a_m\}$, kde $m = |A|$ (viz Fakt 2c.6). Pro $k \in \{1, \ldots, m\}$ uvažujme $B_k = \{(a_k, b);\ b \in B\}$. Pak je zobrazení $T_k(b) = (a_k, b)$ bijekce z B na B_k. Prostota: $x \neq y \in B \implies (a_k, x) \neq (a_k, y) \implies T_k(x) \neq T_k(y)$.

Na: Nechť $(a_k, b) \in B_k$. Pak $b \in B$ a $T_k(b) = (a_k, b)$.

Tohle je zjevné, prostě jsme ke každému prvku z množiny B jakoby přidali značku, také si to můžeme představit, že jsme celou množinu jen posunuli, množina tím samozřejmě nemohla změnit velikost. Máme tedy $|B| = |B_k|$. Teď si uvědomíme, že B_k jsou navzájem disjunktní množiny, nebot pro $k \neq l$ se prvky z B_k liší od prvků z B_l na první souřadnici, a $A \times B = B_1 \cup \cdots \cup B_m$. Můžeme teď opakovaně použít výsledek z (ii) a dostaneme

$$|A \times B| = |B_1| + \cdots + |B_m| = |B| + \cdots + |B| = m \cdot |B| = |A| \cdot |B|.$$

Tím je důkaz hotov.

□

Samozřejmě existují i verze pro více množin.

! **Věta 2c.8.**
(i) Jsou-li A_i pro $i = 1, 2, \ldots, n$ konečné množiny, pak je i $\bigcup_{i=1}^{n} A_i$ konečná a $\left|\bigcup_{i=1}^{n} A_i\right| \leq \sum_{i=1}^{n} |A_i|$.
Jsou-li navíc po dvou disjunktní, tak $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$.
(ii) Jsou-li A_i pro $i = 1, 2, \ldots, n$ konečné množiny, pak je i $A_1 \times \cdots \times A_n$ konečná a

$$|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n| = \prod_{i=1}^{n} |A_i|.$$

Důkaz je indukcí a necháme to do cvičení 5a.11. Vrátíme se ještě k situaci, když sjednocujeme množiny A a B, které nejsou disjunktní. Jakou velikost pak dostaneme? Jestliže zvlášť spočítáme prvky z A a prvky z B, tak jsme vlastně dvakrát započítali ty prvky, které jsou společné, což je třeba napravit. Teď už je asi jasné, jak se to má dělat.

Fakt 2c.9.
(i) Jsou-li A, B konečné množiny, pak $|A \cup B| = |A| + |B| - |A \cap B|$.
(ii) Jsou-li A, B, C konečné množiny, pak

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Důkaz (náznak)**:** Pořádný důkaz by nás zase zavedl do hlubin teorie množin, v knihách se často odvoláme právě na to, kolikrát je který prvek zpočítán nalevo a napravo. Pro (i) jsme to už provedli před Faktem, pro (ii) to uděláme teď.

Na levé straně je samozřejmě každý prvek z $A \cup B \cup C$ započítán jen jednou. Musíme ukázat totéž o pravé straně. Rozdělíme si prvky podle toho, zda do A, B, C patří či nepatří. Víme, že je celkem 8 možností, z toho ta, kdy nejsou ani v jedné množině, nás teď nezajímá. Zbývá 7 ostatních.

a) $x \in A$, ale není v žádné ostatní množině. Pak neleží ani v žádném z průniků, tudíž je napravo započítán jen jednou. Podobná úvaha platí i pro prvky jen z B a prvky jen z C.

b) $x \in A$, $x \in B$, ale $x \notin C$. Pak x leží z těch množin napravo v A, B, $A \cap B$ a žádné jiné, tudíž je tam započítán $1 + 1 - 1 = 1$ krát. Podobná úvaha zase platí pro prvky, které jsou jen v A a C či jen v B a C.

c) Zbývají prvky, které jsou v A, B i v C. Takové prvky jsou pak ve všech množinách napravo, tudíž jsou započítány celkem $1 + 1 + 1 - 1 - 1 - 1 + 1 = 1$ krát.

□

Je užitečné si nakreslit obecný Vennův diagram a rozmyslet si, co se děje. Dá se to zase zobecnit na konečný počet množin, ale pak to začne být docela zajímavé a necháme to do kapitoly 11b.

Teď se podívejme na množiny nekonečné, které asi čtenáře dosud nezasvěceného do magie nekonečna notně překvapí. Začneme faktem, který říká, že nejmenší nekonečné množiny jsou ty spočetné.

Fakt 2c.10.
Nechť A je množina. Jestliže je nekonečná, pak $|\mathbb{N}| \leq |A|$.

Důkaz (náznak)**:** Protože jde o nekonečnou množinu, určitě není prázdná. Vezměme tedy $a_1 \in A$. Pokud něco zbývá v $A - \{a_1\}$, vybereme odtud a_2. Pokud něco zbývá v $A - \{a_1, a_2\}$, vybereme odtud a_3 a tak dále. Jsou dvě možnosti.

a) Pokud se tento proces někdy zarazí, tak to bude tím, že pro nějaké m je $A - \{a_1, \dots, a_m\}$ prázdná množina. Pak ale $A = \{a_1, \dots, a_m\}$ a podle Faktu 2c.6 (ii) by byla A konečná, což je spor s předpokladem tvrzení, že je nekonečná, čili to nemůže nastat.

b) Určitě tedy nastane druhý případ, kdy najdeme nekonečně mnoho navzájem různých prvků $a_n \in A$. Pak $T(n) = a_n$ je bijekce z $\mathbb{N}$ na $A' = \{a_n;\ n \in \mathbb{N}\}$, proto $|A'| = |\mathbb{N}|$. Také máme $A' \subseteq A$, proto $|A'| \leq |A|$, zbytek plyne pomocí Faktu 2c.3 (ii).

□

Připomeňme si Větu 2c.7, která nám říkala, že se pojem velikosti chová u konečných množin přesně tak, jak bychom čekali. Následující věta ukáže, že u množin nekonečných je všechno jinak.

Věta 2c.11.
(i) Každá nekonečná množina má vlastní podmnožinu, která má stejnou mohutnost.
(ii) Nechť A, B jsou množiny, A je nekonečná a $|B| \leq |A|$. Pak $|A \cup B| = |A|$.
(iii) Nechť A, B jsou množiny, A je nekonečná a $|B| \leq |A|$. Pak $|A \times B| = |A|$.
(iv) Nechť A_i pro $i = 1, \dots, m$ nebo $i \in \mathbb{N}$ jsou množiny, kde A_1 je nekonečná, a nechť $|A_i| \leq |A_1|$ pro všechna i. Pak $\left|\bigcup_i A_i\right| = |A_1|$.
(v) Nechť A_i pro $i = 1, \dots, m$ nebo $i \in \mathbb{N}$ jsou množiny, kde A_1 je nekonečná, a nechť $|A_i| \leq |A_1|$ pro všechna i. Pak $|A_1 \times A_2 \times \cdots| = |A_1|$.

Všechny vlastnosti vypadají šíleně. Uberu z množiny prvky a ona zůstane stejně velká. Přidám si k nekonečné množině nějaké prvky (srovnejte s Větou 2c.7 (ii)) a ona je pořád stejně velká. Přidám k nekonečné množině jinou, třeba i disjunktní, třeba i stejně velkou nekonečnou, a ta množina se nezvětší. Dokonce nám (iv) říká, že to nekonečná množina ani velikostně nepozná, když k ní přidám nekonečně (ale spočetně) mnoho takto menších množin. Vlastnosti (iii) a (v) ukazují totéž pro kartéský součin, kde by to člověk čekal ještě méně.

Platí dokonce, že se podle takto divného chování nekonečné množiny poznají: Množina je nekonečná právě tehdy, jestliže má nějakou vlastní podmnožinu stejné mohutnosti.

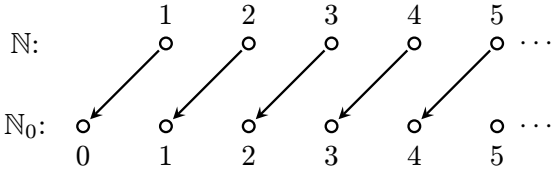
Tvrzení (iii) lze vyjádřit ještě jinak: Když sjednotíme konečný či spočetný soubor množin, z nichž alespoň jedna je nekonečná, tak má toto sjednocení stejnou mohutnost jako největší ze zúčastněných množin. Stejná věc platí pro kartézský součin.

Níže ukážeme, že všechny tyto vlastnosti při bližším pohledu dávají smysl. Problém je v tom, že my se nejsme zvyklí potkávat s nekonečnými množinami, proto si náš mozek nevytvořil příslušné představy. Abychom tedy byli schopni dobře pracovat s mohutností, musíme si naši intuici vycvičit, aby jí ty divné věci přišly normální. To je jedna z věcí, která je na skutečné matematice obtížná, někdy je třeba pracovat ve světech, které se chovají zcela mimo naše představy (mohutnost je ještě v zásadě v pohodě), o to důležitější je pak hlídat si logickou správnost postupů, tvrzení a argumentů v důkazech. Pro většinu lidí je takovéto cvičení vlastního mozku příliš těžké, asi je k tomu třeba nějaká mutace. Možná nejpřekvapivější na tom ale je, že se některé šílené matematické struktury kupodivu vyskytují v převleku kolem nás (teorie relativity, kvantová mechanika).

Důkaz Věty 2c.11 tady dělat nebudeme, místo toho si ukážeme konkrétní případy, kdy k těmto jevům dochází. Pomůže nám to vycvičit naší intuici. Silně doporučujeme následující důkaz nepřeskočit, protože to je spíš zamyšlení nad fungováním nekonečnosti.

! **Věta 2c.12.**
(i) Množina $\mathbb{N}_0$ je spočetná.
(ii) Množina $\mathbb{Z}$ je spočetná.
(iii) Množina $\mathbb{N} \times \mathbb{N}$ je spočetná.
(iv) Množina $\mathbb{Z} \times \mathbb{Z}$ je spočetná.

Důkaz (poučný, dobrý)**:** (i): Ukážeme, že $\mathbb{N}_0$ má stejnou mohutnost jako $\mathbb{N}$. Potřebujeme najít nějakou bijekci $T\colon \mathbb{N} \mapsto \mathbb{N}_0$, často jako inspirace poslouží obrázek, v tomto případě se nápad docela nabízí.



Formálně definujeme $T(n) = n - 1$. Tvrdíme, že toto zobrazení je bijekce.

Na: Nechť $m \in \mathbb{N}_0$. Pak je m celé číslo splňující $m \geq 0$, proto je $n = m + 1$ celé číslo splňující $n \geq 1$, tedy $n \in \mathbb{N}$, a platí $T(n) = n - 1 = m$.

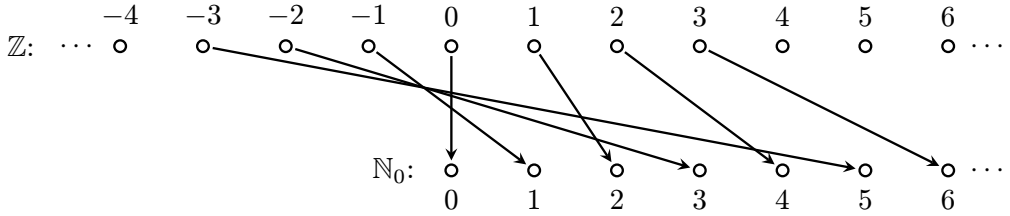
Prosté: Nechť $x, y \in \mathbb{N}$ splňují $T(x) = T(y)$. Pak $x - 1 = y - 1$, tedy $x = y$.

Poznámka: Řečeno hodně nepřesně, klíčovou vlastností nekonečných množin je, že v některém „směru“ nekončí (například rovina nekončí v mnoha směrech, přímka ve dvou). Množinu proto můžeme v takovém směru bez problémů posunout a tím si vytvořit místo pro přidání prvků, aniž by se množina velikostí zvětšila.

V následujícím důkazu množinu $\mathbb{N}$ nejen posuneme, ale zároveň ji rozprostřeme (zředíme), čímž vznikne nekonečně mnoho volných míst.

△

(ii): Ukážeme, že $|\mathbb{Z}| = |\mathbb{N}|$. Protože už máme $|\mathbb{N}| = |\mathbb{N}_0|$, stačí podle Faktu 2c.3 (iii) dokázat, že platí $|\mathbb{Z}| = |\mathbb{N}_0|$. Vytvoříme zobrazení ze $\mathbb{Z}$ na $\mathbb{N}_0$ následovně. Čísla ze $\mathbb{Z}_0^+$ pošleme do $\mathbb{N}_0$, ale šipky roztáhneme, aby v cíli zbyla čísla, na které půjdou poslat záporná čísla ze $\mathbb{Z}$. Obrázek je jasný.



Vzoreček: $T(n) = 2n$ pro $n \geq 0$ a $T(n) = 2|n| - 1$ pro $n < 0$. Tvrdíme, že je to bijekce.

Na: Vezměme $m \in \mathbb{N}_0$. Jestliže je sudé, pak $n = \frac{m}{2} \in \mathbb{Z}$ a $n \geq 0$, tudíž podle definice je $T(n) = 2n = m$.

Jestliže je m liché, pak je $m+1$ sudé, proto $\frac{m+1}{2} \in \mathbb{Z}$. Nechť $n = -\frac{m+1}{2}$. Pak $n \in \mathbb{Z}$. Z $m \geq 1$ máme $\frac{m+1}{2} \geq 1$, tudíž $n < 0$, $|n| = -n = \frac{m+1}{2}$ a podle definice T je $T(n) = 2|n| - 1 = (m+1) - 1 = m$.

Prostota: Nechť $x, y \in \mathbb{Z}$ splňují $T(x) = T(y)$. Pokud by $x \geq 0$ a $y < 0$, tak by $T(x)$ bylo sudé a $T(y)$ liché a nemohly by se rovnat, tento případ tedy nastat nemůže. Podobně nemůže nastat případ $y \geq 0$ a $x < 0$. Zbývají dva.

Jestliže $x, y \geq 0$, pak $T(x) = T(y) \implies 2x = 2y \implies x = y$.

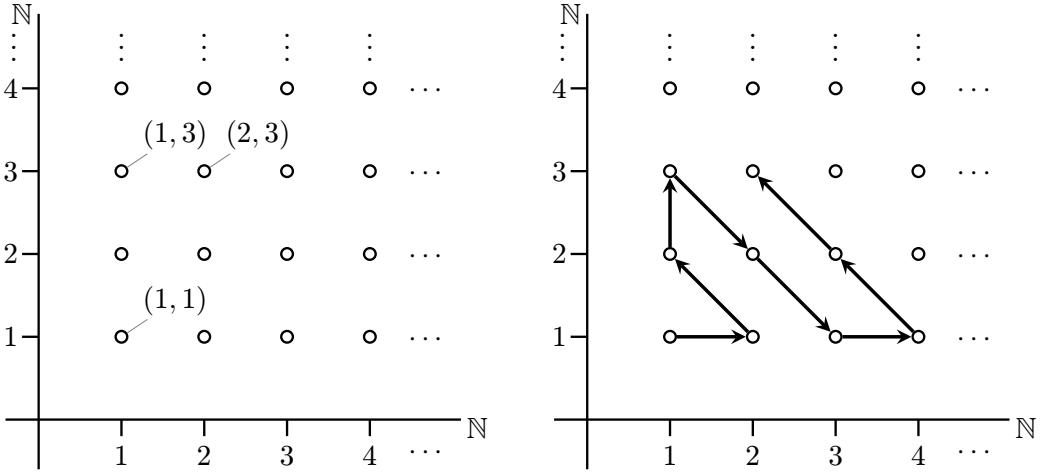
Jestliže $x, y < 0$, pak $T(x) = T(y) \implies 2|x| - 1 = 2|y| - 1 \implies |x| = |y|$. Jenže víme, že jsou obě čísla záporná, tudíž $|x| = |y| \implies -x = -y \implies x = y$. Ve všech případech tedy máme $x = y$ a prostota je také dokázána.

Alternativa: Protože $\mathbb{N} \subseteq \mathbb{Z}$, máme $|\mathbb{N}| \leq |\mathbb{Z}|$. Podle Věty 2c.5 tedy stačí dokázat, že $|\mathbb{Z}| \leq |\mathbb{N}|$, tedy najít nějaké prosté zobrazení ze $\mathbb{Z}$ do $\mathbb{N}$. Tvrdíme, že $T(n) = 2^{|n|+n}3^{|n|-n}$ takové je. Nejprve si připomeneme, že pro $n \geq 0$ je $|n| = n$, tedy $|n| + n = 2n$ a $|n| - n = 0$, zatímco pro $n < 0$ je $|n| = -n$ a tedy $|n| + n = 0$ a $|n| - n = -2n$, což je v tomto případě kladné neboli $3^{-2n} \in \mathbb{N}$. Proto vždy $2^{|n|+n}3^{|n|-n} \in \mathbb{N}$ a navíc vidíme, že $T(0) = 1$, dále $T(n) = 2^{2n}$ pro $n > 0$ a $T(n) = 3^{-2n}$ pro $n < 0$.

Protože čísla s různými prvočíselnými rozklady nemohou být stejná (viz Věta 6b.4), tak hned vidíme, že pro $m \neq n$ také platí $T(n) \neq T(m)$ a proto je T prosté.

Tato alternativa možná není tak pěkně vidět z obrázku jako první důkaz a dá víc práce dokázat prostotu, ale zase je to zobrazení dané jen jedním vzorečkem, což někdy může být výhoda.

(iii): Tady je tradiční důkaz obrázkem. Potřebujeme vytvořit bijekci $T\colon \mathbb{N} \mapsto \mathbb{N}\times\mathbb{N}$, čili potřebujeme říct, kam pošleme 1, kam pošleme 2 atd. Podívejme se na následující obrázek. Nejdříve jsme vlevo reprezentovali kartézský součin $\mathbb{N}\times\mathbb{N}$ a naznačili význam několika bodů, jen abychom se ujistili, že tomu rozumíme, a pak jsme vpravo nakreslili jistou dráhu.



Ta cestička nám ukazuje, jak postupně vybírat hodnoty pro T. Takže $T(1)=(1,1)$, $T(2)=(2,1)$, $T(3)=(1,2)$, $T(4)=(1,3)$, $T(5)=(2,2)$ atd. Při tomto způsobu výběru je jasné, že se hodnoty neopakují, takže T je prosté, a z obrázku se zdá, že dříve či později ta cestička dojde na libovolné místo v té síti, takže T by mělo být i na. Abychom z toho udělali pořádný důkaz, potřebovali bychom toto T přesně definovat, což se dá, ale je to dost komplikované, takže formální důkaz raději uděláme jinak. Nebyl to nicméně ztracený čas, protože tento způsob nám názorně ukázal, že se opravdu může stát, že „dvourozměrná“ síť má stejně bodů jako jednorozměrná. Takovéto názorné představy nám pomáhají vypěstovat správnou intuici o nekonečných množinách.

Formálně korekní důkaz: Nejprve ukážeme, že $|\mathbb{N}| \le |\mathbb{N}\times\mathbb{N}|$. Použijeme klasický trik a vyrobíme si v rámci $\mathbb{N}\times\mathbb{N}$ věrnou kopii množiny $\mathbb{N}$ zcela přirozeným způsobem, matematicky řečeno množinu $\mathbb{N}$ do toho kartézského součinu vnoříme. Je třeba to udělat správně formálně.

Uvažujme množinu $M=\{(n,1);\ n\in\mathbb{N}\}$ (první řádek v té síti). Pak určitě $|M|=|\mathbb{N}|$, což se snadno dokáže přirozenou bijekcí $T(n)=(n,1)$. A protože $M\subseteq\mathbb{N}\times\mathbb{N}$, tak máme $|M|\le|\mathbb{N}\times\mathbb{N}|$, zbytek vyplyne pomocí Faktu 2c.3 (ii).

Zajímavější bude druhý směr, kdy zkusíme vnořit zdánlivě „větší“ množinu do „menší“. Potřebujeme najít prosté zobrazení $T\colon \mathbb{N}\times\mathbb{N}\mapsto\mathbb{N}$. Uvažujme $T(m,n)=2^m3^n$. Evidentně pro $m,n\in\mathbb{N}$ dává $T(m,n)\in\mathbb{N}$, takže jde $\mathbb{N}\times\mathbb{N}\mapsto\mathbb{N}$, ještě zbývá ukázat, že je prosté. Nechť tedy $(m,n),(u,v)\in\mathbb{N}\times\mathbb{N}$ splňují $T(m,n)=T(u,v)$. To znamená, že $2^m3^n=2^u3^v$. Jenže celá čísla se dají zapsat pomocí prvočísel jen jediným způsobem, takže musí jít o stejné výrazy, tedy $m=u$ a $n=v$ čili $(m,n)=(u,v)$. Důkaz je hotov.

(iv): Tady je asi nejlepší zkombinovat (ii) a (iii). Jedna možnost je sloučit použité triky a dokázat, že zobrazení $U(m,n)=2^{|m|+m}3^{|m|-m}5^{|n|+n}7^{|n|-n}$ je prosté $\mathbb{Z}\times\mathbb{Z}\mapsto\mathbb{N}$.

Ukážeme ještě jeden způsob, kde se nemusíme hrabat v detailech, ale pracujeme konceptuálně. Zde využijeme přímo výsledky (ii) a (iii). Podle (ii) víme, že existuje bijekce $S\colon\mathbb{Z}\mapsto\mathbb{N}$. Pomocí ní teď definujeme zobrazení $R(m,n)=(S(m),S(n))$. Tvrdíme, že je to bijekce $\mathbb{Z}\times\mathbb{Z}\mapsto\mathbb{N}\times\mathbb{N}$.

Na: Nechť $(u,v)\in\mathbb{N}\times\mathbb{N}$. Protože je S bijekce, určitě existuje $m\in\mathbb{Z}$ splňující $S(m)=u$ a existuje $n\in\mathbb{Z}$ splňující $S(n)=v$. Pak $(m,n)\in\mathbb{Z}\times\mathbb{Z}$ a $R(m,n)=(S(m),S(n))=(u,v)$.

Prostota: Nechť $(m,n),(u,v)\in\mathbb{Z}\times\mathbb{Z}$ splňují $R(m,n)=R(u,v)$. Pak podle definice R máme $S(m)=S(u)$ a $S(n)=S(v)$ a S je bijekce, tudíž $m=u$ a $n=v$, čili $(m,n)=(u,v)$.

Právě jsme dokázali, že $|\mathbb{Z}\times\mathbb{Z}|=|\mathbb{N}\times\mathbb{N}|$, spolu s (iii) a Faktem 2c.3 (iii) to dává kýžený výsledek.

Všimněte si, že jsme pracovali s bijekcí S, o které jsme vůbec nevěděli, jak vlastně vypadá, jen jsme se odvolávali na její vlastnosti. Začínáme se stávat matematiky.

□

Bod (i) ukázal, že odebráním prvku z $\mathbb{N}_0$ se mohutnost nezměnila, což ukazuje, že u nekonečných množin je opravdu snadné vyrobit vlastní podmnožinu o stejné mohutnosti. Evidentně také nebude problém odebrat i více prvků. Můžeme se na to podívat i z druhé strany, že přidáním jednoho prvku (a tedy indukcí i konečně mnoha prvků) mohutnost nekonečné množiny nezměníme.

Bod (ii) ukazuje, že když dáme dohromady dvě stejně velké nekonečné množiny, tak jim zůstane původní velikost. Víme totiž, že $\mathbb{Z}=\mathbb{N}_0\cup(-\mathbb{N})$, kde jsme označili $-\mathbb{N}=\{-n;\ n\in\mathbb{N}\}$. Snadno ukážeme pomocí bijekce $T(n)=-n$, že množina $-\mathbb{N}$ má stejnou mohutnost jako množina $\mathbb{N}$.

Asi nejzajímavější je (iii), to nám ukazuje dvě věci. Jednak je to příklad toho, že ani kartézským součinem

dvou nekonečných množin nedosáhneme větší mohutnosti, ale dá se to číst i jinak. Pro libovolné $i \in \mathbb{N}$ označme $M_i = \{(n,i);\ n \in \mathbb{N}\}$, takže třeba $M_1 = \{(1,1),(2,1),(3,1),\dots\}$, zatímco $M_{13} = \{(1,13),(2,13),(3,13),\dots\}$. Jde o disjunktní množiny, které mají všechny stejnou mohutnost jako $\mathbb{N}$, což se snadno dokáže bijekcemi $T_i(n) = (n,i)$. Když teď uděláme nekonečné sjednocení, dostaneme $\bigcup_{m=1}^{\infty} M_m = \mathbb{N} \times \mathbb{N}$, což je zase množina mohutnosti $\mathbb{N}$. Je to tedy krásný příklad na (iii) z Věty 2c.11.

Důkazy, které jsme používali, jsou nejen názorné, ale i užitečné, protože tyto nápady se při práci s mohutností používají docela často.

Z (iv) hned plyne toto:

! **Věta 2c.13.**
Množina racionálních čísel $\mathbb{Q}$ je spočetná.

Důkaz (poučný)**:** Protože $\mathbb{N} \subseteq \mathbb{Q}$, platí $|\mathbb{N}| \leq |\mathbb{Q}|$. Potřebujeme teď opačnou nerovnost, podle Věty 2c.12 (iv) nám ale vlastně stačí ukázat, že $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}|$. Vnoření $\mathbb{Q}$ do $\mathbb{Z} \times \mathbb{N}$ pomocí prostého zobrazení se dělá relativně snadno, ale ještě jednodušší je použít alternativní přístup a najít zobrazení T z $\mathbb{Z} \times \mathbb{N}$ na $\mathbb{Q}$ (vi Fakt 2c.1).

Definujme jej takto: $T(p,q) = \frac{p}{q}$. Surjektivita je zjevná, každé racionální číslo lze zapsat jako zlomek $\frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$.

□

Pozorný čtenář si všimne, že už známe mohutnost $\mathbb{N}$, $\mathbb{Z}$ a $\mathbb{Q}$, ale jednu populární množinu jsme ještě nezkoumali. Máme tu také jiný dloužek, definovali jsme nespočetné množiny, ale zatím není vůbec jasné, jestli nějaká taková množina existuje. Tohle může skončit jediným způsobem.

! **Věta 2c.14.**
Interval reálných čísel $\langle 0,1)$ je nespočetný.

Důkaz (poučný)**:** Ukážeme, že žádné zobrazení $T\colon \mathbb{N} \mapsto \langle 0,1)$ nemůže být na. Pro účely tohoto důkazu si budeme čísla z intervalu $\langle 0,1)$ zapisovat jako čísla s nekonečným desetinným rozvojem, což si představíme například tak, že u čísel typu 0.347 doplníme dál nuly (teď narážíme na drobné nejasnosti s tím, že třeba $0.1000... = 0.0999...$, v případě více možných vyjádření jednoho čísla si prostě pro účely tohoto důkazu vždy jeden zápis zvolíme).

Vezměme tedy libovolné zobrazení $T\colon \mathbb{N} \mapsto \langle 0,1)$ a ukážeme, že nemůže být na. Zlobivé číslo b vytvoříme takto: Začíná „0.“ a pak doplňujeme desetinné číslice. Číslice na k-tém místě se určí následovně: Podíváme se na k-tou cifru v rozvoji čísla $T(k)$ a jestliže je to „3“, tak do našeho čísla b jako k-tou cifru dáme „1“, jinak do našeho čísla dáme „3“. Dostaneme tak číslo b, které začíná „0.“ a tudíž určitě leží v $\langle 0,1)$. Zároveň se ale od každého $T(k)$ liší na k-tém místě rozvoje, tudíž se mu nemůže rovnat. Proto neexistuje $n \in \mathbb{N}$ takové, že $T(n) = b$ a T není na.

Formálně: Zapíšeme obrazy T ve tvaru $T(k) = \sum_{i=1}^{\infty} a_{k,i} 10^{-i}$ a definujeme cifry $b_k = \begin{cases} 1, & a_{k,k} = 3; \\ 3, & a_{k,k} \neq 3, \end{cases}$ pak $b = \sum_{k=1}^{\infty} b_k 10^{-k}$ je ono divné číslo.

□

Přiblížíme si obrázkem, jak tento argument funguje, na příkladě jednoho konkrétního T. Jeho hodnoty si vypíšeme do řádků nekonečné tabulky.

$$\begin{array}{rl}
T(1) = & 0\,.\,\boxed{1}\ 3\ 8\ 4\ 0\ \dots \\
T(2) = & 0\,.\,2\ \boxed{3}\ 7\ 4\ 0\ \dots \\
T(3) = & 0\,.\,6\ 0\ \boxed{0}\ 0\ 0\ \dots \\
T(4) = & 0\,.\,9\ 3\ 8\ \boxed{2}\ 1\ \dots \\
T(5) = & 0\,.\,0\ 8\ 5\ 4\ \boxed{3}\ \dots \\
\vdots & \quad \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \dots \\
\hline
b = & 0\,.\,3\ 1\ 3\ 3\ 1\ \dots
\end{array}$$

Procházíme diagonálou a do „našeho“ čísla b dáváme vždy něco jiného, čímž zaručíme, že se naše číslo nebude shodovat s žádným řádkem tabulky. Tomuto argumentu se říká „Cantorův diagonální argument“ a při práci s velikostí množin je velice mocný, přitom tak jednoduchý. Všimněte si, že k tomu, aby nám fungoval, stačí mít možnost volit „něco jiného“, čili v zásadě stačí mít dva různé znaky. Mohli jsme tedy namísto desetinného rozvoje použít třeba zápis ve dvojkové soustavě se znaky 0 a 1, fungovalo by to stejně.

Celá tahle záležitost je další z výzev pro naši intuici. Asi všichni žijeme v představě, že když vezmeme papír a začneme pod sebe psát čísla 1, 2, 3, ... , tak nakonec (pokud budeme žít věčně) napíšeme všechna přirozená čísla. Člověk by si naivně myslel, že to jde udělat s libovolnou množinou čísel (a výše jsme viděli, že s celými i racionálními čísly ano), ale poslední důkaz ukazuje, že s intervalem $(0,1)$ to nepůjde, protože i kdybychom opravdu měli nekonečně mnoho času, tak z té množiny obsáhneme jen zanedbatelnou část. Přitom není selským rozumem zjevné, proč by to nemělo jít. Důkaz je ale nemilosrdě jasný, nejde to, tak to musíme akceptovat a zvyknout si na to. Nespočetné množiny jsou a jsou (nepředstavitelně?) velké.

! **Důsledek 2c.15.**
Množina reálných čísel $\mathbb{R}$ je nespočetná.

Důkaz (rutinní)**:** Víme, že $|\mathbb{N}| < |\langle 0,1)|$, také z $\langle 0,1) \subseteq \mathbb{R}$ máme $|\langle 0,1)| \leq |\mathbb{R}|$, proto $|\mathbb{N}| < |\mathbb{R}|$ (viz cvičení 2c.1). □

Mimochodem, víme už, že množina $\mathbb{Q}$ je spočetná, což znamená, že množina iracionálních čísel musí být nutně nespočetná (viz cvičení 2c.13). Mezi reálnými čísly je tedy nekonečně mnohokrát víc čísel iracionálních než zlomků.

Jakou má vlastně množina $\mathbb{R}$ mohutnost? Snadno se ukáže, že libovolný interval typu $\langle n, n+1)$ má stejnou mohutnost jako $\langle 0,1)$. Protože $\mathbb{R} = \bigcup_{n=-\infty}^{\infty} \langle n, n+1)$ je sjednocení spočetného souboru intervalů, které mají všechny stejnou mohutnost jako $\langle 0,1)$, tak podle Věty 2c.11 (iii) platí $|\mathbb{R}| = |\langle 0,1)|$. Mohutnost množiny reálných čísel či intervalu $\langle 0,1)$ je další ze základních mohutností, které se objevují často.

Ve cvičení 2c.14 si například rozmyslíme, že pro libovolné $a < b$ má $\langle a, b)$ stejnou mohusnost jak $\langle 0,1)$, a protože už víme, že nekonečné množiny jeden bodík nerozhodí, tak vlastně stejnou mohutnost mají všechny intervaly $\langle a, b\rangle$, $\langle a, b)$, $(a, b\rangle$ a (a, b) pro $a < b$, přičemž za a, b připouštíme i nekonečna. Mimochodem ta podmínka $a < b$ je podstatná, vylučuje tzv. degenerované intervaly jako $\langle 13, 13\rangle = \{13\}$ či $\langle 13, 13) = \emptyset$.

Mezi množinami spočetnými a nespočetnými je podstatný rozdíl při praktické práci. Množiny spočetné mohou být očíslovány, čili zapsány jako $A = \{a_1, a_2, \dots\}$. To se udělá jednoduše, pro spočetnou množinu A existuje bijekce z $\mathbb{N}$ na A, tak prostě označíme $a_n = T(n)$ a už nám a_n dají celou množinu (srovnejte Fakt 2c.6). Můžeme je tedy takto alespoň potencionálně spočítat, proto se tak jmenují. V průběhu počítání přitom pracujeme s konečnými množinami, což je přesně parketa diskrétní matematiky. V kapitole o indukci dokonce uvidíme, jak se pomocí množin konečných dozvědět ledacos o spočetných množinách nekonečných.

Naopak do množin nespočetných nedokážeme pomocí postupného počítání ani pořádně nahlédnout, takže jsou povětšinou mimo dosah metod diskrétní matematiky a budeme se jim vyhýbat. Vyplatí se proto umět již na začátku rychle odhadnout, zda je daný problém rázu spočetného či nikoliv. Zkusíme si to.

! **Příklad 2c.b:** Množina A kladných lichých čísel je spočetná.

Protože $A \subseteq \mathbb{N}$, máme jasně $|A| \leq |\mathbb{N}|$. Stačí nám tedy dokázat, že $|\mathbb{N}| \leq |A|$, tedy najít prosté zobrazení z $\mathbb{N}$ do A. To je ale snadné, definujeme $T(n) = 2n - 1$. Určitě pro $n \in \mathbb{N}$ dává kladná lichá čísla, takže jde do A.

Je prosté? Nechť $x, y \in \mathbb{N}$ splňují $T(x) = T(y)$. Pak $2x - 1 = 2y - 1$, tedy $x = y$. Ano, je prosté. Tím je důkaz hotov.

Mimochodem, dokonce jsme tím našli bijekci z $\mathbb{N}$ na A.

△

! **Příklad 2c.c:** Množina A konečných řetězců vytvořených ze znaků 0 a 1 (tzv. binárních řetězců) je spočetná.

Označme si jako A_n množinu binárních řetězců o délce n. Kolik jich je? Na každou pozici máme na výběr ze dvou znaků, celkem je tedy $2 \cdot 2 \cdots 2 = 2^n$ možností. Hlavní teď je, že A_n je konečná.

Protože máme $A = \bigcup_{n=1}^{\infty} A_n$, zajímá nás, co se stane, když sjednotíme spočetně mnoho konečných množin. Na to vlastně nemáme žádný vzorec, buď umíme sjednocovat konečně mnoho konečných množin (Věta 2c.8), nebo nekonečně mnoho nekonečných (Věta 2c.11). Zkusíme si to rozmyslet.

Určitě to bude alespoň spočetná množina, protože kdyby se z každé A_n vzal jeden prvek, tak už máme tolik prvků, kolik je v $\mathbb{N}$ (množiny A_n jsou disjunktní a proto dostáváme různé prvky).

Na druhou stranu nečekáme, že bychom dostali množinu nespočetnou, protože víme z Věty 2c.11, že sjednocením spočetně mnoha spočetně velkých množin dostaneme spočetnou množinu, a naše množiny jsou dokonce menší. Tato úvaha je užitečná a uděláme si ji obecně.

△

Fakt 2c.16.
(i) Jestliže jsou A_n pro $n \in \mathbb{N}$ nejvýše spočetné množiny, pak je $\bigcup_{n=1}^{\infty} A_n$ nejvýše spočetná.
(ii) Jestliže jsou navíc A_n neprázdné a po dvou disjunktní, pak je $\bigcup_{n=1}^{\infty} A_n$ spočetná.

Důkaz (rutinní)**:** (i): Přidáme si jednu množinu navíc, $A_0 = \mathbb{N}$, pak podle Věty 2c.11 (i) už $\left|\bigcup_{n=0}^{\infty} A_n\right| = |\mathbb{N}|$. Protože $\bigcup_{n=1}^{\infty} A_n \subseteq \bigcup_{n=0}^{\infty} A_n$, tak $\left|\bigcup_{n=1}^{\infty} A_n\right| \leq \left|\bigcup_{n=0}^{\infty} A_n\right|$ a zbytek je dle Faktu .

(ii): Teď potřebujeme i dolní odhad. Protože jsou A_n neprázdné, existuje v každé nějaký prvek, nazvěme jej a_n. Definujeme zobrazení $T(n) = a_n$, pak určitě $T\colon \mathbb{N} \mapsto \bigcup_{n=1}^{\infty} A_n$.

Je to prosté zobrazení? Nechť $m \neq n \in \mathbb{N}$. Protože jsou ty množiny po dvou disjunktní, $A_m \cap A_n = \emptyset$, tak nutně $a_m \notin A_n$, tedy i $a_m \neq a_n$, což znamená $T(m) \neq T(n)$. Toto zobrazení je tedy prosté, což dokazuje, že $|\mathbb{N}| \leq \left|\bigcup_{n=1}^{\infty} A_n\right|$.

□

! Příklad 2c.d: Množina A nekonečných binárních řetězců je nespočetná.

Tato množina je evidentně nekonečná, například proto, že obsahuje řetězce 1000..., 0100..., 0010... atd., kterých je spočetně neboli nekonečně mnoho. Zbývá ukázat, že je to množina nespočetná.

Protože jde přímo o řetězce, nabízí se Cantorův diagonální trik. Dokážeme, že žádné očíslování nemůže uspět. Předpokládejme tedy, že jsme se řetězce pokusili očíslovat, můžeme je pak seřadit pod sebe. Následně vytvoříme řetězec, který v seznamu není. Nejprve pro jeden konkrétní příklad:

$$\begin{array}{rl} a_1: & 0\,.\boxed{1}\,0\;1\;0\ldots \\ a_2: & 0\,.\,0\,\boxed{0}\,0\;0\ldots \\ a_3: & 0\,.\,1\;1\,\boxed{0}\,0\ldots \\ a_4: & 0\,.\,0\;0\;1\,\boxed{1}\ldots \\ \vdots & \quad\;\vdots\;\vdots\;\vdots\;\vdots\ldots \\ \hline b: & 0\,.\,0\;1\;1\;0\ldots \end{array}$$

A teď pořádně: Nechť T je nějaké zobrazení z $\mathbb{N}$ do A. Označme $T(n) = (a_{n,1}\ a_{n,2}\ a_{n,3}\ ...)$. Definujeme pak prvek $b \in A$ předpisem $b = (1{-}a_{1,1}\ 1{-}a_{2,2}\ 1{-}a_{3,3}\ ...\ 1{-}a_{n,n}\ ...)$. Ten se liší od každého prvku $T(n) = (a_{n,1}\ a_{n,2}\ a_{n,3}\ ...\ a_{n,n}\ ...)$ na n-tém místě, tedy $b \neq T(n)$ pro všechna $n \in \mathbb{N}$, proto T není na.

Ukázali jsme, že není možné vytvořit bijekci z $\mathbb{N}$ na A.

△

Příklad 2c.e: Uvažujme všechny nekonečné řetězce, které je možné vytvořit z malých písmen anglické abecedy. Z nich do množiny A vybereme takové řetězce, které vždy začínají opakováním jednoho konkrétního písmene, v některém místě pak přejdou na jiné a tím už dál pokračují, viz třeba řetězec *pppphhhhh*.... Tvrdíme, že množina A takovýchto řetězců je spočetná.

Tady je zajímavý ten dělící bod, zkusíme se odpíchnout od něj. Nechť A_n je množina všech řetězců, které mají změnu hned za pozicí n, tedy n-tý člen je ještě jako ten první, ale následující už jsou jiné (a všechny stejné). Kolik má taková množina prvků? Máme 26 možností, jak začít, a 25 možností, jak dál pokračovat, celkem $26 \cdot 25$, čili je to množina konečná (a neprázdná). Máme také $A = \bigcup_{n=1}^{\infty} A_n$ a již z definice jsou ty množiny disjunktní (řetězec se nesmí měnit na více místech), proto podle Faktu 2c.16 je A spočetná.

Alternativa: Pro $\alpha \neq \beta \in \{a, b, c, \ldots, z\}$ nechť je $A_{\alpha\beta}$ množina všech řetězců, které začínají písmenem α a končí písmenem β. Jak je taková množina velká? Písmeno β může začít od pozice $2, 3, 4, \ldots$, taková množina je tedy spočetná. Máme také $A = \bigcup_{\alpha,\beta} A_{\alpha,\beta}$ a jde o sjednocení konečně mnoha množin, podle Věty 2c.11 (v) je A spočetná.

△

S 2c.17 Jak určovat mohutnost

Při práci s množinami je často užitečné umět rychle odhadnout, jak velká množina to je, jmenovitě určit, zda je konečná, spočetná či nespočetná. Konečné množiny asi každý hravě pozná, takže se zaměříme na množiny nekonečné. Zde je základem znát dobře množiny, které jsme zkoumali výše ($\mathbb{Z}$, $(0, 1)$, konečné či nekonečné řetězce

atd.) a ještě probereme níže a také pravidla o sjednocení/kartézském součinu spočetných množin atd. Pomocí těchto znalostí pak odhadujeme (či dokonce dokazujeme) mohutnosti množin jiných. Nejčastěji používáme následující tři přístupy.

1) Přímé porovnání se známou množinou.

Někdy množina svou strukturou vyloženě nabízí porovnání s jinou, nám již známou množinou. V množině všech celočíselných násobků 150 má každý prvek tvar $150k$ pro $k \in \mathbb{Z}$, což zjevně nabízí bijekci na množinu $\mathbb{Z}$ předpisem „$150k \leftrightarrow k$“. Množina všech matic 2×2 nabízí okamžitou bijekci s prostorem čtyřsložkových vektorů. Množina všech vodorovných přímek v rovině nabízí bijekci na $\mathbb{R}$ danou třeba „přímka$\leftrightarrow$hodnota průsečíku přímky s osou y“ atd.

Pokud je také třeba odhadnutou mohutnost dokázat, pak stačí ukázat, že ono přiřazení je opravdu bijekce.

2) Další užitečnou strategií je množinu omezit shora či zdola. U situací, kdy je zkoumaná množina nekonečná, její spočetnost dokážeme tak, že její mohutnost shora omezíme pomocí jiné zaručeně spočetné množiny, což se dá často udělat pomocí vztahu býti podmnožinou, někdy pomocí prostého zobrazení (teď už není třeba surjektivita). Například množina všech matic 4×4 v dolním trojúhelníkovém tvaru s celočíselnými prvky je určitě podmnožinou množiny všech matic 4×4 s celočíselnými prvky, která je spočetná díky bijekci na $\mathbb{Z}^{16}$ (zde vlastně kombinujeme strategie 1 a 2). Mimochodem, je zde také možné použít přímo strategii 1 a vyrobit bijekci na množinu $\mathbb{Z}^{10}$ (dolní trojúhelníkové matice 4×4 mají obecně 10 nenulových prvků). Záleží na tom, co je již považováno za známé, spočetnost matic konečné velikosti s celočíselnými prvky je při pokročilejší práci považována za naprosto jasnou, takže bývá jednodušší toho prostě využít.

Nespočetnost pak dokazujeme tak, že množinu omezíme zdola nějakou nespočetnou množinou, opět buď ve smyslu inkluze, nebo prostým zobrazením. Například množina všech nekonečných řetězců ze znaků $\{1, 2, a, c, \diamond\}$ je nespočetná třeba proto, že obsahuje nekonečné řetězce ze znaků $\{1, 2\}$ a o takových jsme si už dokázali, že je nespočetná (my jsme to tedy udělali pro znaky $0, 1$, ale to je jen otázka obrázku, který pro ony dva symboly používáme).

Podobně pokud u matic připustíme reálné prvky, tak okamžitě dostaneme množinu nespočetnou, protože určitě obsahuje matice s jedním nenulovým prvkem vpravo nahoře a takovýchto matic je přesně stejně jako reálných čísel evidentní bijekcí „$r \leftrightarrow$matice s r vpravo nahoře“.

3) Třetí oblíbenou metodou je rozložit danou množinu na množiny jednodušší, jejichž velikost už snadno rozpoznáme, a pak použít pravidla. Například množina všech čtercových matic s celočíselnými prvky se dá rozložit na spočetně mnoho množin podle velikosti, přičemž pro konkrétní velikost $k \times k$ je množina takovýchto celočíselných matic také spočetná, proto je uvažovaná množina jako celek spočetná.

Také strategie 2 a 3 nabízejí v případě potřeby i důkaz a bývá často velice snadný, protože se v úvahách vlastně odvoláváme na již dokázané věty.

Čtenář si tyto strategie může nacvičit ve cvičení 2c.6 a 2c.9.

△

Škála mohutností ovšem nekončí množinou $\mathbb{R}$, jsou i větší množiny.

Připomeňme si, že je-li A množina, pak $P(A)$ je množina všech jejích podmnožin. Jak je velká, když je A konečná? Při vytváření podmnožin se u každého prvku $a \in A$ můžeme rozhodnout, zda jej vezmeme či ne, a každá odpověď ovlivní výsledek. Celkem je tedy možno udělat $2 \cdot 2 \cdots 2 = 2^{|A|}$ rozhodnutí.

Opravdu? Pro $A = \{1, 2\}$ máme $P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, celkem $4 = 2^2$ podmnožin, pro $A = \{1, 2, 3\}$ máme $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$, celkem $8 = 2^3$ podmnožin, dál to necháme na čtenáři, asi to opravdu takto funguje. Mimochodem, a co prázdná, jde to i tam? $P(\emptyset) = \{\emptyset\}$, takže má velikost $1 = 2^0 = 2^{|\emptyset|}$. Ano, funguje to.

Fakt 2c.18.
Jestliže je A konečná množina, pak $|P(A)| = 2^{|A|}$.

Vlastně jsme to dokázali, ten argument s výběry je obvykle považován za dostačující. Mimo jiné z toho plyne, že pro konečné množiny $|A| < |P(A)|$, následující věta nám o zobecní.

Věta 2c.19. (Cantorova)
Pro každou množinu A platí $|A| < |P(A)|$.

Důkaz (poučný, možná drsný)**:** Ukážeme, že libovolné zobrazení $T\colon A \mapsto P(A)$ nemůže být na. Nechť je tedy T nějaké takové zobrazení.

Když si vezmeme $a \in A$, pak je $T(a) \in P(A)$, čili $T(a)$ je nějaká podmnožina A. Můžeme se zeptat, jestli je a v této množině či ne. Tím vzniká test, pomocí kterého můžeme utvořit podmnožinu.

Nechť $M = \{a \in A;\ a \notin T(a)\}$. To je podmnožina A, proto $M \in P(A)$. Tvrdíme, že neexistuje žádné $b \in A$ takové, že $T(b) = M$, proto T není na.

Sporem: Předpokládejme, že takové b existuje. Ukážeme, že pak zároveň leží i neleží v M, což nejde.

A opravdu: Kdyby $b \in M$, pak $b \in T(b)$, proto podle definice této množiny $b \notin M$. Kdyby naopak $b \notin M$, pak splňuje podmínku definice a $b \in M$. Existence takového prvku by tedy vedla k paradoxu, čímž se ukazuje, že to (v rámci standardní teorie množin) není možné.

□

To je velice zajímavé. Začali jsme „nejmenší“ nekonečnou množinou $\mathbb{N}$ (mohutnost spočetné množiny), pak jsme se dozvěděli, že $\mathbb{R}$ má striktně větší mohutnost, podle Cantora má množina všech podmnožin $\mathbb{R}$ značená $P(\mathbb{R})$ zase striktně větší mohutnost, pak můžeme Cantora aplikovat na $P(\mathbb{R})$ a dostaneme ještě větší mohutnost a tak dále, je tedy vidět, že hierarchie velikostí množin nikdy nekončí, vždy je možné vyrobit ještě zase jednu neporovnatelně větší.

2c.20 Poznámka: Víme, že $\mathbb{R}$ má striktně větší mohutnost než $\mathbb{N}$, to má ovšem podle Cantorovy věty i množina $P(\mathbb{N})$ všech podmnožin $\mathbb{N}$. Jaký je mezi těmito většími množinami vztah?

Každou podmnožinu M přirozených čísel $\mathbb{N}$ je možné zakódovat pomocí nekonečného řetězce (a_k) ze znaků $0, 1$ metodou $a_k = 1$ právě tehdy, pokud $k \in M$ (viz 2a.9 Reprezentace množin). Toto kódování je jednoznačné, takže máme bijekci mezi $P(\mathbb{N})$ a množinou R všech nekonečných řetězců ze znaků $0, 1$.

Každý takovýto řetězec je ovšem možné chápat jako desítkový zápis reálného čísla z množiny $\langle 0, 1)$ ve dvojkové soustavě. Toto přiřazení je na, ale ne prosté, protože některá čísla lze vyjádřit dvěma způsoby (třeba $0.1000... = 0.0111...$). Každopádně vidíme, že množina R nemůže mít větší mohutnost než $\langle 0, 1)$. Snadno se ale nahlédne, že těch nejednoznačných čísel je jen spočetně, což je vzhledem k velikosti $\langle 0, 1)$ pod úrovní rozpoznatelnosti. Mohutnost R je tedy stejná jako mohutnost $\langle 0, 1)$ neboli mohutnost $\mathbb{R}$.

Závěr: Množina všech podmnožin $\mathbb{N}$ má přesně stejnou mohutnost jako množina $\mathbb{R}$.

△

Poznámka: Zajímavá otázka je, zda je $\mathbb{R}$ hned ta další velikost nekonečna po spočetnosti, nebo je mezi nimi třeba ještě nějaký mezikrok. To se zkoumá už přes sto let, Cantor si myslel, že nic mezi není, tomu se říká Hypotéza kontinua, a on se to celý život marně snažil dokázat. Po něm byli i další, až se v 50. letech 20. století ukázalo, že tento fakt je zcela nezávislý na matematické teorii, přesněji řečeno se v rámci klasické teorie množin (ZFC, kterou používáme už někdy od 30. let) nedá ani ukázat, že je HC pravdivá, ani ukázat, že je nepravdivá, je prostě nerozhodnutelná. V zásadě se tedy můžeme rozhodnout, zda ji přijmeme mezi axiomy a dostaneme tím určitou teorii množin, která v sobě nebude obsahovat spory (ta HC ji nepokazí), a přijetím HC se některé věci v té teorii objeví jako pravdivé. Nebo se rozhodneme, že budeme dělat teorii množin bez HC, a pak nám ty věci zase odpadnou. Tím narážíme na problematiku axiomatiky, kterou si raději necháme do kapitoly o uspořádání. Poznamenejme jenom, že pro lidi, kteří s množinami pracují na naši úrovni, je to jedno, rozdíl mezi teoriemi s HC a bez HC nepoznáme.

△

V našich předchozích úvahách jsme odvodili, že podmnožiny $\mathbb{N}$ lze kódovat jako řetězce ze znaků 0, 1, použili jsme (zatím neformálně) pojem posloupnosti, pro číslo $k \in \mathbb{N}$ nám a_k kódovalo přítomnost v dané podmnožině. My jsme již tuto myšlenku poznali ve cvičení 2b.12, kde jsme ji zvedli obecně jako způsob kódování podmnožin dané množiny. Naše úvahy o podmnožinách $\mathbb{N}$ naprosto stejně projdou i pro obecnou množinu M, má tolik podmnožin, kolik jsme schopni vytvořit indikátorových zobrazení. Kolik jich je? TO se dá snadno rozmyslet, tak to rovnou uděláme obecně.

Fakt 2c.21.
Nechť A, B jsou konečné množiny. Množina všech zobrazení $A \mapsto B$ má mohutnost $|B|^{|A|}$.

Důkaz (poučný)**:** Jak vytváříme zobrazení z A do B? Pro každý prvek z $a \in A$ se rozhodujeme zcela svobodně, na který prvek z B jej pošleme, máme tedy $|B|$ možností. Pro každý prvek z A tuto volbu opakujeme nezávisle, takže celkem máme tolik možností voleb: $|B| \cdot |B| \cdots |B|$, násobí se tolikrát, kolik je prvků v A. Je tedy celkem $|B|^{|A|}$ možností, jak vytvořit zobrazení z A do B.

□

Tento výsledek naznačí, kde se vzalo následující obecné značení.

Definice.
Nechť A, B jsou množiny. Symbolem B^A značíme množinu všech zobrazení z A do B.

Pro konečné množiny tedy máme $|B^A| = |B|^{|A|}$. Pomocí nového pojmu šikovně zachytíme naše obecné úvahy o mohutnosti množiny podmnožin.

Fakt 2c.22.
Nechť A je množina. Pak $|P(A)| = |\{0,1\}^A|$.

Důkaz (poučný)**:** Pro každou podmnožinu M množiny A máme zobrazení χ_M: $A \mapsto \{0,1\}$ dané $\chi_M(a) = \begin{cases} 1, & a \in M; \\ 0, & a \notin M \end{cases}$ (viz cvičení). Vzniká tím korespondence mezi podmnožinami množiny A a zobrazeními $A \mapsto \{0,1\}$ neboli zobrazení T: $P(A) \mapsto \{0,1\}^A$ definované $T(M) = \chi_M$.

Toto zobrazení je na, protože každá indikátorová funkce χ dává podmnožinu M, ze které pochází, jmenovitě množinu tvořenou těmi prvky z A, kde je χ rovna jedné. Je také prosté, protože pokud máme dvě různé podmnožiny M_1, M_2, pak musí existovat prvek $a \in A$, který je v jedné z nich a není v druhé, a v tom prvku se pak liší i odpovídající indikátorové funkce.

Našli jsme tedy bijekci z $P(A)$ na $\{0,1\}^A$ a důkaz je hotov.

□

Spojíme-li poslední dvě tvrzení, tak vidíme, že pro konečnou množinu A dostáváme $|P(A)| = |\{0,1\}|^{|A|} = 2^{|A|}$, což souhlasí s našimi předchozími závěry.

Poznámka: Vrátíme se k Větě 2c.12 a podívame se na ni trochu jinak. Operace s přirozenými čísly se musí v matematice také nějak vytvořit a dělá se to právě v teorii množin velice zhruba takto: Chcete vědět, kolik je $3+2$? Je to velikost množiny $\{1,2,3\} \cup \{a,b\}$. Chcete vědět, kolik je $3 \cdot 2$? Je to velikost množiny $\{1,2,3\} \times \{a,b\}$. Iterací násobení se pak člověk naučí i m^n, ale dá se to také (viz výše) dělat i přes množinu všech zobrazení z $\{1,\ldots,n\}$ do $\{1,\ldots,m\}$.

Co by se stalo, kdybychom si zavedli i nekonečno jako kvantitu označující velikost nekonečných množin? Můžeme pak psát $|A| = \infty$ (jakoby číslo), jednotlivá tvrzení z Věty 2c.12 nám pak dávají následující pravidla:

(i) $\infty + n = \infty$,
(ii) $\infty + \infty = \infty$,
(iii) $\infty \cdot n = \infty$ (to se dá i indukcí z (ii) jako opakované sčítání),
(iv) $\infty \cdot \infty = \infty$,
(v) $\infty^n = \infty$ (to se dělá z (iv) opakovaným násobením).

Cantorova věta ovšem ukazuje, že když mocníme na nekonečno, dostaneme víc: $2^\infty > \infty$, tedy i $\infty^\infty > \infty$.

Upřímně řečeno, v okamžiku, kdy si člověk na nekonečna zvykne, tak mu to začne připadat v zásadě normální a přesně toto by očekával, ostatně se nám podobné vzorečky vylíhnou i v analýze.

V teorii množin se zavádí „kardinální čísla“, což jsou symboly pro mohutnosti množin. Začínají $1, 2, 3, \ldots$, po probrání všech přirozených čísel pak přijde velikost spočetných množin značená $\aleph_0$ a pak přijdou další (větší nekonečna), dají se pak pro ně také zavést počítací pravidla. Jde o hlubokou a náročnou látku, která je samozřejmě zajímavá, ale tohle není kniha o teorii množin.

△

Pro doplnění si představíme ještě jeden pojem.

Cvičení

Cvičení 2c.1 (poučné, zkouškové)**:** Dokažte následující tvrzení:
Nechť A, B, C jsou množiny.
(i) Jestliže $|A| < |B|$ a $|B| \leq |C|$, pak $|A| < |C|$.
(ii) Jestliže $|A| \leq |B|$ a $|B| < |C|$, pak $|A| < |C|$.

Cvičení 2c.2 (rutinní)**:** Dokažte, že pro množiny A, B platí $|A \cap B| \leq |A \cup B|$. Kdy je tam rovnost pro konečné množiny?

Cvičení 2c.3 (dobré, poučné)**:** Dokažte, že jestliže $|A| = |B|$, pak $|P(A)| = |P(B)|$.

Cvičení 2c.4 (rutinní, poučné)**:** Dokažte, že jestliže $|A| = |B|$ a $|C| = |D|$, pak $|A \times C| = |B \times D|$.

Cvičení 2c.5 (rutinní, poučné)**:** Dokažte, že jestliže $B \subseteq A$ a B je nekonečná, tak je i A nekonečná.

Cvičení 2c.6 (rutinní, zkouškové)**:** Rozhodněte, zda jsou následující množiny spočetné či ne. Pokud ano, dokažte to.
(i) Množina záporných celých čísel;
(ii) množina sudých celých čísel;
(iii) množina celých násobků 13;
(iv) množina celých čísel větších než 23;
(v) množina lichých záporných celých čísel;
(vi) množina celých čísel, která nejsou násobkem tří;
(vii) množina racionálních čísel, která jsou mezi 0 a $\frac{1}{2}$;
(viii) množina všech binárních řetězců neobsahujících 0;
(ix) množina všechna kladných racionálních čísel, jež nelze napsat pomocí jmenovatele menšího než 4;
(x) množina reálných čísel neobsahujících 0 v desetinném rozvoji;
(xi) množina reálných čísel obsahujících pouze konečný počet číslic 1 v zápisu v desítkové soustavě;
(xii) množina reálných čísel, jejichž zápisy v desítkové soustavě obsahují pouze číslice 1;
(xiii) množina reálných čísel, jejichž zápisy v desítkové soustavě obsahují pouze číslice 1 nebo 3.

Cvičení 2c.7 (poučné)**:** Uvažujte následující předpis: $T(p,q) = \frac{p}{q}$. Dostáváme tak bijekci z $\mathbb{Z} \times \mathbb{N}$ na $\mathbb{Q}$?

Cvičení 2c.8 (poučné)**:** Uvažujte množinu $M = \{n^m;\ n, m \in \mathbb{N} - \{1\}\}$. Definuje předpis $T(n^m) = (m, n)$ bijekci z M na $(\mathbb{N} - \{1\}) \times (\mathbb{N} - \{1\})$?

Cvičení 2c.9 (poučné, zkouškové)**:** Rozhodněte, zda jsou následující množiny spočetné či ne. Pokud ano, dokažte to.
(i) Množina matic 2×2 s celočíselnými prvky;
(ii) množina polynomů, které mají celočíselné koeficienty;
(iii) množina přímek v rovině;
(iv) množina přímek vedoucích skrz bod $(13, 23)$;
(v) množina přímek vedoucích skrz bod $(13, 23)$ s celočíselnými směrnicemi;
(vi) množina trojúhelníků, jejichž vrcholy mají celočíselné souřadnice;
(vii) množina trojúhelníků, jejichž strany mají celočíselné délky.

Cvičení 2c.10 (rutinní)**:** Dokažte, že množina všech slov je nejvýše spočetná.

Cvičení 2c.11 (rutinní)**:** Dokažte, že množina všech programů v jistém programovacím jazyce je spočetná.

Cvičení 2c.12 (poučné)**:** Dokažte, že nadmnožina nespočetné množiny je nespočetná.

Cvičení 2c.13 (poučné)**:** Rozhodněte, zda platí následující tvrzení, odpověď dokažte:
Je-li A nespočetná a B spočetná množina, pak musí být $A - B$ nespočetná.

Cvičení 2c.14 (poučné)**:** Dokažte podle definice, že libovolný konečný interval (a, b) pro $a < b$ má stejnou mohutnost jako $(0, 1)$.

Cvičení 2c.15 (poučné)**:** Dokažte podle definice, že množina $\mathbb{R}$ má stejnou mohutnost jako interval $(0, \infty)$.

Cvičení 2c.16 (poučné)**:** Dokažte podle definice, že množina $\mathbb{R}$ má stejnou mohutnost jako interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.

Cvičení 2c.17 (dobré, poučné)**:** Uvažujte množinu $M = \{(a, b) \in \mathbb{N} \times \mathbb{N};\ a > b\}$. Na této množině definujme zobrazení $S(a, b) = (a - 1)(a - 2) + 2b$. Abychom viděli, jak vlastně S vypadá, uděláme si tabulku jeho hodnot pro kousek M. V řádcích bude a a ve sloupcích b, všimněte si, že pro dané a jsou v M jen dvojice s $1 \leq b < a$. To znamená, že nejmenší možné a, které se v M vyskytuje, je $a = 2$.

$b \to$	1	2	3	4	5
$a = 2:$	2				
$a = 3:$	4	6			
$a = 4:$	8	10	12		
$a = 5:$	14	16	18	20	
$a = 6:$	22	24	26	28	30

Vidíme několik evidentních věcí, toto cvičení bude po vás chtít důkaz toho nejdůležitějšího: Že hodnoty v řádcích rostou a že při přeskoku na další řádek ještě dále vzrostou. Dokažte tedy následující:
(i) Pro každé $a \geq 2$ a pro každé $1 \leq u < v < a$ platí $S(a, u) < S(a, v)$.
(ii) Pro každé $a \geq 2$ platí $S(a, a - 1) < S(a + 1, 1)$.
Poznámka: Pomocí (i) a (ii) už se pak indukcí a pár jednoduchými úvahami dokáže, že S je prosté zobrazení z M do $\mathbb{N}$. Ještě zajímavější je následující: Zobrazení dané vzorcem $\frac{1}{2}S(a, b)$ je prosté zobrazení z M na $\mathbb{N}$.

Cvičení 2c.18 (poučné)**:** Použijte to, že je $\frac{1}{2}S(a,b)$ prosté zobrazení z M na $\mathbb{N}$ (viz předchozí cvičení), k důkazu, že zobrazení dané vzorcem $T(m,n) = (m+n-2)(m+n-1)/2 + m$ je bijekce z $\mathbb{N}\times\mathbb{N}$ na $\mathbb{N}$.
Dostáváme tedy přímý předpis vzorečkem pro bijekci $\mathbb{N}\times\mathbb{N} \mapsto \mathbb{N}$ a dokonce je to vzoreček jednoduchý, polynom.

Cvičení 2c.19 (poučné)**:** Dokažte, že zobrazení $U(n) = (3n+1)^2$ je prosté ze $\mathbb{Z}$ do $\mathbb{N}$.

Cvičení 2c.20 (poučné)**:** Dokažte pomocí předchozích cvičení, že zobrazení dané předpisem

$$V(m,n) = ((3m+1)^2 + (3n+1)^2 - 2)((3m+1)^2 + (3n+1)^2 - 1)/2 + (3m+1)^2$$

je prosté ze $\mathbb{Z}\times\mathbb{Z}$ do $\mathbb{N}$.
Poznámka: Není známo, zda existuje polynom ve dvou proměnných, který by byl bijekce z $\mathbb{Q}\times\mathbb{Q}$ na $\mathbb{N}$.

Řešení:
2c.1: (i): Předpoklad dává prosté zobrazení T: $A \mapsto B$ a bijekci S: $B \mapsto C$. Pak je $S\circ T$ prosté $A \mapsto C$ a proto $|A| \le |C|$.
Kdyby bylo $|A| = |C|$, pak by existovala bijekce U: $A \mapsto C$ a tudíž by $S^{-1}\circ U$ byla bijekce $A \mapsto B$, spor s $|A| < |B|$. Proto $|A| < |C|$.
(ii): Předpoklad dává bijekci T: $A \mapsto B$ a prosté zobrazení S: $B \mapsto C$. Pak je $S\circ T$ prosté $A \mapsto C$ a proto $|A| \le |C|$.
Kdyby bylo $|A| = |C|$, pak by existovala bijekce U: $A \mapsto C$ a tudíž by $U\circ T^{-1}$ byla bijekce $B \mapsto C$, spor s $|B| < |C|$. Proto $|A| < |C|$.
2c.2: Definujeme T: $A\cap B \mapsto A\cup B$ jako $T(a) = a$. To je evidentně prosté. Obecně platí $A\cap B \subseteq A\cup B$, takže aby platilo $|A\cap B| = |A\cup B|$, muselo by platit $A\cap B = A\cup B$, což je jen když $A = B$.
2c.3: Předpoklad dává bijekci T: $A \mapsto B$. Definujeme S: $P(A) \mapsto P(B)$ jako $S(M) = T[M]$ pro $M \subseteq A$ neboli $M \in P(A)$. S je prosté, protože $S(M) = S(N) \implies T[M] = T[N] \implies T^{-1}T[M] = T^{-1}T[N] \implies M = N$. S je na, pro $N \in P(B)$ je $N \subseteq B$, definujeme $M = T^{-1}[N]$, pak $S(M) = TT^{-1}[N] = N$.
2c.4: Předpoklad dává bijekce T: $A \mapsto B$ a S: $C \mapsto D$. Definujeme U: $A\times C \mapsto B\times D$ jako $U(a,b) = (T(a), S(b))$.
Prosté: $U(a,b) = U(x,y) \implies (T(a),S(b)) = (T(u),S(v)) \implies T(a) = T(u) \wedge S(b) = S(v) \implies a = u \wedge b = v \implies (a,b) = (u,v)$, použila se prostota T, S..
Na: Nechť $(x,y) \in C\times D$. T, S jsou na, proto $\exists a \in A$: $T(a) = x$ a $\exists b \in B$: $S(b) = y$. Pak $(a,b) \in A\times B$ a $U(a,b) = (T(a),S(b)) = (x,y)$.
2c.5: Je možný důkaz sporem, pomůže Věta 2c.7 (i). Nebo nepřímý, nejprve napsat jako „Nechť $B \subseteq A$. Jestliže je B nekonečná, pak je A nekonečná“, načež tuto implikaci obměnit.
2c.6: (i): Spočetná, je to nekonečná podmnožina spočetné množiny $\mathbb{Z}$. Alternativa: Přímý důkaz, uvažujme $T(n) = -n$, to je zobrazení z množiny záporných celých čísel do $\mathbb{N}$, evidentně je na i prosté. Pro úplnost prostota: $T(n) = T(m) \implies -n = -m \implies m = n$.
(ii): Spočetná, je to nekonečná podmnožina spočetných celých čísel. Přímý důkaz bijekcí: zobrazení $T(n) = 2n$ je bijekce ze spočetné množiny $\mathbb{Z}$ na množinu sudých celých čísel. Na: Je-li m sudé, pak $m = 2n$ pro nějaké $n \in \mathbb{Z}$ a $T(n) = m$. Prosté: $T(n) = T(m) \implies 2n = 2m \implies m = n$.
(iii): Spočetná, je to nekonečná podmnožina spočetných celých čísel. Přímý důkaz bijekcí: zobrazení $T(n) = 13n$ je bijekce ze spočetné množiny $\mathbb{Z}$ na množinu celých násobků 13. Na: Je-li m celý násobek třinácti, pak $m = 13n$ pro nějaké $n \in \mathbb{Z}$ a $T(n) = m$. Prosté: $T(n) = T(m) \implies 13n = 13m \implies m = n$.
(iv): Spočetná, je to nekonečná podmnožina spočetné množiny $\mathbb{N}$. Alternativa: Přímý důkaz, uvažujme $T(n) = n - 23$, to je zobrazení z množiny celých čísel větších než 23 do $\mathbb{N}$, neboť pak je $T(n)$ celé a $T(n) \ge 1$. Evidentně je na i prosté. Pro úplnost prostota: $T(n) = T(m) \implies n - 23 = m - 23 \implies m = n$.
(v): Spočetná, nechť $T(n) = -(2n+1)$. Je to zobrazení z $\mathbb{N}$ na lichá záporná čísla, je prosté: $T(n) = T(m) \implies 2n+1 = 2m+1 \implies n = m$. Chcete-li zobrazení naopak, zvolte $S(m) = T^{-1}(m) = \frac{1-m}{2}$.
(vii): Spočetná, je obsažena v $\mathbb{Q}$ (tudíž je nejvýše spočetná) a je nekonečná. Zdola se dá velikost odhadnout třeba i tak, že daná množina obsahuje množinu $\left\{\frac{1}{n};\ n \in \mathbb{N}\right\}$, která je určitě spočetná, protože máme bijekci $T(n) = \frac{1}{n}$ mezi touto množinou a $\mathbb{N}$.
(viii): Spočetná, jsou to vlastně konečné řetězce jedniček, které se liší délkou, takže můžeme definovat $T(r)$ jako počet jedniček, je to prosté zobrazení na $\mathbb{N}$.
(ix): Spočetná, je podmnožinou $\mathbb{Q}$, tudíž nejvýše spočetná, a je nekonečná. Dolní odhad lze udělat i tak, že v dané množině najdeme podmnožinu $\left\{\frac{2k+1}{8};\ k \in \mathbb{N}\right\}$, podmnožina to určitě je (zlomky nelze zkrátit, tudíž je opravdu nelze napsat se jmenovatelem menším než 4) a spočetná také (bijekce $k \mapsto \frac{2k+1}{8}$).
(x): Nespočetná, daná množina určitě obsahuje například množinu všech reálných čísel, která mají desetinný rozvoj složený z nekonečně mnoha jedniček a dvojek, ta je nespočetná Cantorovým diagonálním argumentem nebo proto, že je díky bijekci stejně velká, jako množina nekonečných řetězců ze znaků 1, 2 neboli množina zobrazení $\mathbb{N} \mapsto \{1,2\}$, jejíž nespočetnost byla v kapitole dokázána.

(xi): Nespočetná, obsahuje v sobě množinu čísel, která 1 nemají vůbec, a ta je nespočetná, viz předchozí příklad po záměně znaků $0 \mapsto 1$.
(xii): Spočetná, každé takové číslo je jednoznačně dáno dvojicí $(m,n) \in \mathbb{N}_0 \times (\mathbb{N}_0 \cup \{\infty\})$, kde m je počet jedniček před desetinnou tečkou a n počet jedniček za ní. Pozor, dvojice $(0,0)$ nedává žádné číslo, neboť z ní vyleze jen desetinná tečka, je třeba to ošetřit v definici.
(xiii): Nespočetná. Stačí vzít taková čísla mezi 0 a 1, představit si, že by šlo o spočetnou množinu, a aplikovat na ně Cantora, tedy podívat se na diagonálu a vyměnit 3 a 1.
2c.7: Je evidentně na, ale není prosté $T(2,4) = \frac{2}{4} = \frac{1}{2} = T(1,2)$. Takže není bijekce.
2c.8: Je evidentně na, ale není prosté $T(9,2) = 81 = 3^4 = T(3,4)$. Takže není bijekce.
2c.9: (i): Spočetná, jasná bijekce $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mapsto (a_{11}, a_{12}, a_{21}, a_{22}) \in \mathbb{Z}^4$ („seřazení matice do řady“).
(ii): Nejprve ukázat, že množina P_n polynomů stupně n má stejnou mohutnost jako $\mathbb{Z}^{n+1}$, pomocí $a_n x^n + \cdots + a_1 x + a_0 \mapsto (a_n, a_{n-1}, \ldots, a_0)$, pak spočetné sjednocení spočetných je spočetné.
(iii): Nespočetná, obsahuje nespočetnou podmnožinu všech vodorovných přímek $\{y = a;\ a \in \mathbb{R}\}$. Šlo by také zkusit popsat přímky rovnicemi $ax + by = c$ a pak to porovnat se zaručené nespočetnou množinou zobrazením $ax + by = c \mapsto (a,b,c)$, ale tam je problém s přiřazením, protože jednu přímkulze popsat více rovnicemi. To se dá obejít požadavkem, že čísla a, b, c mají být co nejvíce zkrácena, tedy jejich největší společný dělitel má být 1.
(iv): Nespočená, tyto přímky lze jednznačně popsat pomocí směrnice k a těchto směrnic je tolik, kolik je reálných čísel, tedy nespočetně. Vzniká tak bijekce T: $k \mapsto y = k(x-13) + 23$, což ale není na, chybí svislá přímka, tu doplníme tak, že ji vezmeme jako obraz $T(\infty)$, pak T jde z množiny $R \cup \{\infty\}$, která je nespočetná.
(v): Spočetná, viz (iv), T: $k \mapsto y = k(x-13) + 23$ je bijekce ze $\mathbb{Z}$ na danou množinu.
(vi): Spočetná, jasná bijekce na $\mathbb{Z}^6$.
(vii): Nespočetná, vezmu jeden takový trojúhelník a pak ho mohu posouvat ve směru osy x na tolik pozic, kolik je reálných čísel, vznikne nespočetně mnoho trojúhelníků.
2c.10: Slova jsou konečné řetězce nad českou abecedou, tedy nad konečným počtem symbolů (řekněme, že je jich 82). Množina řetězců z 82 znaků o délce k má 82^k znaků, je tedy spočetná. Konečné řetězce vzniknou sjednocením těchto množin přes všechna $k \in \mathbb{N}$, je tedy spočetná. Takže mnžina všech konečných řetězců nad 82 písmeny je spočetná a slova tvoří její podmnožinu, tudíž je nejvýše spočetná.
Patrně bude dokonce konečná, protože neexistuje české slovo libovolné délky, třeba padesátipísmenné slovo asi nenajdeme.
2c.11: Každý program lze považovat za konečný řetězec znaků ASCII. Množina programů je tedy podmnožinou množiny konečných řetězců nad konečnou abecedou, což je spočetná množina, viz výše.
2c.12: Toto je jen obměna tvrzení z kapitoly, že podmnožina nejvýše spočetné množiny je nejvýše spočetná.
2c.13: Nejlépe sporem. Kdyby byla $A - B$ spočetná, pak by byla spočetná i $B \cup (A - B) = A \cup B$ a tudíž i $A \subseteq A \cup B$, což je spor.
2c.14: Nechť $T(x) = a + (b-a)x$, pak je to bijekce z $(0,1)$ na (a,b). 1) Definice má smysl, pro $0 < x < 1$ je $a < T(x) < b$, tedy opravdu t je do (a,b). Je na: Dáno $y \in (a,b)$, pak existuje $x = \frac{y-a}{b-a} \in (0,1)$ takové, že $T(x) = y$. Prosté: $T(x) = T(y) \implies a + (b-a)x = a + (b-a)y \implies x = y$.
2c.15: $T(x) = e^x$ je bijekce $\mathbb{R} \mapsto (0, \infty)$.
2c.16: $T(x) = \operatorname{arctg}(x)$ je bijekce $\mathbb{R} \mapsto \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.
2c.17: (i): Pokud $u < v$, pak $S(a,u) = (a-1)(a-2) + 2u < (a-1)(a-2) + 2v = S(a,v)$.
(ii): $S(a, a-1) = (a-1)(a-2) + 2(a-1) = a^2 - a < a^2 - a + 2 = a(a-1) + 2 = S(a+1, 1)$.
2c.18: Nechť R: $\mathbb{N} \times \mathbb{N} \mapsto M$ je dané $R(m,n) = (m+n, m)$. Je to bijekce. Prosté: $T(m,n) = T(u,v) \implies (m+n, m) = (u+v, u) \implies m+n = u+v \wedge m = u \implies m = u \wedge n = v \implies (m,n) = (u,v)$. Je na: Pro dané $(x,y) \in M$ je $x, y \in \mathbb{N}$ a $x > y$, proto $(m,n) = (y, x-y) \in \mathbb{N} \times \mathbb{N}$ a $T(m,n) = (x,y)$.
Proto je také bijekcí $T = \frac{1}{2}S \circ R$ a $R(m,n) = \frac{1}{2}S(m+n, m) = \frac{1}{2}(m+n-1)(m+n-2) + m$ přesně dle zadání.
2c.19: Pro $n \in \mathbb{Z}$ nelze mít $3n + 1 = 0$, proto $U(n) \in \mathbb{N}$
Nechť $U(x) = U(y)$. Pak $(3x+1)^2 = (3y+1)^2$, tedy $|3x+1| = |3y+1|$. Jaké jsou možnosti? Rozebereme si to podle znamének. Pokud by byla různá, tak jednu absolutní hodnotu odstraníme a druhou nahradíme mínusem, dostaneme tedy $3x + 1 = -(3y+1)$. Do dává $3(x+y) = -2$, ale to nejde, protože $3(x+y)$ je celé číslo dělitelné třemi.
Znaménka tedy musí být stejná, pak se dají absolutní hodnoty odstranit, kdyby náhodou byla obě záporná, tak se obě absolutní hodnoty nahradí mínusy a ty se zkrátí, čili každopádně dostaneme $3x + 1 = 3y + 1$, tedy $x = y$ a prostota je dokázána.
2c.20: Definujme $W(m,n) = (U(m), U(n))$, ak je W prosté $\mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{N} \times \mathbb{N}$, viz např. cvičení 2c.4. Podle předchozích cvičení je pak $T \circ W$ prosté $\mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{N}$ a $(T \circ W)(m,n) = T((3n+1)^2, (3n+1)^2) = V(m,n)$.