

## 9. Zobrazení, mohutnost množin

Pojem zobrazení je jedním ze základních a klíčových matematických nástrojů. V této kapitole si jej představíme a posléze ukážeme, jak s jeho pomocí dokážeme říct zajímavé věci o množinách.

### 9a. Zobrazení

Čtenář jistě zná pojem (reálné) funkce, například  $f(x) = x^2$ . Co to ale vlastně funkce je z pohledu matematického? Lidé si obvykle představí nějaký vzorec, ale to je tím, že jsme rozmazleni školou. Vztah mezi závislou a nezávislou proměnnou totiž může být všelijaký, třeba i takový, pro který vzorec najít nelze.

**Příklad 9a.a:** Definujme funkci  $g$  následovně. Jestliže je reálné číslo  $x$  vyjádřitelné jako desetinné číslo s konečným rozvojem, pak je hodnota  $g(x)$  dána 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  $g(x) = 0$ .

Touto definicí je  $g$  definováno pro všechna reálná čísla, třeba  $g(146824834) = 4$ ,  $g(714.397721) = 7$ ,  $g(0.333) = 3$ , naopak  $g(\pi) = 0$  či třeba  $g(\frac{1}{3}) = 0$ . Je to naprosto normální funkce, umíme spočítat její hodnotu pro libovolnou volbu proměnné, má svůj graf (patříčně divoký), jen ji nelze vyjádřit vzorečkem.

△

Dá se dokonce dokázat, že reálných funkcí, které lze vyjádřit vzorečkem, je mezi možnými závislostmi (nebo mezi možnými grafy v  $\mathbb{R}^2$ , chcete-li) naprostá menšina. To zajímavě kontrastuje s tím, že obvykle pracujeme (i v této knize) právě se vzorci. Je to je způsobeno dvěma vlivy. Za prvé se jiným přiřazením snažíme ve škole vyhýbat, protože s těmi nevzorečkovými se špatně pracuje, a za druhé je na nás matka příroda strašně hodná a na spoustu jevů ten vzoreček nakonec najdeme. To se ovšem týká konkrétních příkladů, spoléhat na to nelze. Pokud chceme vybudovat obecnou teorii, musíme se představy funkce coby vzorce vzdát a najít představu jinou.

Skutečnou podstatou funkce je přiřazování. Je to zařízení, které vytváří propojení mezi čísly na vstupu a na výstupu. Můžeme si také představit, že je to „posílátko“, posílá čísla na nějaká cílová čísla. Například ona  $f(x) = x^2$  posílá  $5 \mapsto 25$  nebo  $(-2) \mapsto 4$ . Jak to zachytíme matematicky? Nástroj se nabízí, prostě ta přiřazení uložíme. Například u funkce  $f$  bychom si uložili uspořádané dvojice  $(5, 25)$ ,  $(-2, 4)$ , také třeba  $(\pi, \pi^2)$ ,  $(\sqrt{13}, 13)$  atd. Dosazení čísla  $a$  do funkce pak probíhá tak, že si v seznamu dvojic najdeme takovou, která má  $a$  na první pozici, a dozvíme se  $f(a)$ . Funkce by se tak stala množinou uspořádaných dvojic.

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 různá lízátká. I fungování takovéto skříňky by šlo zachytit jako množinu dvojic (písmenka, lízátko).

Naskýtá se přirozená otázka, proč máme speciální kapitolu, když přesně tohle jsme už dělali a říkali jsme tomu relace. Důvodem je, že chceme zobecnit pojem reálné funkce, u kterých je jeden zásadní prvek: Když do funkce dosadíme, tak očekáváme, že dostaneme jednoznačnou odpověď. Tuto představu si chceme zachovat i pro obecná posílátka mezi množinami. Takže ano, budeme pracovat s relacemi, ale s velice speciálními, takovými, u kterých z každého prvku výchozí množiny vede přesně jedna šipka. Proto si zaslouží vlastní jméno a vlastní kapitolu.

#### Definice.

Nechť  $A, B$  jsou neprázdné množiny. Definujeme **zobrazení**  $z$   $A$  do  $B$  jako libovolnou podmnožinu  $T$  množiny  $A \times B$  takovou, že pro každé  $a \in A$  existuje právě jedno  $b \in B$  splňující  $(a, b) \in T$ . Zobrazení  $T$  z  $A$  do  $B$  značíme  $T: A \mapsto B$ .

Namísto  $(a, b) \in T$  také píšeme  $T(a) = b$ .

Množina  $A$  je **definiční obor**  $T$ , značeno  $D(T)$ , množina  $B$  je cílová množina  $T$ . Definujeme také **obor hodnot**  $T$  jako

$$\text{ran}(T) = \{T(a) : a \in A\} = \{b \in B : \exists a \in A : T(a) = b\}.$$

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  $\text{ran}(T) = \{T(a) : a \in A\}$ .

Připomeňme, že v kapitole 1a jsme zavedli značení pro „existuje právě jedno“, podmínka z definice by se formálně zapsala  $\forall a \in A \exists! b \in B : (a, b) \in T$ .

V definici nabízíme dva pohledy na zobrazení. Značení  $(a, b) \in T$  odkazuje na oficiální definici zobrazení coby množinu dvojic, což je představa, ke které se budeme vracet v důkazech a při teoretičtějších uvažích. Pak tam máme značení  $T(a) = b$ , používá se také (řídčeji)  $T: a \mapsto b$ , které odkazuje na intuitivní představu zobrazení coby

posílátka a je mnohem praktičtější. Tím  $T(a)$  se ale nesnažíme naznačit, že se dosazuje do nějakého vzorečku, protože ten ani nemusí existovat. Spíš to chápeme tak, že jsme  $a$  vsunuli do vstupu černé skřínky a čekáme, co z ní vyleze na druhém konci. Tento pohodlný a názorný zápis si můžeme dovolit právě proto, že pro každé  $a$  je výstup  $T(a)$  jednoznačně určen. Je s tím spojena terminologie,  $T(a) = b$  se dá vyjádřit slovy, že  $b$  je obraz  $a$  (je přesně jeden), zatímco  $a$  je vzor  $b$  (ten už nemusí být jedinečný, například vzhledem k  $f(x) = x^2$  má  $b = 4$  vzory  $a = \pm 2$ ).

Dodejme ještě poznámku k terminologii. Někteří autoři pojem „zobrazení“ nezavádějí a hovoří o funkcích. Jde tedy o rovnocenné pojmy, někteří autoři si vyberou jeden, jiní druhý, někteří to střídají dle nálady. Já patřím mezi autory, kteří se dobrovolně rozhodli dodržovat následující úmluvu: Název „funkce“ si šetříme pro ta zobrazení, která pracují s čísly (reálné funkce, komplexní funkce), zatímco použitím slova „zobrazení“ čtenáři posíláme vzkaz, že právě pracujeme s obecnější situací. Přejde mi to praktické, ale upozorňuji, že to není univerzálně přijímáno.

**Příklad 9a.b:** Uvažujme množiny  $A = \{\diamond, \bullet\}$  a  $B = \{1, 2, 13\}$ . Pak  $R = \{(\diamond, 13)\}$  není zobrazení  $A \mapsto B$ , protože prvku  $a = \bullet$  není nic přiřazeno. Také  $S = \{(\diamond, 13), (\bullet, 1), (\diamond, 2)\}$  není zobrazení, protože prvku  $a = \diamond$  jsou přiřazena dvě různá  $b$ .

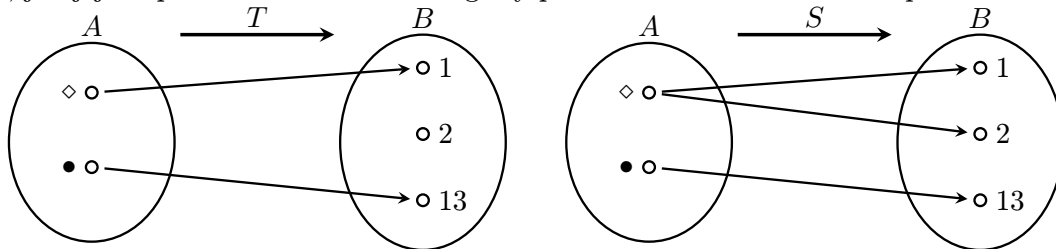
Jak se dá čekat, teď přijde zobrazení, třeba  $T = \{(\diamond, 1), (\bullet, 13)\}$ . Toto je správný formální zápis podle definice, ale máme k dispozici i přirozenější zápis ve formě výčtu  $T(\diamond) = 1$ ,  $T(\bullet) = 13$ .

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

△

Všimněte si, že volba cílové množiny  $B$  nemá vliv na to, jak  $T$  působí, fungovalo by stejně, i kdybychom vzali třeba  $B = \{1, 7, 13, 23\}$ . V mnoha situacích opravdu na volbě cílové množiny nezáleží a lze ji měnit, musíme si ovšem hlídat, aby nová  $B$  obsahovala  $\text{ran}(T)$ . Často ji prostě ignorujeme a pracujeme jen s  $\text{ran}(T)$ . Jsou ovšem také situace, kdy má volba  $B$  význam, jak brzy uvidíme.

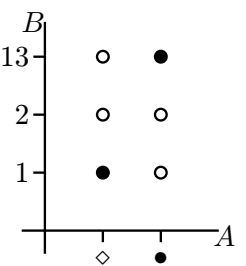
Jak si takové zobrazení můžeme znázornit? Vzhledem k tomu, že zobrazení jsou speciální případy relace, můžeme použít graf tak, jak jej chápou relace. Níže vidíme grafy pro zobrazení  $T$  a relaci  $S$  z příkladu 9a.b.



U funkcí na takovéto znázornění nejsme zvyklí, ale u obecných zobrazení je velice výhodné. V konkrétních příkladech snadno vidíme důležité vlastnosti, 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. Vysoce užitečná je tato představa i při teoretických úvahách.

Jak do tohoto příběhu zapadá graf běžně používaný pro reálné funkce? U nich se ptáme, jak vypadá množina bodů  $(x, f(x))$  v  $\mathbb{R}^2$ . U obecného zobrazení  $T$  je tato množina vlastně přesně to, jak je  $T$  definováno, takže bychom se mohli ptát, jakou polohu má  $T$  jako součást obrázku znázorňujícího  $A \times B$ . U konečných množin se  $A \times B$  tradičně znázorňuje ve formě obdélníkové sítě bodů, v ní zvýrazníme dvojice ležící v  $T$ . Vidíme to na obrázku pro zobrazení  $T$  z příkladu 9a.b.

Hned vidíme, že nějakou informaci bychom asi z toho obrázku vykukali, ale je to méně výmluvné než šipkový obrázek výše. Tím se vysvětluje, proč se v obecné teorii zobrazení tento přístup nepoužívá.



**Příklad 9a.c:** Uvažujme  $A$  coby množinu všech studentů a  $B = \mathbb{R}$ . Pro pevně zvolený den definujeme zobrazení  $T: A \mapsto B$  předpisem, že pro studenta  $a \in A$  udává  $T(a)$  studijní průměr studenta  $a$  k onomu zvolenému dni. Pak by  $T$  mělo být zobrazení.

Je zároveň jasné, že přiřazení (student, předmět zapsaný v tomto semestru) s vysokou pravděpodobností nebude zobrazením. Záleží to na tom, zda se v množině  $A$  najde student, který nám to sabotuje a zapsal si více kursů, pak je třeba jako nástroje použít relace.

Dobrá otázka je, zda je zobrazením relace (občan ČR, rodné číslo). Čísla se rozdávají při narození a získání občanství, takže každý občan je v nějaké dvojici, tohle by fungovalo. Máme ale zaručeno, že je v právě jedné? Teoreticky by tomu tak být mělo, ale chybička se vloudit může.

△

Jakmile umíme posílat někam prvky, tak už umíme posílat i celé množiny, prostě je pošleme po jednotlivých prvcích. Můžeme si také vzít nějakou část cílové množiny a zeptat se, kdo všechno je do ní poslán.

**Definice.**

Nechť  $T: A \mapsto B$  je zobrazení. Pro  $M \subseteq A$  definujeme **obraz** (image)  $M$  jako

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

Pro  $N \subseteq B$  definujeme **vzor** (pre-image)  $N$  jako

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

Pak máme třeba  $\text{ran}(T) = T[A]$ , 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. Vrátime-li se k příkladu 9a.b, tak  $T^{-1}[\{1\}] = T^{-1}[\{1, 2\}] = \{\diamond\}$ ,  $T^{-1}[\{2\}] = \emptyset$ .

Kdy se zobrazení rovnají? Zobrazení jsou podle definice množiny dvojic, takže je umíme takto porovnat. Ukazuje se ovšem, že to ještě nestačí. Z množiny dvojic tvořící konkrétní zobrazení  $T$  totiž poznáme dvě věci, jmenovitě na které množině  $A$  je  $T$  definováno (shromáždíme všechny prvky vyskutuující se v první složce dvojic) a jakým způsobem tyto vstupy posílá. Pokud se tedy dvě množiny dvojic rovnají, pak odpovídající zobrazení mají shodné definiční obory a posílají prvky stejným způsobem. Budou také mít stejné obory hodnot (ty získáme shromážděním prvků z druhé složky všech dvojic). Jednu věc z toho ale nepoznáme, jmenovitě jaké mají deklarované cílové množiny  $B$ . Protože jsou situace, kdy na tomto záleží, musíme si porovnání cílových množin přidat jako podmínku rovnosti.

Protože v praxi zobrazení coby množiny dvojic nepotkáváme, přeložíme svá pozorování do jazyka „posílátek“. Dvě shodná zobrazení musí posílat stejným způsobem a musí se shodovat vstupní a cílová množina.

**Definice.**

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

Jinak řečeno, všechny tři symboly v obrázku „ $T: A \mapsto B$ “ jsou důležité.

Poznamenejme, že ona rovnost  $T(a) = S(a)$  neznamená porovnávání nějakých vzorečků. V praxi to tak sice často dopadá, ale má to dva zádrhle. První je, že ne každé zobrazení lze definovat vzorcem. Další zajímavý zádrhel je v tom, že neznáme spolehlivý proces, který by poznal, že dva vzorce jsou si rovny. Optimista by mohl prohlásit, že si počká, až se to vymyslí, ale to by čekal dlouho. Bylo totiž dokázáno, že spolehlivý algoritmus na rozpoznávání rovnosti algebraických vzorců vůbec nemůže existovat.

My obvykle budeme mít štěstí na příjemné vzorečky. Pak je třeba pamatovat, že když máme třeba  $T(n) = n^2 - 1$  a  $S(n) = (n - 1)(n + 1)$ , tak nebudeme jásat předčasně, že  $T = S$ , ale nejdříve ještě porovnáme, jak vypadají definiční obory a cílové množiny těchto zobrazení.

S těmito dvěma množinami občas potřebujeme manipulovat. Už jsme si všimli, že cílovou množinu  $B$  můžeme v mnoha (většině) situací změnit, aniž by to nějak ovlivnilo výsledné zobrazení, jen si musíme hlídat, aby  $\text{ran}(T)$  pořád zůstávalo její podmnožinou. Jsou také situace, kde bychom rádi upravovali počáteční množinu  $A$ . Tam už ale zasahujeme do fungování zobrazení, protože ke každému  $a \in D(T)$  se nutně váže nějaká dvojice v  $T$ . Zmenšování daného  $A$  je užitečným nástrojem a zaslouží si jméno.

**Definice.**

Nechť  $T: A \mapsto B$  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 9a.b může být omezeno na podmnožinu  $M = \{\diamond\}$ , vznikne pak zobrazení  $T|_M: M \mapsto B$  definované  $T|_M(\diamond) = 1$ .

Vrátime-li se k definici zobrazení, tedy nahlížíme-li na něj jako na nějakou množinu dvojic z  $A \times B$ , pak tato definice přesně souhlasí s definicí restrikce pro relace.

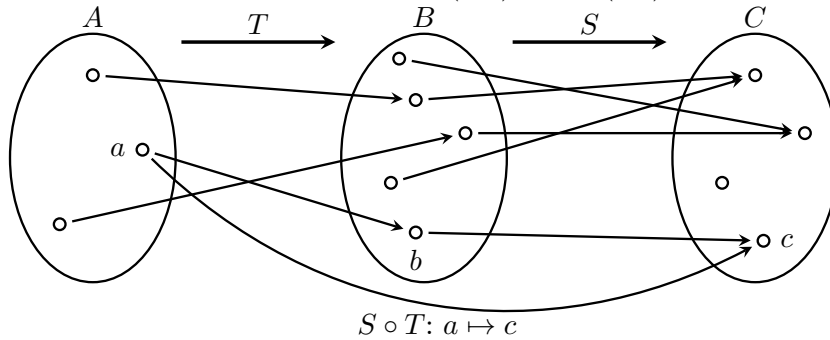
Což nám připomíná, že jsme zobrazení definovali jako speciální případ relací. Znamená to, že pro ně platí vše, co se probírá v kapitole 5. Při bližším pohledu se ovšem ukáže, že většina z toho nemá u zobrazení praktický smysl.

Aplikovat na funkce množinové operace nemá rozumnou interpretaci a navíc to ani obecně nejde, protože bychom jako výsledek nejspíše nedostali zobrazení, viz cvičení 9a.20.

Stejně tak se na funkce neaplikují vlastnosti relací, protože nenesou užitečnou informaci, viz cvičení 9a.21. To je také důvod, proč se zobrazení a relace tradičně probírají odděleně, každý pojem je nástrojem k řešení jiného typu problémů a zajímá nás na něm něco jiného.

Je tu jedna výjimka, skládání relací má smysl i pro zobrazení a je to dokonce klíčový pojem. Mohli bychom přímo převzít definici, bývá ale tradiční používat pohodlnější funkční značení. Jak vypadá překlad?

Mějme zobrazení  $T: A \mapsto B$  a  $S: B \mapsto C$ , už víme od relací, že množiny na sebe musejí navazovat. Dvojice  $(a, c)$  je ve složené relaci  $S \circ T$ , pokud existuje  $b \in B$  takové, že  $(a, b) \in T$  a  $(b, c) \in S$ .



Protože je ale  $T$  zobrazení, tak nemáme u  $b$  na výběr, je jen jeden prvek splňující  $(a, b) \in T$ , jmenovitě  $b = T(a)$ . Aby tedy vznikl navazující dvojkrok, musí mít  $S$  nějakou dvojici  $(b, c)$ , což ale má, je to totiž také zobrazení. A navíc má jen jednu, tu kde  $c = S(b)$ .

Vidíme dvě věci. Za prvé, na rozdíl od relací nemusíme u zobrazení zkoumat, kde vznikají či nevznikají navazující dvojice, zde z každého  $a \in A$  vznikne přesně jedna navazující dvojice a tedy přesně jedna dvojice do  $S \circ T$ . A protože je přesně jedna, bude i výsledná relace  $S \circ T$  zobrazením.

Za druhé vidíme, že u výsledné dvojice  $(a, c)$  máme  $c = S(b) = S(T(a))$ . Takže „posílatko“  $S \circ T$  funguje tak, že se nejprve vstup  $a$  pošle posílatkem  $T$  a jeho výstup se použije jako vstup do posílatka  $S$ , přesně jak jsme zvyklí od funkcí. Teď už víme, co chceme.

**Definice.**

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

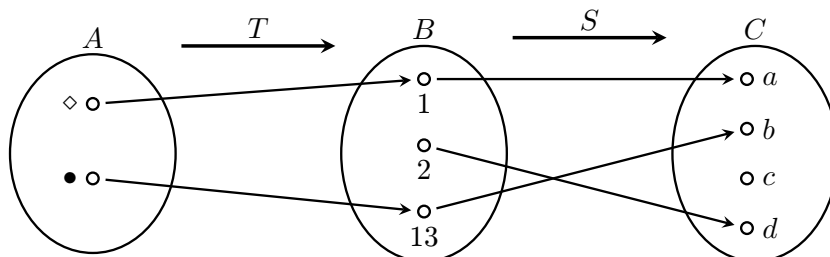
$$(S \circ T) : a \mapsto S(T(a)) \text{ pro } a \in A.$$

Značíme také  $S \circ T = S(T)$ .

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

Zároveň jsme se konečně dozvěděli, proč se kdysi matematici rozhodli pro nepřirozené pořadí ve značení skládání. Dosazení  $a$  totiž vypadá takto:  $S(T(a))$ , první zobrazení je vpravo, druhé vlevo. Mi to tedy přijde jako dost chabá výmluva, ale co s tím nadělám.

**Příklad 9a.d:** Uvažujme naše známé  $T$  z příkladu 9a.b a také zobrazení  $S$  z  $B$  do  $C = \{a, b, c, d\}$  dané  $S(1) = a$ ,  $S(2) = d$ ,  $S(13) = b$ .



Vidíme, že vzniká 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 také vidět, že  $S(2)$  je pro složené zobrazení irelevantní.

△

**Poznámka:** Vidíme, že nápad s navazováním funguje vždy, když je možné hodnoty  $T$  dosadit do  $S$ . Bylo by tedy možné definovat  $S \circ T$  obecně pro zobrazení  $T, S$  splňující  $\text{ran}(T) \subseteq D(S)$ . Není to ale zvykem, protože v aplikacích to obvykle nepotřebujeme a ušetříme si psaní podmínky.

Kdybychom se někdy v takové situaci ocitli, pak si můžeme vzpomenout, že hodnoty  $S$  mimo  $\text{ran}(T)$  na výsledek skládání nemají vliv, takže vždy můžeme skládat  $T$  s restrikcí  $S|_B$ , kde už množiny navazují jako v definici.

△

Diskusi o správném značení skládání bychom se mohli vyhnout, kdyby platilo  $S \circ T = T \circ S$  (komutativní zákon). V to ale doufat nelze. Problém je zásadní. Pokud prohodíme pořadí na  $S: B \mapsto C, T: A \mapsto B$ , tak už není zaručeno správné navázání množin. Možná budeme mít štěstí a  $A = C$ , ale ani pak ještě není vyhráno.

**Příklad 9a.e:** Uvažujme množinu  $A = \{1, 2, 13\}$  a zobrazení  $U, V: A \mapsto A$  definovaná takto:

$$U: 1 \mapsto 1, 2 \mapsto 13, 13 \mapsto 1; \quad V: 1 \mapsto 2, 2 \mapsto 13, 13 \mapsto 1.$$

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 9a.f:** Vraťme se teď k tomu, co čtenář 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  $f(g(x)) = (x + 13)^2$ . Je to jiný vzorec, takže bychom čekali, že půjde o jiné zobrazení. Potřebujeme ale jistotu, může se stát, že různé vzorce dají stejné zobrazení (viz cvičení 9a.3). Různost zobrazení nejsnáze dokážeme ukázkou, že se neshodnou na nějakém prvku. Zkusíme dosadit třeba jedničku a uvidíme.

$$(g \circ f)(1) = 1^2 + 13 = 14, \quad (f \circ g)(1) = (1 + 13)^2 = 196.$$

Teď už jsme si jisti, že změnou pořadí skládání dostáváme jinou funkci.

△

Takže na pořadí záleží, člověk se musí opravdu snažit, aby vytvořil třeba dvě funkce, u kterých  $f(g) = g(f)$ , viz cvičení 9a.8. Proto se na komutativitu nedá spoléhat, naštěstí ji obvykle ani nepotřebujeme. Mnohem významnější praktický dopad má asociativita, kterou u skládání máme.

#### Věta 9a.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  $(R \circ S)[T(a)]$ , použili jsme hranaté závorky, abychom vizuálně vyznačili dosazení, které nás zrovna zajímá. Různé typy závorek jsou samozřejmě pořád jen závorky. Podle definice skládání si rozmyslíme, jak složené zobrazení  $R \circ S$  působí na prvek  $T(a)$ .

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

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:

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

tedy hodnoty jsou stejné.

□

U relací byla ještě jedna zajímavá operace, přechod k inverzní relaci (obracení směru šipek). Podobná věc by se nám hodila i u funkcí a zobrazení. Pokud například máme zobrazení „člověk  $\mapsto \mathbb{R}^{\check{C}}$ “, pak jistě někdy potřebujeme proces opačný, kdy k číslu hledáme člověka. Mohli bychom převzít definici inverzní relace, ale není to zvykem.

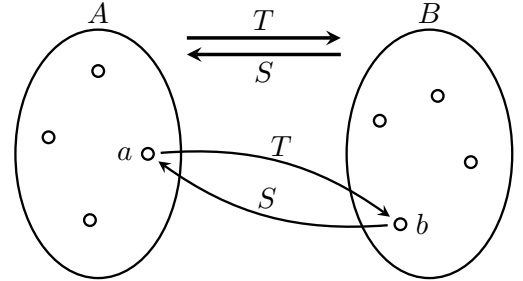
Jedním z důvodů je, že bychom rádi, aby taková inverze zase byla zobrazení, to ale není vůbec zaručeno.

**Příklad 9a.g:** Uvažujme zobrazení  $T$  z příkladu 9a.b. Pokud jej bereme jako relaci, pak můžeme uvažovat inverzní relaci  $T^{-1} = \{(1, \diamond), (13, \bullet)\}$ . Toto ale není zobrazení z  $B$  do  $A$ , protože chybí dvojice pro  $2 \in B$ .

△

Takže pokud chceme vytvořit pojem, který bude u zobrazení obracet směr přiřazení, tak se musíme smířit s tím, že to občas nepůjde. Proto se volí jakási metoda konkursu. Je-li dáno zobrazení  $T: A \mapsto B$ , pak se hledá jiné zobrazení (logicky jdoucí  $B \mapsto A$ ), které by splnilo naše požadavky: Mělo by mít stejné dvojice jako  $T$ , ale v opačném pořadí. My se ale chceme oprostít od jazyka dvojic, podívejme se tedy, co vlastně chceme.

Uvažujme dvojici  $(a, b) \in T$  neboli  $T(a) = b$ . Pokud nějaké inverzní zobrazení  $S$  existuje, tak by mělo mít  $(b, a) \in S$  neboli  $S(b) = a$ . Obrázek vcelku výstižně naznačuje, oč jde. Vnímáme-li  $T$  jako jakousi akci, kterou provedeme s prvkem  $a$ , tak  $S$  ji neutralizuje, dostáváme zpět to, s čím jsme začali. Vzniká tak kolečko, které matematicky vyjádříme rovností  $S(T(a)) = a$ . To bychom chtěli pro všechny prvky  $a$ . Ukazuje se nicméně, že tato podmínka ještě nezaručí, že  $S$  má stejné dvojice jako  $T$ , jen v opačném pořadí. Je proto nutné přidat ještě jednu podmínku, kdy to kolečko začneme v prvku  $b$  a používáme nejdřív  $S$  a pak  $T$ .



Ono „kolečko“ lze vnímat tak, že  $S$  neutralizuje působení  $T$  (a naopak). Je to už třetí představa, co by inverzní zobrazení mělo být. První byla představa inverzní relace, která se štěstím vyšla jako zobrazení, druhá pak představa posílatka, které vznikne obrácením přiřazení z  $T$ . Ukážeme, že všechny tři představy vyjadřují totéž.

#### Fakt 9a.2.

Nechť  $T: A \mapsto B$  je zobrazení. Uvažujme zobrazení  $S: B \mapsto A$ . Následující tři výroky jsou ekvivalentní.

- (i)  $S = \{(b, a) \in B \times A : (a, b) \in T\}$ .
- (ii) Pro  $a \in A, b \in B$  platí, že  $S(b) = a$  právě tehdy, když  $T(a) = b$ .
- (iii)  $S(T(a)) = a$  pro všechna  $a \in A$  a  $T(S(b)) = b$  pro všechna  $b \in B$ .

**Důkaz (poučný):** Uděláme tradiční kolotoč tří implikací.

(i)  $\implies$  (ii):  $S(b) = a$  právě tehdy, když  $(b, a) \in S$ , jde o alternativní značení téhož. To je ale podle (i) právě tehdy, když  $(a, b) \in T$  neboli  $T(a) = b$ .

(ii)  $\implies$  (iii): Vezměme nějaké  $a \in A$ . Označme  $b = T(a)$ . Pak podle (ii) platí  $S(b) = a$  a proto  $S(T(a)) = S(b) = a$ . Důkaz  $T(S(b)) = b$  pro  $b \in B$  je obdobný.

(iii)  $\implies$  (i): Uvažujme nějakou dvojici  $(b, a) \in S$ . Pak  $S(b) = a$ , tudíž i  $T(S(b)) = T(a)$  (dosazujeme do  $T$  tentýž prvek, jen jinak napsaný). Podle (iii) ale  $T(S(b)) = b$  a hodnota zobrazení je jednoznačná, proto  $T(a) = b$  neboli  $(a, b) \in T$ . Ukázali jsme, že  $S \subseteq \{(b, a) \in B \times A : (a, b) \in T\}$ .

Teď opačnou inkluzi. Vezměme  $(b, a) \in \{(b, a) \in B \times A : (a, b) \in T\}$ . Pak  $T(a) = b$  a tedy i  $S(T(a)) = S(b)$ . Podle (iii) ale  $S(T(a)) = a$ , proto  $S(b) = a$  a tedy  $(b, a) \in S$ . □

Vlastnost (iii) má ještě jednu interpretaci, pokud se ve výrazu potkají  $T$  a  $S$  vedle sebe, tak se navzájem jakoby zkrátí a zmizí. To se občas hodí, třeba při řešení rovnic. Podmínka (iii) se tradičně bere jako definice.

#### Definice.

Nechť  $T: A \mapsto B$  je zobrazení. Řekneme, že zobrazení  $S: B \mapsto A$  je **inverzní** k  $T$ , jestliže platí následující podmínky:

- (i) pro všechna  $a \in A$  je  $S(T(a)) = a$ ;
- (ii) pro všechna  $b \in B$  je  $T(S(b)) = b$ .

Pokud takové zobrazení existuje, tak jej značíme  $T^{-1}$  a řekneme, že  $T$  je **invertibilní**.

Let  $T: A \mapsto B$  be a mapping. We say that a mapping  $S: B \mapsto A$  is an **inverse mapping** of  $T$  if it satisfies  $S(T(a)) = a$  for all  $a \in A$  and  $T(S(b)) = b$  for all  $b \in B$ . If such a mapping exists, then we denote it  $T^{-1}$  and say that  $T$  is **invertible**.

Jako důsledek faktu 9a.2 dostáváme, že pokud  $T^{-1}$  existuje, tak je jediné možné. To je důležité, zavádět speciální značení pro pojem, který nevychází jednoznačně, obvykle vede ke komplikacím.

**Příklad 9a.h:**

Nechť  $A = \{1, 13, 14\}$ ,  $B = \{21, 23, 24\}$ . Uvažujme zobrazení  $T: A \mapsto B$  definované takto:  $1 \mapsto 24$ ,  $13 \mapsto 23$ ,  $14 \mapsto 21$ .

Chceme-li mít inverzní zobrazení, stačí podle faktu obrátit přiřazení z  $T$  a doufat, že to dobře dopadne. Uvažujme tedy  $S: 24 \mapsto 1$ ,  $23 \mapsto 13$ ,  $21 \mapsto 14$ . Protože každému prvku z  $B$  přiřazujeme přesně jednou, je to opravdu zobrazení, splňuje (ii) z faktu 9a.2 a tedy  $S = T^{-1}$ . Ověříme to podle definice.

Pro čísla z  $A$  platí, že  $S(T(1)) = S(24) = 1$ ,  $S(T(13)) = S(23) = 13$  a  $S(T(14)) = S(21) = 14$ . Ještě druhá podmínka: pro čísla z  $B$  platí  $T(S(21)) = T(14) = 21$ ,  $T(S(23)) = T(13) = 23$  a  $T(S(24)) = T(1) = 24$ . Vyšlo to.

Teď si připomeňme zobrazení  $T$  z množiny  $A = \{\diamond, \bullet\}$  do  $B = \{1, 2, 13\}$  definované předpisem  $T(\diamond) = 1$ ,  $T(\bullet) = 13$ , viz příklad 9a.b.

Východiskem je obrátit dvojice z  $T$ , dostaneme  $S = \{(1, \diamond), (13, \bullet)\}$ . Toto ale není zobrazení, protože neobsahuje žádné přiřazení pro  $2 \in B$ . To také znamená, že se na něj nevztahuje fakt 9a.2, tam je totiž v předpokladu, že  $S$  musí být zobrazení.

Můžeme chybějící přiřazení doplnit, jsou dvě možnosti, kam poslat 2. Zkusme jednu z nich a uvažujme  $S: B \mapsto A$  předpisem  $S(1) = \diamond$ ,  $S(2) = \bullet$ ,  $S(13) = \bullet$ . Pak pro všechny prvky z množiny  $A$  máme  $S(T(\diamond)) = S(1) = \diamond$  a  $S(T(\bullet)) = S(13) = \bullet$ . Zobrazení  $S$  tedy splňuje první podmínku z definice inverzního zobrazení, ale přitom není tím, co od inverzního zobrazení očekáváme. To ukazuje, že první podmínka sama o sobě nevystihuje to, co chceme, tu druhou jsme přidali oprávněně. V tomto případě správně rozpozná, že  $S$  není dobrým kandidátem:  $T(S(2)) = T(\bullet) = 13$ , nevyšlo to.

Podobně může čtenář ověřit, že přiřazení  $S(2) = \diamond$  nepomůže. Zobrazení  $T$  tedy není invertibilní.

△

**Příklad 9a.i:** Uvažujme množiny  $A = M_{2 \times 2}(\mathbb{R})$  všech čtvercových matic  $2 \times 2$  nad reálnými čísly a  $B = \mathbb{R}^4$ . Zobrazení  $T: A \mapsto B$  definujeme vzorcem

$$T\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = (a, b, c, d).$$

(Protože se obvyčejné závorky používají pro matice a vektory, budeme teď pro vymezení argumentu používat hranaté závorky.) Když toto přiřazení otočíme, dostáváme zobrazení  $S: B \mapsto A$  dané vzorcem

$$S[(a, b, c, d)] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Ověříme podle definice, že  $S = T^{-1}$ :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A: S\left[T\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]\right] = S[(a, b, c, d)] = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

$$\forall (a, b, c, d) \in B: T[S[(a, b, c, d)]] = T\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = (a, b, c, d).$$

△

**Příklad 9a.j:** Vyšetříme několik zobrazení založených na přiřazení  $n \mapsto n + 1$ .

1. Uvažujme zobrazení  $T: \mathbb{Z} \mapsto \mathbb{Z}$  dané vzorcem  $T(n) = n + 1$ .

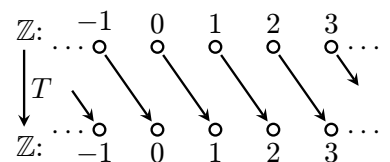
Jako relace obsahuje dvojice typu  $(n, n + 1)$ , přirozeným kandidátem na inverzní zobrazení je tedy množina dvojic  $(n + 1, n)$  neboli  $(n, n - 1)$ . Máme proto kandidáta  $S(m) = m - 1$ , budeme používat  $m$  pro proměnnou branou z cílové množiny zobrazení  $T$  (v obrázku je dole). Podmínky z definice potvrdí, že opravdu  $S = T^{-1}$ :

- $n \in \mathbb{Z} \implies S(T(n)) = S(n + 1) = (n + 1) - 1 = n$ ,
- $m \in \mathbb{Z} \implies T(S(m)) = T(m - 1) = (m - 1) + 1 = m$ .

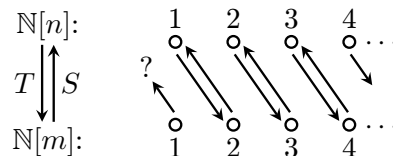
Vyšlo to. Složené funkce jsme rozbalovali „zevnitř“, tedy nejprve jsme vyhodnocovali vnitřní funkci a výsledný výraz dosazovali do vnější. Abychom měli změnu, tak až se zase potkáme s důkazem inverzní funkce, začneme rozbalovat u vnější funkce.

Tento příklad také ukazuje, že vhodná volba proměnných – v tomto případě důsledné používání proměnné  $m$  pro prvky z  $\text{ran}(T)$  – usnadňuje porozumění zejména v situaci, kdy jsou  $D(T)$  a  $\text{ran}(T)$  stejné množiny. Čtenáři také pomůže vyznačení proměnné v grafu tradičním fyzikálním způsobem, což ukážeme níže.

2. Teď uvažujme  $T(n) = n + 1$  coby zobrazení  $\mathbb{N} \mapsto \mathbb{N}$ .



Je  $S(m) = m - 1$  jeho inverzním zobrazením? Není, protože to nedefinuje zobrazení  $\mathbb{N} \mapsto \mathbb{N}$ , jmenovitě  $S(1) \notin \mathbb{N}$ . Co s tím? Nelze tu jedničku vynechat, inverzní zobrazení musí být definováno na celé cílové množině zobrazení  $T$ . Je ale možné tuto hodnotu předefinovat.



Uvažujme tedy zobrazení  $R: \mathbb{N} \mapsto \mathbb{N}$  definované jako  $R(m) = m - 1$  pro  $m \geq 2$  a  $R(1) = 1$ . Našli jsme  $T^{-1}$ ?

Pokud  $n \in \mathbb{N} = D(T)$ , pak  $R(T(n)) = R(n + 1) = (n + 1) - 1 = n$ , zde jsme využili toho, že pro  $n \in \mathbb{N}$  je  $n + 1 \geq 2$ . První podmínka z definice je splněna.

Vezměme  $m \in \mathbb{N} = D(R)$  a uvažujme  $T(R(m)) = R(m) + 1$ . Hodnota  $R(m)$  závisí na  $m$ , musíme ověřit obě možnosti. Pokud  $m \geq 2$ , tak  $T(R(m)) = (m - 1) + 1 = m$ , zase souhlasí. Pokud  $m = 1$ , dostáváme  $T(R(1)) = 1 + 1 = 2$ . Neplatí tedy  $T(R(1)) = 1$  a zobrazení  $R$  není inverzní k  $T$ .

Snadno si rozmyslíme, že ať už za hodnotu  $R(1)$  zvolíme jakékoliv  $a \in \mathbb{N}$ , podmínku  $T(R(1)) = 1$  se nám nepodaří splnit. Zobrazení  $T$  tedy není invertibilní.

**3.** Na závěr uvažujme  $T(n) = n + 1$  coby zobrazení  $\mathbb{N} \mapsto \mathbb{N} \setminus \{1\}$ .

Tato definice má smysl, protože pro  $n \in \mathbb{N}$  je  $T(n) = n + 1 \geq 2$ . Teď už číslo 1 není součástí cílové množiny a snadno ověříme, že zobrazení  $S: \mathbb{N} \setminus \{1\} \mapsto \mathbb{N}$  dané vzorcem  $S(m) = m - 1$  je inverzní k  $T$ . Vlastně už jsme to udělali, stačí v předchozí části ignorovat zkoumání  $m = 1$ .

V posledních dvou příkladech jsou zobrazení  $T$  coby množiny dvojic shodné, liší se pouze deklarovanou cílovou množinou. Vidíme, že to výrazným způsobem ovlivnilo jejich vlastnosti.

△

**9a.3 Poznámka:** V této kapitole ještě potkáme situace, kdy máme představu, jak by námi vytvářené zobrazení mělo působit, ale budeme jej muset trochu upravit. Vzniká pak zobrazení definované různými předpisy podle toho, které proměnné z definičního oboru se dosazují. Tomu se říká definice rozpisem a máme pro to speciální značení, v případě zobrazení  $R$  výše bychom mohli psát

$$R(m) = \begin{cases} m - 1, & m \geq 2; \\ 1, & m = 1. \end{cases}$$

Čistě formálně bychom měli v prvním řádku psát  $m \in \mathbb{N} \wedge m \geq 2$ , ale pokud před definicí deklaruje záměr definovat zobrazení na  $\mathbb{N}$ , tak se nám to odpustí, protože komplikované podmínky snižují čitelnost. V případech, kdy je  $D(R)$  deklarováno předem, se toleruje i další zjednodušení, definice mohla vypadat i takto:

$$R(m) = \begin{cases} 1, & m = 1; \\ m - 1, & \text{jinde.} \end{cases}$$

S takovým zobrazením se pak pracuje v souladu se selským rozumem, při dosazování proměnné se podíváme, do které varianty patří, a použijeme příslušný předpis. Pokud o takovém zobrazení něco dokazujeme, pak je samozřejmě třeba projít všechny možnosti.

Obecně je možné definiční obor rozdělit na více podmnožin než dvě, třeba i na nekonečně mnoho, a pro každou mít speciální vzorec. Je s tím pak víc práce, ale v zásadě na tom není nic těžkého.

△

Při pohledu na obrázky se zdá dost jasné, že když obrátíme směr šipek dvakrát, dostaneme zpět původní přiřazení. V matematickém jazyce to vypadá takto.

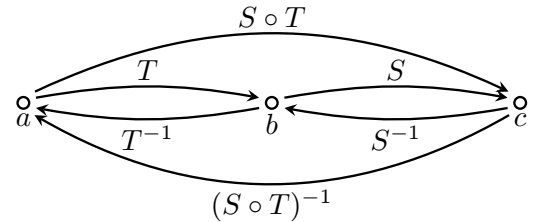
**Fakt 9a.4.**  
 Nechť  $T: A \mapsto B$  je zobrazení.  
 Jestliže je  $T$  invertibilní, pak je i  $T^{-1}$  invertibilní a  $(T^{-1})^{-1} = T$ .

**Důkaz (poučný):** Předpokládejme, že  $T$  je invertibilní, takže máme  $T^{-1}: B \mapsto A$ . Chceme ukázat, že existuje nějaké zobrazení  $S$ , které jde naopak než  $T^{-1}$ , tedy  $A \mapsto B$ , a splňuje rovnosti  $S(T^{-1}(b)) = b$  a  $T^{-1}(S(a)) = a$  pro  $b \in B, a \in A$ .

Zobrazení  $T$  přesně toto splňuje, tudíž je inverzním zobrazením k  $T^{-1}$  a  $T^{-1}$  je invertibilní. □



Umíme dělat inverzi a také umíme skládat, jak to jde dohromady? Rádi bychom našli způsob, jak najít  $(S \circ T)^{-1}$  pomocí znalosti  $T^{-1}$  a  $S^{-1}$ . Obrázek dosti jasně naznačuje, jak to funguje, zejména to, že při hledání inverzního zobrazení pro skládání musíme obrátit pořadí složek. Je to vidět už z toho, že nám musejí navazovat množiny, z původním pořadí máme  $A \xrightarrow{T} B \xrightarrow{S} C$ , u inverzních zobrazení má smysl jedině toto pořadí:  $C \xrightarrow{S^{-1}} B \xrightarrow{T^{-1}} A$ .

**Věta 9a.5.**

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  $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$ .

**Důkaz** (rutinní, poučný): Předpokládejme, že  $T$  a  $S$  jsou invertibilní. Potřebujeme dokázat, že existuje zobrazení inverzní k  $S \circ T$ . Ukážeme, že zobrazení  $U: C \mapsto A$  dané  $U = T^{-1} \circ S^{-1}$  splňuje požadavky.

Abychom čtenáři pomohli se čtením, budeme používat hranatou závorku pro dosazování a oblou pro vyznačení složeného zobrazení. Pomocí definice skládání aplikované opakovaně na rozličná zobrazení odvodíme pro  $a \in A$

$$(T^{-1} \circ S^{-1})[(S \circ T)[a]] = (T^{-1} \circ S^{-1})[S[T[a]]] = T^{-1}[S^{-1}[S[T(a)]]].$$

Teď použijeme definici  $S^{-1}$  s prvkem  $b = T(a)$ , poté definici  $T^{-1}$  a dostáváme

$$(T^{-1} \circ S^{-1})[(S \circ T)[a]] = \dots = T^{-1}[S^{-1}[S[T(a)]]] = T^{-1}[T[a]] = a.$$

Obdobně pro všechna  $b \in B$  platí

$$\begin{aligned} (S \circ T)[(T^{-1} \circ S^{-1})[b]] &= (S \circ T)[T^{-1}[S^{-1}[b]]] = S[T[T^{-1}(S^{-1}(b))]] \\ &= S[S^{-1}[b]] = b. \end{aligned}$$

Potvrdili jsme, že  $T^{-1} \circ S^{-1}$  je to správné zobrazení. □

V sekci 9a.13 uvedeme jazyk, ve kterém je tento důkaz o něco přehlednější, viz cvičení 9a.18.

Vraťme se k problému, že inverzní zobrazení nemusí vždy existovat. Pokusíme se získat nějakou charakterizaci, která nám umožní rozlišit invertibilní zobrazení od těch ostatních. Vyjdeme z toho, že zobrazení  $T$  coby relace určitě má  $T^{-1}$  coby inverzní relaci. Kdy bude toto  $T^{-1}$  zobrazením?

Podmínkou je, aby každý prvek  $B$  byl přesně v jedné dvojici v  $T^{-1}$ . Jsou dvě možnosti, jak toto pokazit. Jedna je, že se nějaký prvek  $b$  nevyskytuje v žádné dvojici v  $T^{-1}$ . Z pohledu zobrazení  $T$  to znamená, že není žádná  $x \in A$  splňující  $T(x) = b$  neboli do tohoto  $b$  nevede žádná šipka (viz příklad 9a.h). Pokud tedy chceme doufat v existenci inverzního zobrazení, musíme toto chování vyloučit.

Druhá nepříznivá možnost je, že se nějaký prvek  $b$  vyskytuje ve více dvojicích v  $T^{-1}$ . Z pohledu  $T$  to znamená, že existuje více dvojic v  $T$ , které mají  $b$  jako druhou složku, neboli najdeme více různých prvků  $x \in A$  takových, že  $T(x) = b$ . Intuitivně to dává smysl: Kdyby do nějakého  $b$  vedlo více šipek, tak máme při pokusu o návrat problém, že nevíme, kterou cestou jít. Pokud tedy doufáme v existenci inverze, tak potřebujeme, aby šipky z různých bodů  $A$  končily v různých místech, nesmějí se sbíhat.

Protože třetí problém není, zdá se, že výše zmíněné vlastnosti jsou pro existenci inverzního zobrazení rozhodující. Než jim dáme oficiální jméno, je potřebná ještě jedna poznámka. Druhá podmínka (že se šipky nesbíhají) se do matematictý přeloží takto:

- Pro všechna  $x, y \in A$  platí, že jestliže  $x \neq y$ , pak  $T(x) \neq T(y)$ .

Je to velmi výstižné, ale nepřiliš praktické, protože (zejména ve složitějších příkladech) se z předpokladu  $x \neq y$  špatně dostáváme k tomu, co potřebujeme. Proto se v konkrétních příkladech téměř vždy dokazuje spíše obměna této implikace, která nám umožní využít bohaté zkušenosti s řešením rovnic:

- Jestliže  $T(x) = T(y)$ , pak  $x = y$ .

Z toho důvodu se tento pohled tradičně bere jako definice. Já sám to nemám rád, protože v této formě není zjevné, co vlastně od takové vlastnosti chceme, a musím vždy studentům vysvětlovat, že pro správné pochopení musí přejít k obměně definice neboli k původní verzi výše. Nakonec jsem se rozhodl (a bylo to bolestné) jít s davem, protože je pro studenty asi nakonec jednodušší mít stejnou definici jako všichni ostatní, kterou navíc mohou rovnou aplikovat v praxi.

**Definice.**

Nechť  $T: A \mapsto B$  je zobrazení.

Řekneme, že  $T$  je **prosté** či **injektivní**, jestliže pro všechna  $x, y \in A$  platí

$$T(x) = T(y) \implies x = y.$$

Řekneme, že  $T$  je **na** či **surjektivní**, jestliže  $\text{ran}(T) = B$ .

Řekneme, že  $T$  je **vzájemně jednoznačné** či **bijekce**, jestliže je prosté a na.

A mapping  $T: A \mapsto B$  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  $\text{ran}(T) = B$ . If it is both 1-1 and onto, then we call it a **bijection**.

Název „vzájemně jednoznačné“ je tradičnější a pěknější, nicméně delší, takže zde budeme preferovat název „bijekce“, který je také všeobecně srozumitelný.

Podmínka  $\text{ran}(T) = B$  se dá také napsat  $T[A] = B$  nebo podrobněji

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

Tato vlastnost je zvláštní v tom, že vlastně nezávisí na samotném fungování  $T$  (tedy jak posílá prvky), ale čistě na tom, jak deklarujeme cílovou množinu  $B$ . Pokud ji můžeme změnit (což v mnoha aplikacích není problém), tak nám nic nebrání zvolit  $B = \text{ran}(T)$ . Fungování  $T$  zůstává stejné (jde stále o stejnou množinu dvojic) a najednou je to zobrazení na neboli surjekce.

Rovnou si také rozmyslíme, že když změna cílové množiny neovlivní fungování zobrazení (samozřejmě za podmínky, že nové  $B$  pořád obsahuje  $\text{ran}(T)$ ), tak také nemůže ovlivnit prostotu, která pro změnu závisí čistě na akci  $T$ . To znamená, že když máme prosté zobrazení, tak stačí zvolit  $B = \text{ran}(T)$  (pokud nám to okolnosti dovolí) a rovnou máme bijekci. Tento postup je velmi oblíbený u reálných funkcí.

To nás přivádí zpět k definici rovnosti dvou zobrazení. Nutili jsme čtenáře, aby kromě kontroly, že dvě zobrazení fungují stejně, ověřoval i to, zda mají stejnou cílovou množinu. Vypadalo to jako formalita, ale teď vidíme, že to má hlubší smysl. Kdybychom toto nekontrolovali, tak by se mohlo stát, že máme dvě zobrazení, která fungují stejným způsobem, ale jedno je na a druhé není kvůli odlišné deklaraci cílových množin. Došlo by pak k tomu, že dvě zobrazení, která oficiálně prohlásíme za stejná, nemají stejné vlastnosti. To bychom určitě nechtěli.

Našli jsme metodu, která umí (někdy) udělat z daného zobrazení surjekci, šlo by něco takového i s prostotou? Tam je to komplikovanější, protože odstranit sbíhavé šipky lze jedině tak, že zasáhneme přímo do fungování zobrazení. Ztrácíme tak část informace, kterou původní  $T$  neslo, je třeba s tím počítat. Někdy to stojí za to, k vyřazení nevhodných dvojic se pak používá jako nástroj restrikce. V reálné analýze je to standardní nástroj k vyrábění prostých funkcí.

Pokud byly naše úvahy před definicí správné, pak by prostota a surjektivita dohromady měly poznat, zda je dané zobrazení invertibilní. To by znamenalo, že bijekce jsou mezi zobrazeními v určitém smyslu ty lepší. Potvrdíme si to.

**Věta 9a.6.**

Nechť  $T: A \mapsto B$  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. Vezměme prvky  $x, y \in A$  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  $T^{-1}(T(x)) = T^{-1}(T(y))$ . Podle definice se  $T$  a  $T^{-1}$  spolu jakoby „zkrátí“ a dostáváme  $x = y$ . Prostota je dokázána.

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

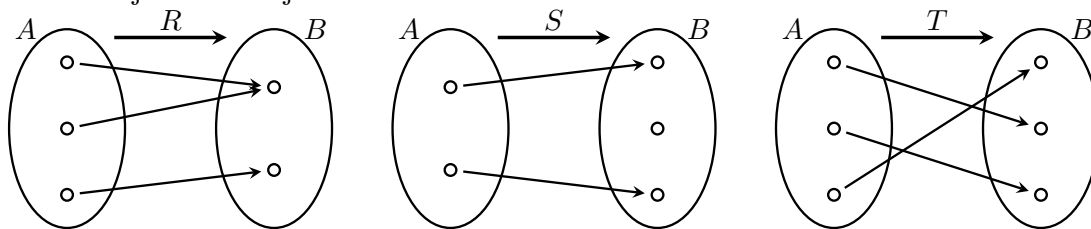
$2) \Leftarrow$ : Předpokládejme, že  $T$  je bijekce. Ukážeme, že je invertibilní. Uvažujme relaci  $S$  z  $B$  do  $A$ , která vznikla jako inverzní relace k  $T$ . Ukážeme, že je to zobrazení. Vezměme nějaké  $b \in B$ , musíme ukázat, že je v právě jedné dvojici v  $S$ .

Protože je  $T$  na, určitě existuje  $a \in A$  takové, že  $T(a) = b$ , tedy  $(a, b) \in T$  a tudíž  $(b, a) \in S$ . Je takových dvojic více? Nechť  $x \in A$  je takové, že  $(b, x) \in S$ . Pak  $(x, b) \in T$  neboli  $T(x) = b$ , také  $T(a) = b$ , z prostoty  $T$  tedy nutně  $x = a$ . To znamená, že  $a$  je jediný prvek z  $A$  takový, že  $(b, a) \in S$ , a  $S$  je zobrazení.

Podle faktu 9a.2 (i)  $\implies$  (iii) pak  $S = T^{-1}$ .

□

**Příklad 9a.k:** Uvažujme následující tři zobrazení.



Vidíme, že  $R$  je na, ale není prosté;  $S$  je prosté, ale není na a  $T$  má obě vlastnosti, je to tedy bijekce. Vidíme také, že u  $R$  a  $S$  bychom nedokázali vytvořit inverzní zobrazení.

Uměli byste v prvním příkladě vytvořit nějaké zobrazení  $A \mapsto B$ , které je prosté? Pokud vás napadá, že by měla být nějaká souvislost mezi prostotou/surjektivitou a počtem prvků v množinách, tak jste na dobré stopě, máme o tom celou část 9b.

△

**Příklad 9a.l:** Uvažujme zobrazení  $T$  z množiny občanů ČR do množiny desetimístných čísel definované tak, že  $T(x)$  je dáno jako rodné číslo člověka  $x$  (doufáme, že je to určeno jednoznačně). 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.

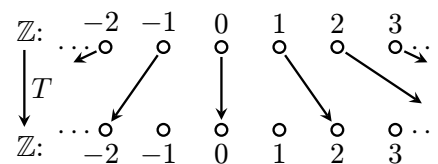
△

**Příklad 9a.m:** Pro následující zobrazení rozhodneme, zda jsou prostá, na a bijekce. Případně najdeme inverzní zobrazení.

1. Uvažujme  $T: \mathbb{Z} \mapsto \mathbb{Z}$  dané vzorcem  $T(n) = 2n$ .

Je prosté? Vezměme libovolné  $x, y \in \mathbb{Z}$  takové, že  $T(x) = T(y)$ . Pak  $2x = 2y$  a tedy  $x = y$ .

Je na? Protože výstupy  $T$  jsou sudá čísla, asi ne. Důkaz: Vezměme  $m = 13$ . Neexistuje  $n \in \mathbb{Z}$  splňující  $2n = 13$ , proto neexistuje  $n \in \mathbb{Z}$  splňující  $T(n) = m$  a  $T$  opravdu není na.



Závěr:  $T$  je prosté a není na.

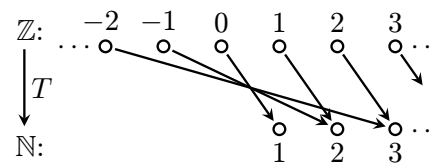
2. Uvažujme  $T: \mathbb{Z} \mapsto \mathbb{N}$  dané vzorcem  $T(n) = |n|$ .

Protože  $T(0) = 0$  neleží v cílové množině, je to nekorektně zadané zobrazení, jinak řečeno blbá otázka. Nemusíme tedy nic zkoumat.

Šlo by nějakou mírnou úpravou vyrobit korektně zadanou otázku? Jedna možnost je přidat nulu do cílové množiny, tedy uvažovat  $T: \mathbb{Z} \mapsto \mathbb{N}_0$ . Druhá možnost je vhodným způsobem „posunout“ obrazy. Vyzkoušíme to.

3. Uvažujme  $T: \mathbb{Z} \mapsto \mathbb{N}$  dané vzorcem  $T(n) = |n| + 1$ .

Je prosté? Vezměme libovolné  $x, y \in \mathbb{Z}$  takové, že  $T(x) = T(y)$ . Pak  $|x| + 1 = |y| + 1$  neboli  $|x| = |y|$ . Zkušenost říká, že jakmile jsou u  $x, y$  povolena obě znaménka, tak z poslední rovnosti už  $x = y$  nevymlátíme. Proto zkusíme udělat protipříklad:  $x = -1$  a  $y = 1$  jsou oba v  $\mathbb{Z}$ , splňují  $T(x) = 1 = T(y)$  a přitom  $x \neq y$ . Zobrazení  $T$  proto není prosté.



Je na? Vezměme libovolné  $m \in \mathbb{N}$ . Potřebujeme najít  $n \in \mathbb{Z}$  splňující  $T(n) = m$  neboli  $|n| + 1 = m$ . Zvolme  $n = m - 1$ . Protože  $m \in \mathbb{N}$ , je  $n \geq 0$  a proto  $|n| = n = m - 1$ . Platí tedy  $n \in \mathbb{Z}$  a  $T(n) = (m - 1) + 1 = m$ .

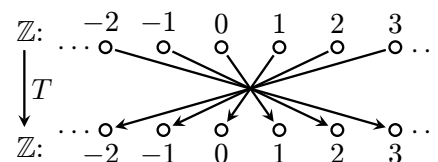
Závěr:  $T$  není prosté a je na.

Všimněte si, že restrikce  $T|_{\mathbb{N}_0}$  by už byla prostá, také na, tedy bijekce. Mělo by proto existovat inverzní zobrazení  $S: \mathbb{N} \mapsto \mathbb{N}_0$ , obrázek naznačuje, že obrácení šipek dá  $S(m) = m - 1$ . Test z definice to potvrdí, jde vlastně o mírnou modifikaci příkladu 9a.j.

4. Uvažujme  $T: \mathbb{Z} \mapsto \mathbb{Z}$  dané vzorcem  $T(n) = 1 - n$ .

Je prosté? Vezměme libovolné  $x, y \in \mathbb{Z}$  takové, že  $T(x) = T(y)$ . Pak  $1 - x = 1 - y$  neboli  $x = y$ . Ano, je prosté.

Je na? Vezměme libovolné  $m \in \mathbb{Z}$  (cílová množina). Hledáme  $n \in \mathbb{Z}$  splňující  $T(n) = m$  neboli  $1 - n = m$ . Zvolme  $n = 1 - m$ . Pak  $n \in \mathbb{Z}$  a platí  $T(n) = 1 - (1 - m) = m$ .



Závěr:  $T$  je prosté a na, je to tedy bijekce.

Mělo by proto existovat inverzní zobrazení. Když zkusíme v obrázku obrátit šipky a čteme je zdola nahoru, tak vidíme, že jde vlastně o stejné přiřazení, tedy  $T^{-1}(m) = T(m) = 1 - m$ . Tento nečekaný nápad si raději potvrdíme podle definice. Pro rozlišení budeme používat  $n$  pro celá čísla coby  $D(T)$  a  $m$  pro čísla z oboru hodnot.

$$n \in \mathbb{Z} \implies T(T(n)) = 1 - T(n) = 1 - (1 - n) = n,$$

$$m \in \mathbb{Z} \implies T(T(m)) = 1 - T(m) = 1 - (1 - m) = m.$$

Vyšlo to. Toto zobrazení je samo sobě inverzí, což není zrovna běžný jev, ale evidentně se to stát může. Viz také cvičení 9a.21.

Všimněte si zajímavé věci. U posledních dvou příkladů odpovídalo nalezené inverzní zobrazení vzorcí, který jsme použili v důkazu surjektivit. Není to náhoda, už jsme dokázali, že hodnota  $a = T^{-1}(b)$  musí splňovat  $T(a) = b$ , tedy lze ji najít řešením stejné rovnice, jako jsme řešili u zkoumání surjektivit.

△

## S 9a.7 Jak na vlastnosti zobrazení

Předpokládejme, že zobrazení je zadáno vztahem.

**Prostota:** Chceme-li určit, zda je  $T$  prosté, vycházíme obvykle z definice. Vezmeme dva libovolné prvky  $x, y \in A$  (tedy obecné prvky, nemůžeme si vybrat dva pěkné konkrétní) a napíšeme rovnost  $T(x) = T(y)$ . Přepíšeme  $T(x)$  a  $T(y)$  vzorcem z definice  $T$  a dostaneme rovnici, ze které se pokusíme odvodit informaci o vztahu  $x$  a  $y$ . Pokud se podaří dojít k  $x = y$ , máme prosté zobrazení. Pokud se to někde zadrhne, tak to obvykle naznačí, kde hledat protipříklad.

Někdy (zejména u snadných příkladů) je pohodlnější dokázat prostotu pomocí obměny definice (viz diskuse před definicí), tedy doloží se, že když  $x \neq y$ , pak určitě  $T(x) \neq T(y)$ . U reálných funkcí je zase často lepší zkoumat prostotu pomocí metod matematické analýzy, viz níže.

**Surjektivita:** 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  $T(x) = y$ . Po dosazení za  $T(x)$  dostáváme rovnici  $T(x) = y$ , kterou se snažíme vyřešit pro  $x$ , přitom bereme  $y$  coby parametr. Cílem není najít úplnou množinu řešení, ale stačí jedno, třeba i uhodnuté. Pokud se najde, tak je zobrazení na.

Pokud se postup někde zadrhne, obvykle to naznačí, kde hledat protipříklad.

**Inverzní zobrazení:** Postup je obdobný jako u surjektivit, rovnici  $T(x) = y$  řešíme pro  $x$ . Tentokrát hledáme  $x$  ve formě vzorce s proměnnou  $y$ .

**Vše:** Pokud se po nás nechce samostatný důkaz pro každou z vlastností, je možno použít tento postup: Rovnici  $T(x) = y$  zkusíme vyřešit pro  $x$ . Možnosti:

- Pokud řešení existuje pro každé  $y$  a je vždy jediné, je  $T$  bijekce a dostáváme vzorec pro inverzní zobrazení.
- Pokud řešení existuje, ale někdy je jich více, je  $T$  na, ale není prosté.
- Pokud řešení existuje jen pro některá  $y$ , ale pak je jedinečné, je  $T$  prosté, ale není na.
- Pokud řešení existuje jen pro některá  $y$ , a navíc je jich někdy víc, pak  $T$  není ani prosté, ani na.

Tento postup funguje velmi dobře zejména u jednodušších zobrazení.

△

**Příklad 9a.n:** Návod si vyzkoušíme na zobrazení  $T: \mathbb{N}^3 \mapsto \mathbb{N}^2$  daném vztahem  $T(r, s, t) = (r^3, s^t)$ .

**Prostota:** Máme vzít libovolné  $x, y \in A$ , v tomto případě jsou to tříslóžkové vektory. Mějme 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  $T(r, s, t) = T(u, v, w)$  neboli  $(r^3, s^t) = (u^3, v^w)$ .

Rovnost vektorů znamená rovnost všech souřadnic, máme tedy  $r^3 = u^3$  a  $s^t = v^w$ . Z toho chceme odvodit rovnost souřadnic u vstupních vektorů  $x, y$ . Co máme k dispozici? 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 experimentovat, 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  $(1, 3, 4) = (1, 9, 2)$ .

**Na:** Vybíráme  $y$  z cílového prostoru  $\mathbb{N}^2$ , je to tedy nějaký vektor, třeba  $y = (u, v)$  pro  $u, v \in \mathbb{N}$ . Hledáme  $x = (r, s, t) \in \mathbb{N}^3$  tak, aby platilo  $T(r, s, t) = (u, v)$  neboli  $(r^3, s^t) = (u, v)$ . Dostáváme rovnice  $r^3 = u$ ,  $s^t = v$  a tuto soustavu zkusíme řešit pro  $r, s, t$ .

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  $A$  se 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 čtenář 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.

△

**S 9a.8 Poznámka:** Studenti se často snaží vyhnout matematickým symbolům, cítí se lépe u přirozeného jazyka. Je pak třeba být opatrný na význam. Občas se setkávám s následujícím pokusem o definici prostého zobrazení: „Ke každému  $a$  existuje právě jedno  $b \in B$  tak, aby  $T(a) = b$ .“ Toto ale neznamená prototu, je to podmínka z definice zobrazení jako takového.

Setkávám se také s verzí „pro každé  $b \in B$  existuje právě jedno  $a \in A$  takové, že  $T(a) = b$ “. To je pro změnu overkill, takto vypadá definice bijekce. Pokud už chceme popsat prototu tímto způsobem, tak správně je to „pro každé  $b \in B$  existuje **nejvýše** jedno  $a \in A$  takové, že  $T(a) = b$ “.

△

### 9a.9 Poznámka o reálných funkcích:

Inverzní funkce a vlastnost prostoty jsou velmi významné v reálné analýze. Začneme prostotou.

Předpoklad  $f(x_1) = f(x_2)$  znamená, že vodorovná přímka o rovnici  $y = f(x_1)$  protne graf nejen v bodě  $(x_1, f(x_1))$ , ale i v bodě  $(x_2, f(x_2))$ . U prostoty chceme, aby pak  $x_1 = x_2$ , tedy chceme, aby žádná vodorovná přímka neprotla graf funkce ve více než jednom bodě.

Pokud jde o spojitou funkci na intervalu, vyjde z toho požadavek, že taková funkce musí být ryze monotónní, tedy ryze rostoucí nebo ryze klesající na celém intervalu. To snadno poznáme z grafu, pokud jej máme k dispozici, jinak použijeme derivaci.

Z toho je jasné, že například funkce  $f(x) = x^2$  nebude prostá na  $\mathbb{R}$ . Naopak funkce  $e^x$  prostá na  $\mathbb{R}$  je.

U reálných funkcí obvykle není důvod preferovat nějakou cílovou množinu, lze tedy téměř vždy volit  $\text{ran}(T)$ . Prosté funkce se pak rovnou stávají bijekcemi a mají své inverzní funkce. Hledají se způsobem, který už známe od obecných zobrazení. Bývají velmi užitečné, 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  $x \in \mathbb{R}$ . Dá se říct, že se tyto dvě funkce navzájem „vykrátí“, když se dostanou vedle sebe ve skládání, což je základem pro řešení rovnic s logaritmy či exponenciálami.

Zde je nutno upozornit na jeden problém se značením. Reálné funkce (stejně jako čísla) násobíme a umocňujeme, například  $f^3$  značí  $f \cdot f \cdot f$  či  $f^{-2}$  značí  $\frac{1}{f \cdot f}$ . Zcela logicky pak  $f^{-1} = \frac{1}{f}$ , třeba  $(e^x)^{-1} = e^{-x}$ . Ovšem zde v obecné teorii používáme  $f^{-1}$  pro inverzní zobrazení neboli inverzní funkci, přičemž nejde o totéž, v tomto smyslu  $(e^x)^{-1} = \ln(x)$ .

Tento rozpor se nepodařilo vyřešit, takže je nutno být na pozoru. Pokud použijeme značení  $f^{-1}$ , je nutno dbát na to, aby byl význam zřejmý. Často je to naštěstí poznat z kontextu (obvykle je to ta mocnina), ale musíme být ostražití a případně připomenout, oč kráčí. Někteří autoři (třeba já) zavádějí u reálných funkcí speciální značení  $f_{-1}$  pro inverzní funkce, třeba se to časem ujme.

△

**Příklad 9a.o:** Prozkoumáme prostotu a surjektivitu pro několik funkcí coby zobrazení  $\mathbb{R} \mapsto \mathbb{R}$ . Použijeme postup vycházející z definice.

**1.**  $f(x) = x^3 - x$ . 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, protíná osu  $x$  v bodě  $1$ . Vidíme, že tato funkce dokáže nabýt libovolné reálné hodnoty, je tedy na  $\mathbb{R}$ . Zároveň také vidíme, že není prostá, protože například  $f(0) = 0$  a také  $f(1) = 0$ , tedy  $f(0) = f(1)$  ale neplatí  $0 = 1$ .

**2.**  $f(x) = 2x - 1$ . Tato funkce je prostá. Důkaz: Vezměme libovolné  $x_1, x_2 \in \mathbb{R}$  takové, že  $f(x_1) = f(x_2)$ . Pak  $2x_1 - 1 = 2x_2 - 1$ , odtud hravě dostaneme  $x_1 = x_2$  a důkaz je hotov.

Tato funkce je na  $\mathbb{R}$ . Důkaz: Necht'  $y$  je nějaký prvek z cílové množiny  $\mathbb{R}$ . Chceme najít  $x_0$  splňující  $f(x_0) = y$  neboli  $2x_0 - 1 = y$ . Odtud  $x_0 = \frac{y+1}{2}$ . To je určitě reálné číslo, ještě potvrdíme, že splňuje požadavek:

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

Toto  $f$  je proto bijekce  $\mathbb{R}$  na  $\mathbb{R}$ . 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 pro  $f_{-1}(y) = \frac{1}{2}(y+1)$ , což snadno potvrdíme podle definice:

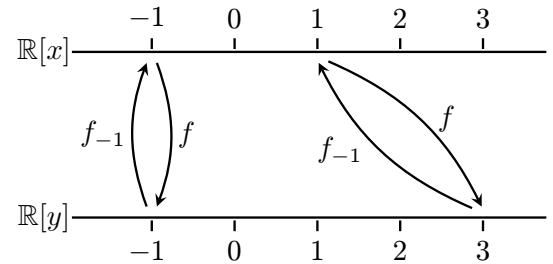
$$x \in \mathbb{R} \implies f_{-1}(f(x)) = \frac{1}{2}(f(x) + 1) = \frac{1}{2}((2x - 1) + 1) = x,$$

$$y \in \mathbb{R} \implies f(f_{-1}(y)) = 2f_{-1}(y) - 1 = 2 \frac{1}{2}(y + 1) - 1 = y.$$

Potvrzeno, funkce  $f_{-1}$  je inverzní funkcí k  $f$ .

Na mnohých středních školách se studenti učí přejít u inverzní funkce zase k proměnné  $x$ , tedy psali by  $f_{-1}(x) = \frac{1}{2}(x+1)$ . Často je to přímo součástí algoritmu, který je prezentován coby „Napište rovnost  $f(x) = y$ , prohoďte proměnné a výslednou rovnici vyřešte pro  $y$ .“

Není to dobrý nápad. Nejenže to není vůbec třeba, ono to dokonce vysílá špatný vzkaz. My totiž pracujeme s dvěma kopiemi množiny reálných čísel, v jedné máme prvky  $x$  a v druhé  $y$ .



Jak vidíme, funkce  $f_{-1}$  vůbec neumí s prvky  $x$  pracovat, protože má jako výchozí množinu úplně jiný svět. Nemá tedy smysl jí tyto proměnné podsouvat, naopak zachováním  $y$  čtenáři jasně sdělujeme, odkud a kam tato funkce jde. Rozdíl se ještě zvýrazní v aplikacích, kdy mají jednotlivé proměnné svůj význam. Jestliže  $x$  značí třeba čas a  $y$  pozici a funkce  $f$  mi říká, kde jsem byl v rozličných časech, pak zcela logicky musí inverzní zobrazení mít jako proměnnou pozici a ne čas.

**3.**  $f(x) = x^2 + 1$ . Grafem je klasická parabola obrácená nahoru a posunutá nahoru o 1, tato funkce tedy rozhodně není prostá na  $\mathbb{R}$ . Není také na coby zobrazení  $\mathbb{R} \mapsto \mathbb{R}$ , ale je na jako zobrazení  $\mathbb{R} \mapsto \langle 1, \infty \rangle$ .

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

Co kdybychom prostotu zkoumali tradičním způsobem, tedy testováním podmínky z definice? Vyšli bychom z rovnosti  $f(x_1) = f(x_2)$  neboli  $x_1^2 + 1 = x_2^2 + 1$ , odtud pak  $x_1^2 = x_2^2$ . Z tohoto ale neumíme přejít k  $x_1 = x_2$ , což ještě nemusí nic znamenat (třeba jen nejsme dost šikovní), ale je to znamení, že máme zpozornět. Pokud si dále všimneme, že z  $x_1^2 = x_2^2$  vyplývá  $x_2 = \pm x_1$ , tak nás to navede k protipříkladu proti prostotě.

Není těžké dokázat, že restrikce  $f|_{(0, \infty)}$  je již prostá a je to bijekce  $\langle 0, \infty \rangle$  na  $\langle 1, \infty \rangle$ . Proto existuje inverzní funkce, najdeme  $f_{-1}(y) = \sqrt{y-1}$ .

△

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

**Fakt 9a.10.**

Nechť  $T: A \mapsto B$  a  $S: B \mapsto C$  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  $A$  na  $C$ .

**Důkaz (poučný):** (i): Prostotu dokážeme pomocí podmínky z definice 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 tedy  $a \in A$  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.)

Alternativa: Jestliže jsou  $T$  a  $S$  bijekce, tak jsou dle věty 9a.6 invertibilní, tudíž dle věty 9a.5 je i  $S \circ T$  invertibilní, tudíž bijekce. □

Stručně řečeno, skládání nepokazí dobré vlastnosti (bude se nám to hodit dále). Jako obvykle se zeptáme, jak je to s opačným směrem: Víme-li, že  $S \circ T$  má nějakou vlastnost, musejí ji mít nutně i složky  $S$  a  $T$ ? Přechodem k obměně získáme jiný pohled na stejný problém: Může skládání vylepsit nedostatek vlastností? Podívejte se na cvičení 9a.13.

Spojením věty 9a.6 a faktu 9a.4 dostaneme následující.

**Fakt 9a.11.**

Jestliže je zobrazení  $T$  bijekce, tak  $T^{-1}$  existuje a je to také bijekce.

Bude se nám to hodit.

**9a.12 Poznámka:** Zobrazení jsme definovali pouze pro neprázdné množiny. Opravdu se musíme omezovat? Kdyby byla některá z množin  $A, B$  prázdná (popřípadě obě), tak je  $A \times B = \emptyset$ , tedy jediná možná relace je  $R = \emptyset$ . Bude to i zobrazení tak, jak jej chápeme? V případě  $A = \emptyset$  to je pravda, protože z každého (žádného) prvku  $A$  vede přesně jedna šipka. Zobrazení  $\emptyset$  tedy existuje, ale je to spíš něco jako právnická klička, prakticky to k ničemu není.

Opravdovým problémem je případ, kdy  $B = \emptyset$ , ale  $A \neq \emptyset$ . Pak jsou totiž v  $A$  prvky, pro které neexistuje v  $R = \emptyset$  přiřazení,  $R$  tedy není zobrazení. Jiná možnost není, takže zobrazení v tomto případě nelze vytvořit.

Když to shrneme, tak v případě prázdných množin máme buď zobrazení prázdné, které je k ničemu, nebo dokonce vůbec žádné neexistuje, takže to nemá smysl definovat.

△

### 9a.13 Další poznatky o skládání

Je jedno zajímavé zobrazení, které existuje pro každou množinu.

#### Definice 9a.14.

Nechť  $A$  je libovolná množina. Zobrazení  $A \mapsto A$  dané vzorcem

$$a \mapsto a \quad \text{pro } a \in A$$

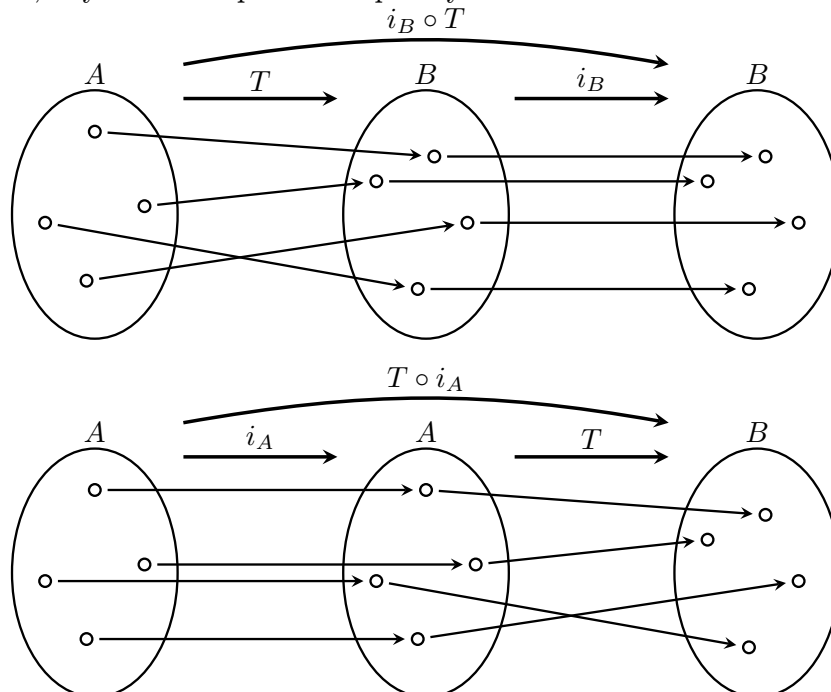
se nazývá **identita** či **identické zobrazení** na  $A$  a značí se  $i_A$ .

Máme tedy  $i_A(a) = a$ . Toto zobrazení už jsme vlastně potkali v kapitole 5b pod jménem  $\Delta(a)$ , jako relace je to množina všech dvojic typu  $(a, a)$ . Ve cvičení 9a.17 by měl čtenář hravě dokázat, že  $i_A$  je vždy invertibilní a jak vypadá inverzní zobrazení. V teorii zobrazení hraje velmi zajímavou roli.

#### Fakt 9a.15.

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  $T: A \mapsto B$  a  $i_B: B \mapsto B$ , 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.

□

Pěkně to vynikne, když si vezmeme zobrazení  $T: A \mapsto A$ , pak totiž máme  $i_A \circ T = T \circ i_A = T$ . To znamená, že zobrazení  $i_A$  se chová vůči skládání jako číslo 1 při násobení čísel. Není to jediná podobnost. Výsledek cvičení 9a.17 silně připomíná známý fakt, že  $1^{-1} = 1$ . Dokonce máme následující.

**Fakt 9a.16.**

Nechť  $T: A \mapsto B$  je zobrazení. Je invertibilní a  $S: B \mapsto A$  je jeho inverzní zobrazení právě tehdy, když  $S \circ T = i_A$  a  $T \circ S = i_B$ .

Je to snadné, podmínka  $S(T(a)) = a$  z definice se totiž dá napsat jako  $(S \circ T)(a) = i_A(a)$ , porovnáváme tedy hodnoty dvou zobrazení, a jejich definiční obory i cílové množiny souhlasí, takže první podmínka z definice inverzního zobrazení se přímo přepíše jako  $S \circ T = i_A$ . Obdobně je to i s tou druhou.

Pokud uvažujeme  $T: A \mapsto A$ , tak fakt říká, že  $T^{-1}$  se dá poznat podle splnění podmínek  $T^{-1} \circ T = i_A$  a  $T \circ T^{-1} = i_A$ , což opět velmi silně připomíná známé  $x^{-1} \cdot x = 1$  a  $xx^{-1} = 1$ . Vidíme tedy velice blízkou analogii mezi násobením a jedničkou na straně jedné a skládáním zobrazení typu  $A \mapsto A$  a zobrazením  $i_A$  na straně druhé. V obou případech také neexistuje inverzní prvek vždy. Jediný podstatnější rozdíl je v chybějící komutativitě skládání. Některé autory tato analogie inspiruje natolik, že pro zobrazení  $i_A$  používají značení  $\mathbf{1}_A$ .

Násobit umíme i více čísel než dvě. Při pohledu na obrázek znázorňující skládání zobrazení se zdá, že by neměl být problém navázat jich více za sebou, vynecháním všech prostředníků pak vznikne jedno složené zobrazení. Formálně se takováto operace pro více prvků obvykle zavádí indukcí/rekurzí (viz kapitola 8). Funguje to rozumně u operací, které splňují asociativní zákon, což jsme u skládání zobrazení potvrdili větou 9a.1, takže můžeme bez obav definovat.

**Definice.**

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

Jejich složení definujeme vzorcem

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

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  $T$  stejná jako definiční obor, jsme tedy zase u případu  $T: A \mapsto A$ . Výraz  $T \circ T \circ \dots \circ T$  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:

(0) definujeme  $T^0 = i_A$ ;

(1) pro  $n \geq 1$  definujeme  $T^{n+1} = T \circ T^n$ .

Poznamenejme, že díky faktu 9a.15 máme  $T^1 = T^{0+1} = T \circ T^0 = T \circ i_A = T$ , což dává smysl.

**Příklad 9a.p:** Ukážeme si dva jednoduché příklady.

1. Vraťme se k příkladu 9a.e se zobrazeními  $U, V$  na množině  $A = \{1, 2, 13\}$ . Pak máme následující:

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

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

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

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

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

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

2. Uvažujme zobrazení  $T: \mathbb{N} \mapsto \mathbb{N}$  dané vzorcem  $T(n) = 2n$ .

Víme, že  $T^0 = i_{\mathbb{N}}$  a  $T^1 = T$ . Dále počítáme dle indukční definice:

$$\bullet T^2(n) = (T \circ T)(n) = T(T(n)) = 2 \cdot T(n) = 2 \cdot 2n = 4n,$$

$$\bullet T^3(n) = (T \circ T^2)(n) = T(T^2(n)) = 2 \cdot T^2(n) = 2 \cdot 4n = 8n = 2^3n,$$

$$\bullet T^4(n) = (T \circ T^3)(n) = T(T^3(n)) = 2 \cdot T^3(n) = 2 \cdot 2^3n = 8n = 2^4n.$$

Tipneme si, že pro  $k \in \mathbb{N}$  platí  $T^k(n) = 2^k n$ , dokážeme snadno indukci na  $k$ .

△

Skládání více zobrazení si zachovává všechny rozumné vlastnosti probrané výše.



**Věta 9a.17.**

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

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

(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 a je rutinní, viz cvičení 5a.8. Mimochodem, ten druhý vztah vlastně známe z reálných čísel,  $\frac{1}{x^n} = \left(\frac{1}{x}\right)^n$ .

**Cvičení**

**Cvičení 9a.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 9a.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 dává maximum ze dvou reálných čísel.

**Cvičení 9a.3:** Pro následující dvojice zobrazení rozhodněte, zda jsou si rovna.

(i)  $T: \mathbb{N} \mapsto \mathbb{N}$  dáno  $T(n) = |n|$ ,  $S: \mathbb{N} \mapsto \mathbb{N}$  dáno  $S(n) = n$ ;

(ii)  $T: \mathbb{N}_0 \mapsto \mathbb{N}$  dáno  $T(n) = n + 13$ ,  $S: \mathbb{N}_0 \mapsto \mathbb{N}$  dáno  $S(n) = n + 14$ ;

(iii)  $T: \{-1, 0, 1\} \mapsto \mathbb{Z}$  dáno  $T(n) = n^2$ ,  $S: \{-1, 0, 1\} \mapsto \mathbb{Z}$  dáno  $S(n) = n^4$ ;

(iv)  $T: \mathbb{Z} \mapsto \mathbb{Z}$  dáno  $T(n) = 3n + 1$ ,  $S: \mathbb{Z} \mapsto \mathbb{Q}$  dáno  $S(n) = 3n + 1$ ;

(v)  $T: \mathbb{Z} \mapsto \mathbb{N}$  dáno  $T(n) = \cos(2\pi n)$ ,  $S: \mathbb{Z} \mapsto \mathbb{N}$  dáno  $S(n) = 1$ .

**Cvičení 9a.4:** Pro následující zobrazení  $T: \mathbb{N} \mapsto \mathbb{N}$  spočítejte  $T(1)$ ,  $T(2)$ ,  $T(3)$  a  $T(4)$ :

(i)  $T(n) = \begin{cases} n - 1, & n \geq 3; \\ n + 1, & n \leq 2; \end{cases}$

(ii)  $T(n) = \begin{cases} n, & n \text{ sudé}; \\ 2n, & n \text{ liché}; \end{cases}$

(iii)  $T(n) = \begin{cases} 1, & n = k^2 \text{ pro nějaké } k \in \mathbb{N}; \\ 0, & \text{jinde}; \end{cases}$

(iv)  $T(n) = \begin{cases} 13, & n = 1, \\ 14, & n \text{ prvočíslo}, \\ 0, & \text{jinde}. \end{cases}$

**Cvičení 9a.5:** Zobrazení  $T$  přiřazuje každému studentovi jeho studijní průměr a zobrazení  $S$  přiřazuje k jednotlivým studijním průměrům stipendia. Co je zobrazení  $S \circ T$ ?

**Cvičení 9a.6** (rutinní, poučné): Pro následující dvojice funkcí  $f, g: \mathbb{R} \mapsto \mathbb{R}$  najděte  $g \circ f$  a  $f \circ g$ :

(i)  $f(x) = \sin(x)$ ,  $g(x) = \pi x$ ;

(v)  $f(x) = x^3 - 1$ ,  $g(x) = \sqrt[3]{x+1}$ ;

(ii)  $f(x) = x$ ,  $g(x) = e^x$ ;

(vi)  $f(x) = e^x$ ,  $g(x) = \ln(|x|)$  pro  $x \neq 0$  a  $g(0) = 0$ ;

(iii)  $f(x) = x^2$ ,  $g(x) = 13$ ;

(vii)  $f(x) = 1 - x$ ,  $g(x) = 1 - x$ ;

(iv)  $f(x) = 1 + x^2$ ,  $g(x) = 1 + x^2$ ;

(viii)  $f(x) = 1 + x$ ,  $g(x) = 1 + x$ .

**Cvičení 9a.7** (poučné): Pro následující dvojice funkcí  $f, g: \mathbb{Z} \mapsto \mathbb{Z}$  rozhodněte, zda číslo 13 leží v oboru hodnot složené funkce  $g \circ f$ :

(i)  $f(x) = x^2 + 2$ ,  $g(x) = 2x + 1$ ;

(iii)  $f(x) = x^3 + 4$ ,  $g(x) = 2x - 11$ ;

(ii)  $f(x) = x^3 - 1$ ,  $g(x) = 13x$ ;

(iv)  $f(x) = 4x$ ,  $g(x) = x - 1$ .

**Cvičení 9a.8** (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 9a.9** (rutinní, \*dobré): Jsou následující funkce prosté a na? Svou odpověď dokažte.

- |  |  |
|--|--|
| (i) $f(n) = n + 1$ ze $\mathbb{Z}$ do $\mathbb{Z}$ ;                                   | (x) $f(n) = (n + 1, 2n)$ z $\mathbb{N}$ do $\mathbb{N} \times \mathbb{N}$ ;                            |
| (ii) $f(n) = n + 1$ z $\mathbb{N}$ do $\mathbb{N}$ ;                                   | (xi) $f(n) = (n^2, n^2 + 2n)$ ze $\mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$ ;                      |
| (iii) $f(n) = 13n$ ze $\mathbb{Z}$ do $\mathbb{Z}$ ;                                   | (xii) $f(m, n) = (m^2, mn)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$ ;      |
| (iv) $f(x) = 13x$ z $\mathbb{Q}$ do $\mathbb{Q}$ ;                                     | (xiii) $f(x, y) = (x + y, x - y)$ z $\mathbb{Q} \times \mathbb{Q}$ do $\mathbb{Q} \times \mathbb{Q}$ ; |
| (v) $f(n) = n^3$ ze $\mathbb{Z}$ do $\mathbb{Z}$ ;                                     | (xiv) $f(m, n) = (m + n, m - n)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$ ; |
| (vi) $f(x) = x^3$ z $\mathbb{R}$ do $\mathbb{R}$ ;                                     | (xv) $f(m, n) = 2m - n$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$ ;                            |
| (vii) $f(n) = \lfloor \frac{n}{2} \rfloor$ ze $\mathbb{Z}$ do $\mathbb{Z}$ ;           | (xvi)* $f(m, n) = m^2 - n^2$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$ ;                       |
| (viii) $f(n) = (-1)^n n$ z $\mathbb{N}_0$ do $\mathbb{Z}$ ;                            | (xvii) $f(m, n) = m + n + 13$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$ ;                      |
| (ix)* $f(n) = (-1)^n \lfloor \frac{n+1}{2} \rfloor$ z $\mathbb{N}_0$ do $\mathbb{Z}$ ; | (xviii) $f(m, n) = m - n$ z $\mathbb{N} \times \mathbb{N}$ do $\mathbb{Z}$ .                           |

**Cvičení 9a.10** (poučné): (i) Uvažujte následující předpis:  $T(p, q) = \frac{p}{q}$ . Dostáváme tak bijekci ze  $\mathbb{Z} \times \mathbb{N}$  na  $\mathbb{Q}$ ?  
(ii) Uvažujte následující předpis:  $T(\frac{p}{q}) = (p, q)$ . Dostáváme tak bijekci z  $\mathbb{Q}$  na  $\mathbb{Z} \times \mathbb{N}$ ?

**Cvičení 9a.11** (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 9a.12** (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  $\mathbb{N}$ .

Nápověda: Pokud vám to nejde jedním vzorcem, zkuste zobrazení definované po částech.

**Cvičení 9a.13** (poučné, dobré): Nechť  $T: A \mapsto B$  a  $S: B \mapsto C$  jsou zobrazení. Rozhodněte, zda následující implikace platí, ty pravdivé dokažte, ty nepravdivé vyvráťte protipříkladem.

U všech implikací napište i její obměnu, může vám pomoci s rozhodováním, zda dotyčné tvrzení platí nebo neplatí.

- |   |   |
|---|---|
| (i) Jestliže $T$ není prosté, tak $S \circ T$ není prosté.  | (iv) Jestliže $S$ není na, tak $S \circ T$ není na.           |
| (ii) Jestliže $S$ není prosté, tak $S \circ T$ není prosté. | (v) Jestliže $T$ není bijekce, tak $S \circ T$ není bijekce.  |
| (iii) Jestliže $T$ není na, tak $S \circ T$ není na.        | (vi) Jestliže $S$ není bijekce, tak $S \circ T$ není bijekce. |

**Cvičení 9a.14** (poučné): Nechť  $T: A \mapsto B$  je prosté zobrazení. Dokažte, že pro libovolnou podmnožinu  $M$  množiny  $A$  je  $T|_M$  prosté zobrazení.

**Cvičení 9a.15** (poučné, \*dobré): Pro následující zobrazení odhadněte vzorec pro mocninu  $T^k$ .

- |  |   |
|--|---|
| (i) $T: \mathbb{N} \mapsto \mathbb{N}, T(n) = n + 1$ ; | (iii) $T: \mathbb{Z} \mapsto \mathbb{Z}, T(n) = 1 - n$ ;          |
| (ii) $T: \mathbb{N} \mapsto \mathbb{N}, T(n) = n^2$ ;  | (iv)* $T: \mathbb{N} \mapsto \mathbb{N}, T(n) = \max(1, n - 1)$ . |

Nápověda: Zejména u (iv) pomohou šipkové obrázky.

**Cvičení 9a.16** (poučné, \*dobré): Nechť  $T: A \mapsto B$  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 9a.17** (poučné): Dokažte, že pro každou množinu  $A$  je zobrazení  $i_A$  bijekce a tedy invertibilní a najděte  $i_A^{-1}$ .

**Cvičení 9a.18** (poučné): Připomeňte si alternativní charakterizaci inverzního zobrazení pomocí  $i_A$  a  $i_B$ . Použijte tento přístup a vlastnosti  $i_A$  k důkazu, že  $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$ .

**Cvičení 9a.19** (poučné, dobré): Uvažujte zobrazení  $T: A \mapsto B$ . Dokažte následující tvrzení:

- (i) Jestliže je  $T$  invertibilní, pak pro každou podmnožinu  $M \subseteq A$  platí  $T^{-1}[T[M]] = M$  a pro každou podmnožinu  $N \subseteq B$  platí  $T[T^{-1}[N]] = N$ .
- (ii)  $T$  je bijekce/invertibilní právě tehdy, pokud existuje zobrazení  $S: B \mapsto A$  takové, že pro každou podmnožinu  $M \subseteq A$  platí  $S[T[M]] = M$  a pro každou podmnožinu  $N \subseteq B$  platí  $T[S[N]] = N$ .

Vidíme, že ke „krácení“  $T$  a  $T^{-1}$  dochází i při zobrazování množin a dalo by se to použít jako alternativní definice inverzního zobrazení.

**Cvičení 9a.20** (poučné, dobré): Uvažujme množiny  $A, B$  a zobrazení  $T: A \mapsto B$  a  $S: A \mapsto B$ . Připomeňme, že formálně jde o množiny dvojic z  $A \times B$ .

Rozmyslete si, za jakých okolností by  $R \cap S$ ,  $R \cup S$  a  $R \setminus S$  zase byly zobrazeními.

**Cvičení 9a.21** (poučné, dobré): Uvažujme reálnou funkci  $f$  definovanou na  $\mathbb{R}$ , podívejme se na ni jako na relaci, tedy množinu jistých dvojic čísel  $(x, f(x)) \in \mathbb{R} \times \mathbb{R}$ .

Jestliže se dozvíme, že coby relace je funkce  $f$  reflexivní, co nám to o ní říká? (Nápověda: Zde existuje velice jednoduchá odpověď.)

Jestliže se dozvíme, že coby relace je funkce  $f$  symetrická, co nám to o ní říká? Toto ještě není otázka, ale návod k zamyšlení. Otázka: Umíte najít příklad funkce, která je coby relace symetrická? Umíte najít ještě jiný příklad?

**Cvičení 9a.22** (poučné, dobré): Necht  $U$  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  $M, N \subseteq U$ :  $\chi_{M \cup N} = \chi_M + \chi_N - \chi_{M \cap N}$ .

### Řešení:

**9a.1:** (i): ano. (ii): Co když je  $r$  prázdný, co když neobsahuje 0?

**9a.2:** (i):  $D(T) = \mathbb{N}_0$ ,  $\text{ran}(T) = \{0, 1, 2, \dots, 8, 9\}$ . (ii):  $D(T) = \mathbb{N}$ ,  $\text{ran}(T) = \{2, 3, 4, \dots\} = \mathbb{N} - \{1\}$ . (iii):  $D(T)$  je množina konečných binárních řetězců,  $\text{ran}(T) = \mathbb{N}_0$ . (iv):  $D(T)$  je množina konečných binárních řetězců,  $\text{ran}(T) = \mathbb{N}_0$ . (v):  $D(T)$  je množina konečných binárních řetězců,  $\text{ran}(T) = \mathbb{Z}$ . (vi):  $D(T) = \mathbb{R} \times \mathbb{R}$ ,  $\text{ran}(T) = \mathbb{R}$ .

**9a.3:** (i)  $T = S$ : Množiny souhlasí. Pro  $n \in \mathbb{N}$  je  $n \geq 0$ , proto  $T(n) = |n| = n = S(n)$ . (ii):  $T \neq S$ : Například  $T(1) = 14$ ,  $S(1) = 15$ . (iii):  $T = S$ : Množiny souhlasí. Pro  $n = 0$  je  $T(0) = 0^2 = 0 = 0^4 = S(0)$ , pro  $n = \pm 1$  je  $T(\pm 1) = (\pm 1)^2 = 1 = (\pm 1)^4 = S(\pm 1)$ . (iv):  $T \neq S$ : Nesouhlasí cílové množiny. (v):  $T = S$ : Množiny souhlasí. Pro  $n \in \mathbb{Z}$  je  $T(n) = \cos(2\pi n) = 1 = S(n)$ .

**9a.4:** (i)  $T(1) = 2$ ,  $T(2) = 3$ ,  $T(3) = 2$  a  $T(4) = 3$ . (ii)  $T(1) = 2$ ,  $T(2) = 2$ ,  $T(3) = 6$  a  $T(4) = 4$ . (iii)  $T(1) = 1$ ,  $T(2) = 0$ ,  $T(3) = 0$  a  $T(4) = 1$ . (iv)  $T(1) = 13$ ,  $T(2) = 14$ ,  $T(3) = 14$  a  $T(4) = 0$ .

**9a.5:** Přirazuje studentovi jeho stipendium.

**9a.6:** (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):  $(g \circ f)(x) = g(f(x)) = x + 2$ ,  $(f \circ g)(x) = f(g(x)) = x + 2 = f^2(x)$ .

**9a.7:** Hledáme  $x \in \mathbb{Z}$  tak, aby  $x \xrightarrow{f} y \xrightarrow{g} 13$ . 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  $13 \in \text{ran}(g \circ f)$ .

(ii):  $13y = 13 \implies y = 1$ ,  $x^3 - 1 = 1 \implies x^3 = 2$  nemá řešení v  $\mathbb{Z}$ . Proto  $13 \notin \text{ran}(g \circ f)$ .

(iii):  $2y - 11 = 13 \implies y = 12$ ,  $x^3 + 4 = 12 \implies x = 2$ . Ano,  $g(f)(2) = 13$ , proto  $13 \in \text{ran}(g \circ f)$ .

(iv):  $y - 1 = 13 \implies y = 14$ ,  $4x = 14$  nemá řešení v  $\mathbb{Z}$ . Proto  $13 \notin \text{ran}(g \circ f)$ .

**9a.8:** Musí platit  $ad + b = bc + d$  neboli  $b(c - 1) = d(a - 1)$ .

**9a.9:** (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  $1 \notin \text{ran}(T)$ .

(iii): Je prosté:  $T(x) = T(y) \implies 13x = 13y \implies x = y$ . Není na: neexistuje  $x \in \mathbb{Z}$  aby  $13x = 23$ , proto  $23 \notin \text{ran}(T)$ .

(iv): Je prosté:  $T(x) = T(y) \implies 13x = 13y \implies x = y$ . Je na:  $y \in \mathbb{Q} \implies \exists x = \frac{1}{13}y \in \mathbb{Q}$ :  $T(x) = T(\frac{y}{13}) = 13 \cdot \frac{y}{13} = y$ .

(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  $2 \notin \text{ran}(T)$ .

(vi): Je prosté:  $T(x) = T(y) \implies x^3 = y^3 \implies x = y$ . Je na:  $y \in \mathbb{R} \implies \exists x = \sqrt[3]{y} \in \mathbb{R}$ :  $T(x) = T(\sqrt[3]{y}) = (\sqrt[3]{y})^3 = y$ .

- (vii): Není prosté, třeba  $T(2) = T(3)$ . Je na:  $y \in \mathbb{Z} \implies \exists x = 2y \in \mathbb{Z}: T(x) = T(2y) = \lfloor y \rfloor = y$ .  
 (viii): 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  $1 \notin \text{ran}(T)$ .  
 (ix): 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  $\lfloor \frac{x+1}{2} \rfloor = \lfloor \frac{y+1}{2} \rfloor$ , tedy  $\lfloor \frac{x+1}{2} \rfloor = \lfloor \frac{x+1}{2} + k \rfloor = k + \lfloor \frac{x+1}{2} \rfloor$ , 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  $T(x) = 1 \cdot \lfloor y + \frac{1}{2} \rfloor = y + \lfloor \frac{1}{2} \rfloor = y$ .

Pokud  $y < 0$ , pak  $-2y \geq 2$  a existuje  $x = -2y - 1 \in \mathbb{N}_0$  takové, že  $T(x) = (-1) \cdot \lfloor -y \rfloor = y$ .

(x): 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  $(1, 1) \notin \text{ran}(T)$ .

(xi): 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  $(0, 1) \notin \text{ran}(T)$ .

(xii): 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  $(0, 1) \notin \text{ran}(T)$ .

(xiii): 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  $T(x, y) = (u, v)$ .

(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  $(x, y) = (u, v)$ .

Není na: Soustava  $x+y = 1, x-y = 0$  nemá řešení v  $\mathbb{Z}$ , proto  $(1, 0) \notin \text{ran}(T)$ .

(xv): Není prosté, třeba  $T(1, 2) = 0 = T(0, 0)$ . Je na:  $z \in \mathbb{Z} \implies \exists x = 0, y = -z \in \mathbb{Z}: T(x, y) = z$ .

(xvi): Není prosté, třeba  $T(1, 1) = 0 = T(0, 0)$ . Na: Zkusíme třeba  $2 \in \mathbb{Z}$ . Existují celá čísla  $m, n$  tak, aby  $m^2 - n^2 = 2$ ? Kupodivu ne. Omezíme se na nezáporná  $m, n$ . Aby vyšel výsledek kladný, musí být  $m > n$ . Dvě možnosti.  $m = n+1$  dává  $m^2 - n^2 = 2n+1$ , to nikdy nebude 2. Pro  $m \geq n+2$  zase  $m^2 - n^2 \geq 4n+4 > 2$ . Takže  $2 \notin \text{ran}(T)$  a  $T$  není na.

(xvii): 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  $T(x, y) = z$ .

(xviii): Není prosté, třeba  $T(1, 1) = 0 = T(2, 2)$ . Je na: Nechť  $z \in \mathbb{Z}$ . Pokud  $z = 0$ , volíme  $x = 1, y = 1$ . Pokud  $z > 0$ , volíme  $x = z+1, y = 1 \in \mathbb{N}$  a  $T(x, y) = z$ . Pokud  $z < 0$ , volíme  $x = 1, y = -z+1 \in \mathbb{N}$  a  $T(x, y) = z$ .

**9a.10:** (i): Je evidentně na, ale není prosté  $T(2, 4) = \frac{2}{4} = \frac{1}{2} = T(1, 2)$ . Takže není bijekce.

(ii): Toto vůbec není zobrazení! Máme  $0.5 \in \mathbb{Q}$ , ale nevíme, jestli  $T(0.5) = T(\frac{1}{2}) = (1, 2)$  nebo  $T(0.5) = T(\frac{3}{6}) = (3, 6)$  nebo ...

**9a.11:** Není prosté, protože  $T(1) = 4 = T(8)$ . Je na, pro  $y \in \mathbb{N}$  existuje  $x = 2y \in \mathbb{N}$  takové, že  $T(x) = y$ .

**9a.12:**  $\mathbb{N} \mapsto \mathbb{N}: T(n) = n$  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.

$\mathbb{Z} \mapsto \mathbb{N}: T(n) = \begin{cases} 2n+1; & n \geq 0; \\ -2n; & n < 0 \end{cases}$  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.

**9a.13:** 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.

**9a.14:** Nechť  $x, y \in M$  splňují  $T|_M(x) = T|_M(y)$ . Podle definice restrikce tedy  $T(x) = T(y)$  a  $x, y \in A$ , proto dle prostoty  $T$  platí  $x = y$ .

**9a.15:** (i):  $T^2(n) = T(n+1) = (n+1) + 1 = n+2, T^3(n) = T(n+2) = (n+1) + 1 = n+3, T^k(n) = n+k$ . (ii):  $T^2(n) = T(n^2) = (n^2)^2 = n^4, T^3(n) = T(n^4) = (n^4)^2 = n^8, T^k(n) = n^{2^k}$ . (iii):  $T^2(n) = T(1-n) = 1 - (1-n) = n, T^3(n) = T(n) = 1-n, T^4(n) = T(1-n) = 1 - (1-n) = n, T^k(n) = 1-n$  pro  $k$  liché,  $T^k(n) = n$  pro  $k$  sudé.

(iii):  $T(1) = 1$  a  $T(n) = n-1$  pro  $n \geq 2; T^2(1) = T(1) = 1, T^2(2) = T(1) = 1$  a  $T^2(n) = T(n-1) = n-2$  pro  $n \geq 3$  neboli  $T^2(n) = \max(1, n-2); T^3(1) = T(1) = 1, T^3(2) = T(1) = 1, T^3(3) = T(1) = 1$  a  $T^3(n) = T(n-2) = n-3$  pro  $n \geq 4$  neboli  $T^3(n) = \max(1, n-3); T^k(n) = \max(1, n-k)$  neboli  $T^k(n) = 1$  pro  $n \leq k$  a  $T^k(n) = n-k$  pro  $n > k$ .

**9a.16:** (i):  $y \in T[M \cup N] \implies \exists x \in M \cup N: T(x) = y$ . Dvě možnosti.  $x \in M \implies T(x) \in T[M] \implies y = T(x) \in T[M] \cup T[N]$ . Nebo  $x \in N \implies T(x) \in T[N] \implies y = T(x) \in T[M] \cup T[N]$ .

Naopak:  $y \in T[M] \cup T[N]$ , dvě možnosti.  $y \in T[M] \implies \exists x \in M: T(x) = y$ . Pak  $x \in M \cup N$  a tedy  $y = T(x) \in T[M \cup N]$ .

(ii):  $y \in T[M \cap N] \implies \exists x \in M \cap N: T(x) = y$ . Pak  $x \in M$ , tedy  $y = T(x) \in T[M]$ , také  $x \in N$ , tedy  $y = T(x) \in T[N]$ . Proto  $y \in T[M] \cap T[N]$ .

(iii):  $y \in T[M] \cap T[N] \iff y \in T[M] \wedge y \in T[N] \iff (\exists x_1 \in M: T(x_1) = y) \wedge (\exists x_2 \in N: T(x_2) = y)$ . 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):  $A = \{1, 2, 3\}$ ,  $B = \{a, b\}$ ,  $M = \{1, 2\}$ ,  $N = \{2, 3\}$ ,  $T(2) = b$ ,  $T(1) = T(3) = a$ .

**9a.17:** Prosté:  $i_A(x) = i_A(y) \implies x = y$ . Na: Dáno  $b \in A$ , pak pro  $a = b \in A$  platí  $i_A(a) = a = b$ . Platí  $i_A^{-1} = i_A$ : Pro  $a \in A$  je  $i_A(i_A(a)) = i_A(a) = a$ .

**9a.18:**  $(T^{-1} \circ S^{-1}) \circ (S \circ T) = ((T^{-1} \circ S^{-1}) \circ S) \circ T = (T^{-1} \circ (S^{-1} \circ S)) \circ T = (T^{-1} \circ i_B) \circ T = T^{-1} \circ T = i_A$ ,  
 $(S \circ T) \circ (T^{-1} \circ S^{-1}) = ((S \circ T) \circ T^{-1}) \circ S^{-1} = (S \circ (T \circ T^{-1})) \circ S^{-1} = (S \circ i_B) \circ S^{-1} = S \circ S^{-1} = i_C$ .

**9a.19:** (i) Nechť  $a \in A$ . Pak  $T(a) \in T[M]$  a tedy  $T^{-1}(T(a)) \in T^{-1}[T[M]]$ . Ovšem  $T^{-1}(T(a)) = a$ , takže  $a \in T^{-1}[T[M]]$ . Ukázali jsme, že  $M \subseteq T^{-1}[T[M]]$ . Ještě naopak.

Nechť  $a \in T^{-1}[T[M]]$ . Pak existuje  $b \in T[M]$  takové, že  $T^{-1}(b) = a$  (zde se na ten výraz díváme jako na  $T^{-1}[B]$ ). Protože  $b \in T[M]$ , musí existovat  $\tilde{a} \in M$  takové, že  $T(\tilde{a}) = b$ . Ovšem jestliže  $T^{-1}(b) = a$ , pak také  $T(a) = b$ . Protože je  $T$  prosté, nutně  $\tilde{a} = a$ , tedy  $a \in M$ . Opravdu  $T^{-1}[T[M]] \subseteq M$ .

Druhé tvrzení již stručněji:  $b \in N \implies T^{-1}(b) \in T^{-1}[N] \implies b = T(T^{-1}(b)) \in T[T^{-1}[N]]$ .  $b \in T[T^{-1}[N]] \implies \exists a \in T^{-1}[N]$  aby  $T(a) = b$ . Pak  $\exists \tilde{b} \in N$  aby  $T^{-1}(\tilde{b}) = a$ , tedy  $T(a) = \tilde{b}$ . Pak  $b = T(a) = \tilde{b} \in N$ .

(ii)  $\implies$ : je-li  $T$  invertibilní, pak podle (i) splňuje  $S = T^{-1}$  podmínku.

$\Leftarrow$ . Aplikujeme-li podmínku na  $M = \{a\}$  pro  $a \in A$  a  $N = \{b\}$  pro  $b \in N$ , dostaneme přesně podmínku z definice, podle které  $S = T^{-1}$ .

**9a.20:** Aby byla relace zobrazením, musí mít každé  $a \in A$  přesně jednu dvojici.

$R \cap S$ : Pro každé  $a \in A$  chceme nějaké  $(a, b) \in R \cap S$ , musí tedy být v  $R$  i  $S$ . A protože jsou  $R, S$  zobrazení, jiné dvojice s  $a$  už v nich být nemohou. Závěr:  $R \cap S$  je zobrazením přesně tehdy, když  $R = S$ .

$R \cup S$ : Nechť  $a \in A$ . Protože v zobrazení nesmí být více dvojic s  $a$  a každé z  $R, S$  přidá tu svou, pak nutně musí jít o tutéž dvojici. Závěr:  $R \cup S$  je zobrazením přesně tehdy, když  $R = S$ .

$R \setminus S$ : Žádná z dvojic v  $R$  nesmí být odebrána, tedy zobrazení vznikne tehdy, když  $S$  nemá shodné dvojice s  $R$ . Závěr:  $R \setminus S$  je zobrazením přesně tehdy, když  $S(a) \neq R(a)$  pro všechna  $a \in A$ .

Společný závěr: Množinové operace vedou na zobrazení jedině v případech, kdy pak je výsledkem zase  $R$ , takže to nemá smysl dělat.

**9a.21:** R: Pro každé  $x \in \mathbb{R}$  musí platit  $(x, x) \in f$ , tedy funkce  $f$  musí posílat každé  $x$  zase na  $x$ . Přeloženo do řeči funkcí, je to lineární funkce  $f(x) = x$ . Žádná jiná funkce na  $\mathbb{R}$  nemůže být reflexivní.

S: Pro každou dvojici  $(x, y) \in f$  by také mělo platit  $(y, x) \in f$ . Přeložíme do řeči funkcí: Pokud máme  $f(x) = y$  neboli dvojici  $(x, y)$ , tak by v  $f$  měla být také dvojice  $(y, x)$  neboli by mělo platit, že  $f(y) = x$ . Ovšem také  $f_{-1}(y) = x$ , tedy  $f(y) = f_{-1}(y)$ .

Závěr: funkce je jako relace symetrická, pokud je sama sobě inverzní.

Jaké jsou to funkce? Takové, jejichž grafy jsou symetrické vzhledem k hlavní diagonále  $y = x$ . Nakreslit si jich můžeme nekonečně mnoho, úloha má tedy nekonečně mnoho řešení. Otázka se ovšem stane značně zajímavější v okamžiku, kdy budeme chtít funkce zadané (pokud možno jednodušším) vzorcem.

Příklady: Určitě tak bude fungovat funkce  $f(x) = x$  neboli  $x \mapsto x$ , která se sestává coby relace z dvojic  $(x, x)$ , ty jsou symetrické.

Další zajímavý příklad:  $f(x) = -x$ . Obsahuje dvojice typu  $(x, -x)$ , ke každé z nich také symetrickou dvojici  $(-x, x) = (-x, -(-x))$ . Ukažte, že obecně platí, že pro každou volbu parametru  $c$  splní funkce  $f(x) = c - x$  podmínku.

Napadá mě ještě zajímavá funkce  $f(x) = \frac{1}{x}$ , ale ta nepatří do této otázky, protože jsme chtěli funkci definovanou na  $\mathbb{R}$ , zatímco tato je definována jen na  $\mathbb{R} - \{0\}$ . Ze stejného důvodu vyloučíme  $f(x) = \frac{x-13}{x-1}$ . Jsou to ale funkce, které jsou samy sobě inverzní, což je zajímavé.

Bonus: Dobrá otázka je, které z funkcí ve tvaru  $f(x) = \frac{ax+b}{cx+d}$  splňují  $f^{-1} = f$ . Pečlivá analýza vede nakonec na podmínku  $a = -d$ , tedy funkce typu  $f(x) = \frac{ax+b}{cx-a}$ . Všimněte si, že tento typ zahrnuje všechny příklady výše.

**9a.22:** (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 nebylo 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  $\chi_X$  může být jen 0 nebo 1.

(iii): Důkaz se nejlépe dělá rozbořem 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.

## 9b. Zobrazení a konečné množiny

V této kapitole dokážeme věci o konečných množinách, které čtenáře jistě nepřekvapí. Nové ale pro něj mohou být postupy, které se při tom objeví.

Pokud jste si zkoušeli kreslit jednoduchá zobrazení na konečných množinách a přemýšleli o jejich prostotě a surjektivitě, určitě vás napadlo, že tyto vlastnosti mohou být předurčeny počtem prvků v množině. Například pokud má cílová množina méně prvků než definiční obor, tak těžko budeme hledat pro každou šipku jediněčný cílový prvek, tedy nedokážeme splnit podmínku prostoty. Nejprve si tyto představy potvrdíme pro množiny, se kterými se dobře pracuje.

- V této kapitole budeme pro  $n \in \mathbb{N}$  symbolem  $\{1, \dots, n\}$  značit množinu  $\{k \in \mathbb{N} : k \leq n\}$ . Děláme tedy výjimku z pravidla, že tři tečky nejsou pořádná definice množiny.

V následujícím lemma dokážeme několik faktů, které budou základním stavebním kamenem pro další úvahy a argumenty. Důkaz je delší, ale objeví se v něm typické postupy a nápady, ze kterých budeme těžit ve zbytku kapitoly. Obzvláště poučné je, že většinou jde o jednoduchý nápad, který lze snadno nakreslit na papír (proto také budeme často ukazovat obrázky a doporučujeme čtenáři, aby si další kreslil sám), je však jej třeba správně zachytit matematicky a ověřit, že to, co funguje na obrázku, je platné i obecně. Pokud se vám nechce studovat celý důkaz, zkuste se alespoň podívat právě na tuto mezihru mezi obrázky a myšlenkami na straně jedné a jejich matematickým zápisem na straně druhé.

### Lemma 9b.1.

Nechť  $m, n \in \mathbb{N}$ . Uvažujme libovolné zobrazení  $T: \{1, \dots, n\} \mapsto \{1, \dots, m\}$ .

- (i) Jestliže je  $T$  prosté, tak  $m \geq n$ .
- (ii) Jestliže  $m < n$ , tak  $T$  nemůže být prosté.
- (iii) Jestliže je  $T$  na, tak  $m \leq n$ .
- (iv) Jestliže  $m > n$ , tak  $T$  nemůže být na.
- (v) Jestliže je  $T$  bijekce, tak  $m = n$ .
- (vi) Jestliže  $m \neq n$ , pak  $T$  nemůže být bijekce.

Všimneme si, že sudá tvrzení jsou obměnami lichých tvrzení, takže stačí dokázat ta lichá. Tvrzení (v) pak je přímým důsledkem definice bijekce a částí (i) a (iii). Máme tedy dvě třetiny důkazu za sebou, zbývá dokázat (i) a (iii).

**Důkaz** (z povinnosti, možná poučný):

(i): Matematickou indukcí dokážeme, že pro všechna  $n \in \mathbb{N}$  platí vlastnost

- $V(n)$ : Jestliže  $m \in \mathbb{N}$  a  $T$  je prosté zobrazení  $\{1, \dots, n\} \mapsto \{1, \dots, m\}$ , pak  $m \geq n$ .

(0)  $n = 1$ : Mějme nějaké zobrazení  $T: \{1\} \mapsto \{1, \dots, m\}$ . Protože  $m \in \mathbb{N}$ , platí  $m \geq 1 = n$ .

(1) Nechť  $n \in \mathbb{N}$ , předpokládejme, že platí  $V(n)$ . Dokážeme, že platí  $V(n+1)$ .

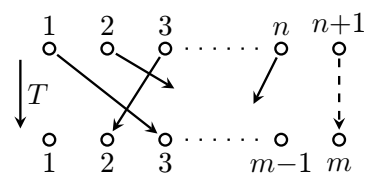
Vezměme tedy nějaké prosté zobrazení  $T: \{1, \dots, n+1\} \mapsto \{1, \dots, m\}$ , kde  $m \in \mathbb{N}$ . Chceme využít  $V(n)$  s velikostí cílové množiny  $m-1$ , takže potřebujeme pomocí  $T$  vyrobit nějaké prosté zobrazení z  $\{1, \dots, n\}$  do  $\{1, \dots, m-1\}$ .

Aby šlo  $V(n)$  vůbec aplikovat, musíme mít  $m-1 \in \mathbb{N}$ . Určitě  $m-1 \in \mathbb{Z}$ . Protože  $n+1 \geq 2$ , obsahuje  $\{1, \dots, n+1\}$  čísla  $1 \neq 2$ , takže díky prostotě  $T$  musí množina  $\{1, \dots, m\}$  obsahovat  $T(1) \neq T(2)$  a tedy  $m \geq 2$  neboli  $m-1 \geq 1$ . Opravdu  $m-1 \in \mathbb{N}$ .

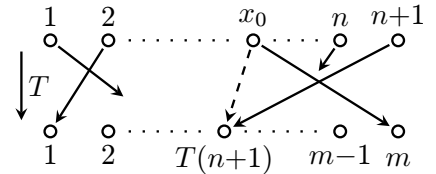
Nyní rozebereme tři možnosti.

1) Může se stát, že  $T(n+1) = m$ . Pak lze příslušnou šipku prostě vynechat. Provedeme to matematicky. Díky prostotě  $T$  pro  $x \in \{1, \dots, n\}$  nutně platí  $T(x) \neq m$ , restrikce  $S = T|_{\{1, \dots, n\}}$  je tedy zobrazení z  $\{1, \dots, n\}$  do  $\{1, \dots, m-1\}$ , které je prosté (viz cvičení 9a.14). Protože také  $m-1 \in \mathbb{N}$ , jsou splněny všechny předpoklady, které jsou pro zobrazení  $S$  vyžadovány vlastností  $V(n)$ . Podle tohoto indukčního předpokladu pak  $m-1 \geq n$ , tedy  $m \geq n+1$  a  $V(n+1)$  platí.

2) Druhá možnost je, že  $T(n+1) < m$  a neexistuje  $x \in \{1, \dots, n\}$  takové, že  $T(x) = m$ . Pak je  $T$  vlastně zobrazení do množiny  $\{1, \dots, m-1\}$ , toto musí platit i pro restrikci  $S = T|_{\{1, \dots, n\}}$ . Můžeme tedy zopakovat argument z případu 1).



3) Zbývá možnost, že  $T(n+1) < m$ , ale existuje  $x_0 \in \{1, \dots, n\}$  takové, že  $T(x_0) = m$ . Protože je  $T$  prosté, je pak  $x_0$  nutně jediné, které toto splňuje. V tomto případě restrikce na  $\{1, \dots, n\}$  nevede do  $\{1, \dots, m-1\}$ . Nápad: V obrázku vygumujeme šipku vedoucí z  $n+1$  do  $T(n+1)$ , čímž se toto číslo uvolní (díky prostotě  $T$  tam žádná jiná šipka nesmí vést). Můžeme tam tedy přesměrovat šipku vedoucí z  $x_0$ , aniž bychom zkazili prostotu. Teď je potřeba to udělat formálně, ať máme jistotu, že jsou naše úvahy správné.



Uvažujme zobrazení

$$S(x) = \begin{cases} T(x), & x \in \{1, \dots, n\} \setminus \{x_0\}; \\ T(n+1), & x = x_0. \end{cases}$$

Tvrdíme, že je to prosté zobrazení z  $\{1, \dots, n\}$  do  $\{1, \dots, m-1\}$ .

Nejprve ověříme, že to vůbec má smysl. Zobrazení  $S$  je zjevně definováno pro všechna čísla z  $\{1, \dots, n\}$ . Dále si všimneme, že díky prostotě  $T$  a  $T(x_0) = m$  musí platit, že pro  $x \in \{1, \dots, n\} \setminus \{x_0\}$  je  $S(x) = T(x) \neq m$  neboli  $S(x) \leq m-1$ , stejně tak  $S(x_0) = T(n+1) \leq m-1$ , takže hodnoty  $S$  opravdu leží v množině  $\{1, \dots, m-1\}$ .

Prosté: Tentokrát použijeme obměnu podmínky a definice. Vezměme  $x, y \in \{1, \dots, n\}$  splňující  $x \neq y$ . Pokud není ani jedno z  $x, y$  rovno  $x_0$ , pak  $S(x) = T(x)$  a  $S(y) = T(y)$ . Z prostoty  $T$  pak díky  $x \neq y$  dostaneme  $T(x) \neq T(y)$  neboli  $S(x) \neq S(y)$ .

Druhá možnost je, že právě jedno (nejsou si rovny) z  $x$  nebo  $y$  je  $x_0$ , ze symetrie si stačí zvolit jeden případ, třeba  $y = x_0$ . Pak  $S(y) = S(x_0) = T(n+1)$ . Protože  $x \neq x_0$ , je  $S(x) = T(x)$ , díky  $x \neq n+1$  a prostotě  $T$  pak  $T(x) \neq T(n+1)$  neboli  $S(x) \neq S(y)$ .

Máme tedy prosté zobrazení  $S$  z  $\{1, \dots, n\}$  do  $\{1, \dots, m-1\}$  a pomocí indukčního předpokladu odvodíme  $m \geq n+1$ .

Vyčerpali jsme všechny možnosti, pravdivost  $V(n+1)$  je potvrzena.

(iii): Matematickou indukcí dokážeme, že pro všechna  $m \in \mathbb{N}$  platí vlastnost

- $V(m)$ : Jestliže  $n \in \mathbb{N}$  a  $T$  je zobrazení  $\{1, \dots, n\}$  na  $\{1, \dots, m\}$ , pak  $m \leq n$ .

(0)  $m = 1$ : Mějme nějaké zobrazení  $T: \{1, \dots, n\}$  na  $\{1\}$ . Protože  $n \in \mathbb{N}$ , platí  $m = 1 \leq n$ .

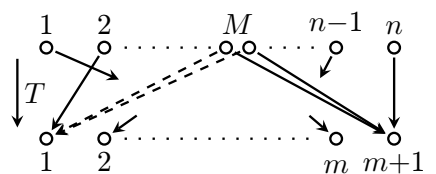
(1) Nechť  $m \in \mathbb{N}$ , předpokládejme, že platí  $V(m)$ . Dokážeme, že platí  $V(m+1)$ .

Vezměme tedy nějaké zobrazení  $T$  z  $\{1, \dots, n\}$  na  $\{1, \dots, m+1\}$ , kde  $n \in \mathbb{N}$ . Podobně jako u (i) chceme vytvořit zobrazení  $S$  z  $\{1, \dots, n-1\}$  na  $\{1, \dots, m\}$ . Aby pak šlo využít  $V(n)$ , musíme mít  $n-1 \in \mathbb{N}$ : Množina  $\{1, \dots, m+1\}$  obsahuje čísla 1, 2 a tudíž díky surjektivitě  $T$  musí existovat  $x, y \in \{1, \dots, n\}$  takové, že  $T(x) = 1$  a  $T(y) = 2$ . Z definice zobrazení vyplývá, že nutně  $x \neq y$ , tedy množina  $\{1, \dots, n\}$  obsahuje alespoň dva prvky. Proto  $n \geq 2$  neboli  $n-1 \in \mathbb{N}$ .

Potřebujeme vynechat  $m+1$  z cílové množiny, určitě tedy budeme chtít přesměrovávat šipky tam vedoucí. Označme si jako  $M$  množinu všech  $x \in \{1, \dots, n\}$ , které splňují  $T(x) = m+1$ . Protože je  $T$  na, tato množina není prázdná. Budeme také chtít vynechat šipku vedoucí z  $n$ , tam záleží, kam vede. Rozebereme dvě možnosti.

1) Předpokládejme, že  $T(n) = m+1$ . Definujme zobrazení  $S$  předpisem

$$S(x) = \begin{cases} T(x), & x \in \{1, \dots, n-1\} \setminus M; \\ 1, & x \in M \setminus \{n\}. \end{cases}$$



Zobrazení je tedy definováno na množině  $\{1, \dots, n-1\}$ .

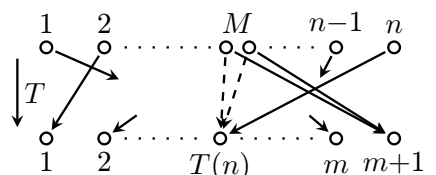
Tvrdíme, že je do množiny  $\{1, \dots, m\}$ . Vezměme  $n \in \{1, \dots, n-1\}$ . Pokud  $x \in M$ , tak  $S(x) = 1 \leq m$ . Pokud  $x \notin M$ , tak  $T(x) \neq m+1$ , tedy  $S(x) = T(x) \leq m$ .

Ještě ověříme, že toto zobrazení je na  $\{1, \dots, m\}$ : Vezměme libovolné  $b \in \{1, \dots, m\}$ . Protože je  $T$  na, musí existovat  $x \in \{1, \dots, n\}$  takové, že  $T(x) = b$ . My jsme ale předpokládali, že  $T(n) = m+1 \neq b$ , tedy  $x \neq n$ , jinak řečeno  $x \in \{1, \dots, n-1\}$ . Díky  $T(x) = b \neq m+1$  také platí  $x \notin M$ , podle definice je  $S(x) = T(x) = b$ .

Máme tedy zobrazení  $S$  z  $\{1, \dots, n-1\}$  na  $\{1, \dots, m\}$ , přičemž  $n-1 \in \mathbb{N}$ . Lze tedy využít indukční předpoklad  $V(m)$ , podle kterého  $m \leq n-1$  neboli  $m+1 \leq n$ .

2) Předpokládejme, že  $T(n) < m+1$ . To mimo jiné znamená, že  $n \notin M$ , tedy  $M$  je neprázdná podmnožina  $\{1, \dots, n-1\}$ . Je dobře, že ji máme k dispozici, protože pokud vynecháme šipku vedoucí z  $n$ , tak je možné, že už žádná šipka nepovede do  $T(n)$ , což musíme napravit. Opět přesměrujeme šipky a definujeme

$$S(x) = \begin{cases} T(x), & x \in \{1, \dots, n-1\} \setminus M; \\ T(n), & x \in M. \end{cases}$$



Zobrazení je definováno na množině  $\{1, \dots, n-1\}$ .

Pro  $x \notin M$  platí  $S(x) = T(x) \leq m$ , pro  $x \in M$  zase  $S(x) = T(n) \leq m$ , tudíž je  $S$  zobrazení do  $\{1, \dots, m\}$ . Tvríme, že je dokonce na.

Vezměme libovolné  $b \in \{1, \dots, m\}$ . Pokud  $b = T(n)$ , tak vezmeme  $x \in M \subseteq \{1, \dots, n-1\}$ , pak  $S(x) = T(n) = b$ . Pokud  $b \neq T(n)$ , tak díky surjektivitě  $T$  najdeme  $x \in \{1, \dots, n\}$  takové, že  $T(x) = b$ . Ovšem  $b \neq T(n)$ , proto nutně  $x \neq n$ , takže  $x$  je vlastně z  $\{1, \dots, n-1\}$ . Také nemůže být z  $M$ , proto  $S(x) = T(x) = b$ .

Máme tedy zobrazení  $S$  z  $\{1, \dots, n-1\}$  na  $\{1, \dots, m\}$  a jako v předchozím případě odvodíme  $m+1 \leq n$ .  $\square$

Tě bychom rádi odvodili obdobné tvrzení pro obecné konečné množiny, nejdříve ale musíme rozhodnout, jak v matematice zjišťujeme počet prvků množiny. Ve školce děti používají ukazovací metodu: Ukazují na jednotlivé věci a říkají jedna, dvě,  $\dots$ . Vzniká tak přiřazení mezi přirozenými čísly a věcmi v hromádce. Toto přiřazení je prosté (pokud se dítě nespletlo a neukázalo dvakrát na tutéž věc) a také na, tedy bijekce.

### Definice.

Množina  $A$  se nazve **konečná**, jestliže platí některá z následujících možností:

(i)  $A = \emptyset$ , pak píšeme  $|A| = 0$ .

(ii) Pro nějaké  $n \in \mathbb{N}$  existuje bijekce z  $\{1, \dots, n\}$  na  $A$ . Pak píšeme  $|A| = n$  a říkáme, že  $A$  má  $n$  prvků.

We say that a set  $A$  is **finite** if either  $A = \emptyset$ , then we write  $|A| = 0$ , or if there exists  $n \in \mathbb{N}$  and some bijection of  $\{1, \dots, n\}$  onto  $A$ , then we write  $|A| = n$  and say that  $A$  has  $n$  elements.

V anglosaské literatuře se také lze setkat s alternativním značením, počet prvků v množině  $A$  se značí  $\#A$ . Vychází to z obecného používání znaku  $\#$  („kriminál“) pro počet v angličtině.

Tak, jak je napsána, definice připouští možnost, že by konečná množina měla více velikostí. To by se nám nelíbilo, rychle to vyloučíme.

Začneme tím, že jakmile má množina nula prvků, tak je prázdná, čímž je vyloučena možnost, že by do  $A$  vedla nějaká bijekce. Množiny s nula prvky tedy nemohou mít zároveň  $n \in \mathbb{N}$  prvků.

Pak musíme prozkoumat případ, kdy pro množinu  $A$  platí zároveň  $|A| = n$  a  $|A| = m$ , kde  $m, n \in \mathbb{N}$ . Pak musí existovat bijekce  $T$  z  $\{1, \dots, m\}$  na  $A$  a bijekce  $S$  z  $\{1, \dots, n\}$  na  $A$ . Podle faktu 9a.11 je  $S^{-1}$  bijekce z  $A$  na  $\{1, \dots, n\}$ , podle faktu 9a.10 pak  $S^{-1} \circ T$  musí být bijekce z  $\{1, \dots, m\}$  na  $\{1, \dots, n\}$ . Podle lemma 9b.1 tedy nutně  $m = n$ , počet prvků je určen jednoznačně. Uf, to jsme si oddechli.

Vidíme, že množiny typu  $\{1, \dots, n\}$  se stávají etalonem, měřítkem, kterým poměřujeme konečné množiny. Někteří autoři pro ně dokonce zavádějí speciální značení (třeba  $I_n$  nebo  $\bar{n}$ ), ale my se nebudeme pouštět tak hluboko do teorie, aby to stálo za to.

**Příklad 9b.a:** Tvríme, že  $|\{a, b, a\}| = 2$ . Zobrazení  $T: \{1, 2\} \mapsto \{a, b, a\}$  dané předpisem  $T(1) = a, T(2) = b$  je zjevně prosté a také na.

$\triangle$

**9b.2 Poznámka:** Je trochu nešikovné, že množiny velikosti nula definujeme jinak. Nabízí se nápad, že bychom řekli, že množiny velikosti nula jsou ty množiny  $A$ , pro které existuje bijekce z  $\emptyset$  na  $A$ . Pak bychom mohli všechny konečné množiny zkoumat pomocí zobrazení, tedy jednotným způsobem, což v matematice preferujeme. Bohužel, zobrazení pracující s prázdnými množinami nemáme definovány, a i kdybychom je zavedli (viz poznámka 9a.12), tak bychom časem zjistili, že některá z tvrzení by pro ně neplatila. Proto nezbývá, než případ množiny nulové velikosti řešit zvlášť. Buď pro ně musíme v důkazu udělat speciální odbočku (obvykle to bývá zřejmé), nebo je v tvrzení ani nepřipouštíme, viz hned to následující.

$\triangle$

Okamžitým důsledkem definice je vcelku jednoduché tvrzení, které se ale občas hodí.

### Fakt 9b.3.

Množina  $A$  je konečná a  $|A| = n \in \mathbb{N}$  právě tehdy, když ji lze zapsat jako  $A = \{a_1, \dots, a_n\}$ , kde  $a_k$  jsou navzájem různé prvky.

**Důkaz (rutinní):**  $1) \implies$ : 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 surjektivit  $T$  vyplývá, že  $A = \{a_1, a_2, \dots, a_n\}$ .



2)  $\Leftarrow$ : Jestliže  $A = \{a_1, \dots, a_n\}$ , pak stačí definovat  $T(k) = a_k$ . Snadno nahlédneme, že je to zobrazení  $\{1, \dots, n\}$  na  $A$ . Prostota: Jestliže pro nějaká  $i, j \in \{1, \dots, n\}$  platí  $T(x) = T(y)$ , pak  $a_i = a_j$ , ale  $a_k$  jsou navzájem různá. Proto nutně  $i = j$ . □

Tento fakt není nic hlubokého, je to jen překlad definice do jiného jazyka: Namísto prostoty a surjektivit se diskutuje, zda jsou prvky  $a_k$  různé a zda dají celou množinu  $A$ . Bývá to mnohem příjemnější na čtení i porozumění, i složité věci mohou vypadat jednoduše, takže se to nabízí jako užitečný nástroj ke zkoumání velikosti množin. Bohužel má jednu nevýhodu, právě tou zdánlivou jednoduchostí svádí k tomu, aby člověk některé věci prohlásil za jasné, i když třeba ve skutečnosti nejsou, vznikají pak chyby. Budeme tedy raději (až na výjimky) pracovat s definicí, je to spolehlivější, zejména pro ty, kdo ještě nejsou ostrílenými důkazotvůrci.

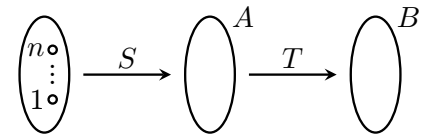
Definice a vlastnosti zobrazení umožňují některá snadná pozorování.

**Fakt 9b.4.**

Nechť  $A$  je konečná množina. Pokud je  $T$  bijekce z  $A$  na nějakou množinu  $B$ , tak je  $B$  konečná a  $|B| = |A|$ .

**Důkaz (poučný):** Protože z prázdné množiny bijekce vést nemůže, platí  $A \neq \emptyset$ . Podle předpokladu proto existuje  $n \in \mathbb{N}$  a bijekce  $S$  z  $\{1, \dots, n\}$  na  $A$ . Podle věty 9a.10 (iii) je pak  $T \circ S$  bijekce z  $\{1, \dots, n\}$  na  $B$ , proto je podle definice  $B$  konečná a  $|B| = n = |A|$ . □

Tento důkaz je jakýmsi prototypem pro významnou část důkazů v této kapitole, spojování vhodných zobrazení se stane naší oblíbenou kratochvílí. Silně doporučujeme kreslit si obrázky, většinou je pak hned jasné, jak vytvářet zobrazení a následně i důkazy.



Když už víme, jak se počítají prvky v konečných množinách, potvrdíme si intuici o vlastnostech zobrazení.

**Fakt 9b.5.**

Nechť  $T: A \mapsto B$  je zobrazení a  $A, B$  jsou konečné.

- (i) Jestliže je  $T$  prosté, tak  $|B| \geq |A|$ .
- (ii) Jestliže má  $B$  méně prvků než  $A$ , pak  $T$  není prosté.
- (iii) Jestliže je  $T$  na, tak  $|B| \leq |A|$ .
- (iv) Jestliže má  $B$  více prvků než  $A$ , pak  $T$  není na.
- (v) Jestliže je  $T$  bijekce, tak  $|B| = |A|$ .
- (vi) Jestliže  $A$  a  $B$  nemají stejně prvků, pak  $T$  není bijekce.

Opět tam máme páry obměn, stačí tedy dokázat třeba ta lichá tvrzení. Ukážeme první, zbytek necháme čtenáři jako cvičení 9b.1. Čtenář by si měl k důkazu nakreslit obrázek.

**Důkaz (poučný):** (i): Existence zobrazení vylučuje prázdné množiny, máme tedy  $|A| = m_A$  a  $|B| = m_B$  pro nějaká  $m_A, m_B \in \mathbb{N}$  a existují bijekce  $S_A$  z  $\{1, \dots, m_A\}$  na  $A$  a  $S_B$  z  $\{1, \dots, m_B\}$  na  $B$ . Pak existuje  $S_B^{-1}$  a vznikne řetízek  $\{1, \dots, n\} \xrightarrow{S_A} A \xrightarrow{T} B \xrightarrow{S_B^{-1}} \{1, \dots, n\}$ . Zobrazení  $S_A, S_B^{-1}$  jsou automaticky prostá, podle faktu 9a.10 je pak  $S_B^{-1} \circ T \circ S_A$  prosté zobrazení z  $\{1, \dots, m_A\}$  do  $\{1, \dots, m_B\}$ , podle lemma 9b.1 tedy nutně  $m_B \geq m_A$  neboli  $|B| \geq |A|$ . □

U tohoto faktu je užitečné si uvědomit, že pracujeme s daným zobrazením, nad kterým nemáme kontrolu. Může nám jej dávat někdo zlomyslný, proto není možné očekávat, že by v oněch šesti implikacích mohly obecně platit opačné směry. Pokud například víme, že dvě množiny mají stejný počet prvků, tak to ještě neznamená, že zrovna to konkrétní dané zobrazení je nutně bijekce, jen víme, že to není vyloučeno. Zkuste si pro každou implikaci z faktu nakreslit konkrétní množiny a z zobrazení, pro které neplatí opačný směr, viz cvičení 9b.2 a pro doplnění také 9b.3.

Jiná situace je, pokud začneme uvažovat všechna možná zobrazení mezi  $A$  a  $B$ .

**Věta 9b.6.**

Nechť  $A, B$  jsou konečné neprázdné množiny.

- (i) Tyto množiny mají stejný počet prvků právě tehdy, když mezi nimi existuje bijekce.
- (ii)  $|B| \geq |A|$  právě tehdy, pokud existuje zobrazení  $T: A \mapsto B$ , které je prosté.
- (iii)  $|B| \leq |A|$  právě tehdy, pokud existuje zobrazení  $T$  z  $A$  na  $B$ .

**Důkaz (poučný):** U všech tvrzení vyplývá směr  $\Leftarrow$  z faktu 9b.5. Budeme tedy dokazovat, že z předpokladu o počtu prvků lze vytvořit žádané zobrazení.

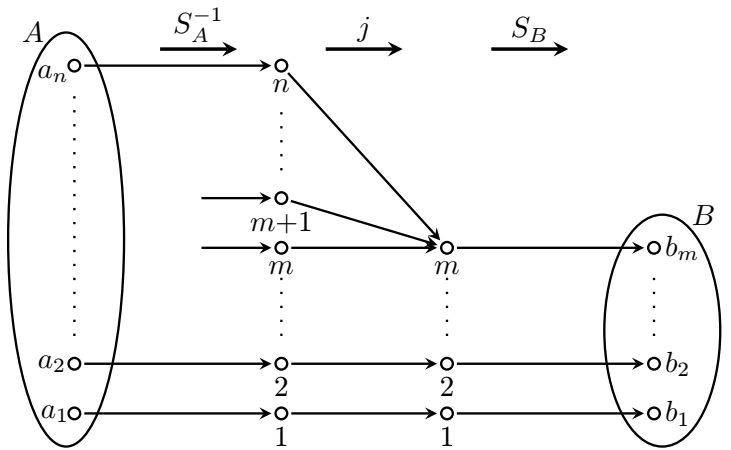
Nechť  $|A| = n$  a  $S_A$  je bijekce z  $\{1, \dots, n\}$  na  $A$ , nechť  $|B| = m$  a  $S_B$  je bijekce z  $\{1, \dots, m\}$  na  $B$ . Nakreslili jsme obrázek zachycující situaci (iii) a doporučujeme, aby si čtenář nakreslil ty další.

(i): Pokud  $m = n$ , je  $T = S_B \circ S_A^{-1}$  hledaná bijekce  $A$  na  $B$ .

(ii): Pokud  $m \geq n$ , je  $i(a) = a$  prosté zobrazení z  $\{1, \dots, n\}$  do  $\{1, \dots, m\}$ . Také  $S_A^{-1}, S_B$  jsou prostá, proto je  $T = S_B \circ i \circ S_A^{-1}$  hledané prosté zobrazení  $A \mapsto B$ .

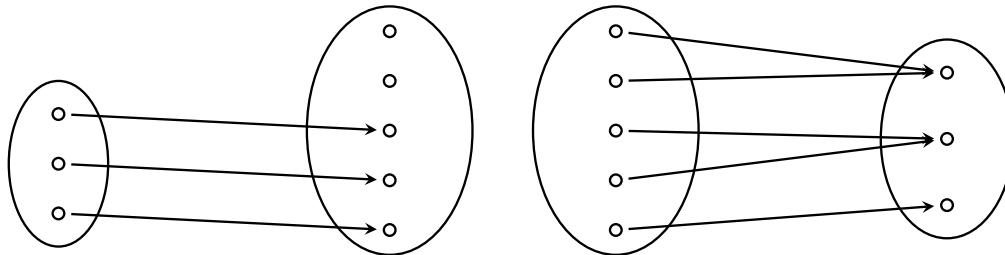
(iii): Pokud  $m \leq n$ , potřebujeme ukuchtit zobrazení z  $\{1, \dots, n\}$  na  $\{1, \dots, m\}$ . Pro  $x \leq m$  definujeme  $j(x) = x$  a pro  $x > m$  definujeme  $j(x) = m$ .

Protože jsou  $S_A, S_B, j$  zobrazení na, je  $T = S_B \circ j \circ S_A^{-1}$  hledané zobrazení  $A$  na  $B$ .



□

Výsledky jsou v souladu s intuicí.



Protože  $|B| \geq |A|$  je totéž jako  $|A| \leq |B|$ , máme vlastně vždy na výběr, jaké zobrazení vytvořit. K důkazu  $|B| \geq |A|$  stačí prosté zobrazení  $A \mapsto B$  nebo surjektivní zobrazení  $B \mapsto A$ . V praxi bývá obvyklé snažší pracovat s prostotou než surjektivitou, ale jsou výjimky, viz třeba důkaz faktu 9c.12.

Vidíme, že zobrazení nabízejí způsob, jak spolehlivě provnovávat velikosti množin. Děti ze školky to samozřejmě dávno znají, porovnávají počty tohodle a támdletoho tak, že jednotlivé položky spojují po párech pastelkou a snaží se, aby se jim čáry na nějakém konci nesešly. Tato věta se stane se východiskem pro část 9c.

Nyní si o konečných množinách dokážeme několik základních vlastností. I zde tu nejtechničtější pasáž schováme do lemátka.

**Lemma 9b.7.**

Nechť  $A$  je konečná množina v nějakém universu  $U$ .

- (i) Pro každé  $a \in U \setminus A$  platí, že  $A \cup \{a\}$  je konečná a  $|A \cup \{a\}| = |A| + 1$ .
- (ii) Pro každé  $a \in A$  platí, že  $A \setminus \{a\}$  je konečná a  $|A \setminus \{a\}| = |A| - 1$ .

**Důkaz (poučný):** Pro prázdnou množinu má smysl pouze (i) a snadno se ověří. Uvažujme tedy neprázdnou konečnou množinu  $A$ , pak existuje  $n \in \mathbb{N}$  a zápis  $A = \{a_1, \dots, a_n\}$ , viz fakt 9b.3.

(i): Protože  $a \notin A$ , můžeme definovat  $a_{n+1} = a$  a dostáváme navzájem různé prvky  $a_1, \dots, a_n, a_{n+1}$  takové, že  $A \cup \{a\} = \{a_1, \dots, a_n, a_{n+1}\}$ . Podle faktu 9b.3 je proto  $A \cup \{a\}$  konečná a  $|A \cup \{a\}| = n + 1 = |A| + 1$ .

(ii): Kdyby  $n = 1$ , tak  $A \setminus \{a\} = \emptyset$ , což je jistě konečná množina a velikosti souhlasí. Uvažujme tedy případ  $n \geq 2$ . Protože  $a \in A$ , musí existovat index  $m$  takový, že  $a_m = a$ .

Kdyby  $m = n$ , tedy  $a = a_n$ , tak  $A \setminus \{a\} = \{a_1, \dots, a_{n-1}\}$ , proto podle faktu 9b.3 je  $A \setminus \{a\}$  konečná množina a  $|A \setminus \{a\}| = n - 1 = |A| - 1$ .

Kdyby  $m < n$ , pak je třeba prvky přecíslovat, což se nejjednodušeji dělá definováním nových. Nechť

$$b_k = \begin{cases} a_k, & k \in \{1, \dots, n-1\} \setminus \{m\}; \\ a_n, & k = m. \end{cases}$$

Podobně jako v důkazu lemma 9b.1 ukážeme, že se zase pro různá  $k \neq l$  musí  $b_k, b_l$  lišit a  $A \setminus \{a\} = \{b_1, \dots, b_{n-1}\}$ , což vede ke kýženému závěru. □

Právě jsme viděli, jak je pohodlné pracovat s vyjádřením konečné množiny seznamem prvků. Pokud se to čtenáři zdá až příliš snadné a bojí se, zda se někde něco nepřehlédlo, může si toto lemma dokázat pomocí definice, tedy s bijekcemi, viz cvičení 9b.6.

Teď jsme již připraveni na to hlavní.

### Věta 9b.8.

- (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  $|A \times B| = |A| \cdot |B|$ .

**Důkaz (poučný):** (i): Příklad, kdy  $B = A$ , platí zcela zjevně, proto se rovnou zaměříme na vlastní podmnožiny. Pak nemá smysl uvažovat  $A = \emptyset$ . Pro  $|A| \in \mathbb{N}$  použijeme matematickou indukci, dokážeme

•  $V(n)$ : Pro všechny množiny o  $n$  prvcích platí, že jejich vlastní podmnožiny jsou konečné a mají méně než  $n$  prvků.

(0)  $n = 1$ : Pokud  $|A| = 1$ , pak jediná vlastní podmnožina je  $B = \emptyset$ , ta je konečná a  $|B| = 0 < 1 = n$ .

(1) Nechť  $n \in \mathbb{N}$  je libovolné, předpokládejme platnost  $V(n)$ . Ukážeme, že pak platí i  $V(n+1)$ . Vezměme tedy nějakou množinu  $A$  o  $n+1$  prvcích a její vlastní podmnožinu  $B$ .

Pokud  $B = \emptyset$ , je konečná a  $|B| = 0 < 1 \leq n < n+1$ .

Pokud je neprázdná, zvolme nějaké  $b \in B$ . Podle lemma 9b.7 je  $A \setminus \{b\}$  konečná a  $|A \setminus \{b\}| = (n+1) - 1 = n$ . Je  $B \setminus \{b\}$  její vlastní podmnožinou? Zjevně  $B \setminus \{b\} \subseteq A \setminus \{b\}$ . Z předpokladu, že  $B$  je vlastní podmnožina, najdeme  $x \in A \setminus B$ , pak nutně také  $x \neq b$ , tedy  $x \in A \setminus \{b\}$  a  $x \notin B \setminus \{b\}$ , proto je  $B \setminus \{b\}$  vlastní podmnožinou  $A \setminus \{b\}$  a  $|A \setminus \{b\}| = n$ . Podle indukčního předpokladu je tedy  $B \setminus \{b\}$  konečná a  $|B \setminus \{b\}| < |A \setminus \{b\}| = n$ . Opět díky lemma 9b.7 je proto  $B = (B \setminus \{b\}) \cup \{b\}$  konečná a  $|B| = |B \setminus \{b\}| + 1 < n + 1$ .

(ii): Pokud je některá z množin prázdná (či obě), tvrzení zjevně platí. Dále tedy uvažujme neprázdné množiny.

1) Nejprve dokážeme případ, kdy jsou  $A$  a  $B$  disjunktní. Podle faktu 9b.3 máme  $A = \{a_1, \dots, a_n\}$  a  $B = \{b_1, \dots, b_m\}$ , kde jde vždy o navzájem různé prvky. Pak  $A \cup B = \{a_1, \dots, a_n, b_1, \dots, b_m\}$ . Jde o  $m+n$  prvků, ještě potřebujeme ukázat, že jsou navzájem různé.

Víme již, že  $a_k$  jsou navzájem různé a  $b_l$  jsou navzájem různé. Kdyby se stalo, že  $a_k = b_l$  pro nějaké  $k, l$ , tak  $a_k \in A \cap B$ , což je ve sporu s předpokladem  $A \cap B = \emptyset$ . Různost je tedy potvrzena a podle faktu 9b.3 je  $|A \cup B| = n + m = |A| + |B|$ .

Pro důkaz podle definice, tedy s bijekcemi, viz cvičení 9b.7.

2) Obecný případ: Uvažujme množiny  $A \setminus B$ ,  $A \cap B$  a  $B \setminus A$  (nakreslete si Vennův diagram). Pak jsou  $B \setminus A$  a  $A \cap B$  podmnožiny  $B$ , proto jsou podle (i) konečné. Navíc jsou disjunktní, proto podle 1) výše musí platit

$$|B \setminus A| + |A \cap B| = |(B \setminus A) \cup (A \cap B)| = |B|,$$

viz cvičení 1d.2 (ii) a 1d.1 (ii).

Protože jsou také množiny  $A$  a  $B \setminus A$  disjunktní (a konečné), máme díky cvičení 1d.1 (vii) a 1) výše

$$|A \cup B| = |A \cup (B \setminus A)| = |A| + |B \setminus A| \leq |A| + |B \setminus A| + |A \cap B| = |A| + |B|.$$

(iii): Příklad prázdných množin je triviální. Předpokládejme tedy, že  $|A| = n$  a  $|B| = m$  pro nějaká  $n, m \in \mathbb{N}$ . Podle faktu 9b.3 pak lze psát  $A = \{a_1, \dots, a_n\}$  a  $B = \{b_1, \dots, b_m\}$ . Podle definice je

$$A \times B = \{(a_k, b_l) : k = 1, \dots, n \wedge l = 1, \dots, m\}.$$

Těchto dvojic je  $n \cdot m$ . Jde o navzájem různé dvojice: Pokud máme  $(a_k, b_l)$  a  $(a_u, b_v)$ , kde se indexy neshodují, tak se liší index u první nebo druhé souřadnice, tedy  $a_k \neq a_u$  respektive  $b_l \neq b_v$ , každopádně dostáváme  $(a_k, b_l) \neq (a_u, b_v)$ .

Podle faktu 9b.3 je tedy  $|A \times B|$  konečná a  $|A \times B| = nm = |A| \cdot |B|$ .

U kartézského součinu je užitečná vizuální představa situace. Jeho přirozeným grafem je obdélníková síť bodů, kde  $|A|$  udává počet sloupců a  $|B|$  počet řádků. Celkový počet bodů by pak měl být  $|A| \cdot |B|$ . Ono obdélníkové

uspořádání může připomenout matici a my si umíme takovou matici přeorganizovat jako vektor, třeba tak, že její jednotlivé řádky seřadíme za sebe. Vzniká tak nápad na zobrazení, které převádí matici  $m \times n$  na vektor z  $\mathbb{R}^{m \cdot n}$ , tato bijekce pak zase dodá inspiraci k obecnému zobrazení  $A \times B$  na množinu vhodné velikosti. Tím se dostáváme k doporučení, aby čtenář navštívil cvičení 9b.8. □

Zbývají ještě dvě populární množinové operace, průnik a rozdíl, u kterých už je vše potřebné ukryté ve větě 9b.8, viz cvičení 9b.9.

Pravidla platná pro dva objekty obvykle není problém zobecnit pro více, funguje to i zde.

**Věta 9b.9.**

(i) Jsou-li  $A_i$  pro  $i = 1, \dots, n$  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  $i = 1, \dots, n$  konečné množiny, pak je i  $A_1 \times \dots \times A_n$  konečná a

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

Důkaz je dle očekávání indukcí, viz cvičení 9b.11.

Onen rozklad sjednocení na tři disjunktní části v důkazu (ii) 2) nabízí příležitost pro přesnější vyjádření.

**Fakt 9b.10.**

(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

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

Uvedený vzorec je v souladu s intuicí. Když sčítáme  $|A| + |B|$ , tak vlastně prvky z  $A \cap B$  započítáváme dvakrát. Výraz  $|A| + |B| - |A \cap B|$  to napraví, všechny prvky z  $A$  a  $B$  jsou teď započítány přesně jednou.

**Důkaz:** (i): Množiny  $A \setminus B$ ,  $A \cap B$  a  $B \setminus A$  jsou navzájem disjunktní a jejich sjednocení je  $A \cup B$ , proto podle Věty 9b.9 dostáváme

$$\begin{aligned} |A \cup B| &= |A \setminus B| + |A \cap B| + |B \setminus A| = (|A \setminus B| + |A \cap B|) + (|B \setminus A| + |A \cap B|) - |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

□

Důkaz části (ii) vyžaduje rozdělení  $A \cup B \cup C$  na celkem sedm částí, viz ten vzorec a Vennův diagram pro tři množiny, jsou všechny navzájem disjunktní, takže se to nakonec poskládá (nakreslete si to). Úplný důkaz nabídneme v kapitole 13b, kde představíme obecný vzorec.

Věta 9b.8 pomůže dokázat jedno zajímavé pozorování. Předpokládáme, že čtenář si v průběhu této kapitoly kreslil obrázky a snad si všimnul zajímavé věci. Když si nakreslíme dvě množiny se stejným počtem prvků a začneme vytvářet různá zobrazení, tak se vlastnosti prostoty a surjektivit zdají souviset. Pokud například pokazíme prostotu, tak se dvě šipky sejdou v jednom cílovém bodě, pak už se ale nedostává šipek, aby pokryly celou cílovou množinu. Potvrdíme si to.

**Fakt 9b.11.**

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

**Důkaz:** Protože existuje  $T: A \mapsto B$ , nejsou  $A, B$  prázdné, mějme tedy  $|A| = |B| = n \in \mathbb{N}$ .

1)  $\implies$ : Předpokládejme, že je  $T$  prosté. Pak je  $T$  bijekce na  $\text{ran}(T)$ , proto je podle faktu 9b.4  $\text{ran}(T)$  konečná a  $|\text{ran}(T)| = |A| = n$ . Zároveň je  $\text{ran}(T)$  podmnožinou  $B$ . Kdyby byla vlastní, tak by podle věty 9b.8 platilo  $n = |\text{ran}(T)| < |B| = n$  neboli  $n < n$ , což není možné. Proto musí být  $\text{ran}(T) = B$  a  $T$  je na.

2)  $\Leftarrow$ : Teď předpokládejme, že  $T$  je na. Důkaz, že je i prosté, provedeme sporem. Předpokládejme tedy dále, že existují  $a \neq b \in A$  takové, že  $T(a) = T(b)$ . Označme  $C = A \setminus \{b\}$  a uvažujme restrikcí  $S = T|_C$ . Podle lemma 9b.7 je  $C$  konečná a  $|C| = n - 1$ . Snadno si rozmyslíme, že  $S$  je stále na, proto podle věty 9b.5  $|B| \leq |C|$ , tedy  $n \leq n - 1$  neboli  $0 \leq -1$ , což je spor.  $\square$

Pokud již předem známe velikosti množin, ušetří nám toto tvrzení půlku práce s dokazováním, že nějaké zobrazení je bijekce.

O konečných množinách už toho víme docela dost, ale ne každá množina je konečná.

**Definice.**

Množina  $A$  se nazve **nekonečná**, jestliže není konečná.

We say that a set  $A$  is **infinite** if it is not finite.

Protože být nekonečnou množinou je negace konečnosti, o které už ledacos víme, dokážeme některé vlastnosti nekonečných množin získat velice snadno.

**Fakt 9b.12.**

Nechť  $A$  je nekonečná množina. Pokud je  $T$  bijekce z  $A$  na nějakou množinu  $B$ , tak je  $B$  nekonečná.

Nabízí se důkaz sporem, protože nás rovnou přivede ke konečným množinám, viz cvičení 9b.12.

**Věta 9b.13.**

- (i) Jestliže je  $A$  nekonečná množina, pak je i každá její nadmnožina  $B$  nekonečná.
- (ii) Nechť  $A, B$  jsou množiny. Je-li některá z nich nekonečná, tak je i  $A \cup B$  nekonečná.
- (iii) Nechť  $A, B$  jsou množiny. Je-li některá z nich nekonečná a druhá neprázdná, tak je i  $A \times B$  nekonečná.

I zde stačí chytře poskládat, co už víme, viz cvičení 9b.13.

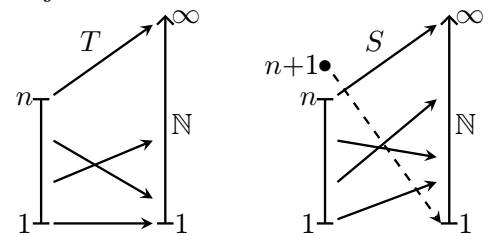
Pěkně si povídáme o nekonečných množinách, ale existují vůbec nějaké? Myslíme si, že jich známe docela dost, ale je potřeba to dokázat podle definice. To není snadné. Zatímco k důkazu konečnosti stačí najít jednu vhodnou bijekci, pro důkaz nekonečnosti je třeba vyvrátit možnost existence jakékoliv bijekce na množinu typu  $\{1, \dots, n\}$ , což je obvykle obtížnější úkol. Rozhodně jako důkaz nestačí, že si takovou bijekci neumíme představit (třeba zrovna nejsme ve formě). Obvykle se tvrzení tohoto typu dokazují sporem.

**Věta 9b.14.**

Množina  $\mathbb{N}$  je nekonečná.

**Důkaz (poučný):** Důkaz povedeme sporem. Předpokládejme, že  $\mathbb{N}$  je konečná, a protože zjevně není prázdná, tak pak existuje  $n \in \mathbb{N}$  a bijekce  $T$  z  $\{1, \dots, n\}$  na  $\mathbb{N}$ . Vytvoříme pomocí něj nové zobrazení.

Nejprve popíšeme intuitivní myšlenku, viz symbolický obrázek nahoře. U všech šipek v  $T$  změním cíl přičtením jedničky. Protože  $T$  je bijekce a posouváme cíle všech šipek najednou, neměly by vzniknout kolize, vznikne tedy prosté zobrazení. Zároveň se v cílové množině uvolní 1, na kterou lze poslat jednu šipku navíc z  $n + 1$ , aniž by se tím zkazila prostota, a touto šipkou vyčerpáme cílovou množinu  $\mathbb{N}$ , takže nové zobrazení by mělo být na. Teď vše uděláme formálně. Uvažujme následující zobrazení:



$$S(x) = \begin{cases} T(x) + 1, & x \in \{1, \dots, n\}; \\ 1, & x = n + 1. \end{cases}$$

Tvrdíme, že je to bijekce z  $\{1, \dots, n + 1\}$  na  $\mathbb{N}$ .

1) Z definice je zjevné, že  $S$  je zobrazení z  $\{1, \dots, n + 1\}$  do  $\mathbb{N}$ .

2) Na: vezměme  $b \in \mathbb{N}$ . Pokud  $b = 1$ , tak existuje  $a = n + 1 \in \{1, \dots, n + 1\}$  splňující  $S(a) = S(n + 1) = 1$ .

Pokud  $b > 1$ , pak  $b - 1 \in \mathbb{N}$  a díky surjektivitě  $T$  musí existovat  $a \in \{1, \dots, n\} \subseteq \{1, \dots, n + 1\}$  splňující  $T(a) = b - 1$ . Pak  $S(a) = T(a) + 1 = (b - 1) + 1 = b$ .

3) Prostota: Uvažujme  $x, y \in \{1, \dots, n+1\}$  splňující  $S(x) = S(y)$ . Pokud  $S(x) = S(y) = 1$ , tak nutně  $x = y = n+1$ , protože pro  $x \leq n$  platí  $S(x) = T(x) + 1 \geq 2$ . Druhá a poslední možnost je  $S(x) = S(y) > 1$ , pak podle definice  $S$  nutně  $x, y \in \{1, \dots, n\}$ . Proto  $S(x) = T(x) + 1$  a  $S(y) = T(y) + 1$ , tedy z rovnice  $S(x) = S(y)$  dostáváme  $T(x) = T(y)$  a díky prostotě  $T$  pak  $x = y$ .

Bijekce je potvrzena. Pak  $S^{-1} \circ T$  je bijekce z  $\{1, \dots, n\}$  na  $\{1, \dots, n+1\}$ , podle lemma 9b.1 tedy  $n = n+1$  neboli  $0 = 1$ , což je hledaný spor. □

Trik s posunutím cílů bylo možné provést jedinečně díky tomu, že množina  $\mathbb{N}$  „nekončí“, takže ať už byla hodnota nějakého  $T(x)$  jakkoliv velká, vždy jsme v  $\mathbb{N}$  dokázali najít i  $T(x) + 1$ . Souvislost s nekonečností je zjevná a budeme ji opakovaně využívat.

Máme tedy potvrzeno, že existují nekonečné množiny, díky předchozí větě o nadmnožinách mezi ně patří i klasické množiny  $\mathbb{Z}$ ,  $\mathbb{Q}$  a  $\mathbb{R}$ . Má smysl se začít ptát, jaké jsou možné velikosti nekonečných množin, což uděláme v následující části.

## Cvičení

**Cvičení 9b.1:** Nechť  $A, B$  jsou konečné neprázdné množiny a  $T$  zobrazení  $A \mapsto B$ . Dokažte následující tvrzení, viz fakt 9b.5.

- (i) Jestliže je  $T$  na, tak  $|B| \leq |A|$ .
- (ii) Jestliže je  $T$  bijekce, tak  $|B| = |A|$ .

**Cvičení 9b.2:** Pro každou z následujících podmínek najděte příklady množin  $A, B$  a zobrazení  $T: A \mapsto B$ , které ji splňují (stačí obrázek)

- (i)  $|B| \geq |A|$  a  $T$  není prosté;
- (ii)  $|B| \leq |A|$  a  $T$  není na;
- (iii)  $|B| = |A|$  a  $T$  není bijekce.

Viz fakt 9b.5.

**Cvičení 9b.3** (poučné, dobré, možná humorné): Uvažujme dvojice množin  $A, B$  takové, že  $|A| = |B|$ . Existuje nějaká podmínka na množiny  $A, B$ , která by zaručila, že když ji ty množiny splní, tak už automaticky budou všechna zobrazení  $T: A \mapsto B$  bijekcemi?

**Cvičení 9b.4** (rutinní): Následující dvojice množin mají vždy stejný počet prvků, proto podle věty 9b.6 musí existovat mezi nimi bijekce. Pro každou dvojici takovou bijekci vytvořte.

- (i)  $A = \{3, 4, 5, 6\}$ ,  $B = \{6, 7, 8, 9\}$ ;
- (ii)  $A = \{a, b, c\}$ ,  $B = \{\beta, \gamma, \delta\}$ ;
- (iii)  $A = \{2, 4, 6, 8, 10\}$ ,  $B = \{1, 2, 3, 4, 5\}$ ;
- (iv)  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{1, 4, 9, 16, 25\}$ ;
- (v)  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{2, 4, 8, 16, 32\}$ ;
- (vi)  $A = \{2, 3, 4, 5, 6\}$ ,  $B = \{5, 8, 11, 14, 17\}$ ;
- (vii)  $A = \{1, 2\}$ ,  $B = \{-1, 1\}$ ;
- (viii)  $A = \{1, 2, 3, 4\}$ ,  $B = \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}\}$ ;
- (ix)  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{1, 2, 3, 4, 7\}$ ;
- (x)  $A = \{1, 2, 3, 8, 10, 12\}$ ,  $B = \{1, 2, 3, 4, 5, 6\}$ .

**Cvičení 9b.5** (rutinní, poučný): Množina  $A = \{2, 4, 6, 8, 10\}$  má méně prvků než množina  $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$ . Podle věty 9b.6 existují prosté zobrazení z  $A$  do  $B$  a zobrazení z  $B$  na  $A$ . Vytvořte taková zobrazení.

**Cvičení 9b.6** (poučné, dobré): Nechť  $A$  je konečná neprázdná množina v nějakém universu  $U$ . Dokažte pomocí definice (tedy vytvořením bijekcí) následující tvrzení.

- (i) Pro každé  $a \in U \setminus A$  platí, že  $A \cup \{a\}$  je konečná a  $|A \cup \{a\}| = |A| + 1$ .
- (ii) Pro každé  $a \in A$  platí, že  $A \setminus \{a\}$  je konečná a  $|A \setminus \{a\}| = |A| - 1$ .

Viz lemma 9b.7.

**Cvičení 9b.7** (poučné, dobré): Dokažte z definice, tedy vytvořením bijekce, že pokud jsou konečné množiny  $A, B$  disjunktní, pak  $|A \cup B| = |A| + |B|$ .

**Cvičení 9b.8** (poučné): Nechť  $A, B$  jsou konečné.

- (i) Vymyslete bijekci  $T$  z  $A \times B$  na  $\{1, \dots, mn\}$ .
- (ii) Vyjádřete  $A \times B$  jako sjednocení navzájem disjunktních množin, které jsou kopiemi množiny  $B$ , načež použijte větu 9b.9 (i) k odvození vzorce pro  $|A \times B|$ .

Viz věta 9b.8.

**Cvičení 9b.9** (poučné): Nechť  $A, B$  jsou konečné množiny.

- (i) Dokažte, že pak je  $A \cap B$  konečná, a najděte vzorec pro  $|A \cap B|$ .
- (ii) Za předpokladu, že  $B \subseteq A$ , dokažte, že  $A \setminus B$  je konečná a odvoďte vzorec pro  $|A \setminus B|$ .
- (iii) Upravte vzorec z části (ii) tak, aby platil pro libovolné dvě konečné množiny.

**Cvičení 9b.10** (rutinní): Dokažte, že pro množiny  $A, B$  platí  $|A \cap B| \leq |A \cup B|$ . Kdy je tam rovnost pro konečné množiny?

**Cvičení 9b.11:** Dokažte, že jsou-li  $A_i$  pro  $i = 1, 2, \dots, n$  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 navzájem disjunktní, tak  $\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i|$ .

(Viz výta a.)

**Cvičení 9b.12** (poučné): Dokažte, že jsou-li  $A, B$  množiny,  $T$  bijekce z  $A$  na  $B$  a  $A$  je nekonečná, tak je i  $B$  nekonečná.

Nápověda: Důkaz sporem.

**Cvičení 9b.13** (poučné): Nechť  $A$  je nekonečná. Dokažte následující tvrzení:

(i) Splňuje-li množina  $B$  inkluzi  $A \subseteq B$ , tak je nekonečná.

(ii) Pro libovolnou množinu  $B$  je  $A \cup B$  nekonečná.

(iii) Není-li  $B$  prázdná, tak je  $A \times B$  nekonečná.

Nápověda: Použijte již známé poznatky, u (iii) zkuste vyrobit v  $A \times B$  kopii množiny  $A$ .

**Řešení:**

**9b.1:** Máme  $m_A, m_B \in \mathbb{N}$  a bijekce  $S_A$  z  $\{1, \dots, m_A\}$  na  $A$  a  $S_B$  z  $\{1, \dots, m_B\}$  na  $B$ .

(i): Zobrazení  $S_A$  i  $S_B^{-1}$  jsou na, proto je podle faktu 9a.10 i  $S_B^{-1} \circ T \circ S_A$  zobrazení z  $\{1, \dots, m_A\}$  na  $\{1, \dots, m_B\}$ . Podle lemma 9b.1 tedy nutně  $m_B \leq m_A$ .

(ii) Zobrazení  $S_A$  i  $S_B^{-1}$  jsou bijekce, proto je podle faktu 9a.10 i  $S_B^{-1} \circ T \circ S_A$  bijekce z  $\{1, \dots, m_A\}$  na  $\{1, \dots, m_B\}$ . Podle lemma 9b.1 tedy nutně  $m_B = m_A$ .

**9b.2:** Společný příklad:  $A = \{1, 2\}$ ,  $B = \{a, b\}$ ,  $T(1) = T(2) = a$ .

**9b.3:** Existuje jediná podmínka, která to dokáže zaručit: Množiny  $A, B$  musí být jednoprvkové. Pak existuje jen jediné zobrazení a to je bijekce.

Jakmile množinám povolíme více prvků, tak už bijekci nevynutíme, vždy bude možné vyrobit příklad z řešení cvičení 9b.2.

**9b.4:** (i):  $T(n) = n + 3$ . (ii):  $T(a) = \gamma$ ,  $T(b) = \beta$ ,  $T(c) = \delta$ . (iii):  $T(n) = \frac{n}{2}$ . (iv):  $T(n) = n^2$ . (v):  $T(n) = 2^n$ . (vi):  $T(n) = 3n - 1$ . (vii):  $T(n) = (-1)^n$ . (viii):  $T(n) = \frac{1}{n+1}$ . (ix)  $T(n) = n$  pro  $n = 1, 2, 3, 4$ ,  $T(5) = 7$ . (x)

$$T(n) = \begin{cases} n, & n \leq 3; \\ n/2, & n \geq 8. \end{cases}$$

**9b.5:** Zobrazení  $T(n) = \frac{n}{2}$  jde z  $A$  do  $B$  a je prosté: Pro  $m, n \in A$  splňující  $T(n) = T(m)$  dostáváme  $\frac{n}{2} = \frac{m}{2}$  neboli  $n = m$ .

K vytvoření zobrazení  $B \mapsto A$ , které je na, nebude stačit vzorec jeden, je třeba použít definici po částech. Jedna možnost:  $T(n) = 2n$  pro  $n = 1, \dots, 5$  a  $T(n) = 6$  pro  $n > 5$ . Jiná možnost:  $T(n) = n$  pro  $n$  sudé a  $T(n) = 10$  pro  $n$  liché. Další jistě vymyslíte sami.

**9b.6:** Nechť  $|A| = n \in \mathbb{N}$ , máme bijekci  $S$  z  $\{1, \dots, n\}$  na  $A$ .

(i): Definice  $T: T(x) = S(x)$  pro  $x \in \{1, \dots, n\}$  a  $T(n+1) = a$ . Pak  $S: \{1, \dots, n+1\} \mapsto A \cup \{a\}$ . Podobně jako v důkazu lemma 9b.1 je  $T$  prosté a na neboli bijekce, proto je  $A \cup \{a\}$  konečná a  $|A \cup \{a\}| = n + 1 = |A| + 1$ .

(ii):  $S$  je na, tedy  $\exists x_0 \in \{1, \dots, n\}$  aby  $S(x_0) = a$ .

Jestliže  $x_0 = n$ , tak je restrikce  $T = S|_{\{1, \dots, n-1\}}$  bijekcí  $\{1, \dots, n-1\}$  na  $A \setminus \{a\}$ , proto je  $A \setminus \{a\}$  konečná množina a  $|A \setminus \{a\}| = n - 1 = |A| - 1$ .

Pokud  $x_0 < n$ , pak je nutno přesměrovat šipky,  $T(x) = S(x)$  pro  $x \in \{1, \dots, n-1\} \setminus \{x_0\}$  a  $T(x_0) = S(n)$ . Vznikne bijekce  $\{1, \dots, n-1\}$  na  $A \setminus \{a\}$ .

**9b.7:** Podle předpokladu existují čísla  $m, n \in \mathbb{N}$  a bijekce  $S_A: A \mapsto \{1, \dots, m\}$  a  $S_B: A \mapsto \{1, \dots, n\}$ .

Předpis pro  $T: T(x) = S_A(x)$  pro  $x \in A$  a  $T(x) = S_B(x) + m$  pro  $x \in B$ .

Díky disjunktnosti je dobře definováno (pro žádné  $x$  nejsou dvě různé definice). Zjevně  $T$  vede do  $\{1, \dots, m+n\}$ .

Je na? Pro  $k \in \{1, \dots, m+n\}$  dvě možnosti. Pokud je  $k \leq m$ , pak ze surjektivit  $S_A$  je  $a \in A$  aby  $S_A(a) = k$ , tedy  $a \in A \cup B$  a  $T(a) = S_A(a) = k$ . Pokud je  $k > m$ , pak  $1 \leq k - m \leq n$  a ze surjektivit  $S_B$  je  $b \in B$  splňující  $S_B(b) = k - m$ . Pak  $b \in A \cup B$  a  $T(b) = S_B(b) + m = (k - m) + m = k$ .

Je  $T$  prosté? Pro  $x \neq y \in A \cup B$  tři možnosti. Jestliže  $x, y \in A$ , pak  $T(x) = S_A(x)$  a  $T(y) = S_A(y)$ . Protože  $S_A$  prosté, musí  $T(x) \neq T(y)$ . Obdobně  $x, y \in B$ . Nakonec  $x \in A$  a  $y \in B$  (naopak je to stejný argument). Pak ale  $T(x) = S_A(x) \leq m$ , zatímco  $T(y) = S_B(y) + m > m$ , tedy  $T(x) \neq T(y)$ .  $T$  je prosté.

**9b.8:** Necht  $A = \{a_1, \dots, a_m\}$ .

(i):  $T(a_k, b_l) = (k-1) \cdot m + l$ .

(ii): Pro  $k = 1, \dots, m$  necht  $B_k = \{(a_k, b) : b \in B\}$ . 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: Necht  $(a_k, b) \in B_k$ . Pak  $b \in B$  a  $T_k(b) = (a_k, b)$ .

Takže  $|B_k| = |B|$ .  $B_k$  jsou navzájem disjunktní množiny, neboť pro  $k \neq l$  se prvky z  $B_k$  liší od prvků z  $B_l$  na první souřadnici. Protože  $A \times B = B_1 \cup \dots \cup B_m$ , platí

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

**9b.9:** (i):  $A \cap B$  je konečná coby podmnožina  $A$ , vzorec se odvodí úpravou vzorce pro  $A \cup B$  (viz věta 9b.8) a zní  $|A \cap B| = |A| + |B| - |A \cup B|$ .

(ii):  $A \setminus B$  je podmnožinou konečné množiny  $A$ , proto je konečná. Také platí  $(A \setminus B) \cup B = A$  a ty dvě množiny vlevo jsou disjunktní, proto pomocí vzorce pro  $\cup$  vyjde  $|A \setminus B| = |A| - |B|$ .

(iii): Obecný vzorec je  $|A \setminus B| = |A| - |A \cap B|$ .

**9b.10:** Platí  $A \cap B \subseteq A \cup B$ , proto  $|A \cap B| \leq |A \cup B|$ . Aby platilo  $|A \cap B| = |A \cup B|$ , muselo by platit  $A \cap B = A \cup B$ , což je jen když  $A = B$ .

**9b.11:** Důkaz povedeme indukci, lze udělat pro obě tvrzení najednou (obecný případ a disjunktní případ).

(0) Pro  $n = 1$  evidentně platí.

(1) Necht  $n \in \mathbb{N}$ . Indukční předpoklad: obě tvrzení platí pro  $n$  množin. Chceme to pro  $n + 1$ .

Mějme konečné množiny  $A_1, \dots, A_n, A_{n+1}$ . Podle indukčního předpokladu je množina  $B = \bigcup_{i=1}^n A_i$  konečná a

platí  $|B| \leq \sum_{i=1}^n |A_i|$ . Pak podle věty je konečná i množina  $B \cup A_{n+1} = \bigcup_{i=1}^{n+1} A_i$  a platí  $\left| \bigcup_{i=1}^{n+1} A_i \right| = |B \cup A_{n+1}| \leq$

$$|B| + |A_{n+1}| \leq \sum_{i=1}^{n+1} |A_i|.$$

Pokud jsou navíc disjunktní, pak podle indukčního předpokladu  $|B| = \sum_{i=1}^n |A_i|$ , množiny  $B$  a  $A_{n+1}$  jsou disjunktní

a proto obdobně  $\left| \bigcup_{i=1}^{n+1} A_i \right| = \sum_{i=1}^{n+1} |A_i|$ .

**9b.12:** Kdyby byla  $B$  konečná, tak díky bijekci  $T^{-1}$  z  $B$  na  $A$  by byla konečná i  $A$ , spor.

**79b.13:** (i): Kdyby byla  $B$  nekonečná, tak by byla  $A$  konečná dle věty 9b.8 (i).

(ii): Platí  $A \subseteq A \cup B$ , použít právě dokázané tvrzení (i).

(iii): Díky  $B \neq \emptyset$  lze zvolit  $b \in B$  a definovat  $A_b = \{(a, b) : a \in A\}$ . Pak  $T: a \mapsto (a, b)$  je bijekce  $A$  na  $A_b$ , proto je  $A_b$  nekonečná, a  $A_b \subseteq A \times B$ , pak použít (i).

## 9c. Mohutnost množin

V předchozí části jsme si zavedli porovnávací škálu  $\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}$  atd. pro určování velikosti konečných množin. Šlo by vyrobit úplnou škálu tím, že by se ještě k těmto množinám přidala množina  $\mathbb{N}$  jako univerzální zástupce všech nekonečných množin?

Tento nápad naráží na několik problémů. Tím prvním je, jak vlastně poznáme, že nějaká nekonečná množina má stejnou velikost jako  $\mathbb{N}$ . U konečných množin je to jednoduché, každá má velikost danou číslem a ta se dají porovnat, jenže to u nekonečných nejde. Mohli bychom zkusit prohlásit, že všechny nekonečné jsou prostě stejně velké, ale není jisté, zda to má smysl. Je sudých přirozených čísel stejně jako všech přirozených čísel, nebo méně? A není náhodou reálných čísel pro změnu víc?

Naším prvním úkolem je tedy naučit se porovnávat velikosti množin. Jako inspirace nám poslouží věta 9b.6. Protože nás čeká velkolepá teorie, nebudeme už mluvit o obyčejné velikosti množin, zavedeme si speciální pojem.

### Definice.

Uvažujme množiny  $A$  a  $B$ .

Řekneme, že mají stejnou **mohutnost** či **kardinalitu**, značeno  $|A| = |B|$ , jestliže existuje bijekce z  $A$  na  $B$  nebo  $A = B = \emptyset$ .

Řekneme, že mohutnost  $A$  je menší nebo rovna mohutnosti  $B$ , značeno  $|A| \leq |B|$ , jestliže existuje prosté zobrazení z  $A$  do  $B$  nebo  $A = \emptyset$ . Pak také můžeme říct, že mohutnost  $B$  je větší nebo rovna mohutnosti  $A$ , značeno  $|B| \geq |A|$ .

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 than or equal to cardinality of  $B$ , denoted  $|A| \leq |B|$ , if there exists a 1-1 mapping from  $A$  to  $B$ .

Pro konečné množiny teď máme dvě definice umožňující porovnávat jejich velikosti. naštěstí věta 9b.6 zaručuje, že jsou spolu ve shodě. Jinak řečeno, tato definice mohutnosti zobecňuje původní definici velikosti pro konečné množiny na pojem, který lze již použít pro všechny množiny.

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  $|A|$ .

Oba pojmy jsou v souladu s intuicí. Pokud se nám u dvou množin (třeba i nekonečných) podaří prvky spárovat, pak jsou asi stejně velké. To zní rozumně. Co ten druhý pojem? Pokud existuje prosté zobrazení  $T$  z  $A$  do  $B$ , pak je toto  $T$  bijekce z  $A$  na  $\text{ran}(T)$ . Pak  $|\text{ran}(T)| = |A|$  a  $\text{ran}(T) \subseteq B$ , pak dá se čekat  $|\text{ran}(T)| \leq |B|$  neboli  $|A| \leq |B|$ . Dává to smysl. Intuitivně řečeno se nám podařilo v množině  $B$  vytvořit pomocí  $T$  kopii množiny  $A$ , tato představa se stane jedním z našich oblíbených nástrojů.

Ve větě 9b.6 byl ještě jeden způsob, jak získat nerovnost pro velikost množin, jmenovitě pomocí surjektivního zobrazení. Ukážeme, že jsme jej mohli použít v obecné definici a vyšlo by to nastejno.

### Věta 9c.1.

Nechť  $A, B$  jsou neprázdné množiny.

$|A| \leq |B|$  právě tehdy, když existuje zobrazení  $T: B \mapsto A$ , které je na.

Toto se občas hodí, ale většinou je výrazně snadnější pracovat s prostými zobrazeními jako v definici. Důkaz věty zase spočívá v překladu obrázku do matematictinity.

### Důkaz (poučný):

1)  $\implies$ : Jestliže  $|A| \leq |B|$ , pak existuje zobrazení  $S: A \mapsto B$ , které je prosté. Je to bijekce jako zobrazení  $A \mapsto \text{ran}(S)$ , proto máme zobrazení  $S^{-1}$  z  $\text{ran}(S)$  na  $A$ . Zvolme nějaké  $a \in A$  a definujme zobrazení  $T: B \mapsto A$  takto:

$$T(y) = \begin{cases} S^{-1}(y), & y \in \text{ran}(S); \\ a, & x \in B \setminus \text{ran}(S). \end{cases}$$

Pak je  $T$  opravdu definováno pro všechna  $y \in B$  a má hodnoty v  $A$ . Zbývá dokázat, že je na. Pro  $x \in A$  máme  $y = S(x) \in \text{ran}(S)$ , pak  $y \in B$  a  $T(y) = S^{-1}(y) = x$ .

2)  $\impliedby$ : Uvažujme případ, kdy existuje zobrazení  $T$  z  $B$  na  $A$ . Pro každé  $a \in A$  pak je množina  $M_a = \{b \in B : T(b) = a\}$  neprázdná. Vyberme si z každé  $M_a$  jeden prvek  $b_a$ , můžeme pak definovat zobrazení  $S$  z  $A$  do  $B$  předpisem  $S(a) = b_a$ . Tvrdíme, že je prosté. Vezměme  $x, y \in A$  takové, že  $S(x) = S(y)$ . Podle definice  $S$  to znamená  $b_x = b_y$ , podle definice těchto prvků zase  $T(b_x) = x$  a  $T(b_y) = y$ . Protože  $b_x = b_y$  a  $T$  je zobrazení, nutně  $x = y$ .

Máme tedy prosté zobrazení z  $A$  do  $B$  a proto podle definice  $|A| \leq |B|$ .

Poznamenejme, že tato část důkazu je hluboká. To, že jsme si byli schopni vybrat z množin  $M_a$  po jednom prvku, není vůbec samozřejmé, musíme se zde odvolat na známý Axiom výběru, který ovšem někteří matematici neuznávají. To ale není náš případ, my tu děláme mainstream matematiku, která (AC) akceptuje.  $\square$

Nyní se podíváme na vlastnosti našich nových pojmů. Nejprve ověříme základní vlastnosti, které bychom od pojmů spojených s velikostí určitě očekávali.

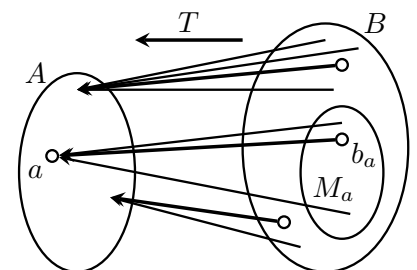
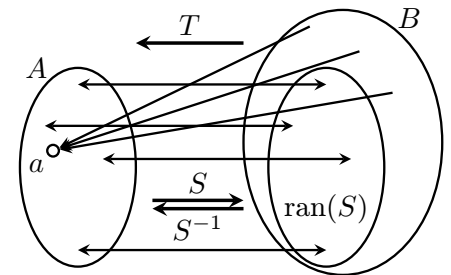
### Fakt 9c.2.

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  $i_A: A \mapsto A$ . 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  $i_B$ , 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. □

Mimochodem, my tady vlastně máme dvě relace na množinách. První a třetí část faktu by šlo vyjádřit slovy, že relace  $|A| \leq |B|$  je reflexivní a relace  $|A| = |B|$  je reflexivní a symetrická.

Na první pohled by se části (i) a (ii) mohly zdát samozřejmé, ale je to tím, že zvolené značení trochu klame tělem. U konečných množin mělo  $|A|$  svůj význam, bylo to číslo, takže pak samozřejmě platí  $|A| = |A|$  a podobně. Jenže teď je tomu úplně jinak. Pro obecné množiny jsme zatím symbol  $|A|$  nedefinovali (a ani nebudeme), nemá sám o sobě žádný význam. Význam má jen obrázek „ $|A| = |B|$ “, což je vlastně zkratka pro matematický výrok o existenci jisté bijekce. Obdobně to platí pro obrázek „ $|A| \leq |B|$ “.

To znamená, že sice ty rovnosti a nerovnosti vypadaly povědomě, ale ve skutečnosti to s rovností a nerovností mezi čísly nemá vůbec nic společného a každý takový vzoreček, ať už nám přijde sebevíc povědomý, vlastně schovává nějaké tvrzení o zobrazeních, je pak nutné ho takto dokázat.

To se samozřejmě vztahuje i na „jasné“ vztahy níže. Uvidíme, že se nové pojmy opravdu chovají, jako by šlo o rovnost a nerovnost, což je příjemné, protože se nemusíme učit nic nového. Jen si musíme být vědomi, že to nejsou triviální věci, ale vyžadují důkaz (občas hodně drsný). Teď už chápete, proč jsme následující tvrzení nezařadili do cvičení jako trivialitku, jakkoliv tak na první pohled působí.

**Fakt 9c.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  $|A| = |C|$ .

Takže relace  $|A| \leq |B|$  a  $|A| = |B|$  jsou vlastně tranzitivní. Dohromady to znamená, že  $|A| = |B|$  je ekvivalence. Ještě se k tomu vrátíme.

**Důkaz (rutinní, poučný):** (i): Z předpokladu  $|A| \leq |B|$  dostáváme existenci zobrazení  $T: A \mapsto B$ , které je i prosté. Podobně z předpokladu  $|B| \leq |C|$  dostaneme prosté zobrazení  $S: B \mapsto C$ . Podle faktu 9a.10 (i) je i složené zobrazení  $S \circ T: A \mapsto C$  prosté, proto podle definice  $|A| \leq |C|$ .

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

(iii): Stejný důkaz, jen se použije fakt 9a.10 (iii). □

Rovněž klasický vztah mezi rovností a nerovností se přenáší do světa mohutností.

**Fakt 9c.4.**

Nechť  $A, B$  jsou množiny.

Jestliže  $|A| = |B|$ , pak  $|A| \leq |B|$  a  $|B| \leq |A|$ .

Důkaz viz cvičení 9c.1. Ještě nám chybí opačný směr. Ten také platí, 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 9c.5.** (Cantor-Bernstein-Schroeder)

Nechť  $A, B$  jsou množiny. Jestliže  $|A| \leq |B|$  a  $|B| \leq |A|$ , pak  $|A| = |B|$ .

Důkaz je dost těžký, je totiž třeba ze dvou prostých zobrazení  $A \mapsto B$  a  $B \mapsto A$ , které spolu nikterak nesouvisí, vyrobit bijekci. Zvídavý (a odvážný) čtenář může zkusit prakticky jakoukoliv tlustší knihu o teorii množin či Internet. Každopádně je to věta zajímavá nejen z hlediska teoretického, ale i z hlediska praktického. Umožňuje totiž dokázat shodnou mohutnost dvou množin vytvořením dvou prostých zobrazení, což bývá obvykle snazší než vytvářet bijekci. Budeme to často používat.

Je možné zavést ještě jeden blízký pojem, viz cvičení 9c.3.

Umíme porovnávat mohutnost množin, je načase vrátit se k otázce, jak velké mohou být nekonečné množiny. Přírodním etalonem je množina  $\mathbb{N}$ .

**Definice.**

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 **countable** if  $|A| = |\mathbb{N}|$ . We say that  $A$  is **uncountable** if it is infinite but not countable.

Máme tedy výchozí nekonečnou mohutnost a uvidíme, zda je jediná, to bychom nespočetné množiny definovali zbytečně. Spočetnost hraje mezi nekonečnými množinami speciální roli, například proro, že je to nejmenší možná nekonečná množina.

**Fakt 9c.6.**

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

**Důkaz (poučný):** Protože prázdná množina je konečná, určitě  $A \neq \emptyset$ . Definujme nekonečnou posloupnost různých prvků  $a_n \in A$  indukci:

(0) Protože  $A \neq \emptyset$ , zvolme libovolné  $a_1 \in A$ .

(1) Nechť  $n \in \mathbb{N}$ . Jsou definovány navzájem různé prvky  $a_1, \dots, a_n$ . Kdyby bylo  $A = \{a_1, \dots, a_n\}$ , tak by podle faktu 9b.3 byla  $A$  konečná, což není možné. Proto je množina  $A \setminus \{a_1, \dots, a_n\}$  neprázdná, můžeme z ní tedy zvolit nějaký prvek  $a_{n+1}$ .

Máme tedy navzájem různé prvky  $a_n \in A$  pro  $n \in \mathbb{N}$ . Definujme zobrazení  $T(n) = a_n$  z  $\mathbb{N}$  do  $A$ . Díky různosti těch  $a_n$  je prosté, podle definice mohutnosti tedy  $|\mathbb{N}| \leq |A|$ . □

Tento výsledek jinými slovy říká, že mezi spočetností a konečnými množinami už žádný další typ mohutnosti není. Tyto dvě kategorie jsou si tedy blízké, což naznačuje i následující pozorování.

**Fakt 9c.7.**

Množina  $A$  je spočetná, pokud ji lze napsat jako  $A = \{a_n : n \in \mathbb{N}\}$ , kde  $a_n$  jsou navzájem různé.

Důkaz je podobný jako u faktu 9b.3.

Vidíme tedy silnou podobnost, konečné a spočetné množiny se vyznačují tím, že jejich prvky lze vypsát seznamem neboli „spočítat“ (ukazujeme si prstem: první, druhý, třetí, viz ta školka). V některých situacích mezi nimi není příliš rozdílu a používají se stejné nástroje. Někteří autoři proto definují pojmy jinak, název „spočetná“ u nich zahrnuje i množiny konečné.

My v této knize používáme definici spočetnosti, která je rozšířenější. Pokud chceme říct, že množina  $A$  je konečná nebo spočetná, tak řekneme, že je „nejvýše spočetná“ neboli máme nerovnost  $|A| \leq |\mathbb{N}|$ . Teď už víme, že je to korektní, žádná jiná mohutnost se tam nevetře.

Dostáváme zajímavou věc: Když z množiny  $\mathbb{N}$  nějaké prvky odebereme tak, aby jich stále zůstalo nekonečně mnoho, tak ta zmenšená množina bude mít stejnou mohutnost jako původní  $\mathbb{N}$ . To je pro nás nové chování, podíváme se na ně zblízka. Začneme tím nejjednodušším, odebereme jeden prvek.

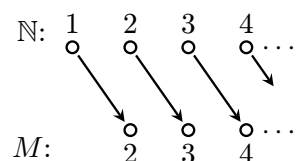
**Příklad 9c.a:** Uvažujme množinu  $M = \mathbb{N} \setminus \{1\} = \{2, 3, 4, \dots\}$ . Protože  $M \subseteq \mathbb{N}$ , musí podle faktu 9c.2 platit  $|M| \leq |\mathbb{N}|$ . Podle faktu 9c.6 zase  $|\mathbb{N}| \leq |M|$ , tudíž  $|M| = |\mathbb{N}|$  neboli  $M$  je spočetná. Vlastně jsme to tímto dokázali, ale zkusíme i přímý důkaz.

Potřebujeme najít bijekci z  $\mathbb{N}$  na  $M$  (nebo i naopak), jinak řečeno chceme spárovat prvky z  $\mathbb{N}$  s prvky z  $M$ . Obrázek vpravo naznačuje, jak to uděláme. Definujme  $T: \mathbb{N} \rightarrow M$  předpisem  $T(n) = n + 1$ . Obrázek silně naznačuje, že by to měla být bijekce.

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

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

Dokázali jsme, že  $|M| = |\mathbb{N}|$ , tedy  $M$  je spočetná. △



Tento výsledek má velice názornou interpretaci. Na reálné ose vidíme  $\mathbb{N}$  jako nekonečnou množinu korálků. Když ji posuneme o jedno doprava, tak se počet korálků nezmění. Protože na pravém konci není žádná zarážka (množina

je nekonečná), není třeba žádný korálek odebírat, je tam dost místa na posun celé původní množiny neboli pořadí je kam posílat šipky. Dává to tedy smysl.

Není důvod posouvat jen o jedno. Důkaz lze snadno modifikovat pro posun o libovolný konečný počet míst. Fakt, že „velikost“ nekonečné množiny se nezmění odebráním (rozumného počtu) prvků, je pro nekonečné množiny charakteristický (tedy dají se podle toho poznat).

**Věta 9c.8.**

Množina  $A$  je nekonečná právě tehdy, když má vlastní podmnožinu  $B$  splňující  $|B| = |A|$ .

V důkazu využijeme dva triky, které jsme teď viděli, tedy vyrobíme si v  $A$  kopii přirozených čísel a v ní pak provedeme posun.

**Důkaz (poučný):** 1)  $\Leftarrow$ : Pokud má  $A$  vlastní podmnožinu splňující  $|B| = |A|$ , pak podle Věty 9b.8 nemůže být konečná, tudíž je dle definice nekonečná.

2)  $\Rightarrow$ : Pokud je  $A$  nekonečná, tak dle důkazu Faktu 9c.6 najdeme nekonečnou množinu  $\{a_n : n \in \mathbb{N}\}$  různých prvků z  $A$ . Nechť  $B = A \setminus \{a_1\}$ . Protože  $a_1 \in A$ , je  $B$  vlastní podmnožinou  $A$ . Uvažujme zobrazení definované jako  $T(a) = a$  pro  $a \in A \setminus \{a_n : n \in \mathbb{N}\}$  a  $T(a_n) = a_{n+1}$  pro  $n \in \mathbb{N}$ . Snadno ukážeme, že  $T$  je bijekce z  $A$  na  $B$ , proto  $|A| = |B|$ . □

Někteří autoři dokonce touto podmínkou nekonečné množiny definují. Naše definice byla výhodnější v teorii, protože jsme dokázali spoustu tvrzení o konečných množinách snadno převést na nekonečný případ, ale v konkrétních příkladech může být problém nekonečnost dokázat (vyvracení všech možných bijekcí). Tam je zase výhodnější tento alternativní pohled, stačí vytvořit jednu zajímavou podmnožinu.

Teď se podíváme na rozsáhlejší zásah do množiny  $\mathbb{N}$ .

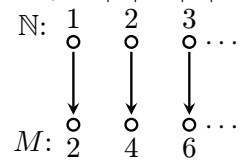
**Příklad 9c.b:** Uvažujme množinu  $S = \{2k : k \in \mathbb{N}\}$  kladných sudých čísel. Protože jde o nekonečnou podmnožinu  $\mathbb{N}$ , získáme snadno odhady z obou stran pro mohutnost jako v předchozím příkladě a vidíme, že  $|S| = |\mathbb{N}|$ .

Opět to zkusíme potvrdit podle definice, obrázek naznačí. Definujme  $T: \mathbb{N} \mapsto S$  předpisem  $T(n) = 2n$ . Měla by to být bijekce.

Prosté: Pro libovolné  $x, y \in \mathbb{N}$  splňující  $T(x) = T(y)$  platí  $2x = 2y$  neboli  $x = y$ .

Na: Každé  $m \in S$  je ve tvaru  $m = 2n$  pro  $n \in \mathbb{N}$ , pak  $T(n) = m$ .

Potvrdili jsme, že množina  $S$  kladných sudých čísel je spočetná. △



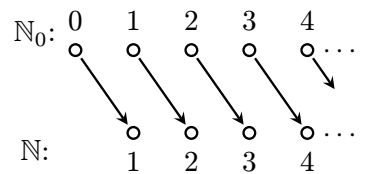
Obdobně snadno dokážeme, že množina  $L$  lichých kladných čísel je také spočetná, například pomocí zápisu  $L = \{2k - 1 : k \in \mathbb{N}\}$ . Máme také  $\mathbb{N} = S \cup L$ . Co to znamená? Že množinu  $\mathbb{N}$  lze rozdělit na dvě poloviny, které jsou každá stejně „velká“ jako původní množina  $\mathbb{N}$ . Jinak řečeno,  $\mathbb{N}$  obsahuje dvě kopie sebe sama.

Inspiruje nás to k trochu jinému pohledu na bijekce, které jsme právě vytvořili. Obě lze totiž chápat jako prostá zobrazení  $\mathbb{N} \mapsto \mathbb{N}$  a my víme, že když máme prosté zobrazení  $T: A \mapsto B$ , tak jakoby vytváříme v množině  $B$  kopii  $\text{ran}(T)$  množiny  $A$ . V prvním příkladě jsme tak dokázali v množině  $\mathbb{N}$  najít její kopii  $\{2, 3, \dots\}$  a zbylo ještě jedno volné místo, kam se nám může vejít ještě něco navíc. To naznačuje, že by se mohutnost  $\mathbb{N}$  neměla změnit ani přidáním (několika) prvků.

**Příklad 9c.c:** Jakou mohutnost má množina  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ?

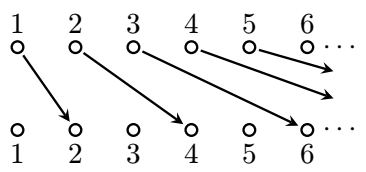
Čekáme, že  $|\mathbb{N}_0| = |\mathbb{N}|$ . Uvažujme zobrazení  $T: \mathbb{N}_0 \mapsto \mathbb{N}$  dané vzorcem  $T(n) = n+1$ . Jde o stejný vzorec jako v příkladě 9c.a a důkaz, že je to bijekce, je také stejný.

Mimochodem, díky  $\mathbb{N} \subseteq \mathbb{N}_0$  víme, že  $|\mathbb{N}| \leq |\mathbb{N}_0|$ . Proto podle věty 9c.5 už jen stačilo doplnit  $|\mathbb{N}_0| \leq |\mathbb{N}|$ , jinými slovy u zobrazení  $T$  stačilo jen ověřit prostotu. △



Intuitivně, zobrazení  $T$  zasunulo  $\mathbb{N}$  do množiny  $\mathbb{N}$  o jedno doprava, čímž se vyšetřilo místo na zasunutí nuly. Teď se z tohoto pohledu podíváme na příklad se sudými čísly.

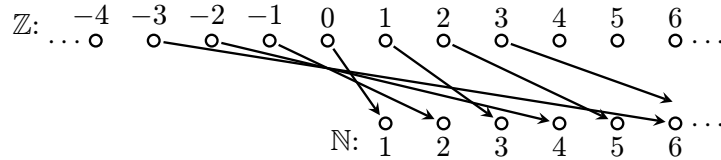
Pomocí zobrazení  $T(n) = 2n$  vlastně horní množinu  $\mathbb{N}$  „rozprostíráme“ v té dolní množině  $\mathbb{N}$ . Šipky posíláme čím dál více napravo, ale díky „nekonečnému konci“ je tam pro všechny dost místa. Pěkně názorně vidíme, že v  $\mathbb{N}$  je dost místa pro kopii  $\mathbb{N}$  a ještě pro nekonečně mnoho dalších objektů. Zajímavým kandidátem na doplnění těch neobsazených míst jsou záporná celá čísla. Směřujeme tím k jednomu užitečnému výsledku.



**Fakt 9c.9.**Množina  $\mathbb{Z}$  je spočetná.

Vlastně už to máme vymyšleno, vytvoříme zobrazení  $\mathbb{Z} \mapsto \mathbb{N}$ . „Kladnou“ část  $\mathbb{Z}$  rozprostře způsobem, který už známe, tentokrát použijeme vzorec  $2n + 1$ , abychom mohli posílat i nulu. Do neobsazených míst pak pošleme „zápornou polovinu“  $\mathbb{Z}$ .

**Důkaz (poučný):** Uvažujme toto zobrazení  $\mathbb{Z} \mapsto \mathbb{N}$ :



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

Na: Vezmeme  $m \in \mathbb{N}$ . Jestliže je liché, pak jej lze napsat jako  $2n + 1$  pro jisté  $n \in \mathbb{N}_0$ . Pak  $n \in \mathbb{Z}$  a dle definice zobrazení pro  $n \geq 0$  platí  $T(n) = 2n + 1 = m$ .

Jestliže je  $m$  sudé, pak je  $n = -\frac{m}{2}$  záporné celé číslo. Podle definice zobrazení pak  $T(n) = 2|-\frac{m}{2}| = | -m |$ , díky  $m > 0$  tedy  $T(n) = m$ .

Prostota: Necht  $x, y \in \mathbb{Z}$  splňují  $T(x) = T(y)$ . Pokud by  $x \geq 0$  a  $y < 0$ , tak by  $T(x)$  bylo liché a  $T(y)$  sudé 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  $T(x) = T(y)$  znamená  $2x + 1 = 2y + 1$  neboli  $x = y$ .

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

**9c.10 Poznámka:** Ukážeme zajímavý alternativní důkaz.

Protože  $\mathbb{N} \subseteq \mathbb{Z}$ , máme  $|\mathbb{N}| \leq |\mathbb{Z}|$ . Podle věty 9c.5 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 ukážeme, že hodnoty  $T$  jsou přirozená čísla. Protože  $|n| + n \in \mathbb{N}_0$ , je  $2^{|n|+n} \in \mathbb{N}$ . Víme také, že  $|n| - n$  je celé číslo, z nerovnosti  $n \leq |n|$  pak máme  $|n| - n \geq 0$  a zase  $3^{|n|-n} \in \mathbb{N}$ .

Dále si všimneme, že pro  $n \geq 0$  je  $|n| = n$ , proto  $T(n) = 2^{2n}$ , zatímco pro  $n < 0$  je  $|n| = -n$  a tedy  $T(n) = 3^{-2n}$ . Protože čísla s různými prvočíselnými rozklady nemohou být stejná (viz věta 2b.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 jediným vzorečkem, což někdy může být výhoda. Ještě se nám to bude hodit.

$\triangle$

Viděli jsme, že když množinu  $\mathbb{N}$  jakoby rozpůlíme či zdvojnásobíme (intuitivně vzato vypadá  $\mathbb{Z}$  jako dvě spojené kopie  $\mathbb{N}$ ), tak se její mohutnost nezmění. Pomocí zobrazení  $n \mapsto 3n$ ,  $n \mapsto 4n$  atd. si snadno rozmyslíme, že  $\mathbb{N}$  lze rozdělit na libovolný konečný počet stejně velkých částí a všechny budou pořád stejně velké jako  $\mathbb{N}$ . Jinak řečeno, do množiny  $\mathbb{N}$  lze vměstnat libovolný konečný počet kopií  $\mathbb{N}$ , což znamená, že kdybychom množinu  $\mathbb{N}$  jakoby zněkolikanásobili, bude pořád stejně mohutná.

Při prvním setkání toto vypadá velmi podivně. Je to samozřejmě díky tomu, že v běžném životě se s nekonečny neseťkáváme a naše mozky na ně nejsou zvyklé. Co evoluce zanedbala, doženeme v této kapitole. Smířit nás s touto novou situací může například známá pohádka o Holbertově hotelu.

**Příklad 9c.d:**

Hilbertův hotel je speciální hotel, který má spočetně mnoho jednolůžkových pokojů číslovaných pomocí  $n \in \mathbb{N}$ . Před chvílí jsme ukázali, že i když je plný, ještě tam dokážeme vytvořit pokoj pro jednoho člověka navíc. Všechny nájemníky pošleme o pokoj dál (vážený zákazník, prosím přestěhujte se okamžitě do pokoje s číslem o jedno větším) a první pokoj je náhle prázdný.

Stejně snadno se vypořádáme se situací, kdy máme plný hotel a přijede pár na svatební cestě, fotbalové družstvo nebo třeba všichni účastníci světového sletu příznivců Star Treku.

Hilbertův hotel zvládne i víc. Představme si, že konkurence si také jeden postavila, má plno a náhle musí zavřít (kontrola našla šváby). Vyhrne se z něj nekonečně mnoho (ale spočetně) hostů. Co uděláme? Necháme se inspirovat postupem použitým v důkazu o  $\mathbb{Z}$ . Nejprve pošleme zprávu všem svým hostům, aby se laskavě z pokoje  $n$  přesunuli do pokoje  $2n$ . Zoufalým zákazníkům konkurence pak řekneme, že pokud měli původně pokoj  $m$ , u nás najdou jistě volný pokoj  $2m - 1$ .

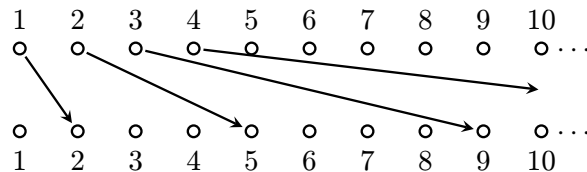
Kdyby bylo v okolí  $N$  Hilbertových hotelů a u všech našli šváby (to začíná být drobet podezřelé), tak nejprve své hosty přemístíme podle schématu  $n \mapsto (N + 1)n$ . Když si nakreslíte obrázek, uvidíte, že v našem hotelu teď bude vždy  $N$  pokojů volných, pak jeden obsazený, pak zase  $N$  volných a jeden obsazený atd. Lidi z prvního zavřeného hotelu pak pošlete na první pokoj v každém volném bloku, lidi z druhého hotelu na druhý pokoj v každém volném bloku atd. Matematicky, hosta z pokoje  $m$  v hotelu  $k$  pošleme na místo  $(N + 1)(m - 1) + k$ . Tohle opravdu volá po tom, abyste si nakreslili obrázek pro nějaké rozumné  $N$  (já jsem si kreslil případ  $N = 3$ ).

△

Poslední výsledek z Hilbertova hotelu přesvědčivě ukazuje, že konečný počet kopií  $\mathbb{N}$  je zase stejně velký jako  $\mathbb{N}$ . Protože  $\mathbb{N}$  je zástupcem všech spočetných množin, dalo by se očekávat, že sjednocení konečně mnoha spočetných množin je zase spočetné. Je to pravda a potvrdíme si to oficiálním tvrzením, ale až později, protože v tom tvrzení toho bude ještě víc.

**Příklad 9c.e:** Vraťme se k Hilbertově hotelu. Představme si, že se v okolí postaví nekonečně mnoho Hilbertových hotelů, ale abychom to nepřehnali, nechť je jich spočetně, tedy dají se očíslovat  $k = 1, 2, \dots$ . Všechny jsou plné, i my máme plno, ale najednou se všichni jejich zákazníci (nekonečně krát nekonečně mnoho) objeví u nás a chtějí se ubytovat. Dá se to zvládnout? Ano.

Klíčem je následující rozprostření.



Takže první volný prostor má jedno místo, druhý má dvě místa, třetí má tři místa, čtvrtý čtyři a tak dále. Není těžké spočítat, že správný vzorec pro úvodní přesun našich vlastních hostů je  $n \mapsto \frac{1}{2}n^2 + \frac{3}{2}n$ .

Pak si zavoláme zákazníky z prvního vyprázdněného hotelu a dáme do každé skupiny prázdných míst jednoho z nich. První prázdná skupina se tím zaplní, ale počínaje druhou nám zbyde nekonečně mnoho prázdných skupin, jejichž velikosti jdou 1,2,3 atd. Do každé z nich dáme jednoho zákazníka z druhého vyprázdněného hotelu, původně druhá volná skupina je teď už také plná, ale zase jich zbývá nekonečně mnoho a mají kapacitu postupně 1,2,3, ... atd. Je vcelku jasné, že tento postup se nikde nezarazí, dokážeme tak dojít k libovolnému vyprázdněnému hotelu a jeho hosty ubytovat u nás.

Můžete si odvodit vzoreček, kam poslat hosta z hotelu  $k$ , který tam bydlel na pokoji  $m$ .

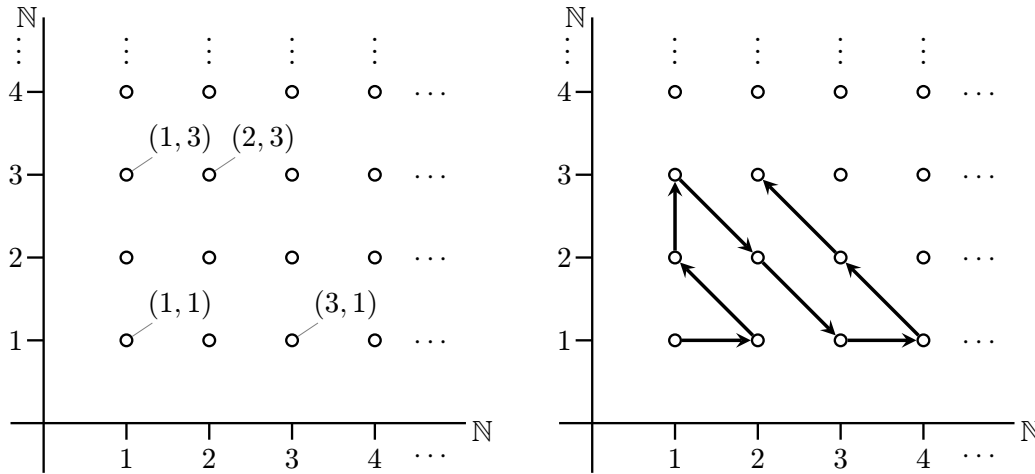
Prostě Hilbertův hotel je třída. Až se někdy doslechnete, že někde v Arabském zálivu staví opravdu ale opravdu vysoký hotel, vzpomeňte si na tento příklad.

△

Takže do  $\mathbb{N}$  se vejde dokonce nekonečně mnoho (přesněji spočetně mnoho) kopií  $\mathbb{N}$ . Tento výsledek naznačuje, že můžeme vzít spočetně mnoho spočetných množin, sjednotit je a vznikne zase spočetná množina. Než se konečně dostaneme k oficiálnímu tvrzení, podívejme se na ten výsledek jinak. Jak si vlastně představíme spočetně mnoho kopií  $\mathbb{N}$ ? Obvykle jsme si  $\mathbb{N}$  zobrazovali jako řadu koleček (řekněme vodorovnou), která se na jednu stranu jakoby táhne do nekonečna (třeba doprava). Druhou kopii  $\mathbb{N}$  si můžeme zakreslit na ni, třetí ještě nad ni a tak dále. Vznikne čtvercová síť koleček, která se táhne směrem doprava a nahoru bez omezení. Čtvercová síť, to připomíná obrázek kartézského součinu.

**Příklad 9c.f:** Jaká je mohutnost množiny  $\mathbb{N} \times \mathbb{N}$ ?

Zde máme dvojrozměrnou síť bodů, která se táhne do nekonečna ve dvou směrech, doprava a nahoru (obrázek vlevo). Je evidentně nekonečná, proto  $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$ , viz fakt 9c.6.



Je spočetná? Jinak řečeno, dokázali bychom tuto síť celou očíslovat? Ano, obrázek vpravo naznačuje jak. Cestička nám ukazuje, jak postupně číslovat neboli vybírat hodnoty pro zobrazení  $T: \mathbb{N} \mapsto \mathbb{N} \times \mathbb{N}$ . 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 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. Takovému názorné představě nám pomáhají vypěstovat správnou intuici o nekonečných množinách.

Důkaz: Díky faktu 9c.6 již máme  $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$ , stačí tedy dokázat  $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$  neboli najít prosté zobrazení z  $\mathbb{N} \times \mathbb{N}$  do  $\mathbb{N}$ . Definujme  $T(m, n) = 2^m 3^n$ . Evidentně pro  $m, n \in \mathbb{N}$  platí  $T(m, n) \in \mathbb{N}$ , takže jde  $\mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ . 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  $2^m 3^n = 2^u 3^v$ . 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.

Poznamenejme, že jsou i jiné vzorce, jak zobrazit prostým způsobem  $\mathbb{N} \times \mathbb{N}$  do  $\mathbb{N}$ , k jednomu lze dojít i z pohádky o Hilbertově hotelu.

△

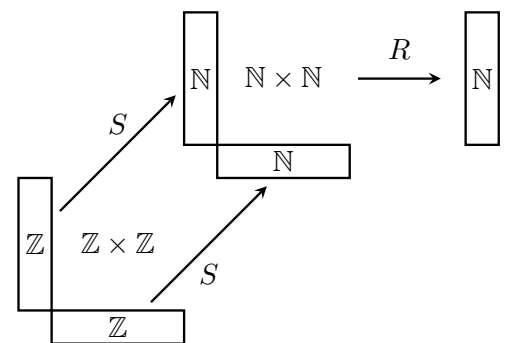
Důkaz byl typický. Při porovnávání dvou mohutností máme obvykle jeden směr téměř zdarma, zajímavější pak je druhý, při kterém zkoušíme vnořit zdánlivě „větší“ množinu do „menší“. Teď do posledního výsledku zakomponujeme již dokázanou spočetnost  $\mathbb{Z}$ .

**Příklad 9c.g:** Jaká je mohutnost množiny  $\mathbb{Z} \times \mathbb{Z}$ ? Tvrdíme, že stejná jako  $\mathbb{Z}$ , což je spočetná velikost. Šlo by zase udělat vzorec, třeba se povrtat v  $U(m, n) = 2^{|m|+m} 3^{|m|-m} 5^{|n|+n} 7^{|n|-n}$ , ale zajímavější bude zkombinovat již známé výsledky.

Již víme, že  $|\mathbb{Z}| = |\mathbb{N}|$ , proto musí existovat bijekce  $S$  ze  $\mathbb{Z}$  na  $\mathbb{N}$ . Dle 9c.f existuje také bijekce  $R$  z  $\mathbb{N} \times \mathbb{N}$  na  $\mathbb{N}$ . Pomocí nich teď definujeme zobrazení  $T(m, n) = R(S(m), S(n))$ . Tvrdíme, že je to bijekce  $\mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{N}$ .

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

Prostota: Nechť  $(m, n), (u, v) \in \mathbb{Z} \times \mathbb{Z}$  splňují  $T(m, n) = T(u, v)$ . Pak podle definice  $T$  máme  $R(S(m), S(n)) = R(S(u), S(v))$ . Protože je  $R$  prosté, musí platit  $(S(m), S(n)) = (S(u), S(v))$  v  $\mathbb{N} \times \mathbb{N}$  neboli  $S(m) = S(u)$  a  $S(n) = S(v)$ . Protože je  $S$  bijekce, platí  $m = u$  a  $n = v$  neboli  $(m, n) = (u, v)$  v  $\mathbb{Z} \times \mathbb{Z}$ .



Všimněte si, že jsme pracovali s bijekcemi  $S$  a  $R$ , o kterých jsme vůbec nevěděli, jak vlastně vypadají, jen jsme se odvolávali na jejich vlastnosti. Začínáme se stávat matematiky.

△

Hned dostáváme zajímavý důsledek.

**Věta 9c.11.**

Množina racionálních čísel  $\mathbb{Q}$  je spočetná.

**Důkaz (poučný):** Protože  $\mathbb{N} \subseteq \mathbb{Q}$ , platí  $|\mathbb{N}| \leq |\mathbb{Q}|$ . Potřebujeme ještě opačnou nerovnost.

Uvažujme zobrazení  $T: \mathbb{Z} \times \mathbb{N} \mapsto \mathbb{Q}$  dané vzorcem  $T(p, q) = \frac{p}{q}$ . Protože lze každé racionální číslo zapsat jako zlomek  $\frac{p}{q}$  s  $p \in \mathbb{Z}$  a  $q \in \mathbb{N}$ , je toto zobrazení zjevně na, proto dle věty 9c.1  $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}|$ . Máme také  $\mathbb{Z} \times \mathbb{N} \subseteq \mathbb{Z} \times \mathbb{Z}$  neboli  $|\mathbb{Z} \times \mathbb{N}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$ , dle tranzitivity proto  $|\mathbb{Q}| \leq |\mathbb{N}|$ . □

Tím, že jsme dokázali  $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ , se nám také otevřela cesta k důkazu, že sjednocením spočetně mnoha spočetných množin nevznikne nic většího, zase to bude spočetná množina. Tento výsledek se často používá při zkoumání mohutnosti množin, takže si jej uvedeme ve dvou praktických podobách.

**Fakt 9c.12.**

- (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.

Bylo by pěkné, kdybychom mohli prostě každou z množin  $A_n$  „posadit“ na jeden řádek oné čtvercové sítě pomocí vhodné bijekce, ale má to několik zádrhelů. Ve větě připouštíme množiny nejvýše spočetné, takže mohou být i konečné. S prázdnými se vypořádáme snadným technickým trikem, u těch konečných neprázdných to bude chtít něco víc. Nabízí se myšlenka, že konečné i spočetné množiny nabízejí prosté zobrazení  $A_n \mapsto \mathbb{N}$ , které by šlo využít k vytvoření kopie množiny  $A_n$  na řádku  $\{(i, n) : i \in \mathbb{N}\}$ . Má to ale problém, o kterém se podrobněji rozepíšeme po důkazu, až bude čtenář lépe vidět do detailů. V této nemilé situaci nás zachrání věta 9c.1, která pro případ  $|A_n| \leq |\mathbb{N}|$  nabízí zobrazení z  $\mathbb{N}$  na  $A_n$ , to nám bude stačit.

**Důkaz (poučný):** (i): Kdyby byly všechny množiny prázdné, tvrzení platí. Předpokládejme tedy, že alespoň jedna z množin je neprázdná, třeba  $A_N$ . Pak můžeme přejít k množinám  $B_n$ , definovaným tak, že  $B_n = A_n$  pro  $A_n \neq \emptyset$  a  $B_n = A_N$  pro  $A_n = \emptyset$ . Pak jsou  $B_n$  nejvýše spočetné, neprázdné a  $\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} B_n$ .

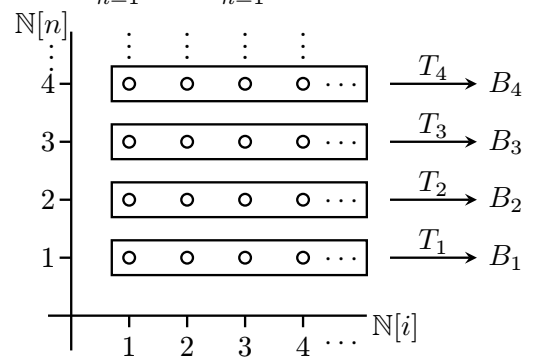
Protože jsou  $B_n$  neprázdné a nejvýše spočetné neboli  $|B_n| \leq |\mathbb{N}|$ , existují podle věty 9c.1 zobrazení  $T_n$  z  $\mathbb{N}$  na  $B_n$ . Pak definujeme zobrazení  $T$  z  $\mathbb{N} \times \mathbb{N}$  na  $\bigcup_{n=1}^{\infty} B_n$  předpisem  $T(i, n) = T_n(i)$ . Protože  $T(i, n) \in B_n$ , je určitě  $T(i, n) \in \bigcup_{n=1}^{\infty} B_n$ , takže jsme cílovou množinu určili správně. Tvrdíme, že zobrazení je na tuto množinu.

Vezměme libovolné  $b \in \bigcup_{n=1}^{\infty} B_n$ . Pak musí existovat  $n \in \mathbb{N}$  takové, že  $b \in B_n$ . Protože je  $T_n$  zobrazení na  $B_n$ , najdeme  $i \in \mathbb{N}$  takové, že  $T_n(i) = b$ . Pak  $(i, n) \in \mathbb{N} \times \mathbb{N}$  a  $T(i, n) = T_n(i) = b$ .

Zobrazení  $T$  je tedy na, podle faktu 9c.1 je  $\left| \bigcup_{n=1}^{\infty} A_n \right| = \left| \bigcup_{n=1}^{\infty} B_n \right| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ .

(ii): Podle (i) máme  $\left| \bigcup_{n=1}^{\infty} A_n \right| \leq |\mathbb{N}|$ .

Protože jsou všechny  $A_n$  neprázdné, existuje pro každé  $n \in \mathbb{N}$  nějaké  $a_n$ . Definujme zobrazení  $T(n) = a_n$ , pak určitě  $T: \mathbb{N} \mapsto \bigcup_{n=1}^{\infty} A_n$ . 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  $|\mathbb{N}| \leq \left| \bigcup_{n=1}^{\infty} A_n \right|$ . □



Tato věta je jedním z oblíbených nástrojů, jak poznávat spočetné množiny. Uvidíme jej v akci níže.

**9c.13 Poznámka:** Vraťme se k otázce, proč jsme nevyužili předpokladu  $|A_n| \leq |\mathbb{N}|$  a nepracovali s prostým zobrazením  $T_n$  z  $A_n$  do  $\mathbb{N}$ , což je intuitivně velmi příjemné, jakoby zasouváme množinu  $A_n$  do  $\mathbb{N}$ . Předpisem  $a \mapsto (T_n(a), n)$  se pak vyrobí kopie  $A_n$  v  $n$ -tém řádku sítě.

Pak se nabízí přirozená definice pro zobrazení  $T$  z  $\bigcup_{n=1}^{\infty} A_n$  do  $\mathbb{N} \times \mathbb{N}$ . Každé  $a \in \bigcup_{n=1}^{\infty} A_n$  leží v nějakém  $A_n$ , takže můžeme definovat  $T(a) = (T_n(a), n)$ . Zásadní problém je v tom, že dotyčné  $a$  klidně může ležet ve více množinách



$A_n$ , my si ale nemůžeme dovolit poslat jej na více míst (to by pak  $T$  nebylo zobrazení). Šlo by z toho vybruslit volbou preferovaného zástupce, ale důkaz se tím zkomplikuje. Námí zvolený postup se problémům vyhne.

△

Udělejme si malou inventuru. Zjistili jsme, že máme nekonečné množiny, jmenovitě  $\mathbb{N}$ , jejíž mohutnost jsme nazvali spočetnost. Pak jsme zjistili, že spočetných množin je více (třeba  $\mathbb{Z}$  a  $\mathbb{Q}$ ), a že množiny jiných nekonečných mohutností nelze získat zmenšením. Potvrdili jsme také, že když sjednotíme nekonečně (spočetně) mnoho spočetných množin, zase bude výsledek spočetný. Viděli jsme také, že nám příliš nepomůže kartézský součin dvou množin, indukci se to dá zobecnit na libovolný konečný kartézský součin. Spočetná mohutnost je tedy značně rezistentní i vůči zvětšování množin. Vkrádá se myšlenka, zda vůbec jsou nějaké nespočetné množiny. Nezavedli jsme ten pojem zbytečně?

Čtenář si jistě všiml, že jsme ještě nezkoumali jednu populární množinu, což je velmi podezřelé.

**Věta 9c.14.**

Interval reálných čísel  $\langle 0, 1 \rangle$  je nespočetný.

**Důkaz (poučný):** Ukážeme, že žádné zobrazení  $T: \mathbb{N} \mapsto \langle 0, 1 \rangle$  nemůže být na. Pro účely tohoto důkazu si budeme čísla z intervalu  $\langle 0, 1 \rangle$  zapisovat jako čísla s nekonečným desetinným rozvojem. To se dá vždy zařídít, například  $0.347 = 0.3469999\dots$

Vezměme tedy libovolné zobrazení  $T: \mathbb{N} \mapsto \langle 0, 1 \rangle$ . Vytvoříme číslo  $b$ , které neleží v  $\text{ran}(T)$ . Začíná „0.“ a pak doplňujeme desetinné číslice tak, aby se číslice na  $k$ -tém místě vždy lišila od  $k$ -té desetinné číslice čísla  $T(k)$ . To má velmi pěknou grafickou interpretaci, když si čísla  $T(k)$  vypíšeme do řádků, viz příklad napravo.

Musíme přesně specifikovat, jak to děláme, z mnoha možností si vybereme třeba tuto: Zvolíme trojku. Podíváme se na  $k$ -tou cifru v rozvoji čísla  $T(k)$  a jestliže není „3“, tak do našeho čísla  $b$  jako  $k$ -tou cifru dáme právě „3“ (ať se lišíme). Kdyby ta  $k$ -tá desetinná cifra v  $T(k)$  byla trojka, tak do našeho čísla dáme řekněme „1“. Dostaneme tak číslo  $b$ , které začíná „0.“ a tudíž určitě leží v  $\langle 0, 1 \rangle$ . 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.

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

Formálně: Zapišeme hodnoty  $T$  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

$$b = \sum_{k=1}^{\infty} b_k 10^{-k} \text{ neleží v } \text{ran}(T).$$

□

Celá tahle záležitost je další výzvou pro naši intuici. Asi všichni žijeme v představě, že když vezmeme papír a začneme pod sebe psát čísla 1, 2, 3,  $\dots$ , 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  $\langle 0, 1 \rangle$  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, máme přece nekonečno času. Důkaz je ale nemilosrdě jasný, nejde to, tak to musíme akceptovat a zvyknout si na to. Nespočetné množiny existují a jsou (nepředstavitelně?) velké.

U takto neintuitivního výsledku je dobré, když člověk důkazu dobře rozumí, aby mu uvěřil. Zde může čtenáře napadat spousta otázek, jedna populární vypadá takto: Proč by stejný trik nešel s množinou  $\mathbb{Q}$ ? Když se pokusíme vypsát racionální čísla pod sebe, tak přece také můžeme projít diagonálou a vytvořit  $b$ . Zde je finta v tom, že aby bylo  $b$  prvkem  $\mathbb{Q}$ , tak by ten rozvoj, který vytváříme, musel být nutně periodický, ale to tím diagonálním trikem nejsme schopni zajistit. Ještě se k té metodě vrátíme, je užitečná a říká se jí „Cantorův diagonální argument“. Nejdříve dořešíme situaci ohledně populárních množin.

**Důsledek 9c.15.**

Množina reálných čísel  $\mathbb{R}$  je nespočetná.

**Důkaz (rutinní):** Protože  $\langle 0, \infty \rangle \subseteq \mathbb{R}$ , platí  $|\langle 0, 1 \rangle| \leq |\mathbb{R}|$  a tedy existuje zobrazení  $T$  z  $\mathbb{R}$  na  $\langle 0, \infty \rangle$ . Kdyby byla  $\mathbb{R}$  spočetná, tak najdeme bijekci  $S$  z  $\mathbb{N}$  na  $\mathbb{R}$ . Zobrazení  $T \circ S$  by pak bylo z  $\mathbb{N}$  na  $|\langle 0, 1 \rangle|$ , ale tuto možnost jsme již vyloučili.

□

Pro jiné možnosti vedení důkazu viz cvičení 9c.4.

Víme už, že množina  $\mathbb{Q}$  je spočetná, což znamená, že množina iracionálních čísel musí být nutně nespočetná (viz cvičení 9c.15). 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  $\langle n, n+1 \rangle$  má stejnou mohutnost jako  $\langle 0, 1 \rangle$ , viz také cvičení 9c.11. Protože  $\mathbb{R} = \bigcup_{n=-\infty}^{\infty} \langle n, n+1 \rangle$  je sjednocení spočetného souboru intervalů, které mají všechny stejnou mohutnost jako  $\langle 0, 1 \rangle$ , tak bychom si podobně jako u spočetných množin tipnuli, že  $\mathbb{R}$  nebude větší než jedna ze složek. To pravidlo o sjednocení opravdu platí, viz obecná věta 9c.18, takže máme  $|\mathbb{R}| = |\langle 0, 1 \rangle|$ . Dokážeme přímo obecnější tvrzení.

**Věta 9c.16.**

Pro libovolné  $a, b \in \mathbb{R}$  splňující  $a < b$  platí

$$|(a, b)| = |\langle a, b \rangle| = |(a, b)| = |\langle a, b \rangle| = |\mathbb{R}|.$$

**Důkaz (poučný):** 1) Nejprve dokážeme, že  $|(a, b)| = |\mathbb{R}|$ . Uvažujme  $T(x) = \frac{1}{x-b} + \frac{1}{x-a}$  coby zobrazení  $(a, b) \mapsto \mathbb{R}$ . Pomocí derivace se snadno ukáže, že  $T$  je klesající funkce neboli prosté zobrazení a že limity v krajních bodech jsou nekonečno a mínus nekonečno, tedy obor hodnot je  $\mathbb{R}$ . Proto je  $T$  bijekce a důkaz je hotov. (Náčrtněte si graf  $T$ .)

2) Ostatní rovnosti plynou z inkluzí, všechny intervaly jsou podmnožinou  $\mathbb{R}$  a nadmnožinou  $(a, b)$ . Pro každý takový interval  $I$  pak máme  $|(a, b)| \leq |I|$  a  $|I| \leq |\mathbb{R}|$ , vzhledem k části (i) to vlastně je  $|\mathbb{R}| \leq |I|$  a  $|I| \leq |\mathbb{R}|$ , odtud díky větě 9c.5  $|I| = |\mathbb{R}|$ . □

Důkaz by šlo snadno upravit i pro případy, kdy  $a = -\infty$  nebo  $b = \infty$ . Mimochodem ta podmínka  $a < b$  je podstatná, vylučuje tzv. degenerované intervaly jako  $\langle 13, 13 \rangle = \{13\}$  či  $\langle 13, 13 \rangle = \emptyset$ .

Mohutnost množiny reálných čísel či intervalu  $\langle 0, 1 \rangle$  je další ze základních mohutností, které se objevují často. Potkali jsme tedy dvě základní mohutnosti, mohutnost spočetných množin (která se v teorii množin značí  $\aleph_0$ , jde o hebrejské písmeno alef) a mohutnost „kontinua“ neboli  $|\mathbb{R}|$  (v teorii množin ji značíme  $c$ ). Dá se říct, že při běžné matematické práci se s jinými mohutnostmi nekonečných množin už nepotkáme.

Zejména v diskrétní matematice je dobré umět u různých množin poznat, zda jsou spočetné či nespočetné. Je mezi nimi podstatný rozdíl při praktické práci. Množiny spočetné mohou být očíslovány čili zapsány jako  $A = \{a_1, a_2, \dots\}$ . Proto pro ně funguje matematická indukce (konečná či nekonečná), je to přesně parketa diskrétní matematiky. Naopak do množin nespočetných nedokážeme pomocí postupného počítání ani pořádně nahlédnout, takže jsou povětšinou mimo dosah metod diskrétní matematiky a budeme se jim vyhýbat. Kde je vlastně rozmezí mezi těmito množinami? Podíváme se na dva velmi typické příklady.

**Příklad 9c.h:** Dokážeme, že množina  $A$  konečných řetězců vytvořených ze znaků 0 a 1 (tzv. binárních řetězců) je spočetná.

Umíme kombinatoricky spočítat, kolik je binárních řetězců určité dané délky, ale tady se délka mění. Pomůžeme si tak, že množinu  $A$  rozdělíme na podmnožiny právě podle délky řetězců, na každou se pak podíváme zvlášť. Jdeme na to.

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, jinak řečeno nejvýše spočetná. Množiny  $A_n$  jsou neprázdné a navzájem disjunktní, podle faktu 9c.12 je  $A = \bigcup_{n=1}^{\infty} A_n$  spočetná.

△

**Příklad 9c.i:** Dokážeme, že množina  $B$  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, procházením diagonály, vždy volíme znak, který na ní není. Při formálním zápisu nám pomůže, že u binárních číslic se „jiná číslice“ vytvoří snadno pomocí vzorečku  $1 - x$  (ověřte).

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

$$\begin{array}{r} a_1 : \quad \boxed{1} \ 0 \ 1 \ 0 \ \dots \\ a_2 : \quad 0 \ \boxed{0} \ 0 \ 0 \ \dots \\ a_3 : \quad 1 \ 1 \ \boxed{0} \ 0 \ \dots \\ a_4 : \quad 0 \ 0 \ 1 \ \boxed{1} \ \dots \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \hline b : \quad 0 \ 1 \ 1 \ 0 \ \dots \end{array}$$

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

△

Tento příklad ukázal podstatu Cantorovy diagonální metody. Jakmile vybíráme na nekonečně mnoho míst, přičemž vybíráme svobodně alespoň ze dvou možností (čímž Cantorovi umožníme volit „něco jiného“ na diagonále), pak vzniká nespočetná množina. Je samozřejmě nutné, aby výsledný prvek ležel ve zkoumané množině. Právě proto Cantorův diagonální argument nezabere u předchozího příkladu.

Představme si, že jsme ty konečné řetězce srovnali pod sebe a procházíme diagonálou. První problém je, že řetězce jsou konečné, tudíž se může stát, že na diagonále v nějakém řádku nenajdeme nic. To ale znamená, že můžeme volit libovolně a od dotyčného řádku se lišíme, je to vlastně v pořádku. Klíčová otázka je, kdy skončíme.

Pokud se zastavíme po konečném počtu kroků, tak vzniklý konečný řetězec sice v  $A$  leží, ale nemůžeme vyloučit, že úplně stejný není v některém z dalších řádků (a on tam samozřejmě bude, množina je spočetná). Když se tedy pokusíme tabulku projít až do konce, tak vznikne nekonečný řetězec, který v  $A$  neleží a tudíž nevzniká spor se spočetností.

Stejným způsobem si také rozmyslíme, proč nelze diagonálním trikem ukázat, že je množina  $\mathbb{Q}$  nespočetná. My bychom sice mohli racionální čísla srovnat pod sebe, pak procházet diagonálu a vytvořit číslo s nekonečným desetinným rozvojem, které v seznamu neleží, jenže nedokážeme zajistit, aby toto číslo bylo v  $\mathbb{Q}$ , tam jsou totiž jen taková čísla, jejichž desetinný rozvoj je periodický.

Je také snadné si představit, že diagonální metodu aplikujeme na vektory. I ty lze psát pod sebe, namísto číslic pracujeme s jednotlivými souřadnicemi. Například binární řetězce délky 3 lze vnímat jako třísložkové vektory, jejich množinu lze pak zapsat jako  $\{0, 1\} \times \{0, 1\} \times \{0, 1\} = \{0, 1\}^3$ . Množina  $A$  z dotyčného příkladu je pak vlastně zapsatelná jako  $A = \bigcup_{n=1}^{\infty} \{0, 1\}^n$ . Dostáváme se tak zase k již zmíněnému výsledku, že když uděláme kartézský součin konečně mnoha spočetných množin, je výsledek spočetný. Intuitivně řečeno, pokud se objekty naší množiny podobají konečným vektorům se souřadnicemi vybíranými z nejvýše spočetné množiny, například  $\mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ , tak je ta množina spočetná.

Na druhou stranu, pokud pracujeme s vektory nekonečnými (čemuž odpovídá kartézský součin nekonečně množin) a máme svobodnou volbu souřadnic, vzniká množina nespočetná.

Množina nespočetná také vznikne, pokud povolíme nespočetnou množinu na některé souřadnici. Třeba  $\mathbb{N} \times \mathbb{R} \times \mathbb{N}$  je určitě nespočetná, protože obsahuje kopii  $\mathbb{R}$ , například má podmnožinu  $\{(13, r, 14) : r \in \mathbb{R}\}$ , která je kopií  $\mathbb{R}$  skrz bijekci  $r \mapsto (13, r, 14)$ .

Naopak i nekonečné vektory mohou tvořit spočetnou množinu, pokud omezíme výběr souřadnic.

**Příklad 9c.j:** 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 *ppphhhhh...* Tvrdíme, že množina  $A$  takovýchto řetězců je spočetná.

Tady je zajímavý ten dělicí 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 9c.12 je  $A$  spočetná.

Alternativa: Pro  $\alpha \neq \beta \in \{a, b, c, \dots, z\}$  nechť je  $A_{\alpha\beta}$  množina všech řetězců, které začínají písmenem  $\alpha$  a končí písmenem  $\beta$ . Jak je taková množina velká? Písmeno  $\beta$  může začít od pozice 2, 3, 4, ..., taková množina je tedy spočetná. Máme také  $A = \bigcup_{\alpha, \beta} A_{\alpha, \beta}$  a jde o sjednocení konečně mnoha množin, podle věty 9c.18 (v) je  $A$  spočetná.

Ukážeme si ještě jeden přístup. Množiny poměříme bijekcemi, které lze chápat jako kódování. Představme si, že bychom řetězce z naší množiny chtěli zapsat v počítači, a to samozřejmě úsporným způsobem. Zkušeného programátora rychle napadne, že by na zápis daného řetězce měla stačit tři čísla: kód prvního znaku (třeba ASCII), počet jeho výskytů, kód druhého znaku. Vzniká tak zobrazení  $a \mapsto (x, y, z)$ , které vede  $A \mapsto \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ . Není na, ale to nevadí. Snadno si rozmyslíme, že toto zobrazení je prosté, proto  $|A| \leq |\mathbb{N}^3| = |\mathbb{N}|$ .

△

V této kapitole jsme viděli řadu přístupů, jak k množině najít a dokázat její mohutnost. Shrňme si to pro množiny nekonečné (u konečných je to snadné).

## S 9c.17 Jak určovat mohutnost

Základem je znát množiny, které jsme zkoumali výše, tvoří porovnávací škálu. Je také třeba vědět, že mohutnost neovlivní spočetné sjednocení a konečný kartézský součin. Pomocí těchto znalostí pak odhadujeme (a dokazujeme) mohutnosti množin jiných.

### 1) Porovnání pomocí inkluze

Toto je jedna z nejjednodušších metod, jak omezit mohutnost dané množiny shora či zdola. Pokud se podaří získat omezení obdobného typu z obou stran, máme vyhráno. Pokud se snažíme o důkaz spočetnosti, lze jeden směr získat snadno, každá nekonečná množina  $A$  splňuje  $|\mathbb{N}| \leq |A|$ . Pak už jen stačí najít směr opačný. Například množina sudých čísel je podmnožinou  $\mathbb{Z}$  a hned vidíme, že je spočetná.

### 2) Porovnání pomocí bijekce

Jde vlastně o nalezení způsobu, jak dané objekty zakódovat pomocí objektů, které již známe. Například matice vyloženě volá po tom, abychom dali její řádky za sebe a tím ji zakódovali jako vektor, o kartézském součinu už máme hotové výsledky. Podobně lze kódovat polynomy pomocí koeficientů (vzniknou zase vektory), přímky pomocí průsečíků s osami a podobně. Takovéto zakódování pak často dá bijekci. Do mohutnosti výsledku pak výrazně promluví, odkud se při vytváření objektů vybírají jejich složky, například matice mohou mít prvky celočíselné (pak jsou totožné s  $\mathbb{Z}^{n \cdot m}$ ), ale také reálné, pak je kódujeme pomocí  $\mathbb{R}^{n \cdot m}$ .

### 3) Vnoření

Jde o kombinaci předchozích dvou postupů, kdy danou množinu nezkoušíme najít přímo jako podmnožinu jiné, ale vytváříme její kopii. Například reálná čísla určitě nebudou podmnožinou množiny  $\mathbb{R}^3$ , ale umíme si tam vytvořit kopii  $\mathbb{R}$  předpisem  $r \mapsto (0, r, 0)$  či jiným, čtenář si jistě takových vnoření hravě vymyslí tucty. Výhoda je, že nemusíme ověřovat, že toto zobrazení je na (ono také není), stačí ověřit prostotu a již máme jednu nerovnost mezi mohutnostmi.

Kombinování strategií je obvyklé a často účinné. Například množina  $M$  všech matic  $4 \times 4$  v dolním trojúhelníkovém tvaru s celočíselnými prvky je určitě podmnožinou množiny všech matic  $4 \times 4$  s celočíselnými prvky, která je spočetná díky bijekci na  $\mathbb{Z}^{16}$ . Proto je  $M$  spočetná. To by šlo dokázat i přímo vytvořením bijekce, dolní trojúhelníkové matice  $4 \times 4$  mají obecně 10 nenulových prvků a tudíž se nabízí kódování těchto matic vektory ze  $\mathbb{Z}^{10}$ .

### 4) Rozklad

Tato metoda obvykle přichází vhod ve chvíli, kdy máme kandidáta na kódování, ale cílový prostor není jednoznačně určen či vychází komplikovaněji, než by se nám líbilo. Mnohdy pak pomůže si situaci rozdělit na případy.

Pokud máme například zkoumat množinu  $M$  všech čtvercových matic nad  $\mathbb{Z}$ , tak víme, že si každou  $n \times n$  matici umíme zakódovat pomocí vektoru ze  $\mathbb{Z}^{n^2}$ , obrazem takového kódování jsou pak ale vektory rozdílných délek. To by se dalo zvládnout, prohlásíme za cílový prostor množinu  $\bigcup_{n=1}^{\infty} \mathbb{Z}^{n^2}$ , o které umíme odvodit, že je spočetná, ale stejně dobrou alternativou je množinu  $M$  rozdělit podle velikosti na podmnožiny  $M_n$  matic velikosti  $n \times n$ .

△

Čtenář si tyto strategie může nacvičit ve cvičení 9c.7 a 9c.8.

Vraťme se k obecné problematice nekonečných množin. Máme teď dvě mohutnosti nekonečných množin, množiny spočetné a množiny mohutnosti  $\mathbb{R}$  neboli mohutnosti  $\aleph_0$  a  $c$ . Jsou ještě nějaké jiné mohutnosti nekonečných množin než tyto dvě? Jde vlastně o dvě otázky.

Tou první je, jak to vypadá mezi  $\mathbb{N}$  a  $\mathbb{R}$ . Skrývá se tam ještě nějaká další mohutnost? Tuto otázku si kladl již Cantor a myslel si, že tam nic není, po mohutnosti spočetných množin by hned měla následovat mohutnost  $\mathbb{R}$ . Myslí si to i mnoho dalších matematiků, říká se tomu Hypotéza kontinua. Bohužel, „hypotéza“ se říká věcem, které bychom rádi, ale neumíme je dokázat. Cantor se o to marně snažil celý život, po něm byli další, až přišel v 50. letech 20. století zajímavý výsledek. Matematici dokázali dokázat, že dokázat či vyvrátit hypotézu kontinua není v rámci standardní teorie množin možné. Protože tuto teorii množin (ZFC) už úspěšně používáme asi sto let, musíme se s tím smířit. Můžeme se tedy rozhodnout, že hypotézu kontinua přijmeme mezi axiomy a dostaneme 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. Pro lidi, kteří s množinami pracují na naší úrovni, je to jedno, rozdíl mezi teoriemi s HC a bez HC nepoznáme.

Podívejme se tedy na druhou otázku: Jsou ještě nějaké mohutnosti za  $c$ ? A pokud ano, jak se k nim dokážeme dostat?

Už jsme viděli, že kategorie spočetných množin je značně odolná vůči různým manipulacím (sjednocení, kartézský součin). Platí to dokonce o všech nekonečných množinách, takže tudy cestička nevede.

**Věta 9c.18.**

(i) Nechť  $A_i$  pro  $i = 1, \dots, m$  nebo  $i \in \mathbb{N}$  jsou množiny, kde  $A_1$  je nekonečná, a necht'  $|A_i| \leq |A_1|$  pro všechna  $i$ . Pak  $\left| \bigcup_i A_i \right| = |A_1|$ .

(ii) Nechť  $A_i$  pro  $i = 1, \dots, n$  jsou neprázdné množiny, kde  $A_1$  je nekonečná, a necht'  $|A_i| \leq |A_1|$  pro všechna  $i$ . Pak  $|A_1 \times A_2 \times \dots \times A_n| = |A_1|$ .

Důkazy jsou značně netriviální, dokonce už i jednoduchý případ dvou množin  $|A \cup B| = |A|$  pro  $|B| \leq |A|$  vyžaduje hluboký ponor do teorie množin.

Prakticky řečeno, když spojujeme množiny sjednocením (až spočetně mnoha) nebo kartézským součinem (konečně mnoha), tak nikdy nedostaneme nic většího, než co jsme vložili. Vidíme tam ale možnou skulinu, nekonečné kartézské součiny. S těmi se ale nepracuje nejlépe, zejména když si položíme otázku, kolik těch množin vlastně „násobíme“, takže se preferuje jiný přístup.

Připomeňme si, že je-li  $A$  množina, pak  $P(A)$  značí množinu 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  $2 \cdot 2 \cdot \dots \cdot 2 = 2^{|A|}$  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, to souhlasí. Mimochodem, a co prázdná množina, platí to i pro ni?  $P(\emptyset) = \{\emptyset\}$ , takže má velikost  $1 = 2^0 = 2^{|\emptyset|}$ . Ano, funguje to.

**Fakt 9c.19.**

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 platí  $|A| < |P(A)|$ , následující věta nám o zobecní.

**Věta 9c.20.** (Cantorova)

Pro každou množinu  $A$  platí  $|A| < |P(A)|$ .

**Důkaz** (poučný, možná drsný): Ukážeme, že libovolné zobrazení  $T: A \mapsto P(A)$  nemůže být na. Necht' 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.

Necht'  $M = \{a \in A : a \notin T(a)\}$ . 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  $b \in M$ . 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, kdykoliv nám někdo dá nějakou strašlivě velkou množinu, vždycky ji můžeme rovnou vzít a vyrobit pomocí ní a této věty množinu ještě mohutnější.

Dostáváme se tak k poslední otázce ohledně mohutnosti. Když jsme se zkusili dostat od  $\mathbb{N}$  k větším číslům, našli jsme  $\mathbb{R}$ . Cantorova věta teď nabízí jinou možnost, množinu  $P(\mathbb{N})$ . Není to náhodou totéž?

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 1d.8 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  $\langle 0, 1 \rangle$  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  $\langle 0, 1 \rangle$ . Snadno se ale nahlédne, že těch nejednoznačných čísel je jen spočetně, což je vzhledem k velikosti  $\langle 0, 1 \rangle$  pod úrovní rozpoznatelnosti. Mohutnost  $R$  je tedy stejná jako mohutnost  $\langle 0, 1 \rangle$  neboli mohutnost  $\mathbb{R}$ .

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

Na závěr ještě jednu zajímavost. Naše úvahy o mohutnosti byly založeny na pojmu zobrazení. Kolik jich existuje?

**Fakt 9c.21.**

Nechť  $A, B$  jsou konečné neprázdné 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  $|B^A| = |B|^{|A|}$ , to vypadá moc pěkně. Teď to spojíme s jiným tématem. 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. Toto lze udělat obecně pro libovolnou množinu  $M$  pomocí indikátorové funkce, viz cvičení 9a.22. To znamená, že  $M$  má tolik podmnožin, kolik jsme schopni vytvořit indikátorových zobrazení, a to nejen ve smyslu počtu (pro konečné množiny), ale i pro množiny nekonečné, tedy ve smyslu mohutnosti.

**Fakt 9c.22.**

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

**Důkaz (poučný):** Pro každou podmnožinu  $M$  množiny  $A$  máme indikátorové zobrazení  $\chi_M: A \mapsto \{0, 1\}$  dané  $\chi_M(a) = \begin{cases} 1, & a \in M; \\ 0, & a \notin M \end{cases}$  (viz cvičení 9a.22). 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  $\chi$  dává podmnožinu  $M$ , ze které pochází, jmenovitě množinu tvořenou těmi prvky z  $A$ , kde je  $\chi$  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.

**Cvičení**

**Cvičení 9c.1 (poučné):** Dokažte, že jestliže množiny  $A, B$  splňují  $|A| = |B|$ , tak  $|A| \leq |B|$  a  $|B| \leq |A|$ . Viz fakt 9c.4.

**Cvičení 9c.2:**

Nechť  $A$  je spočetná množina. Dokažte, že pak je i  $A \cup \{a\}$  spočetná.

**Cvičení 9c.3 (poučné):** Uvažujme následující definici: Pro množiny  $A, B$  řekneme, že  $|A| < |B|$ , jestliže  $|A| \leq |B|$ , ale neplatí  $|A| = |B|$ . Dokažte následující tvrzení: Nechť  $A, B, C$  jsou množiny.

- (i) Jestliže  $|A| < |B|$  a  $|B| \leq |C|$ , pak  $|A| < |C|$ . (iv) Jestliže  $|A| < |B|$  a  $|B| = |C|$ , pak  $|A| < |C|$ .  
(ii) Jestliže  $|A| \leq |B|$  a  $|B| < |C|$ , pak  $|A| < |C|$ . (v) Jestliže  $|A| = |B|$  a  $|B| < |C|$ , pak  $|A| < |C|$ .  
(iii) Jestliže  $|A| < |B|$  a  $|B| < |C|$ , pak  $|A| < |C|$ .

**Cvičení 9c.4 (poučné):** Dokázali jsme, že množina  $\mathbb{R}$  je nespočetná, sporem a vytvořením bijekce. Dokončete další dva způsoby, jak to dokázat.

(i) Sporem: Předpokládejte, že  $|\mathbb{R}| = |\mathbb{N}|$ . Inkluze  $\langle 0, 1 \rangle \subseteq \mathbb{R}$  pak dává  $|\langle 0, 1 \rangle| \leq |\mathbb{N}|$ . Ukažte, že platí i opačná „nerovnost“ a jejich spojením dojdete ke sporu s něčím, co už známe.

(ii) Dokažte  $|\mathbb{N}| < |\mathbb{R}|$  přímo pomocí faktu 9c.14 a cvičení 9c.3.

**Cvičení 9c.5 (dobré, poučné):** Dokažte, že jestliže  $|A| = |B|$ , pak  $|P(A)| = |P(B)|$ .

**Cvičení 9c.6** (rutinní, poučné): Dokažte, že jestliže  $|A| = |B|$  a  $|C| = |D|$ , pak  $|A \times C| = |B \times D|$ .

**Cvičení 9c.7** (rutinní): Rozhodněte, zda jsou následující množiny spočetné či ne. Pokud ano, dokažte to.

- (i) Množina  $M$  záporných celých čísel;
- (ii) množina  $M$  sudých celých čísel;
- (iii) množina  $M$  celých násobků 13;
- (iv) množina  $M$  celých čísel větších než 23;
- (v) množina  $M$  lichých záporných celých čísel;
- (vi) množina  $M$  celých čísel, která nejsou násobkem tří;
- (vii) množina  $M$  racionálních čísel, která jsou mezi 0 a  $\frac{1}{2}$ ;
- (viii) množina  $M$  všech binárních řetězců neobsahujících 0;
- (ix) množina  $M$  všechna kladných racionálních čísel, jež nelze napsat pomocí jmenovatele menšího než 4;
- (x) množina  $M$  reálných čísel neobsahujících 0 v desetinném rozvoji;
- (xi) množina  $M$  reálných čísel obsahujících pouze konečný počet číslic 1 v zápisu v desítkové soustavě;
- (xii) množina  $M$  reálných čísel, jejichž zápisy v desítkové soustavě obsahují pouze číslice 1;
- (xiii) množina  $M$  reálných čísel, jejichž zápisy v desítkové soustavě obsahují pouze číslice 1 nebo 3.

**Cvičení 9c.8** (poučné): Rozhodněte, zda jsou následující množiny spočetné či ne. Pokud ano, dokažte to.

- (i) Množina  $M$  matic  $2 \times 2$  s celočíselnými prvky;
- (ii) množina  $M$  polynomů, které mají celočíselné koeficienty;
- (iii) množina  $M$  přímek v rovině;
- (iv) množina  $M$  přímek v rovině vedoucích skrz bod  $(13, 23)$ ;
- (v) množina  $M$  přímek v rovině vedoucích skrz bod  $(13, 23)$  s celočíselnými směrnici;
- (vi) množina  $M$  trojúhelníků v rovině, jejichž vrcholy mají celočíselné souřadnice;
- (vii) množina  $M$  trojúhelníků v rovině, jejichž strany mají celočíselné délky.

**Cvičení 9c.9** (rutinní): Dokažte, že množina všech slov je nejvýše spočetná.

**Cvičení 9c.10** (rutinní): Dokažte, že množina všech programů v jistém programovacím jazyce je spočetná.

**Cvičení 9c.11** (poučné):

(i) Dokažte podle definice, že libovolný konečný interval  $\langle a, b \rangle$  pro  $a < b$  má stejnou mohutnost jako  $\langle 0, 1 \rangle$ .

Nápověda: Zkuste nejprve interval typu  $\langle 0, B \rangle$ .

(ii) Najděte co nejvíce prostých reálných funkcí, které převádějí konečný interval na nekonečný či naopak. Odvoďte nějaká tvrzení o mohutnosti, která lze pomocí nich získat.

**Cvičení 9c.12** (poučné): Dokažte podle definice, že množina  $\mathbb{R}$  má stejnou mohutnost jako interval  $(0, \infty)$ .

**Cvičení 9c.13** (poučné): Dokažte, že nadmnožina nespočetné množiny je nespočetná.

**Cvičení 9c.14** (poučné): Dokažte, že je-li  $A$  nespočetná a  $B$  spočetná množina, pak musí být  $A - B$  nespočetná.

**Cvičení 9c.15** (dobré, poučné):

Uvažujte množinu  $M = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a > b\}$ . Na této množině definujeme 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  $a = 2$ .

$b \rightarrow$	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

Toto cvičení bude po vás chtít důkaz klíčového faktu: Že hodnoty v řádcích a při přeskočení na další řádek rostou o dva. Dokažte tedy následující:

(i) Pro každé  $a \geq 2$  a pro každé  $2 \leq b < a$  platí  $S(a, b) = S(a, b - 1) + 2$ .

(ii) Pro každé  $a \geq 2$  platí  $S(a + 1, 1) = S(a, a - 1) + 2$ .

Poznámka: Pomocí (i) a (ii) se pár jednoduchými úvahami dokáže, že zobrazení dané vzorcem  $\frac{1}{2}S(a, b)$  je bijekce zobrazení z  $M$  na  $\mathbb{N}$ .

Poznámka: Zobrazení je inspirováno příběhem o Hilbertově hotelu, do kterého musíme vměstnat hosty z nekonečně mnoha hotelů, zde  $b$  je číslo hotelu a  $a$  číslo pokoje. Čteme-li čísla v jednotlivých sloupcích (tedy díváme se, jak jsou ubytováni hosté z jednoho hotelu), vidíme, že vznikají stále větší a větší mezery mezi pokoji, do kterých se postupně doplňují lidé z dalších hotelů (další sloupce).

**Cvičení 9c.16** (poučné): Použijte to, že  $\frac{1}{2}S(a, b)$  je bijekce 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 9c.17** (poučné): Dokažte, že zobrazení  $U(n) = (3n + 1)^2$  je prosté ze  $\mathbb{Z}$  do  $\mathbb{N}$ .

**Cvičení 9c.18** (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:

**9c.1:** Jestliže  $|A| = |B|$ , pak existuje bijekce  $T: A \mapsto B$ . Tato bijekce je i prostá, proto  $|A| \leq |B|$ , a je na, tedy  $|A| \geq |B|$ .

**9c.2:** Dle předpokladu existuje bijekce  $T$  z  $\mathbb{N}$  na  $A$ . Pak zobrazení dané  $S(1) = a$ ,  $S(n) = T(n - 1)$  pro  $n \geq 2$  je bijekce z  $\mathbb{N}$  na  $A \cup \{a\}$ .

**9c.3:** (i): Předpoklad dává prostá zobrazení  $T: A \mapsto B$  a  $S: B \mapsto C$ . Pak je  $S \circ T$  prosté  $A \mapsto C$  a proto  $|A| \leq |C|$ . 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 prostá zobrazení  $T: A \mapsto B$  a  $S: B \mapsto C$ . Pak je  $S \circ T$  prosté  $A \mapsto C$  a proto  $|A| \leq |C|$ . 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  $|A| < |C|$ .

(iii): Z  $|A| < |B|$  dostáváme  $|A| \leq |B|$ , také  $|B| < |C|$ , proto podle (ii)  $|A| < |C|$ .

(iv) Z  $|B| = |C|$  máme  $|B| \leq |C|$ , pak použít (i). (v) Z  $|A| = |B|$  máme  $|A| \leq |B|$ , pak použít (ii).

**9c.4:** (i): Předpoklad  $|\mathbb{R}| = |\mathbb{N}|$  a  $\langle 0, 1 \rangle \subseteq \mathbb{R}$  dávají  $|\langle 0, 1 \rangle| \leq |\mathbb{N}|$ . Protože je  $\langle 0, 1 \rangle$  nekonečná množina, platí i  $|\mathbb{N}| \leq |\langle 0, 1 \rangle|$ . Podle věty pak  $|\langle 0, 1 \rangle| = |\mathbb{N}|$ , což je spor s faktem 9c.14.

(ii) Protože je  $\langle 0, 1 \rangle$  nekonečná množina, platí i  $|\mathbb{N}| \leq |\langle 0, 1 \rangle|$ . Fakt 9c.14 z toho udělá  $|\mathbb{N}| < |\langle 0, 1 \rangle|$ . Díky inkluzi také  $|\langle 0, 1 \rangle| \leq |\mathbb{R}|$ , podle cvičení 9c.3 tedy  $|\mathbb{N}| < |\mathbb{R}|$ .

**9c.5:** 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  $S(M) = S(N) \implies T[M] = T[N] \implies T^{-1}T[M] = T^{-1}T[N] \implies M = N$ , zde se použilo cvičení 9a.19.  $S$  je na, pro  $N \in P(B)$  je  $N \subseteq B$ , definujeme  $M = T^{-1}[N]$ , pak  $S(M) = TT^{-1}[N] = N$ .

**9c.6:** 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:  $U(a, b) = U(x, y) \implies (T(a), S(b)) = (T(x), S(y)) \implies T(a) = T(x) \wedge S(b) = S(y) \implies a = x \wedge b = y \implies (a, b) = (x, y)$ , použila se prostota  $T, S$ .

Na: Nechť  $(x, y) \in B \times D$ .  $T, S$  jsou na, proto  $\exists a \in A: T(a) = x$  a  $\exists b \in C: S(b) = y$ . Pak  $(a, b) \in A \times C$  a  $U(a, b) = (T(a), S(b)) = (x, y)$ .

**9c.7:** (i): Spočetná, je to nekonečná podmnožina spočetné množiny  $\mathbb{Z}$ . Alternativa: Přímý důkaz,  $T(n) = -n$  je zobrazení z  $M$  do  $\mathbb{N}$ , evidentně je na i prosté:  $T(n) = T(m) \implies -n = -m \implies m = n$ .

(ii): Spočetná, je to nekonečná podmnožina spočetných celých čísel. Přímý důkaz bijekcí:  $T(n) = 2n$  je bijekce ze spočetné množiny  $\mathbb{Z}$  na  $M$ . 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:  $T(n) = 13n$  je bijekce ze spočetné množiny  $\mathbb{Z}$  na  $M$ . 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,  $T(n) = n - 23$  je zobrazení z  $M$  do  $\mathbb{N}$ , neboť pak je  $T(n)$  celé a  $T(n) \geq 1$ . 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  $\{\frac{1}{n} : n \in \mathbb{N}\}$ , 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 v řetězci  $r$ , je to prosté zobrazení  $M$  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  $\{\frac{2k+1}{8} : k \in \mathbb{N}\}$ , 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  $(m, n) \in \mathbb{N} \times (\mathbb{N}_0 \cup \{\infty\})$ , kde  $m$  je počet jedniček před desetinnou tečkou a  $n$  počet jedniček za ní.

(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.

**9c.8:** (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  $a_n x^n + \dots + a_1 x + a_0 \mapsto (a_n, a_{n-1}, \dots, a_0)$ , pak spočetné sjednocení spočetných je spočetné.

(iii): Nespočetná, obsahuje nespočetnou podmnožinu všech vodorovných přímk  $\{y = a : a \in \mathbb{R}\}$ . 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 přímku lze 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): Nespočetná, tyto přímky lze jednoznačně 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  $\mathbb{R} \cup \{\infty\}$ , 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.

**9c.9:** 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 nejvýše spočetná. Takže množina 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.

**9c.10:** 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.

**9c.11:** (i): Interval  $\langle 0, 1 \rangle$  převedeme na  $\langle 0, B \rangle$  pomocí  $x \mapsto Bx$ .

Obecně:  $T(x) = a + (b - a)x$  je bijekce z  $\langle 0, 1 \rangle$  na  $\langle a, b \rangle$ . Definice má smysl, pro  $0 \leq x \leq 1$  je  $a \leq T(x) \leq b$ . Prostě:  $T(x) = T(y) \implies a + (b - a)x = a + (b - a)y \implies x = y$ . Je na: Dáno  $y \in \langle a, b \rangle$ , pak existuje  $x = \frac{y-a}{b-a} \in \langle 0, 1 \rangle$  takové, že  $T(x) = y$ .

(ii):  $T(x) = \arctg(x)$  je bijekce  $\mathbb{R} \mapsto (-\frac{\pi}{2}, \frac{\pi}{2})$ , množiny tedy mají stejnou mohutnost. Omezíme se na nezáporná čísla, mírná úprava:  $T(x) = \frac{2}{\pi} \arctg(x)$  je bijekce  $\langle 0, \infty \rangle \mapsto \langle 0, 1 \rangle$ . Obdobně lze pracovat s tangensem.

$T(x) = \ln(x)$  je bijekce  $(0, 1)$  na  $(-\infty, 0)$ , proto  $|(0, 1)| = |(-\infty, 0)|$ . Po úpravě:  $T(x) = -\ln(1 - x)$  dává bijekci z  $\langle 0, 1 \rangle$  na  $\langle 0, \infty \rangle$ .

$T(x) = \frac{1}{1-x}$  je bijekce  $(0, 1)$  na  $\langle 1, \infty \rangle$ . Pokud bychom chtěli dokázat  $|(0, 1)| = |\langle 0, \infty \rangle|$ , mohli bychom použít  $T(x) = \frac{1}{1-x} - 1 = \frac{x}{1-x}$ .

**9c.12:**  $T(x) = e^x$  je bijekce  $\mathbb{R}$  na  $(0, \infty)$ .

**9c.13:** Toto je jen obměna tvrzení z kapitoly, že podmnožina nejvýše spočetné množiny je nejvýše spočetná.

**9c.14:** 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.

**9c.15:** (i):  $S(a, b - 1) + 2 = (a - 1)(a - 2) + 2(b - 1) + 2 = (a - 1)(a - 2) + 2b = S(a, b)$ .

(ii):  $S(a, a - 1) + 2 = (a - 1)(a - 2) + 2(a - 1) + 2 = a^2 - a + 2 = a(a - 1) + 2 = S(a + 1, 1)$ .

**9c.16:** Nechť  $R: \mathbb{N} \times \mathbb{N} \mapsto M$  je dané  $R(m, n) = (m + n, m)$ . Je to bijekce. Prostě:  $R(m, n) = R(u, v) \implies (m + n, m) = (u + v, u) \implies m + n = u + v \wedge m = u \implies m = u \wedge n = v \implies (m, n) = (u, v)$ . 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  $R(m, n) = (x, y)$ .

Proto je také bijekcí  $T = \frac{1}{2}S \circ R$ , přičemž  $T(m, n) = \frac{1}{2}S(m + n, m) = \frac{1}{2}(m + n - 1)(m + n - 2) + m$  přesně dle zadání.

**9c.17:** 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  $|3x + 1| = |3y + 1|$ . Možnosti dle znaménka. Různá: 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.

**9c.18:** Definujme  $W(m, n) = (U(m), U(n))$ , pak je  $W$  prosté  $\mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{N} \times \mathbb{N}$ , viz např. cvičení 9c.6. Podle předchozích cvičení je  $T \circ W$  prosté  $\mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{N}$  a  $(T \circ W)(m, n) = T((3n + 1)^2, (3n + 1)^2) = V(m, n)$ .