

8. Zobrazení a posloupnosti

Pojem zobrazení je jedním ze základních matematických nástrojů. V této kapitole probereme jejich klíčové vlastnosti a pak se podíváme na svébytnou podskupinu zvanou posloupnosti.

8a. Zobrazení: Základní vlastnosti a operace

Jedním se základních nástrojů pro zkoumání přírody je pojem funkce. Čtenář se už s nimi jistě setkal, třeba s kvadratickou funkcí $y = x^2$ či $f(x) = x^2$. Běžné použití svádí k tomu, abychom funkce spojovali se vzorci, ale to by bylo příliš omezující.

Příklad 8a.a: Představme si, že v čase nula hodíme kámen, který naši ruku opouští rychlostí v_0 , a chceme vědět, jak se od nás vzdaluje. To zachytíme funkcí $d(t)$, která říká, jak daleko od nás kámen je v čase t pro $t \geq 0$. Evidentně $d(0) = 0$.

Pokud jsme kámen hodili uprostřed prázdnoty vesmíru, kde není nic, ani gravitace, pak se vzdaluje po přímce stále stejnou rychlostí a pro jeho vzdálenost máme povědomý vzorec $d(t) = v_0 t$. Puntičkáři dodají, že tento vzorec platí jen do doby, než se kámen dostane do oblasti s gravitací či mezihvězdnou hmotu.

Pokud jsme kámen hodili z věže postavené na Měsíci směrem dolů, tak je urychlován měsíční gravitací a vzdaluje se od nás po (svislé) přímce, přičemž vzdálenost se mění dle vzorce $d(t) = v_0 t + \frac{1}{2} g_M t^2$, který si čtenář možná ještě vybaví. Tentokrát vzorec platí do chvíle dopadu.

Pokud jsme kámen hodili ze střechy mrakodrapu na Zemi směrem dolů, tak se ke gravitaci přidá působení odporu vzduchu. Kámen poletí po svislé přímce dolů a nějaké měřicí zařízení nám bude schopno pro každé $t \geq 0$ zjistit jeho vzdálenost od nás. Vzdálenostní funkce $d(t)$ tedy existuje, pro konkrétní čas $t > 0$ je určena číselná hodnota $d(t)$. Jenže neexistuje algebraický vzorec, který by tuto funkci dokázal vyjádřit.

△

My samozřejmě preferujeme funkce dané vzorcem a ve škole se s jinými prakticky nesetkáváme, ale jak příklad ukazuje, nelze se omezovat jen na ně. Co je tedy funkce? Intuitivně vzato je to „posílátko“, které bere čísla a posílá je na jiná čísla. Například funkce $f(x) = x^2$ posílá $13 \mapsto 169$. Můžeme si funkci představit jako krabičku se vstupem a výstupem. Podstata konkrétní funkce je právě ve specifickém vztahu mezi čísly na vstupu a čísly na výstupu.

V kapitole o relacích jsme se naučili takové vztahy zaznamenávat pomocí uspořádaných dvojic. Bude to fungovat i pro funkce. Funkci $f(x) = x^2$ lze reprezentovat jako (možná nekonečnou) množinu dvojic typu (x, x^2) a je těmito dvojicemi přesně určena. Když budeme chtít vědět, kolik je $f(-7)$, tak najdeme v seznamu dvojic (a, b) takovou, kde $a = -7$, což je dvojice $(-7, 49)$. Proto $f(-7) = 49$.

Zde využíváme dvou nevyslovených předpokladů, které jsou podstatné. Tím prvním je, že musíme vědět, jaká čísla lze používat coby vstupy. Podobně jako u relací, také u funkcí je podstatný nejen mechanismus vztahu, ale i množina, na které je aplikován. Jak brzy uvidíme, uvažováním předpisu $f(x) = x^2$ pro $x \in \mathbb{R}$ vznikne jiná funkce, než když stejný předpis uvažujeme na množině $\langle 0, \infty \rangle$. Spořivý čtenář může chtít použít tento předpis na množině $\{-2, 0, 2\}$, takto vzniklou funkci pak jednoznačně zachytíme skromnou množinou dvojic

$$\{(-2, 4), (0, 0), (2, 4)\}.$$

Druhý nevyslovený předpoklad je, že když najdeme jednu dvojici (a, b) s $a = -7$, tak už se dozvíme $f(-7)$, protože víc takových dvojic není. Díky tomu má $f(-7)$ jednoznačný smysl, což je pro fungování funkcí klíčové. To znamená, že na rozdíl od relací se nespokojíme s jen tak nějakou množinou dvojic, ale budeme vyžadovat, aby se každé číslo posílalo jen na jeden cíl.

Směřujeme k definici, kdy vnímáme funkce jako speciální typ relace. Protože se matematici neradi zbytečně omezují, nabízí se nápad aplikovat tuto myšlenku také na jiné objekty než čísla. Můžeme si představit třeba černou skříňku, které dáváme písmenka a ona na oplátku vydává různá lízátka. I fungování takovéto skříňky by šlo zachytit jako množinu dvojic (písmenko, lízátko). Abychom ukázali, že jsme od přízemních funkcí přešli k něčemu abstraktnímu, použijeme vznešenější jméno.

!

Definice.

Nechť A, B jsou množiny. Podmnožina T množiny $A \times B$ se nazývá **zobrazení** z A do B , jestliže 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 $\text{ran}(T) = \{T(a); a \in A\}$.

Podmínku z definice lze formálně zapsat $\forall a \in A \exists! b \in B: (a, b) \in T$.

Někteří autoři pojem „zobrazení“ nezavádějí a hovoří o funkcích. Jde tedy o rovnocenné pojmy, jedni 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, funkce na \mathbb{N}), zatímco použitím slova „zobrazení“ čtenáři posíláme vzkaz, že právě pracujeme s obecnější situací. Přijde mi to praktické, ale upozorňuji, že to není univerzálně přijímáno.

Definice vlastně říká, že zobrazení jsou speciální případy relací. Nabízí se otázka, proč po uspořádání nepřišla kapitola nazvaná Speciální relace: Zobrazení. Důvodem je, že podmínka jednoznačné existence b z definice má masivní dopady na to, jak zobrazení fungují, a to zcela jinak než ostatní typy relací. Většina poznatků z kapitol o relacích nedává pro zobrazení smysl, například aplikace množinových operací na funkce nemá rozumnou interpretaci a navíc to ani obecně nejde, protože bychom jako výsledek nejspíše nedostali zobrazení, viz cvičení 8a.14. Stejně tak se na relace neaplikují vlastnosti relací, protože nenesou užitečnou informaci, viz cvičení 8a.15. Naopak je třeba zavést nové nástroje, které pro změnu nefungují u běžných relací. Jak záhy uvidíme, dokonce i pojmy, které jsou pro relace a zobrazení společné, budou u zobrazení specifické. Proto se s nimi nezachází jako se speciálními relacemi, ale zobrazení se bere jako samostatný pojem.

Je to ostatně vidět již v definici. Značení $(a, b) \in T$ odkazuje k relacím a v některých teoretických úvahách s ním budeme pracovat. Pro praktické použití se nabízí alternativní zápis $T(a) = b$, používá se také (zřídka) verze $T: a \mapsto b$, který odkazuje na intuitivní představu zobrazení coby posílatka a dává smysl právě díky tomu, že b je pro každé a jednoznačně určeno. Pro obecné relace toto značení nefunguje.

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 $a = \pm 2$).

Mimochodem, tím $T(a)$ se nesnažíme naznačit, že se dosazuje do nějakého vzorečku, protože ten ani nemusí existovat. Spíš to chápeme tak, že jsme a vsunuli do vstupu černé skříňky a čekáme, co z ní vyleze na druhém konci.

! Příklad 8a.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 také přirozenější zápis ve formě výčtu $T(\diamond) = 1, T(\bullet) = 13$.

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

△

Příklad 8a.c: Uvažujme A coby množinu všech studentů, kteří úspěšně složili alespoň jednu zkoušku, 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 předmětů; 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, tedy má jen jedno RČ? Teoreticky by tomu tak být mělo.

△

8a.1 Poznámka: V praxi se zobrazení obvykle používají v situaci, kdy množiny A, B nejsou prázdné, abychom měli s čím pracovat.

V případě, že $A = \emptyset$, je také $A \times B = \emptyset$ a tedy existuje jediná relace z A do B , jmenovitě $T = \emptyset$. Tato relace je také zobrazení, protože ke každému $a \in A$ (žádné není) opravdu existuje dvojice v T . Pokud to čtenáři přijde podivné, pak lze argumentovat tak, že v A neexistuje protipříklad proti tvrzení, že T je zobrazení.

Pokud je $B = \emptyset$, tak v případě $A = \emptyset$ existuje ono prázdné zobrazení $\emptyset \mapsto \emptyset$, jinak zobrazení z neprázdné A do \emptyset neexistuje vůbec. Pokud by totiž v A existovalo nějaké a , tak by mu případně zobrazení muselo přiřadit nějaký prvek z B , ale není co.

△

Je dobré zdůrazit, že zobrazení (a funkce) jsou kombinací tří informací: O tom, jak posílá vstupy na výstupy, což je reprezentováno symbolem T , a také tím, jaké vstupy se berou neboli identita množiny A (jinak nemůžeme v definici zkontrolovat splnění podmínky) a kam se posílají výstupy. Všechna tři písmenka v obrázku „ $T: A \mapsto B$ “ jsou tedy podstatná a prakticky se to projeví třeba ve chvíli, kdy chceme dvě zobrazení porovnávat.

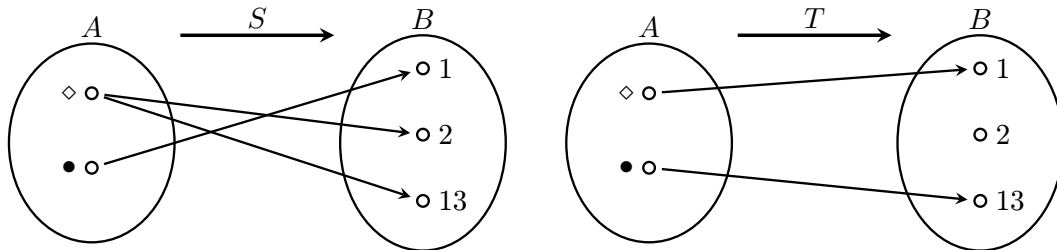
!

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 $T(a) = S(a)$.

Stručně: Shodná zobrazení musí posílat stejným způsobem a musí se shodovat vstupní a cílová množina. Ověřit shodu posílání u zobrazení, které nelze zapsat vzorcem, může být dobrodružné. Často vzorce máme a potřebujeme je porovnat. Zde je zajímavé vědět, že neexistuje a nemůže existovat spolehlivý algoritmus na rozpoznání, zda dva algebraické vzorce jsou si rovny. Ale v běžných situacích nám naše obvyklé triky stačí. 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.

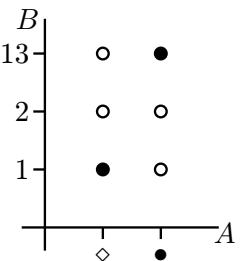
Při práci se zobrazeními často pomůže jejich grafické znázornění. Vzhledem k tomu, že zobrazení jsou speciální případy relace, můžeme použít graf tak, jak jej chápou relace. Níže vidíme grafy pro relaci S a zobrazení T z příkladu 8a.b.



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 nějaká a nemá šipku žádnou, nebo jich má více. Vysoce užitečná je tato představa také při teoretických úvahách.

Jak do tohoto příběhu zapadá graf běžně používaný pro reálné funkce? Je dán jako množina bodů $(x, f(x))$ v \mathbb{R}^2 . U obecného zobrazení T jde o množinu $(a, T(a))$, což je vlastně T samotné coby relace. Je možné tyto dvojice zaznačit v tradičním obrázku pro $A \times B$, což je obdélníková síť bodů. V ní zvýrazníme dvojice ležící v T . Vidíme to na obrázku pro zobrazení T z příkladu 8a.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.



Jakmile umíme posílat někam prvky, tak už umíme posílat i celé množiny, prostě je pošleme po jednotlivých prvcích. Můžeme 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

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

Vrátíme-li se k příkladu 8a.b, tak

$$T[\{\diamond\}] = \{T(\diamond)\} = \{1\}.$$

Také máme

$$T[\{\diamond, \bullet\}] = \{T(\diamond), T(\bullet)\} = \{1, 13\}.$$

Vlastně jsme počítali $T[A] = \text{ran}(T)$.

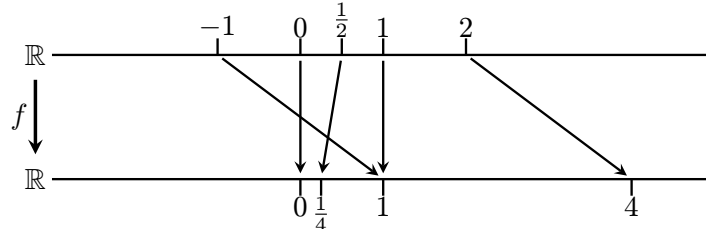
Máme také $T^{-1}[\{1\}] = T^{-1}[\{1, 2\}] = \{\diamond\}$, $T^{-1}[\{2\}] = \emptyset$.

Vždy $T^{-1}[B] = A$, protože každé $a \in A$ se zobrazí někam do B podle definice zobrazení.

Značení T^{-1} pro vzor se může plést se značením pro inverzní zobrazení (viz níže); vzor množiny se pozná podle hranaté závorky. Existuje vždy, i kdyby to měla být prázdná množina.

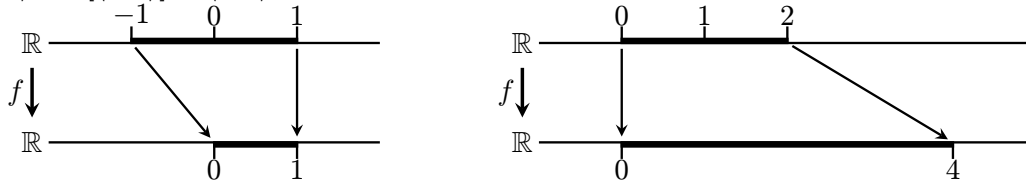
V případě, že naše zobrazení pracuje s nekonečnými množinami, je nemůžeme nakreslit celé, ale šipkové znázornění může být stále užitečné.

Příklad 8a.d: Uvažujme funkci $f(x) = x^2$ coby zobrazení $\mathbb{R} \mapsto \mathbb{R}$. Víme, že jejím grafem je parabola, ale jako posílátka ji lépe vystihne šipkový graf. V rámci úspory místa jej otočíme, šipky teď vedou shora dolů, takže nahoře vidíme definiční obor jako vodorovnou přímku a dole cílovou množinu.



Snadno si rozmyslíme, že $f\{-2, 0, 2, 13\} = \{0, 4, 169\}$ a $f^{-1}\{1, 2\} = \{-1, 1, -\sqrt{2}, \sqrt{2}\}$.

Rozmyslíme si, že intervaly se přenášejí zase na intervaly, neboli že obraz intervalu je interval. Například $T[[-1, 1]] = \langle 0, 1 \rangle$ a $T[\langle 0, 2 \rangle] = \langle 0, 4 \rangle$. Šipková vizualizace to dokáže zachytit.



Vzory intervalů už nemusí být zase intervaly, například $f^{-1}[(1, 4)] = (-2, -1) \cup (1, 2)$.

△

Některé pojmy má smysl přenést z relací na zobrazení, i když s určitými specifiky. Začneme situací, kdy máme zobrazení $T: A \mapsto B$, ale zjistíme, že nás vlastně zajímá jen na nějaké podmnožině M definičního oboru A . U relací k tomu slouží pojem restrikce, který umožňuje zúžit vstupní či cílovou množinu. U zobrazení je ale zužování cílové množiny problematické, protože by se tím mohla vyloučit nějaká klíčová dvojice.

Proto u zobrazení omezuje pouze vstupní množinu, tedy při přechodu z $D(T)$ na podmnožinu M vybereme jen takové dvojice z T , jejichž první souřadnice je v M . Snadno si rozmyslíme, že ve výsledné množině dvojic se každý prvek M vyskytne v právě jedné dvojici, tedy tato nová množina dvojic je zase zobrazení. Protože jsou dvojice přebrány z původního zobrazení, nové zobrazení posílá prvky z M stejným způsobem jako to původní, což vede na definici restrikce v jazyce zobrazení.

! **Definice.**

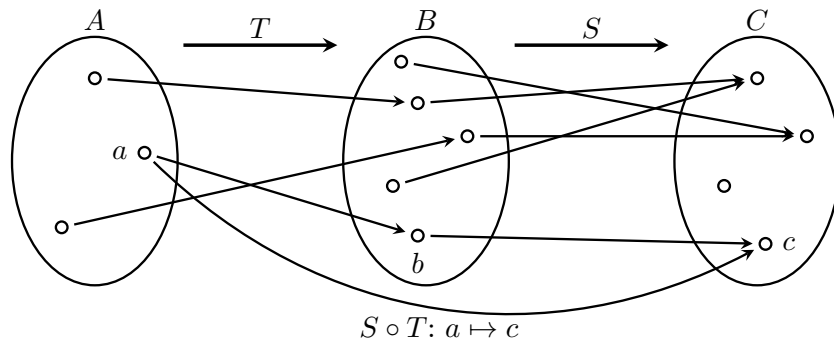
Nechť $T: A \mapsto B$ je zobrazení, nechť $M \subseteq A$. Definujeme **restrikci** zobrazení T na M , značeno $T|_M$, jako zobrazení z M do B definované

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

Zobrazení T z příkladu 8a.b může být omezeno například na podmnožinu $M = \{\diamond\}$, vznikne pak restrikce $T|_M: M \mapsto B$ definovaná vzorcem $T|_M(\diamond) = 1$.

Restrikce je u funkcí velmi užitečným nástrojem, například bychom se bez ní neobešli při definici funkcí jako odmocnina či arkustangens.

Významnou roli hraje u zobrazení skládání. Jeho definici lze přímo převzít od relací, jako obvykle budeme chtít pracovat jazykem přiřazení. Uvažujme zobrazení $T: A \mapsto B$ a $S: B \mapsto C$. Dvojice (a, c) je ve složené relaci $S \circ T$ (upozorníme na pořadí, T jde první, S druhé), pokud existuje $b \in B$ takové, že $(a, b) \in T$ a $(b, c) \in S$.



Protože je 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 $b \in B$. 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 $S \circ T$. Což je ta druhá podstatná věc: Pokud složíme zobrazení T a S jako relace, bude také výsledná relace $S \circ T$ zobrazením.

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

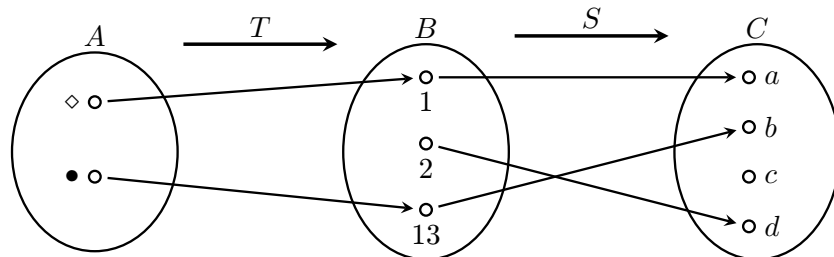
$$(S \circ T) : a \mapsto S(T(a)) \text{ pro } a \in A.$$

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 $a \in A$.

Tak jsme se konečně dozvěděli, proč se kdysi matematici rozhodli pro nepřirozené pořadí ve značení skládání. Dosazení a totiž vypadá takto: $T(S(a))$, první použité zobrazení je vpravo, to následné vlevo. Odtud zkratka $S(T)$ pro složené pořadí, což zase dává $S \circ T$. Mi to tedy přijde jako dost chabá výmluva, ale co s tím nadělám.

Příklad 8a.e: Uvažujme naše známé T z příkladu 8a.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 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.

Čtenář si může rozmyslet, že pokud bude k zobrazením přistupovat podle definice, tedy

$$T = \{(\diamond, 1), (\bullet, 2)\}, \quad S = \{(1, a), (2, d), (13, b)\},$$

tak skládání podle definice pro relace dá stejný výsledek jako podle definice pro zobrazení.

△

Poznámka: Vidíme, že nápad s navazováním funguje vždy, když je možné hodnoty T dosadit do S . Vlastně tedy nepotřebujeme, aby se cílová množina T rovnala definičnímu oboru S . Klidně bychom mohli definovat skládání pro zobrazení $T: A \mapsto B$ a $S: C \mapsto D$ s podmínkou, že $\text{ran}(T) \subseteq C$. Vznikla by zcela funkční a navíc obecnější definice, která by lépe odpovídala tomu, co potkáváme běžně u funkcí. Nicméně není to v obecné teorii zobrazení zvykem. Pokud se s takovou situací potkáme, dokážeme se požadavku naší definice přizpůsobit tím, že místo S vezmeme restrikcí $S|_B$, kde už množiny navazují jako v definici a z hlediska výsledku to vyjde nastejno.

△

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 není zaručeno správné navázání množin. Možná budeme mít štěstí a $A = C$, ale ani pak ještě není vyhráno.

Příklad 8a.f: Uvažujme množinu $A = \{1, 2\}$ a zobrazení $U, V: A \mapsto A$ definovaná takto:

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

neboli $U = \{(1, 2), (2, 1)\}$ a $V = \{(1, 1), (2, 1)\}$.

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

△

Příklad 8a.g: Vraťme se teď k tomu, co čtenář dobře zná, k reálným funkcím. Uvažujme funkce $f(x) = x^2$ a $g(x) = x + 13$ coby zobrazení $\mathbb{R} \mapsto \mathbb{R}$, 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 také začít 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 8a.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 8a.8. Proto se na komutativitu nedá spoléhat, naštěstí ji obvykle ani nepotřebujeme. Mnohem významnější praktický dopad má asociativita, kterou u skládání relací máme a zdědí ji tedy také skládání zobrazení.

!

Věta 8a.2.

Nechť $T: A \mapsto B$, $S: B \mapsto C$ a $R: C \mapsto D$ jsou zobrazení. Pak platí $(R \circ S) \circ T = R \circ (S \circ T)$.

Formálně je to důsledek faktu 4a.9, ale když bereme zobrazení jako svébytnou kategorii, tak budeme chtít i důkaz jazykem přiřazení.

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, ale 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 přepíšeme pomocí definice:

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

tedy hodnoty $((R \circ S) \circ T)(a)$ a $(R \circ (S \circ T))(a)$ jsou stejné. □

U relací byla ještě jedna zajímavá operace, přechod k inverzní relaci (obrácení směru šipek). Podobná věc by se nám hodila také u funkcí a zobrazení. Pokud například máme zobrazení „člověk $\mapsto \mathbb{R}^{\mathbb{C}}$ “, pak jistě někdy potřebujeme proces opačný, kdy k číslu hledáme člověka. V tomto případě ovšem není možné jen aplikovat relační definici na zobrazení.

Příklad 8a.h: Uvažujme zobrazení T z příkladu 8a.b. Pokud jej bereme jako relaci $T = \{(\diamond, 1), (\bullet, 13)\}$, pak existuje inverzní relace $T^{-1} = \{(1, \diamond), (13, \bullet)\}$. Toto ale není zobrazení z B do A , protože chybí dvojice pro $2 \in B$. \triangle

My samozřejmě potřebujeme, aby operace prováděné se zobrazeními zase vyráběly zobrazení. Příklad ukazuje, že u myšlenky obracení směru šipek se musíme smířit s tím, že to občas nepůjde. Nabízí se udělat definici, která by říkala, že inverzní zobrazení se dělá jako inverzní relace za předpokladu, že zase vznikne zobrazení. Fungovalo by to, ale preferujeme vyjádření jazykem přiřazení.

Nepřijatá definice fungovala tak, že aplikací relační inverze na zobrazení T vznikne kandidát S , který bude přijat, pokud je to zobrazení. My to otočíme: Budeme procházet kandidáty S , což už budou libovolná zobrazení, a testovat, zda správně souvisí s T . Co tedy od zobrazení vzniklého obrácením šipek očekáváme?

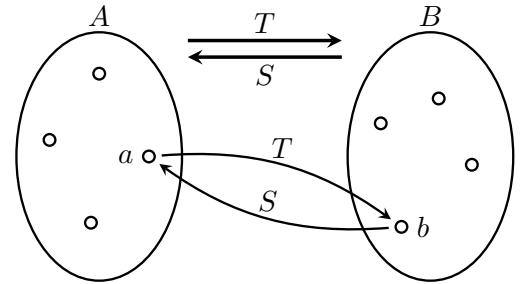
Uvažujme dvojici $(a, b) \in T$ neboli $T(a) = b$. Pokud nějaké inverzní zobrazení S existuje, tak by mělo mít $(b, a) \in S$ neboli $S(b) = a$. Obrázek vcelku výstižně naznačuje, oč jde. Jestliže T někam pošle a , tak S by ten cíl mělo přeposlat zpět.

Zajímavá interpretace je, když vnímáme T jako jakousi akci, která něco provede s prvkem a , třeba jej transformuje v něco jiného. Správný kandidát S na inverzní zobrazení by tuto akci měl neutralizovat, tedy dostáváme zpět to, s čím jsme začali. Vzniká tak kolečko, které matematicky vyjádříme rovností $S(T(a)) = a$.

Tato podmínka je v jazyce zobrazení, tedy má správnou podobu. Chtěli bychom ji mít splněnou pro všechny prvky a .

Ukazuje se nicméně, že tato podmínka ještě nezaručí, že S má stejné dvojice jako T , jen v opačném pořadí, viz příklad 8a.i 2b. Je proto nutné přidat ještě jednu podmínku, kdy to kolečko začneme v prvku $b \in B$ a používáme nejdřív S a pak T : $T(S(b)) = b$.

Ukážeme, že tato dvě kolečka neboli to, že se T a S navzájem neutralizují, pozná správné zobrazení otáčející šipky z T . Pro úplnost přidáme další praktickou podmínku, která vznikne z podmínky (i) prostým přepisem do jazyka přiřazení.



Fakt 8a.3.

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

- (i) $S = \{(b, a) \in B \times A; (a, b) \in T\}$ a je to zobrazení $B \mapsto A$.
- (ii) S je zobrazení $B \mapsto A$ a splňuje
 - $S(T(a)) = a$ pro všechna $a \in A$,
 - $T(S(b)) = b$ pro všechna $b \in B$.
- (iii) S je zobrazení $B \mapsto A$ a pro všechna $a \in A, b \in B$ platí
 - $S(b) = a$ právě tehdy, když $T(a) = b$.

Všimneme si, že jsme u všech třech podmínek museli zahrnout požadavek, že S je zobrazení $B \mapsto A$. U (ii) a (iii) jsme zobrazení potřebovali na to, aby šlo psát $S(b)$ a tedy mělo smysl formulovat testy, ale ty samy o sobě ještě nedokážou vynutit, aby toto S šlo $B \mapsto A$, takže i to musíme zahrnout do podmínek.

Důkaz (poučný):

1) (i) \implies (ii): Podle (i) je S zobrazení $B \mapsto A$.

Vezměme nějaké $a \in A$, označme $b = T(a)$. Pak $(a, b) \in T$, proto $(b, a) \in S$ neboli $S(b) = a$. Odtud $S(T(a)) = S(b) = a$.

Vezměme $b \in B$. Protože je podle (i) S zobrazení $B \mapsto A$, tak musí existovat $a = S(b) \in A$, tedy $(b, a) \in S$. Podle definice S pak $(a, b) \in T$ neboli $T(a) = b$. Pak $T(S(b)) = T(a) = b$.

2) (ii) \implies (i): Máme zobrazení $S: B \mapsto A$, čímž je splněn druhý požadavek z (i). Uvažujme S jako množinu dvojic.

Nechť $(b, a) \in S$. Pak $S(b) = a$, tudíž také $T(a) = T(S(b)) = b$ podle druhé podmínky v (ii). To znamená $(a, b) \in T$. Ukázali jsme, že $S \subseteq \{(b, a) \in B \times A; (a, b) \in T\}$.

Teď vezměme $(b, a) \in \{(b, a) \in B \times A; (a, b) \in T\}$. Pak $T(a) = b$ a tedy $S(b) = S(T(a)) = a$ podle (ii), tedy $(b, a) \in S$. Proto $\{(b, a) \in B \times A; (a, b) \in T\} \subseteq S$.

3) (i) \iff (iii): $S = \{(b, a); (a, b) \in T\}$ lze ekvivalentně přepsat podmínkou

$$\forall a \in A \forall b \in B : (b, a) \in S \iff (a, b) \in T.$$

Protože předpokládáme, že T i S jsou zobrazení, můžeme to přepsat do jazyka přiřazení a dostaneme (iii) a naopak. □

Víme, jak definovat, co potřebujeme.

! Definice.

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

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

Pak jej značíme T^{-1} .

Pokud T^{-1} existuje, tak 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**.

Pokud čtenáři výrazy $S(T(a))$ a $T(S(b))$ připomněly skládání, tak míří správně. Vrátime se k tomu v části 8a.7. Jako důsledek faktu 8a.3 dostáváme, že pokud T^{-1} existuje, tak je jediné možné, jmenovitě jde o onu inverzi ve smyslu relace. Má tedy praktický smysl zavést pro něj značení T^{-1} . Podmínky z definice pak mají podobu $T^{-1}(T(a)) = a$ a $T(T^{-1}(b)) = b$. To má užitečnou interpretaci: Pokud se ve výrazu potkají T a T^{-1} vedle sebe, tak se jakoby navzájem zkrátí a zmizí. To se občas hodí, třeba při řešení rovnic.

Zatím jsme se soustředili na otázku, jak poznat existenci inverzního zobrazení. Jak poznáme, že dané T invertibilní není? Podle definice bychom měli vyzkoušet všechna možná zobrazení $S: B \mapsto A$ a vyloučit je, což není praktické. Naštěstí nám fakt 8a.3 říká, že jediný možný kandidát přichází z relační inverze, popřípadě předpisu v (iii), a pokud selže, tak již více nemusíme zkoušet.

! Příklad 8a.i:

1. Nechť $A = \{13, 14, 23\}$, $B = \{\alpha, \beta, \gamma\}$. Uvažujme zobrazení $T: A \mapsto B$ definované takto: $13 \mapsto \alpha$, $14 \mapsto \gamma$, $23 \mapsto \beta$. Mohli bychom také psát $T(13) = \alpha$, $T(14) = \gamma$, $T(23) = \beta$. Podle definice ovšem

$$T = \{(13, \alpha), (14, \gamma), (23, \beta)\}.$$

Původní myšlenka byla, že využijeme inverzi ze světa relací. Dostáváme novou relaci

$$S = \{(\alpha, 13), (\gamma, 14), (\beta, 23)\} = \{(\alpha, 13), (\beta, 23), (\gamma, 14)\}.$$

Prvky jsme seřadili podle první souřadnice, abychom snadno ověřili, že tato relace je zobrazení $B \mapsto A$. Splňuje tedy požadavky na to, co očekáváme od inverze. Díky tomu, že toto zobrazení vzniklo relační inverzí, splňuje také podmínku (iii) z faktu 8a.3, jmenovitě pro všechna $a \in A$, $b \in B$ platí ekvivalence

$$S(b) = a \iff T(a) = b.$$

Ověříme podle definice, že T je invertibilní a $S = T^{-1}$.

S je zobrazení z B do A , to souhlasí, testy:

$$\begin{aligned} S(T(13)) &= S(\alpha) = 13, & T(S(\alpha)) &= T(13) = \alpha, \\ S(T(14)) &= S(\gamma) = 14, & T(S(\beta)) &= T(23) = \beta, \\ S(T(23)) &= S(\beta) = 23, & T(S(\gamma)) &= T(14) = \gamma. \end{aligned}$$

Potvrdili jsme, že $S = T^{-1}$.

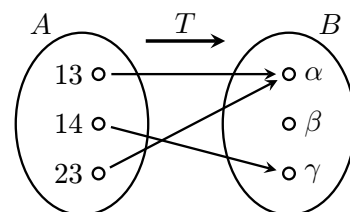
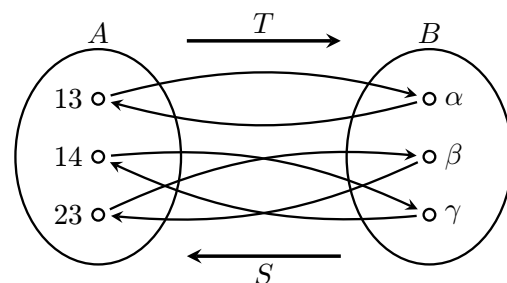
Příklad naznačuje, že definice pozná, kdy jsou věci tak, jak je chceme.

Správná definice by ovšem také měla poznat, kdy věci nefungují, jak by měly.

2. Zde naše T pozměníme, nově bude fungovat takto:

$$T(13) = \alpha, T(14) = \gamma, T(23) = \alpha \text{ neboli } T = \{(13, \alpha), (14, \gamma), (23, \alpha)\}.$$

Když přejdeme k inverzní relaci, dostáváme $S = \{(\alpha, 13), (\alpha, 23), (\gamma, 14)\}$. Toto není zobrazení, protože pro $\alpha \in B$ se najde víc než jedna dvojice, ve které na prvním místě vystupuje toto α . Navíc není dvojice, která by na prvním místě měla β . Když to není zobrazení, tak automaticky nevyhoví žádné z podmínek faktu 8a.3 ani definici. Protože neumíme dosadit β do S , nelze aplikovat ony dva „kolotočové“ testy.



Zobrazení T tedy není invertibilní. Intuitivně by případné inverzní zobrazení mělo „odčinit“ to, co T dělá, a vracet prvky tam, odkud přišly. U našeho modifikovaného T ale nevíme kam vrátit α (dva kandidáti, kterého vybrat?), a nevíme, kam vrátit β .

Zkusíme relaci S modifikovat tak, aby se stala zobrazením, tedy vynecháme jednu z dvojic začínajících α a přidáme dvojici s β . Zkusíme třeba toto: $S = \{(\alpha, 13), (\beta, 23), (\gamma, 14)\}$.

Je to už zobrazení, má tedy smysl psát $S(\alpha) = 13$, $S(\beta) = 23$, $S(\gamma) = 14$. Protože nevzniklo obrácením dvojic z T , tak to samozřejmě není to, co chceme. Zajímavá otázka je, zda to pozná definice, protože teď je první požadavek splněn (máme zobrazení $B \mapsto A$) a je to na algebraických testech.

Neprve projdeme pomocí a množinu A : $S(T(13)) = S(\alpha) = 13$, zatím dobré. $S(T(14)) = S(\gamma) = 14$, OK. $S(T(23)) = S(\alpha) = 13 \neq 23$ a selhání. První podmínka z definice tedy rozpoznala, že S není dobrý kandidát na inverzní zobrazení.

Neplatí ani druhá podmínka: $T(S(\beta)) = T(23) = \alpha \neq \beta$.

Čtenář se může přesvědčit, že nezáleží na tom, kterou z dvojic $(\alpha, 13)$, $(\alpha, 23)$ z původního S vynecháme a jaké číslo svážeme s β , vždy podmínky z definice poznají, že S není inverzní zobrazení. Zdá se tedy, že jsou rozumně zvoleny.

2a. Modifikované T mělo dva problémy při vytváření T^{-1} . Zkusíme je izolovat.

Zde budeme uvažovat $T = \{(13, \alpha), (14, \gamma), (23, \alpha)\}$ jako zobrazení z A do množiny $B' = \{\alpha, \gamma\}$, tedy odpadne problém s tím, jak vracet β . Stále máme problém, kam poslat α . Inverzní relace jej pošle na dvě místa a tudíž nebude inverzním zobrazením, proto ani takto modifikované T není invertibilní.

Vyzkoušíme definici a zobrazení S vytvořené tak, že vybereme jednu možnost. Uvažujeme například $S = \{(\alpha, 13), (\gamma, 14)\}$. Toto je zobrazení z $\{\alpha, \gamma\}$ do A , ale není inverzní k T . Rozpozná to první podmínka, $S(T(23)) = S(\alpha) = 13 \neq 23$.

Pro volbu $S(\alpha) = 23$ zase selže $S(T(13)) = S(\alpha) = 23 \neq 13$.

Zajímavé je, že druhá podmínka z definice bude pro oba kandidáty fungovat (čtenář snadno ověří).

2b. Teď se zaměříme na problém chybějící šipky.

Budeme uvažovat uvažovat restrikcí T na $A' = \{13, 14\}$ jako zobrazení do B :

$$T|_{\{13,14\}} = \{(13, \alpha), (14, \gamma)\}.$$

Opět není invertibilní, protože inverzní relace není zobrazením, nikam neposílá β .

Vyzkoušíme definici s kandidátem S , který vznikne z inverzní relace doplněním přiřazení pro β . Zkusme například $S = \{(\alpha, 13), (\beta, 13), (\gamma, 14)\}$.

Tentokrát první test z definice projde: $T(S(13)) = T(\alpha) = 13$, $T(S(14)) = S(\gamma) = 14$. Selže druhý test: $T(S(\beta)) = T(13) = \alpha \neq \beta$.

△

Poznámka: Příklad 2b ukázal nejen potřebnost druhého testu, ale také význam přítomnosti B v podmínce inverzního zobrazení. Představme si, že by požadavek na S vypadal takto: S je zobrazení, které splňuje

- pro všechna $a \in D(T)$ je $S(T(a)) = a$;
- pro všechna $b \in D(S)$ je $T(S(b)) = b$.

Pro T z příkladu 2b by tyto podmínky splňovalo zobrazení $S = \{(\alpha, 13), (\gamma, 14)\}$. Není to ale zobrazení $B \mapsto A$.

Pokud bychom ovšem začali T uvažovat jako zobrazení $A \mapsto B' = \{\alpha, \gamma\}$, tak už by bylo invertibilní a toto S by bylo jeho inverzním zobrazením. Vidíme, že to, zda je zobrazení invertibilní, lze někdy ovlivnit volbou cílové množiny. Blíže se na to podíváme v následující sekci.

△

Obvykle potkáváme zobrazení daná algebraickým vzorcem.

! Příklad 8a.j: Uvažujme množiny $A = M_{2 \times 2}(\mathbb{R})$ všech čtvercových matic 2×2 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 obyčejné 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 $S = T^{-1}$:

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

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

△

I při práci s inverzí může pomoci vizualizace.

! Příklad 8a.k: Vyšetříme několik zobrazení založených na přiřazení $n \mapsto n + 1$.

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

Podstatu zobrazení vystihuje obrázkem napravo. U definičního oboru jsme poznamenali, že používáme proměnnou n , a v cílové množině budeme používat třeba m .

Jako relace T 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 vyjádřitelného vzorcem $S(m) = m - 1$. Je to zobrazení a podmínky z definice potvrdí, že opravdu $S = T^{-1}$. Nejprve bereme $n \in \mathbb{Z}$, čímž se myslí ta „první“ celá čísla, tedy definiční obor T . U druhé podmínky bereme $m \in \mathbb{Z}$, což je jiné \mathbb{Z} , tentokrát cílová množina T . Obrázek to výmluvně naznačuje.

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

Vyšlo to. Složené funkce jsme rozbalovali „zevnitř“, tedy nejprve jsme vyhodnocovali vnitřní zobrazení a výsledný výraz dosazovali do vnějšího. Někdy lze postupovat i opačně a nejprve vyhodnocovat vnější zobrazení.

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

Toto zobrazení bylo extrémně jednoduché. Mnohdy nedokážeme příslušnou inverzi odhadnout intuitivně, popřípadě z grafu (který třeba ani nelze rozumně načrtnout). Pak je třeba pracovat algebraicky způsobem, který čtenář nejspíše zná: Napíšeme, jak cílovou proměnnou získáme pomocí výchozí proměnné, a pak z této rovnosti vyjádříme původní proměnnou. Tím zjistíme, jakým způsobem se posílá v opačném směru. V našem případě jde o jednoduchou úpravu:

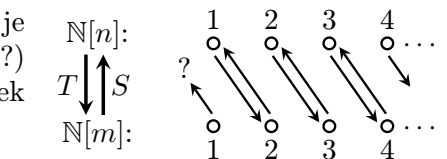
$$m = n + 1 \implies n = m - 1.$$

Tím získáme kandidáta na inverzní zobrazení $S(m) = m - 1$ a pomocí testů z definice ověříme, že je to opravdu T^{-1} .

Tento příklad 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 $\text{ran}(T)$ množiny stejného typu.

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

Coby relace je $T = \{(1, 2), (2, 3), (3, 4), \dots\}$, tedy jediný kandidát na inverzi je $S = \{(2, 1), (3, 2), (4, 3), \dots\}$. Teto předpis ovšem nezahrnuje dvojici typu $(1, ?)$ a proto S není zobrazení $\mathbb{N} \mapsto \mathbb{N}$. To znamená, že T není invertibilní. Obrázek ukazuje, kde je problém. Dokázali bychom to poznat i bez něj?



Standardní postup je odvodit algebraicky z rovnice $m = n + 1$, že $m = n - 1$ neboli $S(m) = m - 1$ je kandidátem na inverzní zobrazení. Nejprve musíme ověřit, že předpis definuje zobrazení $\mathbb{N} \mapsto \mathbb{N}$, ovšem to není pravda, protože $S(1) = 0 \notin \mathbb{N}$. Z toho plyne, že S není vhodným kandidátem. Může uspět jiný? Z faktu 8a.3 (iii) víme, že $S(m) = m - 1$ je jediná možnost pro $m \geq 2$, takže je otázka, jestli je možné přesměrovat $S(1)$ do množiny \mathbb{N} a získat tak zobrazení, které bude fungovat coby inverzní.

Zkusme třeba $S(1) = 1$. Máme tedy nové zobrazení, zase mu budeme říkat S , jehož celá definice se zapisuje takzvanou „funkcí rozpísem“. V tomto případě

$$S(m) = \begin{cases} 1; & m = 1, \\ m - 1, & m \in \mathbb{N}, m \geq 2. \end{cases}$$

Je to T^{-1} ? Je to zobrazení $\mathbb{N} \mapsto \mathbb{N}$, zatím dobré. Ověříme první podmínku z definice, tam se hodí pozorování, že pro $n \in \mathbb{N}$ je $T(n) \geq 2$, a proto se $S(T(n))$ vyhodnocuje dle druhého vzorce v definici S . Pro $n \in \mathbb{N} = D(T)$ tedy máme $S(T(n)) = S(n+1) = (n+1) - 1 = n$, to funguje.

Zbývá druhá podmínka. Vezměme $m \in \mathbb{N}$, kde teď \mathbb{N} je to „druhé“ neboli cílová množina T . Pokud $m \geq 2$, pak podle definice S máme $T(S(m)) = (m-1) + 1 = m$, zatím dobré. Pokud $m = 1$, tak $T(S(1)) = 1 + 1 = 2 \neq 1$ a je problém. Naše nové S také není T^{-1} .

Čtenář by mohl zkoušet jiné cíle pro $S(1)$, ale bude opakovaně zklamáván. Snadno se ukáže, že žádná volba $S(1)$ situaci nezachrání, T není invertibilní.

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

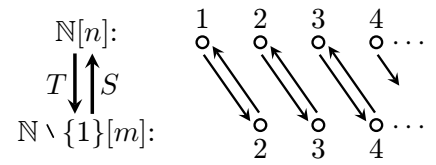
Tato definice má smysl, protože pro $n \in \mathbb{N}$ je $T(n) = n + 1 \geq 2$, tedy T opravdu posílá vstupy do $\mathbb{N} \setminus \{1\}$.

Obvyklý algebraický přístup nabídne kandidáta $S(m) = m - 1$. Nejprve se ptáme, zda je to zobrazení $\mathbb{N} \setminus \{1\} \mapsto \mathbb{N}$. Tentokrát je odpověď kladná, takže postoupíme k testům.

Pro $n \in \mathbb{N}$ máme $S(T(n)) = S(n + 1) = (n + 1) - 1 = n$, v pořádku. Pro $m \in \mathbb{N} \setminus \{1\}$ pak máme $T(S(m)) = (m - 1) + 1 = m$. Ověřili jsme, že $S = T^{-1}$. Toto zobrazení T je tedy invertibilní.

V posledních dvou příkladech jsou zobrazení T coby množiny dvojic shodné, shodují se i vzorcem. Liší se pouze deklarovanou cílovou množinou a viděli jsme, že to výrazným způsobem ovlivnilo jejich vlastnosti. To ukazuje, že jsme v definici rovnosti zobrazení oprávněně zahrnuli také porovnání cílových množin.

△



M Poznámka: Zobrazení definovaná rozpisem jsou užitečným a jednoduchým konceptem. Definiční obor se rozdělí na části a pro každou se vybere vzorec pro generování hodnot funkce. Používá se to pak přirozeným způsobem. Když chceme nějaký objekt dosadit do zobrazení, tak najdeme, do které části specifikované v definici spadá, a vybere se příslušný vzorec.

S těmito funkcemi jsou spojeny určité konvence. Můžeme například zjednodušit určité specifikace tím, že dopředu deklarujeme, na jaké množině zobrazení definujeme. Oblíbená je také specifikace „jinde“, což je formálně vzato na všech částech $D(T)$, které nejsou zmíněny v ostatních variantách. Zobrazení $S(m)$ z příkladu výše tedy mohlo být (po deklaraci, že jde o zobrazení na \mathbb{N}) definováno třeba takto:

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

Čtenář nejspíše zná reálnou funkci absolutní hodnota definovanou jako

$$|x| = \begin{cases} x, & x \geq 0; \\ -x, & x < 0, \end{cases}$$

o něco méně populární je reálná funkce signum neboli určení znaménka:

$$\text{sgn}(x) = \begin{cases} 1, & x > 0; \\ 0, & x = 0; \\ -1, & x < 0. \end{cases}$$

Konceptuálně jde tedy o snadnou věc, z pohledu praktického je to nudná komplikace, protože se důkazy musí dělat přinejmenším dvakrát (pro každou verzi zobrazení jeden).

△

Shrňme algebraický postup

S Algoritmus 8a.4.

pro nalezení inverzního zobrazení $T: A \mapsto B$ daného vzorcem.

0. Pokud není zadáno, vymyslíme označení pro proměnnou z cílové množiny.

1. Fungování daného zobrazení zachytíme rovností $b = T(a)$, pokud tedy je nezávislá proměnná (vstup) označena a a výstupní proměnná b .

Z této rovnosti vyjádříme a jako funkci b .

2. Pokud krok 1 úspěšně vygeneroval algebraický vzorec, využijeme jej jako definici zobrazení S .

Ověříme, že tento vzorec definuje zobrazení $B \mapsto A$.

3. Pokud krok 2 skončil úspěšně, ověříme, zda platí

• $S(T(a)) = a$ pro všechna $a \in A = D(T)$,

• $T(S(b)) = b$ pro všechna $b \in B = D(S)$.

Pokud ano, je T invertibilní a $S = T^{-1}$.

△

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

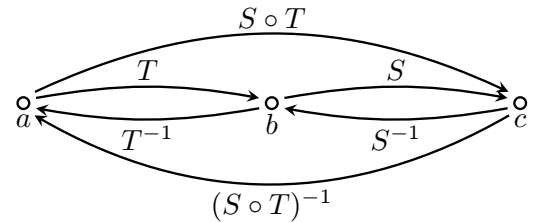
!

Věta 8a.5.Nechť $T: A \mapsto B$ je zobrazení.Jestliže je T invertibilní, pak je také 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 je inverzní k T^{-1} . To znamená, že jde naopak než T^{-1} , tedy $S: A \mapsto B$, 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. V 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 8a.6.

Nechť $T: A \mapsto B$ a $S: B \mapsto C$ jsou zobrazení. Jestliže jsou invertibilní, tak je také $S \circ T$ invertibilní a 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, které se zrovna chystáme řešit, a oblou pro vyznačení složeného zobrazení, popřípadě dosazení, které budeme řešit později.

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. □

Alternativní důkaz je ve cvičení 8a.10.

8a.7 Další poznatky o skládání

Je jedno zajímavé zobrazení, které existuje pro každou množinu.

Definice.

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

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

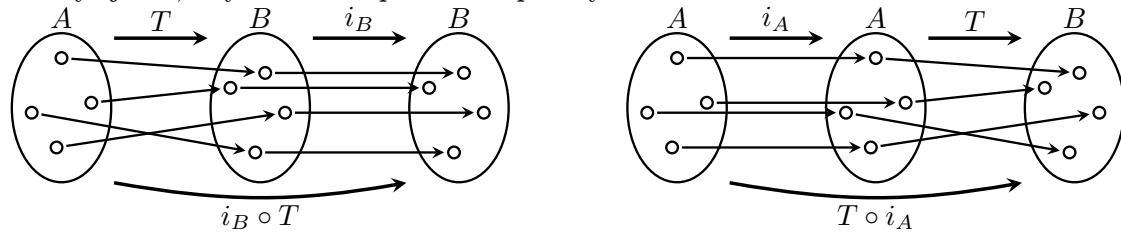
se nazývá **identita** či **identické zobrazení** na A a značí se i_A .

Máme tedy $i_A(a) = a$. Toto zobrazení už jsme vlastně potkali v kapitole 4b pod jménem $\Delta(A)$, jako relace je to množina všech dvojic typu (a, a) . Ve cvičení 8a.9 by měl čtenář hravě dokázat, že i_A je vždy invertibilní a jak vypadá inverzní zobrazení. V teorii zobrazení hraje velmi zajímavou roli.

Fakt 8a.8.

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. Vzniklé zobrazení $i_B \circ T$ vede $A \mapsto B$ stejně jako T , takže má smysl postoupit ke kontrole, že $i_B \circ T$ 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.

□

Zobrazení i_A umožní přepsat podmínku $S(T(a)) = a$ z definice inverzního zobrazení jako $(S \circ T)(a) = i_A(a)$, porovnáváme tedy hodnoty dvou zobrazení. Jejich definiční obory i cílové množiny souhlasí, takže první podmínka z definice inverzního zobrazení se zachytí zápisem $S \circ T = i_A$. Obdobně je to s druhou podmínkou.

Fakt 8a.9.

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 $T \circ S = i_B$.

Uvažujme zobrazení $T: A \mapsto A$. Fakt 8a.8 pak říká, že $i_A \circ T = T \circ i_A = T$. To znamená, že zobrazení i_A se chová vůči skládání jako číslo 1 při násobení čísel. Není to jediná podobnost. Výsledek cvičení 8a.9 silně připomíná známý vzorec $1^{-1} = 1$. Fakt výše pak 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 7). Funguje to rozumně u operací, které splňují asociativní zákon, což jsme u skládání zobrazení potvrdili větou 8a.2, takže můžeme bez obav definovat.

! Definice.

Nechť $n \in \mathbb{N}$, $n \geq 2$. Uvažujme množiny $A_0, A_1, \dots, A_n, A_{n+1}$ a zobrazení $T_k: A_{k-1} \mapsto A_k$ pro $k = 1, \dots, n+1$.

Jejich složení definujeme vzorcem

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

Podobně jako u relací, také u zobrazení je zajímavým speciálním případem skládání zobrazení se sebou samým, čímž vznikne mocnina. Aby $T \circ T$ fungovalo, musí být cílová množina T stejná jako definiční obor, jsme tedy zase u případu $T: A \mapsto A$.

Definice.

Nechť $T: A \mapsto A$ je zobrazení, $n \in \mathbb{N}_0$. Pak definujeme n -tou mocninu T značenou T^n takto:

(0) $T^0 = i_A$;

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

Poznamenejme, že díky faktu 8a.8 máme $T^1 = T^{0+1} = T \circ T^0 = T \circ i_A = T$, což dává smysl.

Příklad 8a.1: Mocninu ilustrujeme na několika příkladech.

1. Uvažujme množinu $A = \{1, 2, 13\}$.

Zobrazení U z A do A definujeme jako $1 \mapsto 1, 2 \mapsto 13, 13 \mapsto 1$. Pak máme následující:

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

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

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

Nyní uvažujme zobrazení V z A do A dané $1 \mapsto 2, 2 \mapsto 13, 13 \mapsto 1$. Pak

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

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

$V^3 = V \circ V^2: 1 \mapsto 13 \mapsto 1, 2 \mapsto 1 \mapsto 2, 13 \mapsto 2 \mapsto 13$. 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 $T^k(n) = 2^k n$, což snadno dokážeme indukcí.

△

Vzorec pro inverzi složeného zobrazení se snadno zobecní.

! Věta 8a.10.

(i) Nechť $n \in \mathbb{N}, n \geq 2$. Uvažujme množiny A_0, A_1, \dots, A_n a zobrazení $T_k: A_{k-1} \mapsto A_k$ pro $k = 1, \dots, n$. Jestliže jsou všechna tato zobrazení invertibilní, pak je také složené zobrazení $T_n \circ \dots \circ T_1$ invertibilní 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 také T^n invertibilní a $(T^n)^{-1} = (T^{-1})^n$.

Důkaz se dělá indukcí a je rutinní, viz cvičení 8a.12 a 8a.13. Mimochodem, ten druhý vztah vlastně známe z reálných čísel, $\frac{1}{x^n} = \left(\frac{1}{x}\right)^n$.

Zobrazení hrají významnou roli v řadě matematických oborů. Uvidíme to hned v příští kapitole. S tím se také pojí specializovanější pojmy a značení spojené se zobrazením, které při běžné práci nejsou potřeba. Jedním takovým tuto kapitolu zakončíme.

Definice.

Nechť A, B jsou množiny. Množina všech zobrazení $A \mapsto B$ se značí B^A .

Tato množina se nám bude hodit v kapitole 9d, kde mimo jiné uvidíme, proč se zobrazení z A do B značí zrovna takto zvláště. O počtech různých zobrazení pojednává příklad 11a.n.

Cvičení

Cvičení 8a.1: Který z následujících předpisů definuje zobrazení?

- Binárnímu řetězci r přiřazujeme počet výskytů znaku 1 v r ;
- Binárnímu řetězci r přiřazujeme pozici prvního výskytu znaku 0 v r ;
- Přirozenému číslu přiřazujeme přirozené číslo se stejným ciferným součtem;
- Přirozenému číslu přiřazujeme jeho poslední číslici (ta nejvíc vpravo neboli jednotky v dekadickém zápisu).

Cvičení 8a.2 (rutinní): Pro následující zobrazení určete jejich definiční obor a obor hodnot.

- Zobrazení přiřazuje každému přirozenému číslu jeho poslední číslici.
- Zobrazení přiřazuje každému přirozenému číslu číslo o jedno větší.
- Zobrazení přiřazuje každému vektoru $(x, y) \in \mathbb{R}^2$ jeho délku.
- Zobrazení dává maximum ze dvou reálných čísel.

Cvičení 8a.3: Pro následující dvojice zobrazení rozhodněte, zda jsou si rovna.

- a) $T: \mathbb{N} \mapsto \mathbb{N}$ dáno $T(n) = |n|$, $S: \mathbb{N} \mapsto \mathbb{N}$ dáno $S(n) = n$;
 b) $T: \mathbb{N}_0 \mapsto \mathbb{N}$ dáno $T(n) = n + 13$, $S: \mathbb{N}_0 \mapsto \mathbb{N}$ dáno $S(n) = n + 14$;
 c) $T: \{-1, 0, 1\} \mapsto \mathbb{Z}$ dáno $T(n) = n^2$, $S: \{-1, 0, 1\} \mapsto \mathbb{Z}$ dáno $S(n) = n^4$;
 d) $T: \mathbb{Z} \mapsto \mathbb{Z}$ dáno $T(n) = 3n + 1$, $S: \mathbb{Z} \mapsto \mathbb{Q}$ dáno $S(n) = 3n + 1$;
 e) $T: \mathbb{Z} \mapsto \mathbb{N}$ dáno $T(n) = \cos(2\pi n)$, $S: \mathbb{Z} \mapsto \mathbb{N}$ dáno $S(n) = 1$.

Cvičení 8a.4: Pro následující zobrazení $T: \mathbb{N} \mapsto \mathbb{N}$ spočítejte $T(1)$, $T(2)$, $T(3)$ a $T(4)$:

- a) $T(n) = \begin{cases} n - 1, & n \geq 3; \\ n + 1, & n \leq 2; \end{cases}$
 b) $T(n) = \begin{cases} n, & n \text{ sudé}; \\ 2n, & n \text{ liché}; \end{cases}$
 c) $T(n) = \begin{cases} 1, & n = k^2 \text{ pro nějaké } k \in \mathbb{N}; \\ 0, & \text{jinde}; \end{cases}$
 d) $T(n) = \begin{cases} 13, & n = 1; \\ 14, & n \text{ prvočíslo}; \\ 0, & \text{jinde}. \end{cases}$

Cvičení 8a.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 8a.6 (poučné): Pro následující dvojice funkcí $f, g: \mathbb{Z} \mapsto \mathbb{Z}$ rozhodněte, zda číslo 13 leží v oboru hodnot složené funkce $g \circ f$:

- a) $f(x) = x^2 + 2$, $g(x) = 2x + 1$;
 b) $f(x) = x^3 - 1$, $g(x) = 13x$;
 c) $f(x) = x^3 + 4$, $g(x) = 2x - 11$;
 d) $f(x) = 4x$, $g(x) = x - 1$.

Cvičení 8a.7 (rutinní, poučné): Pro následující dvojice funkcí $f, g: \mathbb{R} \mapsto \mathbb{R}$ najděte $g \circ f$ a $f \circ g$. Na základě toho rozhodněte, zda $g = f^{-1}$.

- a) $f(x) = \sin(x)$, $g(x) = \pi x$;
 b) $f(x) = x$, $g(x) = e^x$;
 c) $f(x) = 1 + x^2$, $g(x) = 1 + x^2$;
 d) $f(0) = g(0) = 0$, $x \neq 0$: $f(x) = \frac{2}{x}$, $g(x) = \frac{2}{x}$;
 e) $f(x) = x^2$, $g(x) = 13$;
 f) $f(x) = x^3 - 1$, $g(x) = \sqrt[3]{x + 1}$;
 g) $f(x) = x^2$, $g(x) = \sqrt{|x|}$;
 h) $f(x) = e^x$, $g(x) = \ln(|x|)$ pro $x \neq 0$ a $g(0) = 0$;
 i) $f(x) = 1 - x$, $g(x) = 1 - x$;
 j) $f(x) = 1 + x$, $g(x) = 1 + x$.

Cvičení 8a.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 8a.9 (poučné): Dokažte, že pro každou množinu A je zobrazení i_A invertibilní, a najděte i_A^{-1} .

Cvičení 8a.10 (poučné): Připomeňte si alternativní charakterizaci inverzního zobrazení pomocí i_A a i_B . Použijte tento přístup a vlastnosti i_A k důkazu, že pro $T: A \mapsto B$ a $S: B \mapsto C$ platí $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Cvičení 8a.11 (poučné, *dobré): Pro následující zobrazení odhadněte vzorec pro mocninu T^k .

- a) $T: \mathbb{N} \mapsto \mathbb{N}$, $T(n) = n + 1$;
 b) $T: \mathbb{N} \mapsto \mathbb{N}$, $T(n) = n^2$;
 c) $T: \mathbb{Z} \mapsto \mathbb{Z}$, $T(n) = 1 - n$;
 d)* $T: \mathbb{N} \mapsto \mathbb{N}$, $T(n) = \max(1, n - 1)$.

Nápověda: Zejména u (iv) pomohou šipkové obrázky.

Cvičení 8a.12 (rutinní, poučné): Nechť $n \in \mathbb{N}$, $n \geq 2$. Uvažujme množiny A_0, A_1, \dots, A_n a zobrazení $T_k: A_{k-1} \mapsto A_k$ pro $k = 1, \dots, n$. Dokažte, že jestliže jsou všechna tato zobrazení invertibilní, pak je invertibilní také $T_n \circ \dots \circ T_1$ a $(T_n \circ \dots \circ T_1)^{-1} = T_1^{-1} \circ \dots \circ T_n^{-1}$ (viz věta 8a.6 a 8a.10).

Cvičení 8a.13 (rutinní, poučné): Nechť $T: A \mapsto A$ je invertibilní zobrazení. Dokažte, že pro $n \in \mathbb{N}$ platí $(T^n)^{-1} = (T^{-1})^n$ (viz věta 8a.10).

Cvičení 8a.14 (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 $T \cap S$, $T \cup S$ a $T \setminus S$ zase byly zobrazením.

Cvičení 8a.15 (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 8a.16 (poučné, dobré): Necht U je universum. Pro $M \subseteq U$ definujme tzv. **charakteristickou funkci** M jako

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

Také se jí říká indikátorová funkce, protože jedničkami indikuje, které body z U jsou v M . Dokážte následující:

- a) Pro libovolné $M \subseteq U$: $\chi_{\overline{M}} = 1 - \chi_M$.
 b) Pro libovolné $M, N \subseteq U$: $\chi_{M \cap N} = \chi_M \cdot \chi_N$.
 c) Pro libovolné $M, N \subseteq U$: $\chi_{M \cup N} = \chi_M + \chi_N - \chi_{M \cap N}$.

Řešení:

8a.1: a) ano. (ii): ne. Co když r neobsahuje 0? b) ne. Například $13 \mapsto 4$ a $13 \mapsto 22$. c) ano.

8a.2: a) $D(T) = \mathbb{N}$, $\text{ran}(T) = \{0, 1, 2, \dots, 8, 9\}$. b) $D(T) = \mathbb{N}$, $\text{ran}(T) = \{2, 3, 4, \dots\} = \mathbb{N} \setminus \{1\}$. c) $D(T) = \mathbb{R}^2$, $\text{ran}(T) = \langle 0, \infty \rangle$. d) $D(T) = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, $\text{ran}(T) = \mathbb{R}$.

8a.3: a) $T = S$: Množiny souhlasí. Pro $n \in \mathbb{N}$ je $n \geq 0$, proto $T(n) = |n| = n = S(n)$. b) $T \neq S$: Například $T(1) = 14$, $S(1) = 15$. c) $T = S$: Množiny souhlasí. Pro $n = 0$ je $T(0) = 0^2 = 0 = 0^4 = S(0)$, pro $n = \pm 1$ je $T(\pm 1) = (\pm 1)^2 = 1 = (\pm 1)^4 = S(\pm 1)$. d) $T \neq S$: Nesouhlasí cílové množiny. e) $T = S$: Množiny souhlasí. Pro $n \in \mathbb{Z}$ je $T(n) = \cos(2\pi n) = 1 = S(n)$.

8a.4: a) $T(1) = 2$, $T(2) = 3$, $T(3) = 2$ a $T(4) = 3$. b) $T(1) = 2$, $T(2) = 2$, $T(3) = 6$ a $T(4) = 4$. c) $T(1) = 1$, $T(2) = 0$, $T(3) = 0$ a $T(4) = 1$. d) $T(1) = 13$, $T(2) = 14$, $T(3) = 14$ a $T(4) = 0$.

8a.5: Přirazuje studentovi jeho stipendium.

8a.6: Hledáme $x \in \mathbb{Z}$ tak, aby $x \xrightarrow{f} y \xrightarrow{g} 13$. Nejprve y , pak x .

a) $2y + 1 = 13 \rightarrow y = 6$, $x^2 + 2 = 6 \rightarrow x = \pm 2$. Ano, $g(f)(\pm 2) = 13$, proto $13 \in \text{ran}(g \circ f)$.

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

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

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

8a.7: a) $(g \circ f)(x) = g(f(x)) = \pi \sin(x)$, $(f \circ g)(x) = f(g(x)) = \sin(\pi x)$, ne. b) $(g \circ f)(x) = g(f(x)) = e^x$, $(f \circ g)(x) = f(g(x)) = e^x$, ne. c) $(g \circ f)(x) = g(f(x)) = 1 + (1 + x^2)^2$, $(f \circ g)(x) = f(g(x)) = 1 + (1 + x^2)^2$, je to vlastně f^2 (ve smyslu skládání zobrazení, ne ve smyslu násobení funkcí, pozor), ne. d) $(g \circ f)(x) = g(f(x)) = x$, $(f \circ g)(x) = f(g(x)) = x$, ano, $g = f^{-1}$ a $f = g^{-1}$. e) $(g \circ f)(x) = g(f(x)) = 13$ (cokoliv dosazené do konstantní funkce je ta konstanta), $(f \circ g)(x) = f(g(x)) = 13^2$, ne. f) $(g \circ f)(x) = g(f(x)) = x$, $(f \circ g)(x) = f(g(x)) = x$, ano, $g = f^{-1}$ a $f = g^{-1}$. g) $(g \circ f)(x) = g(f(x)) = |x|$, $g(f(x)) = |x|$, ne. h) $(g \circ f)(x) = g(f(x)) = x$ 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 $(f \circ g)(0) = 1$. i) $(g \circ f)(x) = g(f(x)) = x$, $(f \circ g)(x) = f(g(x)) = x$, ano, $g = f^{-1}$ a $f = g^{-1}$. j) $(g \circ f)(x) = g(f(x)) = x + 2$, $(f \circ g)(x) = f(g(x)) = x + 2 = f^2(x)$, ne.

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

8a.9: Prosté: $i_A(x) = i_A(y) \rightarrow x = y$. 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 $i_A(i_A(a)) = i_A(a) = a$.

8a.10: $(T^{-1} \circ S^{-1}) \circ (S \circ T) = ((T^{-1} \circ S^{-1}) \circ S) \circ T = (T^{-1} \circ (S^{-1} \circ S)) \circ T = (T^{-1} \circ i_B) \circ T = T^{-1} \circ T = i_A$,
 $(S \circ T) \circ (T^{-1} \circ S^{-1}) = ((S \circ T) \circ T^{-1}) \circ S^{-1} = (S \circ (T \circ T^{-1})) \circ S^{-1} = (S \circ i_B) \circ S^{-1} = S \circ S^{-1} = i_C$.

8a.11: a) $T^2(n) = T(T(n)) = T(n+1) = (n+1) + 1 = n+2$, $T^3(n) = T(T^2(n)) = T(n+2) = (n+1) + 1 = n+3$,
 $T^k(n) = n + k$. b) $T^2(n) = T(n^2) = (n^2)^2 = n^4$, $T^3(n) = T(n^4) = (n^4)^2 = n^8$, $T^k(n) = n^{2^k}$. c) $T^2(n) = T(1-n) = 1 - (1-n) = n$, $T^3(n) = T(n) = 1 - n$, $T^4(n) = T(1-n) = 1 - (1-n) = n$, $T^k(n) = 1 - n$ pro k liché, $T^k(n) = n$ pro k sudé. d) $T(1) = 1$ 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 $n > k$.

8a.12: Indukce: (0) $n = 2$: $T_2 \circ T_1$ je invertibilní a $(T_2 \circ T_1)^{-1} = T_1^{-1} \circ T_2^{-1}$ podle věty 8a.6.

(1) $n \geq 2$, IP: Pokud T_1, \dots, T_n splňují předpoklady, pak $T_n \circ \dots \circ T_1$ je invertibilní a $(T_n \circ \dots \circ T_1)^{-1} = T_1^{-1} \circ \dots \circ T_n^{-1}$.
 Mějme T_1, \dots, T_n, T_{n+1} splňující předpoklady, označme $S = T_n \circ \dots \circ T_1$, podle indukčního předpokladu je S invertibilní a máme vzorec pro S^{-1} . Podle věty 8a.6 je pak i $T_{n+1} \circ S$ invertibilní a $(T_{n+1} \circ S)^{-1} = S^{-1} \circ T_{n+1}^{-1}$,
 když dosadíme, dostaneme, že $T_{n+1} \circ T_n \circ \dots \circ T_1$ je invertibilní a $(T_{n+1} \circ T_n \circ \dots \circ T_1)^{-1} = T_1^{-1} \circ \dots \circ T_n^{-1} \circ T_{n+1}^{-1}$.

8a.13: (0) $n = 1$: $(T^1)^{-1} = T^{-1} = (T^{-1})^1$.

(1) $n \geq 1$, IP: $(T^n)^{-1} = (T^{-1})^n$ pro každé T invertibilní. Mějme teď invertibilní T , označme $S = T^n$. Pak je dle indukčního předpokladu S invertibilní a $S^{-1} = (T^{-1})^n$. Podle věty 8a.6 je potom $T \circ S$ invertibilní a $(T \circ S)^{-1} = S^{-1} \circ T^{-1}$, po dosazení $(T^{n+1})^{-1} = (T \circ S)^{-1} = S^{-1} \circ T^{-1} = (T^{-1})^n \circ T^{-1} = (T^{-1})^{n+1}$.

8a.14: Aby byla relace zobrazením, musí mít každé $a \in A$ přesně jednu dvojici v této relaci.

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

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

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

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

8a.15: 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 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 $\mathbb{R} \setminus \{0\}$. 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.

8a.16: a) $\chi_{\overline{M}}(x) = 1 \iff x \in \overline{M} \iff x \notin M \iff \chi_M(x) = 0 \iff (1 - \chi_M)(x) = 1$, 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).

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

c) Důkaz se nejlépe dělá rozbořením 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.

8b. Zobrazení prosté, na, bijekce

Příklady ukázaly, že ne každé zobrazení je invertibilní. Podle definice se neexistence inverzního zobrazení potvrdí vyloučením všech kandidátů, což je nepraktické. Příklad 8a.i naznačuje, že vytvoření inverzního zobrazení mohou bránit jisté konkrétní situace, které jsou snadno rozeznatelné. Vyplatí se je pojmenovat.

Uvažujme zobrazení $T: A \mapsto B$. Když se pro $b \in B$ snažíme vytvořit inverzní zobrazení, můžeme narazit na dva problémy. Tím prvním je, že do b vede více šipek, takže nevíme, kterou z nich vybrat k otočení. Pokud tomu chceme zabránit, musíme požadovat, aby se nemohly dvě šipky z rozdílnými začátky sejít ve stejném cíli. Matematicky:

• Pro každé $x \neq y$ z A musí platit $T(x) \neq T(y)$.

Toto je výstižné, ale nepraktické. Abychom platnost takovéto podmínky dokázali, musíme pracovat s „není rovno“, kde nám chybí nástroje. Proto se v praxi tato podmínka chápe jako implikace

• $\forall x, y \in A: x \neq y \implies T(x) \neq T(y)$

a pracuje se s její obměnou, ve které se místo „nerovná se“ objevují rovnosti, se kterými si rozumíme.

• $\forall x, y \in A: T(x) = T(y) \implies x = y$.

Tato praktická podoba se tradičně dává rovnou do definice, což pak definici činí méně intuitivní (čtenář si pro pochopení musí obměnou najít původní verzi).

Druhý možný problém je, že do b nevede žádná šipka, takže nevíme, kam se vracet. Abychom tomu zabránili, musíme požadovat, aby do každého b z cílové množiny nějaká šipka vedla, neboli chceme, aby platila vlastnost

- Pro každé $b \in B$ existuje $a \in A$ splňující $T(a) = b$.

Zde je naopak tato formulace praktická, zatímco v definici je zvykem dávat elegantnější vyjádření. Podmínka vlastně říká, že $T[A] = B$, tedy že $\text{ran}(T) = B$.

!

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 $\text{ran}(T) = B$.

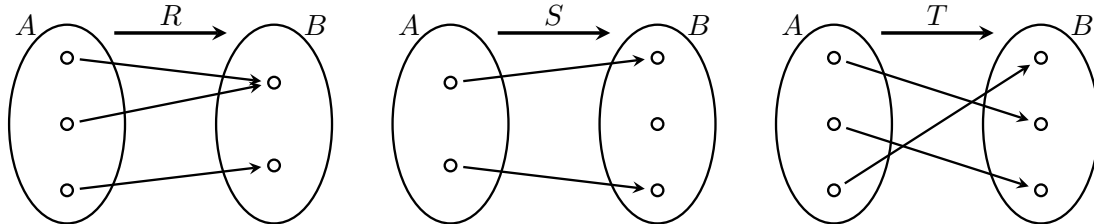
Řekneme, že T je **vzájemně jednoznačné** či **bijekce**, jestliže je prosté a na.

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.

Často potřebujeme název pro vlastnost. Zobrazení může být bijektivní, této vlastnosti můžeme říkat „bijektivita“. Stejně tak vlastnosti „býti prostý“ můžeme říkat „prostota“ (třeba „vyšetřete prostotu funkce“). Ovšem pro vlastnost „býti na“ se neujalo „natota“ a musíme se uchýlit k cizímu názvu „surjektivita“.

! **Příklad 8b.a:** 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, viz příklad 8a.i.

△

Příklad 8b.b: Uvažujme zobrazení T z množiny občanů ČR do množiny přirozených 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.

△

S 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 prostotu, je to podmínka, která v definici specifikuje zobrazení jako speciální typ relace.

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 prostotu tímto způsobem, tak správně je „pro každé $b \in B$ existuje **nejvýše** jedno $a \in A$ takové, že $T(a) = b$.“

△

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 to.

!

Věta 8b.1.

Zobrazení je invertibilní právě tehdy, když je to bijekce.

Důkaz (poučný): Mějme $T: A \mapsto B$.

1) \implies : Předpokládejme, že T je invertibilní, tedy existuje T^{-1} .

Nejprve ukážeme, že T je prosté. Vezměme prvky $x, y \in A$ takové, že $T(x) = T(y)$. Dosadíme tyto shodné prvky do zobrazení T^{-1} , musíme pak dostat stejný výsledek neboli $T^{-1}(T(x)) = T^{-1}(T(y))$. 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) \impliedby : 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 8a.3 (i) \implies (ii) pak $S = T^{-1}$. □

Surjektivita (vlastnost býti na) je zvláštní v tom, že nezávisí jen na samotném fungování T (tedy jak posílá prvky), ale také 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. Opět se potvrzuje, že volba cílové množiny je součástí identity zobrazení, může totiž rozhodnout o platnosti či neplatnosti jedné z vlastností.

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.

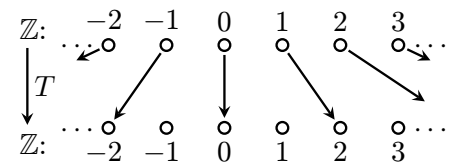
Našli jsme trik, který umí (někdy) udělat z daného zobrazení surjekci. Šlo by něco takového také s prostotou? Tam je to komplikovanější, protože odstranit sbíhavé šipky lze jedinečně tak, že zasáhneme přímo do fungování zobrazení. Ztrácíme tak část informace, kterou původní T neslo, je třeba s tím počítat.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

! Příklad 8b.c: Pro následující zobrazení rozhodneme, zda jsou prostá, na či 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 $x = y$. Obrázek hodně naznačil.

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. I zde obrázek naznačil.



Závěr: T je prosté a není na. Takže to také není bijekce. To je dobrá zpráva, nemusíme hledat inverzní zobrazení.

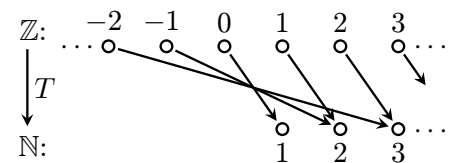
2. Uvažujme $T: \mathbb{Z} \mapsto \mathbb{N}$ dané vzorcem $T(n) = |n|$.

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 najít protipříklad: $x = -1$ a $y = 1$ jsou oba v \mathbb{Z} , splňují $T(x) = 2 = T(y)$ a přitom $x \neq y$. Zobrazení T tedy 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 $n = m - 1$. Pak $n \in \mathbb{Z}$. Protože $m \in \mathbb{N}$, je $n \geq 0$ a proto $T(n) = |n| + 1 = n + 1 = (m - 1) + 1 = m$.

Závěr: T není prosté a je na.

Všimněte si, že restrikce $T|_{\mathbb{N}_0}$ by už byla prostá. Z rovnosti $T(x) = T(y)$ bychom se dostali ke stejné „podezřelé“ rovnosti $|x| = |y|$, ale teď už bychom protipříklad hledali marně. Protože $|x| = x$, $|y| = y$ pro $x, y \in \mathbb{N}_0$, rovnost $|x| = |y|$ vlastně říká $x = y$. Tato restrikce je jako zobrazení 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 8a.k.

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 potvrdíme podle definice. Pro rozlišení budeme používat n pro celá čísla coby $D(T)$ a m pro čísla z oboru hodnot.

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

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

Vyšlo to. Toto zobrazení je samo sobě inverzí, což není zrovna běžný jev, ale evidentně se to stát může. Viz také cvičení 8a.15.

△

Poznámka: V příkladě 3 vedlo zkoumání prostoty na rovnost $|x| = |y|$. Neuměli jsme z toho odvodit $x = y$, ale to ještě neznamená, že jsme vyloučili prostotu, jen neúspěch určitého postupu. Ostatně stejná rovnost nepokazila prostotu u restrikce tohoto zobrazení. Selhání prostoty potvrdilo teprve předvedení konkrétního protipříkladu, který jsme díky $D(T) = \mathbb{Z}$ dokázali najít, ale pro restrikci nikoliv. I při zkoumání prostoty a surjektivit je tedy selhání vlastnosti nutno dokazovat konkrétními protipříklady.

△

Všimněte si zajímavé věci. U příkladů 3 a 4 odpovídalo nalezené inverzní zobrazení vzorci, 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 8b.2 Jak na vlastnosti zobrazení zadaného algebraickým vzorcem.

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 vezmeme libovolný prvek $b \in B$ (z cílového prostoru) a zkusíme k němu najít $a \in A$ takové, aby $T(a) = b$. Vznikne tak algebraická rovnost, ze které se snažíme vyjádřit a , přitom bereme b coby parametr. Cílem není najít úplnou množinu řešení, ale stačí jedno, třeba i uhodnuté. Pokud se vždy najde, tak je zobrazení na.

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

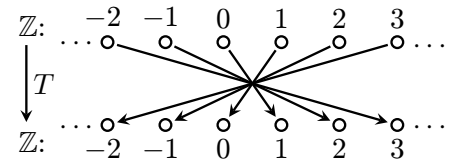
Inverzní zobrazení: Postup je obdobný jako u surjektivit, z rovnosti $T(a) = b$ zkusíme vyjádřit a ve formě vzorce s proměnnou b . Pokud jej najdeme, získáme kandidáta S na inverzní zobrazení T^{-1} . Jeho správnost ověříme pomocí dvou testů z definice: $S(T(a)) = a$ pro $a \in A$ a $T(S(b)) = b$ pro $b \in B$.

Vše: Pokud se po nás nechce samostatný důkaz pro každou z vlastností, jen rozpoznat platnost/neplatnost, pak je možno použít tento postup: Z rovnosti $T(a) = b$ zkusíme vyjádřit a . Možnosti:

- Pokud řešení existuje pro každé b 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 b , ale pak je jedinečné, je T prosté, ale není na.
- Pokud řešení existuje jen pro některá b , a navíc je jich někdy víc, pak T není ani prosté, ani na.

Tento postup funguje velmi dobře zejména u jednodušších zobrazení.

△



! Příklad 8b.d: Uvažujme zobrazení $T: \mathbb{N}^3 \mapsto \mathbb{N}^2$ daném vztahem $T(r, s, t) = (r^3, s^t)$.

Prostota: Máme vzít libovolné $x, y \in D(T)$, v tomto případě jsou to třísložkové vektory. Mějme tedy třeba $x = (r, s, t)$ a $y = (u, v, w)$ pro nějaké neznámé $r, s, t, u, v, w \in \mathbb{N}$. Výchozí rovnost $T(x) = T(y)$ z testované implikace 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 b z cílového prostoru \mathbb{N}^2 , je to tedy nějaký vektor, třeba $b = (u, v)$ pro $u, v \in \mathbb{N}$. Hledáme $a = (r, s, t) \in \mathbb{N}^3 = D(T)$ 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.

△

Podobně jako u relací, také u zobrazení můžeme požádat o „vyšetření vlastností“ daného zobrazení. Očekávají si odpovědi na otázky, zda je zobrazení prosté, zda je na, popřípadě zda je bijekce, a důkazy správnosti těchto odpovědí. U bijekcí se také očekává nalezení inverzního zobrazení a důkazu, že je nalezeno správně.

! Příklad 8b.e: Vyšetříme vlastnosti dvou zobrazení.

1. Uvažujme zobrazení $T: \mathbb{Z}^2 \mapsto \mathbb{Z}^2$ dané vztahem $T(r, s) = (r + 1, r + s)$.

Prostota: $(r, s), (u, v) \in A$ lib., pak

$$\underline{T(r, s) = T(u, v)} \longrightarrow (r + 1, r + s) = (u + 1, u + v) \longrightarrow \begin{cases} r + 1 = u + 1 \\ r + s = u + v \end{cases} \longrightarrow \begin{cases} r = u \\ r + s = u + v \end{cases}$$

První rovnost nám umožní z druhé odvodit $s = v$. Máme tedy $r = u$ a $s = v$, to ale nestačí. Definice prostoty vyžaduje dojít od $T(x) = T(y)$ k $x = y$ (rovnost objektů), tedy správným závěrem je $\underline{(r, s) = (u, v)}$.

T je prosté.

Na: Dáno $(u, v) \in \mathbb{Z}^2$ (cílový prostor). Hledáme $(r, s) \in \mathbb{Z}^2$ aby $T(r, s) = (u, v)$. Tedy chceme:

$$(r + 1, r + s) = (u, v) \longrightarrow \begin{cases} r + 1 = u \\ r + s = v \end{cases} \longrightarrow \begin{cases} r = u - 1 \\ r + s = v \end{cases} \longrightarrow \begin{cases} r = u - 1 \\ u - 1 + s = v \end{cases} \longrightarrow \begin{cases} r = u - 1 \\ s = v - u + 1 \end{cases}$$

Máme kandidáta $(r, s) = (u - 1, v - u + 1)$. Zjevně $(u - 1, v - u + 1) \in \mathbb{Z}^2$ a

$$\underline{T(r, s) = T(u - 1, v - u + 1) = ((u - 1) + 1, (u - 1) + (v - u + 1)) = (u, v)}.$$

T je na.

Je to tedy bijekce a máme také kandidáta $S(u, v) = (u - 1, v - u + 1)$ na inverzní zobrazení. Potvrdíme: S je zobrazení $\mathbb{Z}^2 \mapsto \mathbb{Z}^2$ (naopak než T) a pro $(r, s) \in \mathbb{Z}^2 = D(T)$, popř. $(u, v) \in \mathbb{Z}^2 = D(S)$ máme

$$\underline{S(T(r, s))} = S(r + 1, r + s) = ((r + 1) - 1, (r + s) - (r + 1) + 1) = (r, s),$$

$$\underline{T(S(u, v))} = T(u - 1, v - u + 1) = ((u - 1) + 1, (u - 1) + (v - u + 1)) = (u, v).$$

Potvrzeno, $T^{-1}(u, v) = (u - 1, v - u + 1)$.

2. Uvažujme zobrazení $T: \mathbb{N}^2 \mapsto \mathbb{N}$ dané vztahem $T(r, s) = r + s$.

Prostota: Mějme $(r, s), (u, v) \in \mathbb{N}^2$. Z rovnosti $T(r, s) = T(u, v)$ dostáváme $r + s = u + v$. Nenabízí se cesta, jak z toho získat $r = u$ a $s = v$, proto hledáme protipříklad a najdeme: $T(4, 1) = 5 = T(2, 3)$, přičemž $(4, 1) \neq (2, 3)$ v \mathbb{N}^2 . Lze i jinak, třeba $T(2, 1) = 3 = T(1, 2)$ a $(2, 1) \neq (1, 2)$. T není prosté, proto ani bijekce.

Na: Dáno $b \in \mathbb{N}$. Hledáme $(u, v) \in \mathbb{N}^2 = D(T)$ tak, aby $T(u, v) = b$ neboli aby $u + v = b$. Získat číslo jako součet se zdá být lehké, nabízí se například toto: $r = b, s = 0$. Pak $r + s = b$, ale musíme ověřit, že $(r, s) \in \mathbb{N}^2$. To ale selže, protože $0 \notin \mathbb{N}$.

Modifikace: $r = b - 1, s = 1$. Pak $r + s = b$ a $s = 1 \in \mathbb{N}$. Platí to i pro $r = b - 1$? Pro $b = 1$ je $r = 0$ a máme problém. To nás nasměruje k $b = 1$. Umíme vyjádřit 1 jako součet dvou přirozených čísel? Ne.

T tedy není na. Protipříklad: zvolme $b = 1$. Protože libovolné $r, s \in \mathbb{N}$ splňují $r, s \geq 1$, platí $T(r, s) = r + s \geq 1 + 1 = 2 > 1$, takže nemůže platit $T(r, s) = 1$. Ukázali jsme, že $1 \notin \text{ran}(T)$.

Poznámka: Kdybychom toto T definovali stejným vzorcem jako zobrazení $\mathbb{N}_0^2 \mapsto \mathbb{N}_0$, tak už by bylo na, ukazuje to volba $r = b, s = 0$.

△

S Poznámka: Příklad 2. nám připomněl, že pro vyvrácení prostoty je potřeba uvést konkrétní protipříklad. Podobně pro vyvrácení surjektivit je třeba uvést konkrétní protipříklad, tedy prvek cílové množiny B , pro který neexistuje $a \in D(T)$ splňující $T(a) = b$.

V případě surjektivit je třeba být konkrétní také v důkazu platnosti ve smyslu, že musíme zadat předpis, který k danému obrazu určí jednoznačně jeho vzor. V ideálním případě jde o vzorec či vzorce, které mají onen obraz jako vstup, jak jsme to předvedli výše.

Rozhodně by nestačilo v prvním příkladě napsat toto: „Zvolíme r, s tak, aby platilo $r + 1 = u$ a $r + s = v$.“ Podstatou důkazu surjektivit je právě otázka, zda lze vždy takto zvolit. Zodpověděli jsme ji kladně konkrétními vzorci $r = u - 1, s = v - u + 1$. V zásadě správné ale nikoliv ideální by bylo „Zvolíme $r = u - 1, s = v - r$ “, protože vzorec pro s nemá jako vstup daná data u, v . Nutíme tak čtenáře si argument dokončit.

Nebezpečí ukazuje druhý příklad. „Zvolíme r, s tak, aby platilo $r + s = b$ “ zní lákavě, ale jak jsme viděli, ne vždy to jde. Někdy pokus o vzorec dopadne takto: „Zvolme $r = b - s, s = b - r$ “. Vzniká pak začarovaný kruh, kdy se vzorec pro r odvolává na s a vzorec pro s pro změnu na r . Ve výsledku nevíme, co jsou jejich hodnoty, tedy není to správný argument.

△

! Příklad 8b.f: Prozkoumáme prostotu a surjektivitu pro několik funkcí coby zobrazení $\mathbb{R} \mapsto \mathbb{R}$. U reálných funkcí se tradičně používá y pro hodnoty, proto se u testování prostoty přizpůsobíme a pracujeme s x_1, x_2 .

1. Uvažujme $f(x) = 2x - 1$. Grafem této funkce je šikmá přímka. Taková funkce nemůže nabýt vícekrát stejnou hodnotu, což ukazuje na prostotu. Graf se ve svislém směru táhne od $-\infty$ do ∞ a žádnou hodnotu nevynechá (funkce je spojitá), což ukazuje na surjektivitu. Vypadá to, že tato funkce je bijekce z \mathbb{R} na \mathbb{R} . Nyní vše správným způsobem potvrdíme. Použijeme stručný zápis:

Prostota: $x_1, x_2 \in \mathbb{R}$ libovolné, pak

$$f(x_1) = f(x_2) \quad \longrightarrow \quad 2x_1 - 1 = 2x_2 - 1 \quad \longrightarrow \quad x_1 = x_2.$$

Dokázali jsme podle definice prostotu f .

Na: Dáno $y \in \mathbb{R}$. Najít: x_0 aby $f(x_0) = y$ neboli $2x_0 - 1 = y$. Odtud $x_0 = \frac{y+1}{2}$. Pak $x_0 \in \mathbb{R}$ a

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

Potvrdili jsme i surjektivitu, tedy f je bijekce. Také jsme z $f(x) = y$ odvodili $x = \frac{1}{2}(y + 1)$. Potvrdíme, že $g(y) = \frac{1}{2}(y + 1)$ je inverzní funkce k f .

$$x \in \mathbb{R} = D(f) : g(f(x)) = g(2x - 1) = \frac{1}{2}((2x - 1) + 1) = x,$$

$$y \in \mathbb{R} = D(g) : f(g(y)) = f\left(\frac{1}{2}(y + 1)\right) = 2 \frac{1}{2}(y + 1) - 1 = y.$$

2. Uvažujme $f(x) = x^2 + 1$. Grafem je klasická parabola obrácená nahoru a posunutá nahoru o 1. Víme, že téměř všechny hodnoty se nabydou dvakrát, což naznačuje, že tato funkce není prostá. Víme také, že tato funkce nedokáže poskytnout hodnoty menší než 1, proto nemůže být na \mathbb{R} .

Nyní ji vyšetříme standardním způsobem.

Prostota: $x_1, x_2 \in \mathbb{R}$, předpoklad $f(x_1) = f(x_2)$. Pak $x_1^2 + 1 = x_2^2 + 1$, tedy $x_1^2 = x_2^2$. Z toho $x_1 = x_2$ neodvodíme a máme inspiraci na protipříklad prostoty: Zvolme $x_1 = 1, x_2 = -1$. Pak $f(1) = 2 = f(-1)$, ale $1 \neq -1$, což vyvrací prostotu f .

Na: Zvolme $y = 0 \in \mathbb{R}$. Protože pro $x \in \mathbb{R}$ platí $x^2 \geq 0$, máme $f(x) = x^2 + 1 \geq 1$ a tedy nemůže existovat $x \in \mathbb{R}$ splňující $f(x) = 0$.

Jiný argument: Pro $y = 0$ hledáme $x \in \mathbb{R}$ splňující $f(x) = 0$. Pak $x^2 + 1 = 0$ neboli $x^2 = -1$, což je nemožné.

Bonus: Uvažujme restrikcí $g = f|_{\langle 0, \infty \rangle}$. Toto je již prosté zobrazení: Dáno $x_1, x_2 \in \langle 0, \infty \rangle$, předpoklad $f(x_1) = f(x_2)$. Pak

$$x_1^2 + 1 = x_2^2 + 1 \quad \longrightarrow \quad x_1^2 = x_2^2 \quad \longrightarrow \quad |x_1| = |x_2|.$$

Protože $x_1, x_2 \geq 0$, absolutní hodnotu lze odebrat a máme $x_1 = x_2$.

Toto zobrazení je na množinu $\langle 1, \infty \rangle$. Důkaz: Dáno $y \in \langle 1, \infty \rangle$. Chceme, $f(x) = y$ neboli $x^2 + 1 = y$, odtud $x = \pm\sqrt{y-1}$. Protože $y \geq 1$, odmocnina má smysl a můžeme zvolit $x_0 = \sqrt{y-1}$. Pak $x_0 \in \langle 0, \infty \rangle$ a platí

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

Dokázali jsme, že f je bijekce, a také našli kandidáta na inverzní funkci $g(y) = \sqrt{y-1}$. Jeho správnost se potvrdí obvyklým způsobem.

3. Uvažujme $f(x) = x^3 - x$. 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 $0 = 1$. Tím jsme našli protipříklad. Protože nejde o bijekci, nemá ani inverzní funkci.

Zjistit to standardním postupem vede na problémy. Testování prostoty nás zavede od $f(x_1) = f(x_2)$ k rovnosti $x_1^3 - x_1 = x_2^3 - x_2$, se kterou algebraicky nic nesvedeme, ale možná někoho napadne, že pro $x_1 = 1$ a $x_2 = 0$ je pravdivá, což vede na protipříklad. Je to ovšem nejisté. Testování surjektivit vede od $f(x) = y$ ke snaze vyjádřit z rovnice $x^3 - x = y$ proměnnou x , což je nemožné. To ovšem neznamená, že f není na; možná správné x existuje (taky že ano), jen ho neumíme najít.

Bonus: Uvažujme restrikcí tohoto f na množinu $\langle 1, \infty \rangle$. Je to bijekce z $\langle 1, \infty \rangle$ na $\langle 0, \infty \rangle$, ovšem standardním postupem to nemáme šanci dokázat, dokonce ani rozpoznat, protože to vede na stejnou problematickou algebru jako u původního f . Zde pomohou nástroje matematické analýzy. Například pomocí derivace snadno ukážeme, že f je na intervalu $\langle 1, \infty \rangle$ rostoucí, což již implikuje prostotu.

△

Poznámka o reálných funkcích:

Prostota a pojem inverzní funkce hrají významnou roli v reálné analýze.

Prosté funkce poznáme podle toho, že jejich grafy nikdy nenabývají stejnou hodnotu vícekrát. Vizualně to znamená, že neexistuje vodorovná přímková čára, která by graf protla vícekrát. V praxi se prostota obvykle dokazuje pomocí ryzí monotonie, tedy dokáže se (pomocí derivace), že zkoumaná funkce je rostoucí, popřípadě klesající.

U reálných funkcí je prostota primární, protože cílová množina nebývá dána, ale určuje se podle potřeby. Jakmile tedy máme prostou funkci, tak si jako cílovou množinu vezmeme její obor hodnot a hned máme i bijekci, tedy také inverzní funkci k ní.

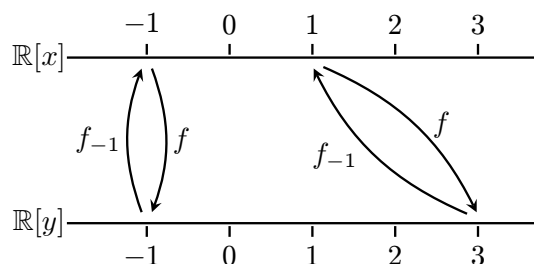
Navzájem inverzní funkce se při skládání navzájem „vykrátí“, například $e^{\ln(x)} = x$ pro $x > 0$ a $\ln(e^x) = x$ pro $x \in \mathbb{R}$. To se velmi hodí při praktické práci s těmito funkcemi.

Z pohledu teorie zde máme problém se zápisem. 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. Pokud u reálných funkcí 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, díky čemuž se vyhneme nejasnostem. Například u funkce číslo 2 v předchozím příkladě máme $f_{-1}(y) = \sqrt{y-1}$. Třeba se to časem ujme.

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 presentován coby „Napište rovnost $f(x) = y$, prohodte 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 . Obrázek jasně ukazuje, že funkce f_{-1} vůbec neumí s prvky x pracovat, protože má jako výchozí množinu úplně jiný svět. Nemá tedy smysl tyto proměnné prohazovat, naopak zachováním y čtenáři jasně sdělujeme, odkud a kam funkce f_{-1} jde.



Rozdíl se ještě zvýrazní v aplikacích, kdy mají jednotlivé proměnné svůj význam. Jestliže t značí čas, s pozici a funkce $s = f(t)$ mi říká, kde jsem byl v rozličných časech, pak zcela logicky musí inverzní zobrazení mít jako proměnnou pozici, tedy $t = f_{-1}(s)$.

△

Poznámka: V poznámce 8a.1 jsme viděli, že pro $A = \emptyset$ existuje jediné, a to prázdné zobrazení do nějaké množiny B . Takové zobrazení je prosté. Pokud je také $B = \emptyset$, tak je prázdné zobrazení bijekce.

△

Zavedli jsme tři nové vlastnosti a hodí se vědět, jak interagují s operacemi.

**Věta 8b.3.**

Nechť $T: A \mapsto B$ a $S: B \mapsto C$ jsou zobrazení. Pak platí:

- (i) Jestliže jsou T a S prosté, tak je také $S \circ T$ prosté.
- (ii) Jestliže jsou T a S na, tak je také $S \circ T$ na.
- (iii) Jestliže jsou T a S bijekce, tak je také $S \circ T$ 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 8b.1 invertibilní, tudíž dle věty 8a.6 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 vylepšit nedostatek vlastností? Podívejte se na cvičení 8b.7.

Spojením věty 8b.1 a faktu 8a.5 dostaneme následující.

**Věta 8b.4.**

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

Bude se nám to hodit.

Cvičení

Cvičení 8b.1 (rutinní, zkouškové): Pro následující funkce $\mathbb{R} \mapsto \mathbb{R}$ rozhodněte, zda jsou prosté a zda jsou na. Svě odpovědi dokažte.

Pokud je některé f bijekce, najděte k němu inverzní zobrazení a dokažte, že je správně.

- a) $f(x) = 2x + 4$;
- b) $f(x) = 1 - x^2$;
- c) $f(x) = x^3 + 13$;
- d) $f(x) = |x|$;
- e) $f(x) = e^x$;
- f) $f(x) = \sin(x)$.

Cvičení 8b.2 (rutinní, zkouškové, *dobré): Pro následující zobrazení rozhodněte, zda jsou prosté a zda jsou na. Svě odpovědi dokažte.

Pokud je některé T bijekce, najděte k němu inverzní zobrazení a dokažte, že je správně.

- a) $T(n) = n + 1$ ze \mathbb{Z} do \mathbb{Z} ;
- b) $T(n) = n + 1$ z \mathbb{N} do \mathbb{N} ;
- c) $T(n) = 13n$ ze \mathbb{Z} do \mathbb{Z} ;
- d) $T(x) = 13x$ z \mathbb{Q} do \mathbb{Q} ;
- e) $T(n) = n \pmod{3}$ z \mathbb{N} do \mathbb{N}_0 ;
- f) $T(n) = n^3$ ze \mathbb{Z} do \mathbb{Z} ;
- g) $T(x) = x^3$ z $\langle 0, \infty \rangle$ do \mathbb{R} ;
- h) $T(n) = \lfloor \frac{n}{2} \rfloor$ ze \mathbb{Z} do \mathbb{Z} ;
- i)* $f(n) = (-1)^n n$ z \mathbb{N}_0 do \mathbb{Z} ;
- j)* $f(n) = (-1)^n \lfloor \frac{n+1}{2} \rfloor$ z \mathbb{N}_0 do \mathbb{Z} .

Cvičení 8b.3 (rutinní, zkouškové, *dobré): Pro následující zobrazení rozhodněte, zda jsou prosté a zda jsou na. Svě odpovědi dokažte.

Pokud je některé T bijekce, najděte k němu inverzní zobrazení a dokažte, že je správně.

- a) $T(n) = (n + 1, 2n)$ z \mathbb{N} do $\mathbb{N} \times \mathbb{N}$;
- b) $T(n) = (n^2, n^2 + 2n)$ ze \mathbb{Z} do $\mathbb{Z} \times \mathbb{Z}$;
- c) $T(m, n) = (m + 1, m - n)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
- d) $T(m, n) = (m + 1, mn)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
- e) $T(m, n) = (m^2, mn)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
- f) $T(x, y) = (x + y, x - y)$ z $\mathbb{Q} \times \mathbb{Q}$ do $\mathbb{Q} \times \mathbb{Q}$;
- g) $T(m, n) = (m + n, m - n)$ ze $\mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z} \times \mathbb{Z}$;
- h) $T(m, n) = 2m - n$ ze $\mathbb{Z} \times \mathbb{Z}$ do \mathbb{Z} ;
- i) $T(m, n) = m + n + 13$ ze $\mathbb{Z} \times \mathbb{Z}$ do \mathbb{Z} ;
- j)* $T(m, n) = m - n$ z $\mathbb{N} \times \mathbb{N}$ do \mathbb{Z} ;
- k)* $T(m, n) = 2^n 3^m$ ze $\mathbb{N} \times \mathbb{N}$ do \mathbb{N} ;
- l)* $T(m, n) = m^2 - n^2$ ze $\mathbb{Z} \times \mathbb{Z}$ do \mathbb{Z} .

Cvičení 8b.4 (poučné): a) Uvažujte následující předpis: $T(p, q) = \frac{p}{q}$. Dostáváme tak bijekci ze $\mathbb{Z} \times \mathbb{N}$ na \mathbb{Q} ?

b) Uvažujte následující předpis: $T\left(\frac{p}{q}\right) = (p, q)$. Dostáváme tak bijekci z \mathbb{Q} na $\mathbb{Z} \times \mathbb{N}$?

Cvičení 8b.5 (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} .

Viz poznámka 7d.b.

Cvičení 8b.6 (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 8b.7 (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.

a) Jestliže T není prosté, tak $S \circ T$ není prosté.

d) Jestliže S není na, tak $S \circ T$ není na.

b) Jestliže S není prosté, tak $S \circ T$ není prosté.

e) Jestliže T není bijekce, tak $S \circ T$ není bijekce.

c) Jestliže T není na, tak $S \circ T$ není na.

f) Jestliže S není bijekce, tak $S \circ T$ není bijekce.

Obrázky mohou významně pomoci.

Cvičení 8b.8 (poučné): Nechť $T: A \mapsto B$ je prosté zobrazení.

a) Dokažte, že pro libovolnou podmnožinu M množiny A je restrikce $T|_M$ prosté zobrazení.

b) Dokažte, že jestliže pro libovolnou nadmnožinu D množiny B uvažujeme zobrazení $S: A \mapsto D$ dané $S(x) = T(x)$ pro $x \in A$, pak S je prosté.

Poznámka: Prostě zachováme T , jen mu změňme cílovou množinu, čímž vznikně formálně jiné zobrazení.

Cvičení 8b.9 (rutinní, poučné): Nechť $n \in \mathbb{N}$, $n \geq 2$. Uvažujme množiny A_0, A_1, \dots, A_n a zobrazení $T_i: A_{i-1} \mapsto A_i$ pro $i = 1, \dots, n$. Dokažte následující:

a) Jestliže jsou všechna tato zobrazení prostá, pak je prosté i $T_n \circ \dots \circ T_1$.

b) Jestliže jsou všechna tato zobrazení na, pak je na i $T_n \circ \dots \circ T_1$.

c) Jestliže jsou všechna tato zobrazení bijekce, pak je bijekce i $T_n \circ \dots \circ T_1$.

(Viz fakt 8b.3.)

Cvičení 8b.10 (poučné, *dobré): Nechť $T: A \mapsto B$ je zobrazení, $M, N \subseteq A$. Dokažte, že pak platí:

a) $T[M \cup N] = T[M] \cup T[N]$;

b) $T[M \cap N] \subseteq T[M] \cap T[N]$.

c)* Je-li T prosté, pak $T[M \cap N] = T[M] \cap T[N]$.

d) Ukažte, že obecně $T[M \cap N] = T[M] \cap T[N]$ neplatí.

Cvičení 8b.11 (poučné, dobré): Uvažujte zobrazení $T: A \mapsto B$. Dokažte následující tvrzení:

a) 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 $T[T^{-1}[N]] = N$.

b) 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.

Řešení:

8b.1: a) Je prosté: $f(x) = f(y) \rightarrow 2x + 4 = 2y + 4 \rightarrow x = y$. Je na: $y \in \mathbb{R}$, $2x + 4 = y \rightarrow \exists x = \frac{1}{2}(y - 4) \in \mathbb{R}$. Je to bijekce, $f_{-1}(y) = \frac{1}{2}(y - 4)$. Ověření: $f_{-1}(f(x)) = f_{-1}(2x + 4) = \frac{1}{2}((2x + 4) - 4) = x$, $f(f_{-1}(y)) = f\left(\frac{1}{2}(y - 4)\right) = 2 \cdot \frac{1}{2}(y - 4) + 4 = y$.

b) Není prosté, třeba $f(1) = 0 = f(-1)$. Není na: nelze $T(x) = 13$ pro $x \in \mathbb{R}$ neboť $1 - x^2 \leq 1$.

c) Je prosté: $f(x) = f(y) \rightarrow x^3 + 13 = y^3 + 13 \rightarrow x = y$. Je na: $y \in \mathbb{R}$, $x^3 + 13 = y \rightarrow \exists x = (y - 13)^{1/3} \in \mathbb{R}$. Je to bijekce, $f_{-1}(y) = (y - 13)^{1/3}$. Ověření: $f_{-1}(f(x)) = f_{-1}(x^3 + 13) = ((x^3 + 13) - 13)^{1/3} = x$, $f(f_{-1}(y)) = f\left((y - 13)^{1/3}\right) = \left((y - 13)^{1/3}\right)^3 + 13 = y$.

d) Není prosté, třeba $f(1) = 1 = f(-1)$. Není na: nelze $f(x) = -13$ pro $x \in \mathbb{R}$ neboť $|x| \geq 0$.

e) Je prosté: $f(x) = f(y) \rightarrow e^x = e^y \rightarrow x = y$. Není na: nelze $f(x) = -13$ pro $x \in \mathbb{R}$ neboť $e^x > 0$.

f) Není prosté, třeba $f(0) = f(2\pi)$. Není na: nelze $f(x) = 13$ pro $x \in \mathbb{R}$ neboť $|\sin(x)| \leq 1$.

8b.2: a) Je prosté: $T(x) = T(y) \rightarrow x + 1 = y + 1 \rightarrow x = y$. Je na: $b \in \mathbb{Z}, n + 1 = b \rightarrow \exists n = b - 1 \in \mathbb{Z}$. Je to bijekce, $T^{-1}(b) = b - 1$. Ověření: $T^{-1}(T(a)) = T^{-1}(a + 1) = (a + 1) - 1 = a$, $T(T^{-1}(b)) = T(b - 1) = (b - 1) + 1 = b$.

b) Je prosté: $T(x) = T(y) \rightarrow x + 1 = y + 1 \rightarrow x = y$. Není na: neexistuje $n \in \mathbb{N}$ aby $n + 1 = 1$, proto $1 \notin \text{ran}(T)$.

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

d) Je prosté: $T(x) = T(y) \rightarrow 13x = 13y \rightarrow x = y$. Je na: $y \in \mathbb{Q} \rightarrow \exists x = \frac{1}{13}y \in \mathbb{Q}: T(x) = T(\frac{y}{13}) = 13 \cdot \frac{y}{13} = y$. Je to bijekce, $T^{-1}(y) = \frac{1}{13}y$. Ověření: $T^{-1}(T(x)) = T^{-1}(13x) = \frac{1}{13}(13x) = x$, $T(T^{-1}(y)) = T(\frac{1}{13}y) = 13 \cdot \frac{1}{13}y = y$.

e) Není prosté, třeba $T(1) = T(4) = 1$. Není na: neexistuje $n \in \mathbb{Z}$ aby $n \pmod{3} \geq 3$, proto $23 \notin \text{ran}(T)$.

f) Je prosté: $T(x) = T(y) \rightarrow x^3 = y^3 \rightarrow x = y$. Není na: neexistuje $n \in \mathbb{Z}$ aby $x^3 = 2$, proto $2 \notin \text{ran}(T)$.

g) Je prosté: $T(x) = T(y) \rightarrow x^3 = y^3 \rightarrow x = y$. Není na: neexistuje $x \geq 0$ aby $x^3 = -1$, proto $-1 \notin \text{ran}(T)$.

h) Není prosté, třeba $T(2) = 1 = T(3)$. Je na: $b \in \mathbb{Z} \rightarrow \exists n = 2b \in \mathbb{Z}: T(n) = T(2b) = \lfloor b \rfloor = b$.

i) Je prosté: $T(x) = T(y) \rightarrow (-1)^x x = (-1)^y y \rightarrow |(-1)^x x| = |(-1)^y y| \rightarrow |x| = |y|$. Pak také $(-1)^x = (-1)^y$, tedy z $(-1)^x x = (-1)^y y$ je $x = y$. Není na: neexistuje $n \in \mathbb{Z}$ aby $(-1)^n n = 1$, proto $1 \notin \text{ran}(T)$.

j) 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 $b \in \mathbb{Z}$. Pokud $b \geq 0$, pak existuje $n = 2b \in \mathbb{N}_0$ a $T(n) = 1 \cdot \lfloor b + \frac{1}{2} \rfloor = b + \lfloor \frac{1}{2} \rfloor = b$.

Pokud $b < 0$, pak $-2b \geq 2$ a existuje $n = -2b - 1 \in \mathbb{N}_0$ takové, že $T(n) = (-1) \cdot \lfloor -b \rfloor = b$. Je to bijekce, $T^{-1}(b) = 2|b|$ pro $b \geq 0$ a $T^{-1}(b) = 2|b| - 1$ pro $b < 0$. Ověření necháme čtenáři.

8b.3: a) Je prosté: $T(x) = T(y) \rightarrow (x + 1, 2x) = (y + 1, 2y) \rightarrow 2x = 2y \rightarrow x = y$. Není na: neexistuje $n \in \mathbb{N}$ aby $n + 1 = 1$ a $2n = 1$, proto $(1, 1) \notin \text{ran}(T)$.

b) Je prosté: $T(x) = T(y) \rightarrow (x^2, x^2 + 2x) = (y^2, y^2 + 2y) \rightarrow x^2 = y^2 \wedge x^2 + 2x = y^2 + 2y \rightarrow 2x = 2y \rightarrow x = y$. Není na: neexistuje $n \in \mathbb{Z}$ aby $n^2 = 0$ a $n^2 + 2n = 1$, proto $(0, 1) \notin \text{ran}(T)$.

c) Je prosté: $T(m, n) = T(u, v) \rightarrow (m + 1, m - n) = (u + 1, u - v) \rightarrow m + 1 = u + 1 \wedge m - n = u - v \rightarrow m = u \wedge m - n = m - v \rightarrow m = u \wedge n = v \rightarrow (m, n) = (u, v)$. Je na: $(u, v) \in \mathbb{Q}^2, (m + 1, m - n) = (u, v) \rightarrow \exists m = u - 1, n = u - 1 - v \in \mathbb{Z}$ a $T(m, n) = (u, v)$. Je to bijekce, $T^{-1}(u, v) = (u - 1, u - 1 - v)$. Ověření: $T^{-1}(T(m, n)) = T^{-1}(m + 1, m - n) = ((m + 1) - 1, (m + 1) - 1 - (m - n)) = (m, n)$, $T(T^{-1}(u, v)) = T(u - 1, u - 1 - v) = ((u - 1) + 1, (u - 1) - (u - 1 - v)) = (u, v)$.

d) Není prosté: $T(m, n) = T(u, v) \rightarrow (m + 1, mn) = (u + 1, uv) \rightarrow m + 1 = u + 1 \wedge mn = uv \rightarrow m = u \wedge mn = mv$. Z toho nejde získat $n = v$ pokud $m = 0$. Takže $T(0, 13) = (1, 0) = T(0, 23)$. Není na: neexistuje $m, n \in \mathbb{N}$ aby $m + 1 = 23$ a $mn = 13$, proto $(23, 13) \notin \text{ran}(T)$. Taky nejde $m + 1 = 1$ a mn nenulové.

e) Není prosté, třeba $T(2, 0) = (4, 0) = T(-2, 0)$. Není na: neexistují $m, n \in \mathbb{Z}$ aby $m^2 = 0$ a $mn = 1$, proto $(0, 1) \notin \text{ran}(T)$. Taky nejde $m^2 = 2$ atd.

f) Je prosté: $T(m, n) = T(u, v) \rightarrow (m + n, m - n) = (u + v, u - v) \rightarrow m + n = u + v \wedge m - n = u - v$, sečteme: $2m = 2u \rightarrow m = u$, odečteme: $2n = 2v \rightarrow n = v$, proto $(m, n) = (u, v)$.

Je na: $(u, v) \in \mathbb{Q}^2, (m + n, m - n) = (u, v) \rightarrow \exists m = \frac{1}{2}(u + v), n = \frac{1}{2}(u - v) \in \mathbb{Q}$ a $T(m, n) = (u, v)$.

Bijekce, inverze $T^{-1}(u, v) = (\frac{1}{2}(u + v), \frac{1}{2}(u - v))$. Ověření standardní.

g) Je prosté: $T(m, n) = T(u, v) \rightarrow (m + n, m - n) = (u + v, u - v) \rightarrow m + n = u + v \wedge m - n = u - v$, sečteme: $2m = 2u \rightarrow m = u$, odečteme: $2n = 2v \rightarrow n = v$, proto $(m, n) = (u, v)$.

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

h) Není prosté, třeba $T(1, 2) = 0 = T(0, 0)$. Je na: $b \in \mathbb{Z} \rightarrow \exists m = 0, n = -b \in \mathbb{Z}: T(m, n) = b$.

i) Není prosté, třeba $T(1, -1) = 13 = T(-1, 1)$. Je na: $b \in \mathbb{Z} \rightarrow \exists m = b, n = -13 \in \mathbb{Z}$ a $T(m, n) = b$.

j) Není prosté, třeba $T(1, 1) = 0 = T(2, 2)$. Je na: Nechť $b \in \mathbb{Z}$. Pokud $b = 0$, volíme $m = 1, n = 1$. Pokud $b > 0$, volíme $m = b + 1, n = 1 \in \mathbb{N}$ a $T(m, n) = b$. Pokud $b < 0$, volíme $m = 1, n = -b + 1 \in \mathbb{N}$ a $T(m, n) = b$.

k) Je prosté: $T(m, n) = T(u, v) \rightarrow 2^m 3^n = 2^u 3^v \rightarrow m = u \wedge n = v$ dle jednoznačnosti rozkladu, proto $(m, n) = (u, v)$. Není na: Pro $m, n \in \mathbb{Z}$ nelze $2^m 3^n = 13$, proto $13 \notin \text{ran}(T)$.

l) 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.

8b.4: a) Je evidentně na, ale není prosté $T(2, 4) = \frac{2}{4} = \frac{1}{2} = T(1, 2)$. Takže to není bijekce.

b) 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 ...

8b.5: Není prosté, protože $T(1) = 4 = T(8)$. Je na, pro $b \in \mathbb{N}$ existuje $n = 2b \in \mathbb{N}$ takové, že $T(n) = b$.

8b.6: $\mathbb{N} \mapsto \mathbb{N}: T(n) = n$ 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, nebo $T(n) = \lfloor \frac{1}{2}n \rfloor + 1. T(n) = (n - 3)^2 + 2$ není prosté ani na, nebo $T(n) = \lfloor \frac{1}{2}n \rfloor + 2$.

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

8b.7: Obměny: a) Jestliže je $S \circ T$ prosté, tak T je prosté. b) Jestliže je $S \circ T$ prosté, tak S je prosté.

c) Jestliže je $S \circ T$ na, tak T je na. d) Jestliže je $S \circ T$ na, tak S je na.

e) Jestliže je $S \circ T$ bijekce, tak T je bijekce. f) Jestliže je $S \circ T$ bijekce, tak S je bijekce.

a) Platí, T není prosté $\rightarrow \exists x \neq y \in A: T(x) = T(y)$, pak $S(T(x)) = S(T(y))$ neboli $(S \circ T)(x) = (S \circ T)(y)$.

d) 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.

b), c), e), f) 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.

8b.8: a) 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 $x = y$.

b) Nechť $x, y \in A$ splňují $S(x) = S(y)$. Podle definice pak $T(x) = T(y)$ a T je prosté, proto $x = y$.

8b.9: Hromadný důkaz pro a) až c). (0) Pro $n = 1$ zjevně platí.

(1) $n \geq 1$, IP: viz vlastnosti. Nechť dány $T_1, T_2, \dots, T_n, T_{n+1}$, které mají příslušnou vlastnost (prosté pro (i), na pro (ii), bijekce pro (iii)). Podle indukčního předpokladu má i $S = T_n \circ \dots \circ T_1$ příslušnou vlastnost, pak podle faktu 8b.3 tu vlastnost má i $T_{n+1} \circ S$ neboli $T_{n+1} \circ T_n \circ \dots \circ T_1$.

8b.10: a) $b \in T[M \cup N] \rightarrow \exists a \in M \cup N: T(a) = b$. Dvě možnosti. $a \in M \rightarrow T(a) \in T[M] \rightarrow b = T(a) \in T[M] \cup T[N]$. Nebo $a \in N \rightarrow T(a) \in T[N] \rightarrow b = T(a) \in T[M] \cup T[N]$.

Naopak: $b \in T[M] \cup T[N]$, dvě možnosti. $b \in T[M] \rightarrow \exists a \in M: T(a) = b$. Pak $a \in M \cup N$ a tedy $b = T(a) \in T[M \cup N]$. Nebo $b \in T[N]$ atd.

b) $b \in T[M \cap N] \rightarrow \exists a \in M \cap N: T(a) = b$. Pak $a \in M$, tedy $b = T(a) \in T[M]$, také $a \in N$, tedy $b = T(a) \in T[N]$. Proto $b \in T[M] \cap T[N]$.

c) $b \in T[M] \cap T[N] \iff b \in T[M] \wedge b \in T[N] \iff (\exists a_1 \in M: T(a_1) = b) \wedge (\exists a_2 \in N: T(a_2) = b)$. Protože je T prosté, musí nutně být $a_1 = a_2$, označme $a = a_1 = a_2$ a vidíme, že $a \in M \cap N$, proto $a \in M \cap N$ a $T(a) = b$, tedy $b \in T[M \cap N]$.

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

8b.11: a) Nechť $a \in A$. Pak $T(a) \in T[M]$ a tedy i $T^{-1}(T(a)) \in T^{-1}[T[M]]$. 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 $T^{-1}(b) = a$, tedy $T(a) = b$. Protože $b \in T[M]$, musí existovat $\tilde{a} \in M$ takové, že $T(\tilde{a}) = b$. Protože je T prosté, nutně $\tilde{a} = a$, tedy $a \in M$. Opravdu $T^{-1}[T[M]] \subseteq M$.

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

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

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

8c. Posloupnosti

V řadě aplikací jsme v situaci, kdy nám postupně přicházejí data, jedno číslo po druhém. Rádi bychom to matematicky zachytili. Přirozený přístup je ta přicházející čísla označit jako první, druhé, třetí atd. a uložit třeba ve vektoru. Pokud například přišla čísla 1, 3, 5, tak bychom je uložili jako (1, 3, 5), což přirozeně vede na značení (a_1, a_2, a_3) , kde $a_1 = 1$, $a_2 = 3$, $a_3 = 5$. Mohli bychom tedy pracovat s prostory vektorů, třeba \mathbb{R}^n .

To ovšem nestačí v případě, že počet dat není omezen a je tedy potřeba mít místo na nekonečně mnoho. Pomohlo by něco jako „nekonečný vektor“, ale budeme tomu říkat posloupnost. Potřebujeme ji nějak zavést pomocí pojmů, které už známe, a na to se vrátíme k představě, že si jednotlivá data očíslováme a značíme $a_1 = 1$, $a_2 = 3$ atd. Vzniká tak přiřazení neboli zobrazení, v našem případě a z $\{1, 2, 3\}$ třeba do \mathbb{R} , které splňuje $a(1) = 1$, $a(2) = 3$, $a(3) = 5$. Pokud nám přichází nekonečně dat, tak číslování první, druhé, atd. vede přirozeně na zobrazení z \mathbb{N} do \mathbb{R} .

Jsme skoro zralí na definici, zbývá poznamenat, že někdy je praktické nečíslovat přicházející data jako první, druhé, \dots , ale spíše nulté, první, druhé, \dots , nebo třeba šesté, sedmé, osmé, \dots . Abychom to umožnili, dovolíme zobrazením, která taková data zachycují, aby měly definiční obor typu $\{n \in \mathbb{Z}; n \geq n_0\}$ pro nějaké $n_0 \in \mathbb{Z}$.

**Definice.**

Posloupnost je libovolné zobrazení a z nějaké množiny $\{n_0, n_0 + 1, n_0 + 2, \dots\}$ do \mathbb{R} , kde $n_0 \in \mathbb{Z}$.

Takovou posloupnost značíme $(a_k)_{k=n_0}^{\infty}$, kde $a_k = a(k)$.

By a **sequence** we mean any mapping a from a set $\{n_0, n_0 + 1, n_0 + 2, \dots\}$ into \mathbb{R} , where $n_0 \in \mathbb{Z}$.

Such a sequence is denoted $(a_k)_{k=n_0}^{\infty}$, where $a_k = a(k)$.

! Rovnou varujeme čtenáře, že v českém prostředí je pro posloupnosti obvyklejší značení $\{a_k\}_{k=n_0}^{\infty}$, také já jsem na něm vyrostl a dlouho jsem je používal (třeba i v původní verzi této knihy), než jsem usoudil, že bych měl být na straně rozumu a ne tradice. Značky $\{ \}$ značí množinu, tedy kolekci, ve které na pořadí nezáleží a každý konkrétní prvek se počítá jen jednou, i když jej do množiny vložíme vícekrát. Takže $\{1, 1, 1, \dots\}$ je jednoprvková množina $\{1\}$.

Na druhou stranu posloupnost je kolekce hodnot, u kterých na pořadí záleží a hodnoty se mohou opakovat, aniž by z posloupnosti zmizely. Konečný počet uspořádaných hodnot, které se mohou opakovat, se standardně zaznamenává jako uspořádaná n -tice neboli vektor, je tedy přirozené vidět posloupnost jako nekonečný vektor a značení $(1, 1, 1, \dots)$ je intuitivní.

! **Příklad 8c.a:** Proč zavádíme nové jméno, když už máme zobrazení? Protože u posloupností měníme úhel pohledu natolik, že to vede na odlišné postupy.

Představme si, že nám jako data postupně přicházejí všechna kladná lichá čísla $1, 3, 5, 7, 9, 11, 13, \dots$. Zachytíme je jako posloupnost $(1, 3, 5, 7, \dots)$ a jednotlivá čísla můžeme číslovat jako první, druhé třetí, atd. To vede formálně na zobrazení $a(1) = 1, a(2) = 3$ atd. U posloupností ovšem preferujeme zápis $a_1 = 1, a_2 = 3$, atd. Dokonce máme obecný vzorec $a_k = 2k - 1$ pro $k \geq 1$.

Pokud se ovšem rozhodneme data číslovat jako nulté, první, druhé, atd., pak dostáváme zobrazení $b(0) = 1, b(1) = 3$ atd. Toto je jiné zobrazení než a , protože přiřazuje jinak: a posílá $2 \mapsto 3$, zatímco b posílá $2 \mapsto 5$. Proto jde o dvě různá zobrazení. Posloupnost je to nicméně stejná. To ukazuje, že tyto dva úhly pohledu jsou opravdu rozdílné.

Pokud přejdeme ke značení b_k , dostáváme $b_0 = 1, b_1 = 3$ atd., obecný vzorec je $b_k = 2k + 1$ pro $k \geq 0$. Vzorce $a_k = 2k - 1, k \geq 1$ a $b_k = 2k + 1, k \geq 0$ jsou různé, ale generují stejnou posloupnost. To znamená, že pokud nás zajímají jen data $1, 3, 5, 7, \dots$, tak se vyjádření zobrazením či vzorcem stává jen technickým nástrojem k získání hodnot, pro práci s těmito daty budeme potřebovat specializované postupy. Vyvineme nástroje, které respektují, že posloupnosti pocházejí ze zobrazení, ale zohledňují, že jedna posloupnost může pocházet z různých zobrazení (vzorců).

Zvolený nástroj se odvíjí od účelu. Zobrazení $T(n) = n^2$ pro $n \in \mathbb{N}$ vygeneruje čísla $1, 4, 9, 16, \dots$. Pokud by pro nás byla podstatná vazba devítky na trojku nebo třeba 81 na 9, pak bychom chtěli pracovat s tímto zobrazením. Pokud by nás ale zajímala čísla $1, 4, 9, 25, \dots$ jako taková, pak by byly vhodným přístupem posloupnosti.

△

Abychom mohli s posloupnostmi pracovat, potřebujeme nějak zadat její hodnoty. V jednoduchých případech lze použít slovní popis (posloupnost kladných lichých čísel uspořádaných dle velikosti, konstantní posloupnost jedniček atd.), ale perspektivnější je exaktnější přístup. Jsou tři populární možnosti specifikace posloupnosti.

1. Explicitní vzorec udává přímý výpočet hodnoty k -tého prvku posloupnosti pro k ze specifikovaného rozsahu. Možných zápisů je více, ukážeme to pro naši posloupnost lichých čísel:

- $a_k = 2k - 1, k \geq 1$;
- $a_k = 2k - 1$ pro $k \geq 1$;
- $(2k - 1)_{k=1}^{\infty}$ nebo $(2k - 1)_{k \geq 1}$ nebo $(2k - 1)_{k \in \mathbb{N}}$;
- $\{2k - 1\}_{k=1}^{\infty}$ nebo $\{2k - 1\}_{k \geq 1}$ nebo $\{2k - 1\}_{k \in \mathbb{N}}$.

Všimneme si, že první dva zápisy nám zároveň poskytly pro posloupnost jméno, což je ono „ a “, zatímco další dva zápisy ne. Je také možno psát $(a_k)_{k \in \mathbb{N}} = (2k - 1)_{k \in \mathbb{N}}$, tím je posloupnost pojmenovaná a definovaná.

Rovnou pozorníme, že rozsah pro indexy je klíčovou součástí specifikace. Pokud bychom napsali jen $a_k = 2k - 1$, tak nevznikne posloupnost, protože nejsme schopni určit její členy. Co je její první člen? Nevíme. Teprve specifikace $k \geq 7$ by nám řekla, že první člen je $a_7 = 13$. My jsme výše použili $k \geq 1$, pak je první člen $a_1 = 1$. Jinak řečeno, rozsah pro indexy má na identitu posloupnosti stejně významný dopad jako algebraický vzorec.

2. Implicitní specifikace je jen jiné jméno pro induktivní definici, například

(0) $a_1 = 1$;

(1) $a_{k+1} = a_k + 2$ pro $k \geq 1$.

3. Specifikace „výpisem“ zadá několik prvních členů následovaných třemi tečkami, čímž naznačujeme, že posloupnost pokračuje „stejným způsobem“, například $(1, 3, 5, 7, \dots)$. Jak už jsme zmiňovali, toto ve skutečnosti není definice, protože není jasné, co to je ten „stejný způsob“. Jde nicméně o účinný způsob prezentace, budeme jej tedy používat k ilustrativním účelům.

! Příklad 8c.b: Vraťme se k posloupnosti $(1, 3, 5, 7, \dots)$. Našli jsme explicitní předpisy $a_k = 2k - 1$, $k \geq 1$. Uvedení rozsahu pro index je povinné, nicméně volba proměnné pro index je nepodstatná a lze ji ve specifikaci zaměnit za jinou (ovšem všude). Například specifikace $a_n = 2n - 1$, $n \geq 1$ udává stejnou posloupnost, $a_1 = 1$, $a_2 = 3$, atd. Index je jen pracovní proměnná, která je v definici lokální.

Viděli jsme také implicitní specifikaci, podívejme se blíže na „třítečkový“ pokus $(1, 3, 5, 7, \dots)$. Varovali jsme, že to není korektní specifikace, což lze vidět například na tom, že vůbec není jasné, jaké číslo přijde po sedmičce.

Mohlo by jít o posloupnost $a_k = 2k - 1$, $k \geq 1$ lichých čísel, pak by další číslo v seznamu bylo 9. Klidně by to ovšem mohlo být číslo 11, pokud by to byla posloupnost lichých nesložených čísel (tedy jednička a pak lichá prvočísla). Tato alternativní verze není nijak méně přirozená než ta první (má snad někdo méně rád prvočísla než lichá čísla)?

Ovšem také by to další číslo mohla být třináctka, pokud by šlo o posloupnost definovanou předpisem

$$(0) \ c_0 = 1, \ c_1 = 3, \ c_2 = 5;$$

$$(1) \ c_{k+1} = c_k + 2c_{k-2} \text{ pro } k \geq 2.$$

I toto je dozajista pěkný vzorec. No a také by dalším číslem mohla být dvojka, pokud by šlo o posloupnost $d_k = \frac{1}{2}k - \frac{1}{2}k^2 + 2^{k+1} - k!$ pro $k \geq 0$. Možná to není nejpěknější vzorec, ale na to se nehraje.

△

Studium posloupností začneme otázkou, jak poznáme, že dva zápisy $(a_k)_{k \geq n_0}$ a $(b_k)_{k \geq m_0}$ specifikují stejnou posloupnost. Rozhodne, zda generují stejné hodnoty. Chceme, aby obě posloupnosti měly shodný první člen, tedy $a_{n_0} = b_{m_0}$, shodný druhý člen, tedy $a_{n_0+1} = b_{m_0+1}$, shodný třetí člen, tedy $a_{n_0+2} = b_{m_0+2}$ atd.

Definice.

Posloupnosti $(a_k)_{k \geq n_0}$ a $(b_k)_{k \geq m_0}$ jsou shodné, psáno $(a_k)_{k \geq n_0} = (b_k)_{k \geq m_0}$, jestliže pro všechna $n \in \mathbb{N}_0$ platí $a_{n_0+n} = b_{m_0+n}$.

Pokud jsou obě posloupnosti zadány explicitně, pak tento test odpovídá otázce, zda lze jeden vzorec převést na druhý „substitucí“ v indexu. Posun indexu je u posloupností (a sum) oblíbený nástroj, který někdy může zjednodušit vzorec pro členy posloupnosti, jindy zase umožní nastavit začátek indexace na žádanou hodnotu (což se hodí, když chceme posloupnosti sčítat či odčítat a podobně).

Substituce je proces, kdy jednu indexační proměnnou, řekněme k , chceme nahradit jinou proměnnou, řekněme n , pomocí konkrétního vzorce $k = f(n)$. Při tomto procesu musí být posloupnost zachována, tedy nesmí se žádné členy ztratit ani přibýt a musí zůstat v původním pořadí. To klade striktní nároky na substituční funkci f :

- f musí být rostoucí,
- f musí převádět množinu $\{k \in \mathbb{Z}; k \geq n_0\}$ indexů k na množinu typu $\{n \in \mathbb{Z}; n \geq m_0\}$.

Těmto požadavkům vyhoví jedině posuny, tedy substituce typu $k = n + c$ pro nějaké $c \in \mathbb{Z}$. Substituce se provede takto:

S Algoritmus 8c.1.

Substituce indexu v posloupnosti $(f(k))$ pro $k \geq n_0$.

0. Zvolíme $c \in \mathbb{Z}$ určující posun, nový index $n = k - c$ splňuje $k = n + c$.

1. Všechny výskyty k nahradíme výrazem $n + c$, dostaneme tak posloupnost $(f(n + c))$ pro $n + c \geq n_0$.

2. Upravíme specifikaci rozsahu, někdy také vzorec pro posloupnost a obdržíme předpis $(g(n))$ pro $n \geq n_0 - c$.

△

Příklad 8c.c: Vraťme se k příkladu 8c.a. Chceme zjistit, zda se rovnají posloupnosti $a_k = 2k - 1$ pro $k \geq 1$ a $b_k = 2k - 1$, $k \geq 0$.

Podle definice máme ověřit, zda pro všechna $n \in \mathbb{N}_0$ platí $a_{1+n} = b_{0+n}$. To znamená testovat rovnost $2(1+n) - 1 = 2(0 + n) + 1$ neboli $0 = 0$, což platí.

Alternativní postup: Máme posloupnost $(2k - 1)_{k \geq 1}$. Zkusíme posunout index tak, aby začínal číslem 0, a uvidíme, zda se pak členy budou shodovat s posloupností (b_n) . Nový index n má být 0 když $k = 1$, což zařídí posun $n = k - 1$. Pak $k = n + 1$ a substituce do $(a_k)_{k \geq 1}$ dává posloupnost

$$(2(n + 1) - 1)_{n+1 \geq 1} = (2n + 1)_{n \geq 0}.$$

Shoda s $(b_n)_{n \geq 0}$ potvrzena.

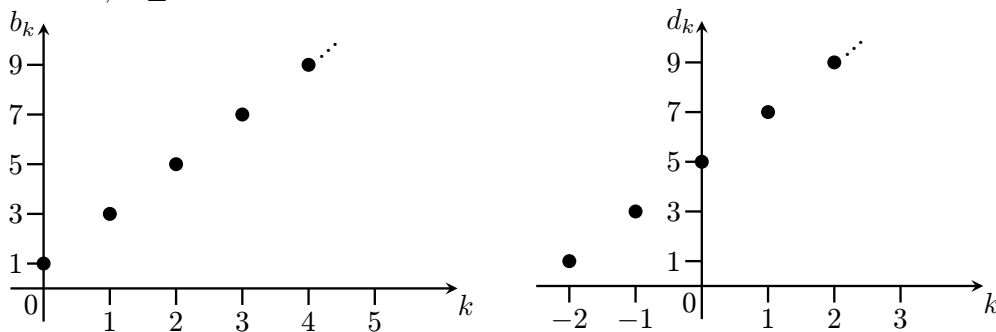
Jako trénink ještě odvodíme vzorec pro stejnou posloupnost, jehož indexace začne řekněme pětkou. Vyjdeme ze vzorce $(a_k)_{k \geq 1}$ a v případě $k = 1$ chceme mít $m = 5$, což zařídí posun $m = k + 4$. Pak $k = m - 4$ a dostáváme nový vzorec

$$(2(m-4) - 1)_{m-4 \geq 1} = (2m-9)_{m \geq 5}.$$

Označme třeba $c_m = 2m - 9$ pro $m \geq 5$, pak $c_5 = 1$, $c_6 = 3$, $c_7 = 5$ atd., to souhlasí.

△

Při zkoumání posloupností nám pomáhá jejich vizualizace. Coby zobrazení je můžeme zobrazit pomocí grafu. Vlevo vidíme graf posloupnosti $(1, 3, 5, 7, \dots)$ vyjádřený předpisem $b_k = 2k + 1$, $k \geq 0$. Svislou osu jsme naškalovali, aby se nám těch bodů vešlo do obrázku víc. Na obrázku vpravo vidíme tutéž posloupnost, tentokrátoby graf posloupnosti $d_k = 2k + 5$, $k \geq -2$.



Vidíme, že druhá posloupnost má stejné hodnoty, jen posunutá doleva, což z hlediska posloupností není podstatné. Vodorovná pozice posloupnosti na grafu je tedy irelevantní.

Kromě posunu lze u posloupností dělat ještě jeden užitečný trik: vynechání začátku. Dělá se to snadno, prostě se místo původního n_0 použije nějaké větší n_1 . Pokud například namísto $(2k + 1)_{k \geq 0}$ uvažujeme $(2k + 1)_{k \geq 3}$, tak jsme z původní posloupnosti vynechali členy 1, 3, 5 a naše posloupnost teď začíná $(7, 9, 11, 13, \dots)$. Není to nic hlubokého, ale občas se tato představa hodí.

Pro posloupnosti existují dvě základní operace: Posloupnosti můžeme sčítat (popřípadě odčítat) a násobit konstantou. Jako inspirace poslouží operace s vektory. Abychom mohli operace definovat, potřebujeme mít posloupnosti popsány a ke sčítání dvou posloupností je potřeba, aby příslušné popisy používaly stejnou indexaci. To se pro dvě dané posloupnosti snadno zařídí posunem indexu.

Definice.

Nechť $(a_k)_{k \geq n_0}$ a $(b_k)_{k \geq n_0}$ jsou posloupnosti a $c \in \mathbb{R}$. Definujeme následující operace:

$$(a_k)_{k \geq n_0} + (b_k)_{k \geq n_0} = (a_k + b_k)_{k \geq n_0},$$

$$c(a_k)_{k \geq n_0} = (ca_k)_{k \geq n_0}.$$

Například $(1, 1, 1, 1, 1, \dots) + (1, 2, 3, 4, 5, 6, \dots) = (2, 3, 4, 5, 6, 7, \dots)$ a $3 \cdot (1, 2, 3, 4, 5, 6, \dots) = (3, 6, 9, 12, 15, 18, \dots)$.

Množina všech posloupností s těmito operacemi tvoří vektorový prostor. Pro nás budou tyto operace užitečné zejména v kapitole 10.

Posloupnosti se tradičně studují v matematické analýze, zde se proto omezíme jen na vlastnosti, které jsou užitečné pro diskrétní matematiku a informatiku. Protože nechceme zavádět analytické nástroje (třeba derivace), u řady tvrzení důkazy vynecháme, čtenář se s nimi seznámí v předmětu matematické analýzy neboli kalkulu.

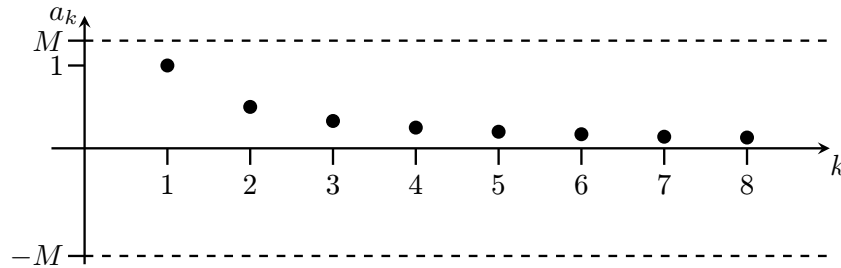
Definice.

Nechť $(a_k)_{k \geq n_0}$ je posloupnost. Řekneme, že je **omezená**, pokud existuje $M \in \mathbb{R}$ takové, že $|a_k| \leq M$ pro všechna $k \geq n_0$.

Protože u všech posloupností máme $|a_k| \geq 0$, tak je zjevné, že M splňující podmínku z definice musí také splňovat $M \geq 0$, je zbytečné zkoušet záporné kandidáty.

Příklad 8c.d: Uvažujme posloupnost $(\frac{1}{k})_{k \geq 1} = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots)$. Tvrdíme, že tato posloupnost je omezená. Zvolme $M = 1.3$. Pro $k \geq 1$ pak platí $\frac{1}{k} \leq 1 \leq 1.3$ neboli $|a_k| \leq M$.

Je zjevné, že stejnou práci by pro nás udělalo třeba $M = 13$, v podstatě jakékoliv číslo $M \geq 1$. Jakmile nějaké vhodné M podle definice najdeme, tak už jich je nekonečně mnoho.



Obrázek ukazuje smysl pojmu. Posloupnost je omezená, pokud její hodnoty dokážeme v grafu zavřít do vodorovného pruhu vymezeného hodnotami $-M$ a M .

Připomeňme posloupnost $a_k = 2k - 1$, $k \geq 1$. Tato posloupnost není omezená, což naznačuje její graf, který zjevně utíká do nekonečna a nedá se zavřít do vodorovného pruhu. Formálně: Zvolme nějaké $M \geq 0$. Pak existuje $k \in \mathbb{N}$ splňující $k > M - 1$, potom také $|a_k| = 2k + 1 > k + 1 > M$, tedy M nesplňuje podmínku z definice omezenosti. Vyloučili jsme všechny kandidáty, proto (a_k) není omezená.

Zde je dobré upozornit, že opakem omezené posloupnosti není posloupnost utíkající do nekonečna (popřípadě do mínus nekonečna). Na to, aby posloupnost pokazila podmínku z definice, nemusí nikam utíkat, stačí, aby občas „zazlobila“. Uvažujme následující posloupnost. Prvních 9 členů jsou nuly, desátý je 1. Dalších 89 členů jsou nuly, stý je 2. Dalších 899 členů jsou nuly, tisíc je 3. Dalších 8999 členů jsou nuly, člen na pozici 10000 je 4. A tak pokračujeme dále, skoro všechny členy posloupnosti jsou nula s výjimkou členů s indexem typu 10^n , jejich hodnota je n . Tyto členy zaručí, že posloupnost nelze omezit, ale rozhodně nelze říct, že by její členy byly nějak velké, protože naprostá většina z nich jsou nuly.

△

V matematické analýze se zavádí také pojmy omezená zdola a omezená shora, ale zde je vynecháme.

! Poznámka: Víme, že konečně mnoho čísel má své maximum a minimum, tedy lze je omezit nerovností typu $|a_k| \leq M$. Pokud toto vztáhneme na první členy z nějaké zkoumané posloupnosti, tak vidíme, že o její omezenosti či neomezenosti tyto první členy nerozhodnou. Omezenost posloupnosti je tedy rozhodnuta tím, co se děje na jejím „konci“, kterému se také neformálně říká „ocas“ (tail).

V situaci, kdy nám jde čistě o omezenost nějaké posloupnosti, tak vlastně ani nemusíme vědět, jak vypadá její začátek, tedy kde začínají její indexy.

△

Situace, kdy posloupnost opravdu utíká do nekonečna, nás bude velmi zajímat, je to vlastně hlavní téma následující části. Formálně jde o pojem limity.

! Definice.

Nechť $(a_k)_{k \geq n_0}$ je posloupnost.

Řekneme, že tato posloupnost jde do nekonečna, popřípadě že má limitu nekonečno, značeno

$\lim(a_k) = \infty$ popřípadě $a_k \rightarrow \infty$, jestliže

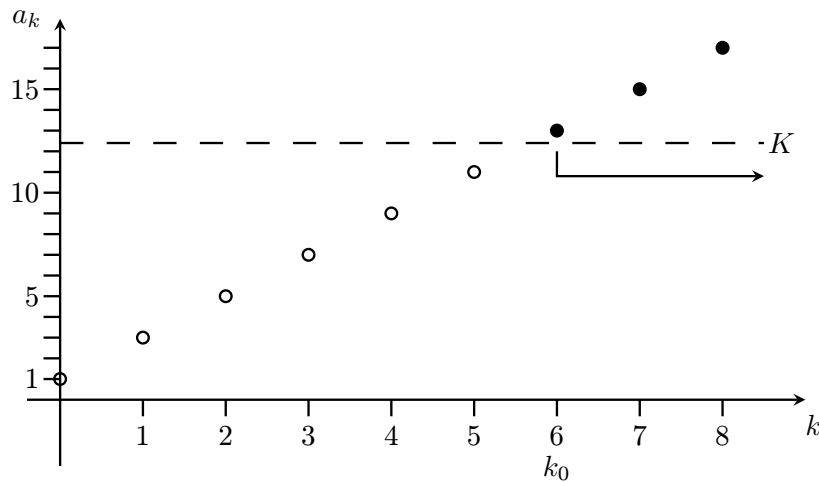
pro každé $K > 0$ existuje k_0 tak, aby $a_k > K$ pro všechna $k \geq k_0$.

Let $(a_k)_{k \geq n_0}$ be a sequence.

We say that it goes to infinity, or that its limit is infinity, denoted $\lim(a_k) = \infty$ or $a_k \rightarrow \infty$, if for all $K > 0$ there is k_0 such that $a_k > K$ for all $k \geq k_0$.

Příklad 8c.e: Intuice nám říká, že $(2k - 1)_{k \geq 1} = (1, 3, 5, 7, \dots)$ jde do nekonečna. Abychom to potvrdili podle definice, musíme vyhrát následující hru:

Kdykoliv nám někdo zadá $K > 0$, což je specifická úroveň pro hodnoty členů posloupnosti, tak bychom měli být schopni najít „odřezávací index“ k_0 takový, že pokud ignorujeme začátek posloupnosti před tímto indexem, tak její zbytek už zůstává nad zadanou úrovní K .



Když platí $a_k > K$? Chceme $2k + 1 > K$, což nastane pro $k > \frac{1}{2}(K - 1)$. Toto je specifikace typu „pro dost velká k “, což vyhovuje. Zvolíme třeba $k_0 = K$, pak pro $k \geq k_0$ platí $a_k = 2k + 1 > 2k_0 + 1 = 2K + 1 > K$.

S definicí nebudeme příliš pracovat, je užitečné jí rozumět. Nejprve si všimneme, že limita posloupnosti je opět určena tím, co se děje na jejím konci, protože při testování podmínky z definice stejně její začátky ignorujeme.

Dále si všimneme, že když jde posloupnost do nekonečna, tak není vyžadováno, aby tam šla nějak spěšně, jak to dělá třeba naše $(2k - 1)_k$. Hodnoty mohou klidně poskakovat nahoru a dolů, podstatné je, že nakonec zůstanou nad libovolnou zvolenou úrovní.

Když například uvažujeme (a_k) zadanou jako $a_k = k$ pro k liché a $a_k = 1$ pro k sudé, dostáváme posloupnost $(1, 1, 3, 1, 5, 1, 7, \dots)$, která nejde do nekonečna. Když nám totiž někdo zadá $K = 2$, tak tuto posloupnost neumíme donutit, aby zůstala nad touto úrovní, odříznutím nějakého jejího začátku. Ať zvolíme jakékoliv k_0 , tak se vždy najde větší sudý koeficient k a pak $a_k = 1$ nesplní $a_k > K$.

Nyní tuto posloupnost modifikujeme, pro k sudé definujeme $a_k = \frac{1}{2}k$. Vznikne posloupnost $(1, 1, 3, 2, 5, 3, 7, 4, \dots)$, která už jde do nekonečna. Dáno $K > 0$, zvolíme jako k_0 libovolné přirozené číslo větší než $2K$. Pak pro $k \geq k_0$ platí následující: Pokud je k liché, tak $a_k = k \geq k_0 > 2K > K$. Pokud je k sudé, tak $a_k = \frac{1}{2}k \geq \frac{1}{2}k_0 > \frac{1}{2} \cdot 2K = K$.
 \triangle

Viděli jsme, že při práci s limitou či omezeností vlastně nepotřebujeme vědět, kde začíná indexace posloupnosti. Pak je zbytečné to uvádět.

Úmluva.

V situaci, kdy u dané posloupnosti nepotřebujeme u rozsahu $k \geq n_0$ pro index znát konkrétní n_0 , můžeme namísto plného zápisu $(a_k)_{k \geq n_0}$ také psát jen (a_k) , popřípadě $(a_k)_k$, zejména pokud je ve vzorci pro a_k více proměnných a my potřebujeme určit, která z nich je index.

Budeme také používat frázi „pro všechna k “ a myslet tím „pro všechna k z množiny indexů dotyčné posloupnosti“.

V matematické analýze se také definuje limita pro případy, kdy (a_k) jde do mínus nekonečna, popřípadě konverguje k číslu L , ale zde to v zásadě nebudeme potřebovat s jednou výjimkou, u které se dokážeme vyhnout technické podmínce.

!

Definice.

Nechť (a_k) je posloupnost.

Řekneme, že tato posloupnost konverguje k nule, popřípadě že má limitu nula, značeno $\lim(a_k) = 0$ popřípadě $a_k \rightarrow 0$, jestliže $\frac{1}{|a_k|} \rightarrow \infty$.

Protože $2k - 1 \rightarrow \infty$, dostáváme $\frac{1}{2k-1} \rightarrow 0$. U posloupnosti $(1, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \dots)$ nás to nejspíše nepřekvapuje. Obdobně $\frac{1}{k} \rightarrow 0$ a graf této posloupnosti výše ukazuje, jak si to máme představit. I tento případ je příliš pěkný, u posloupnosti konvergující k nule se její členy nemusejí zmenšovat nějak organizovaně, ale mohou různě kolísat.

Podívejme se na limitu posloupností, které jsou zajímavé z hlediska informatiky.

Fakt 8c.2.

- (i) Nechť $a > 0$. Pak $k^a \rightarrow \infty$.
(ii) Jestliže $q > 1$, pak $q^k \rightarrow \infty$.
 Jestliže $|q| < 1$, pak $q^k \rightarrow 0$.
(iii) $k! \rightarrow \infty$.
(iv) $k^k \rightarrow \infty$.
(v) Nechť $b > 0$. Pak $[\ln(k)]^b \rightarrow \infty$.

Ve faktu jsme použili přirozený logaritmus, ale v computer science se často dává přednost logaritmu dvojkovému. I pro něj platí tvrzení z faktu, protože máme přepis $\log_a(k) = \frac{1}{\ln(a)} \ln(k)$. Pak také máme rovnost $[\log_a(k)]^b = \frac{1}{\ln^b(a)} [\ln(k)]^b$, takže se při změně základu jen modifikuje rychlost růstu konstantou, při libovolném základě $a > 1$ logaritmus pořád utíká do nekonečna.

V příští části si položíme otázku, které z těchto posloupností jdou do nekonečna rychleji a které pomaleji.

Jedna z posloupností ve faktu je speciálním případem zajímavého typu. Podíváme se na něj blíže spolu s další populární posloupností.

! Definice.

Uvažujme posloupnost $(a_k)_{k=n_0}^{\infty}$.

Řekneme, že je to **aritmetická posloupnost (arithmetic sequence)**, jestliže existují $a, d \in \mathbb{R}$ tak, aby pro všechna $k \geq n_0$ platilo $a_k = a + dk$.

Řekneme, že je to **geometrická posloupnost (geometric sequence)** jestliže existují $a, q \in \mathbb{R}$ tak, aby pro všechna $k \geq n_0$ platilo $a_k = aq^k$.

! Příklad 8c.f: Posloupnost $(1, 3, 5, 7, 9, \dots)$ všech lichých přirozených čísel je aritmetická, protože se dá zapsat jako $a_k = 1 + 2k$ pro $k \geq 0$.

Konstantní posloupnost $(1, 1, 1, 1, \dots)$ je aritmetická, protože se dá zapsat jako $a_k = 1 + 0k$ pro $k \geq 0$. Je ovšem také geometrická, protože se dá zapsat jako $a_k = 1 \cdot 1^k$ pro $k \geq 0$.

△

Bývá tradiční indexovat tyto posloupnosti od nuly. Nikterak se tím neomezujeme, každou aritmetickou a geometrickou posloupnost lze takto upravit. Například posloupnost $(13^7, 13^8, 13^9, \dots)$ je přirozeně zapsat jako $a_k = 13^k$ pro $k \geq 7$ a v mnoha situacích to bude nejlepší. Jsou ale situace, kdy se hodí indexování od nuly, pak použijeme třeba toto: Číslo $a = 13^7$ se dá vytknout ze všech členů, pak vidíme, že naši posloupnost popisuje také vzorec $b_k = 13^7 \cdot 13^k$ pro $k \geq 0$.

Aritmetické a geometrické posloupnosti poznáme snadno.

Fakt 8c.3.

Uvažujme posloupnost $(a_k)_k$.

Je to geometrická posloupnost právě tehdy, když existuje $q \in \mathbb{R}$ takové, že

$$\frac{a_{k+1}}{a_k} = q \text{ pro všechna } k.$$

Je to aritmetická posloupnost právě tehdy, když existuje $d \in \mathbb{R}$ takové, že

$$a_{k+1} - a_k = d \text{ pro všechna } k.$$

Například lichá čísla mají mezi sebou vždy rozdíl 2, proto tvoří aritmetickou posloupnost. Když je ale postupně dělíme, $\frac{3}{1}, \frac{5}{3}, \frac{7}{5}, \dots$, tak nedostáváme totéž, není to proto posloupnost geometrická. Naopak v tom příkladě s 13^k máme vždy $\frac{13^8}{13^7} = 13, \frac{13^9}{13^8} = 13, \frac{13^{10}}{13^9} = 13, \dots$, je to tedy posloupnost geometrická.

Tento fakt nás inspiruje k následujícím rekurzivním neboli induktivním definicím:

Aritmetická posloupnost:

(0) $a_0 = a.$

(1) $a_{k+1} = a_k + d$ pro $k \in \mathbb{N}_0.$

Geometrická posloupnost:

(0) $a_0 = a.$

(1) $a_{k+1} = a_k \cdot q$ pro $k \in \mathbb{N}_0.$

Snadno dokážeme indukci, že tato definice souhlasí s naší původní definicí. Podívejme se na ně blíže.

Příklad 8c.g: Aritmetická posloupnost $a_k = a + dk$ jde do nekonečna, pokud $d > 0$, pak také není omezená. V případě $d = 0$ dostáváme konstantní posloupnosti $a_k = a$ neboli (a, a, a, \dots) , které jsou omezené.

△

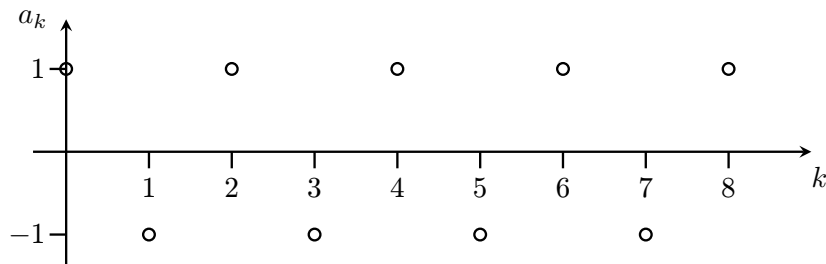
Příklad 8c.h: U geometrických posloupností existuje několik typických chování. Uvažujme posloupnost danou vzorcem $a_k = q^k$.

- Pokud $q > 1$, tak $a_k \rightarrow \infty$ a nejde o omezenou posloupnost. Typickým zástupcem je třeba posloupnost $(2^k)_{k \geq 0} = (1, 2, 4, 8, 16, \dots)$, která se často vyskytuje v informatice.

- Volba $q = 1$ dává konstantní posloupnost $(1, 1, 1, \dots)$, která je omezená.

- Pro $|q| < 1$ dostáváme posloupnost, která jde k nule. Asi nejznámějším příkladem je posloupnost $a_k = \left(\frac{1}{2}\right)^k$ neboli $\left(\frac{1}{2^k}\right)_{k \geq 0} = \left(1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots\right)$, kterou lze potkat například v oblíbených paradoxech typu Achilles a želva.

- Volba $q = -1$ vede na **alternující posloupnost** $\left((-1)^k\right)_{k \geq 0} = (1, -1, 1, -1, 1, \dots)$, která je velmi užitečná v situacích, kdy chceme modelovat střídání znamének, popřípadě další periodické změny v posloupnosti. Tato posloupnost je omezená.



- Pro $q < -1$ dostáváme posloupnost, která v sobě spojuje alternující znaménko a hodnoty, jejichž velikost utíká do nekonečna, například $a_k = (-2)^k = (-1)^k 2^k$ pro $k \geq 0$, tedy $(1, -2, 4, -8, 16, \dots)$. Tyto posloupnosti nejsou omezené, ale také nejdu do nekonečna. Členy takové posloupnosti se rozbíhají střídavě do plus a minus nekonečna, což nemá nějaký speciální název.

△

8c.4 Konečné posloupnosti, sumy

Pro účely diskrétní matematiky se vyplatí definovat také **konečné posloupnosti** $(a_k)_{k=n_0}^{m_0}$. Ty pak slouží jako jeden z možných matematických modelů pro řetězce znaků čili slova.

Vzhledem k tomu, že u počítačů pracujeme výhradně s konečnými řetězci znaků, má vůbec smysl zabývat se nekonečnými posloupnostmi? Ano, ze dvou důvodů. Za prvé, jsou situace, kdy nevíme dopředu, kolik znaků budeme mít ke zpracování. Je pak možné pracovat s množinou konečných posloupností všech možných délek, ale prodloužením na nekonečné posloupnosti někdy ušetříme formální komplikace například u operací. Druhý důvod je ten, že nás často zajímá otázka dlouhodobých trendů, pak nám přechod na nekonečné posloupnosti nabízí užitečné nástroje.

Někdy se ale hodí jako nástroj i konečné posloupnosti, teď už je máme zavedeny. Jedou takovou situací je, když se pokoušíme počítat čísla. Sumu jsme zavedli v kapitole 7, a pokud chceme sečíst $\sum_{k=n_0}^{m_0} a_k$, tak ta čísla nejdříve musíme mít, neboli potřebujeme příslušnou konečnou posloupnost.

Podobně jako u posloupností je také u sum index k jen pracovní proměnnou, která existuje jen uvnitř výpočtu.

$$\sum_{k=1}^4 (2k+1) = (2 \cdot 1 + 1) + (2 \cdot 2 + 1) + (2 \cdot 3 + 1) + (2 \cdot 4 + 1) = 3 + 5 + 7 + 9 = 24.$$

Dá se tedy libovolně přejmenovat či dokonce pomocí substituce posunout, což se někdy hodí. Postup je obdobný jako u posloupností.

Příklad 8c.i: V dané sumě $\sum_{k=3}^7 a_k$ posuneme index tak, aby ten nový začínal jedničkou. Zvolený vzorec $i = k - 2$ vede na výraz $k = i + 2$, pomocí kterého nahradíme všechny výskyty k včetně specifikace mezí, které pak upravíme.

$$\sum_{k=3}^7 a_k = \left| \begin{array}{l} i = k - 2 \\ k = i + 2 \end{array} \right| = \sum_{i+2=3}^{i+2=7} a_{i+2} = \sum_{i=1}^5 a_{i+2}.$$

Je také možné dopředu spočítat novou dolní a horní mez pomocí substituční rovnice.

$$\sum_{k=3}^7 a_k = \left| \begin{array}{l} i = k - 2 \\ k = i + 2 \\ k = 3 \mapsto i = 3 - 2 = 1 \\ k = 7 \mapsto i = 7 - 2 = 5 \end{array} \right| = \sum_{i=1}^5 a_{i+2}.$$

Je nová suma opravdu stejná jako původní? Porovnáme je:

$$\begin{aligned} \sum_{k=3}^7 a_k &= a_3 + a_4 + a_5 + a_6 + a_7, \\ \sum_{i=1}^5 a_{i+2} &= a_{1+2} + a_{2+2} + a_{3+2} + a_{4+2} + a_{5+2} = a_3 + a_4 + a_5 + a_6 + a_7. \end{aligned}$$

△

Posuny indexu se hodí například v situaci, kdy potřebujeme sumy sčítat pomocí vzorců.

! **Věta 8c.5.** (součet geometrické posloupnosti)
Uvažujme $q \in \mathbb{R}$. Pak

$$\sum_{k=0}^n q^k = \begin{cases} \frac{1 - q^{n+1}}{1 - q}, & q \neq 1; \\ n + 1, & q = 1. \end{cases}$$

Důkaz se snadno provede indukcí, což jsme udělali ve cvičení 7a.14, ovšem ta nedokáže správný vzorec objevit. Proto ukážeme ještě jiný důkaz.

Důkaz (poučný): Označme $s_n = \sum_{k=0}^n q^k = 1 + q + q^2 + \dots + q^n$. Pak $q \cdot s_n = q + q^2 + q^3 + \dots + q^{n+1}$, proto $qs_n - s_n = q^{n+1} - 1$, tedy $(q - 1)s_n = q^{n+1} - 1$. Jestliže je $q \neq 1$, můžeme vydělit a máme $s_n = \frac{q^{n+1} - 1}{q - 1}$.

Kdyby $q = 1$, tak rovnou vidíme, že $\sum_{k=0}^n 1 = 1 + 1 + \dots + 1$, sčítáme 1 celkem $(n + 1)$ -krát (opravdu? začínáme s indexem 0, tím to vyskočí o jedno, zkuste si pár sum), takže $s_n = n + 1$. □

Sčítání úseků obecných geometrických posloupností se pak převádí na tento základní vzorec vytknutím a posunem indexu.

$$\sum_{k=N}^n aq^k = \sum_{k=N}^n aq^N q^{k-N} = aq^N \sum_{k=N}^n q^{k-N} = \left| \begin{array}{l} i = k - N \\ k = 3 \mapsto i = N - N = 0 \\ k = n \mapsto i = n - N \end{array} \right| = aq^N \sum_{i=0}^{n-N} q^i.$$

Dalším populárním typem výrazu, který často sčítáme, jsou mocniny.

Věta 8c.6. (součty mocnin)
Následující vzorce platí pro všechna $n \in \mathbb{N}$:

- (i) $\sum_{k=1}^n 1 = n$;
- (ii) $\sum_{k=1}^n k = \frac{1}{2}n(n + 1)$;
- (iii) $\sum_{k=1}^n k^2 = \frac{1}{6}n(n + 1)(2n + 1)$;
- (iv) $\sum_{k=1}^n k^3 = \frac{1}{4}n^2(n + 1)^2$.

Takovéto vzorce se evidentně dokazují matematickou indukcí, (ii) a (iii) máme jako cvičení 7a.3 v kapitole o indukcí, (iv) si laskavý čtenář během 17 vteřin dodělá sám. Správná otázka ale zní, jak se na ty vzorce přijde. Tak (i) je snadné, prostě sčítáme n jedniček. Což takhle (ii)?

Vzorec pro tento součet vymyslel Gauss, když byl malé nechutně chytré dítě. Učitel jej nechal sečíst prvních 100 čísel, ať má od něj chvíli pokoj, takže byl notně překvapen, když mu malý Johann za chvíli hlásil výsledek. Jak na to přišel? Představme si takový součet, pro začátek pro sudé n :

$$1 + 2 + 3 + \cdots + (n-2) + (n-1) + n.$$

Všimněte si, že první a poslední číslo dají dohromady $n+1$. Také druhé číslo zleva a zprava dají dohromady $n+1$. Také třetí ... Takových dvojic je přesně $\frac{n}{2}$, takže součet je $\frac{n}{2}(n+1)$.

Co když je n liché? Pak máme $\frac{1}{2}(n-1)$ dvojic a prostřední číslo zůstane osamocené, je to číslo $\frac{1}{2}(n+1)$ (zkuste si to na nějakém příkladě). Celkový součet je tedy $\frac{1}{2}(n-1)(n+1) + \frac{1}{2}(n+1) = \frac{1}{2}n(n+1)$.

Jiný trik jak to vidět: Napíšeme tu sumu dvakrát pod sebe, jednou jako $s = 1 + 2 + \cdots + (n-1) + n$, podruhé jako $s = n + (n-1) + \cdots + 2 + 1$, když sečteme, dostaneme nalevo $2s$, napravo n dvojic se součtem $n+1$, teď už nemusíme rozlišovat mezi sudými a lichými n .

Někteří autoři tu příhodu s Gaussem považují za bajku, takže si ukážeme jiný postup. Víme, že $(k+1)^2 - k^2 = 2k + 1$. Co dostaneme, když takovéto členy začneme sčítat? Nejprve příklad:

$$\sum_{k=1}^3 [(k+1)^2 - k^2] = [2^2 - 1^2] + [3^2 - 2^2] + [4^2 - 3^2] = 4^2 - 1^2.$$

Jinými slovy, všechny „prostřední“ členy se pokrátí, je to teleskopická suma, viz příklad 7a.j. V důkazu to provedeme obecně.

Důkaz (poučný): (ii): Sečtením rovností $(k+1)^2 - k^2 = 2k + 1$ pro k mezi 1 a n získáme nalevo

$$\sum_{k=1}^n [(k+1)^2 - k^2] = (n+1)^2 - 1^2,$$

zatímco napravo je

$$\sum_{k=1}^n [(k+1)^2 - k^2] = \sum_{k=1}^n [2k + 1] = 2 \sum_{k=1}^n k + \sum_{k=1}^n 1 = 2 \sum_{k=1}^n k + n.$$

Proto

$$(n+1)^2 - 1 = 2 \sum_{k=1}^n k + n \implies \sum_{k=1}^n k = \frac{1}{2}[(n+1)^2 - 1 - n] = \frac{1}{2}n(n+1).$$

(iii): Sečtením $(k+1)^3 - k^3$ dostaneme nalevo

$$\sum_{k=1}^n [(k+1)^3 - k^3] = (n+1)^3 - 1^3,$$

zatímco napravo je

$$\sum_{k=1}^n [(k+1)^3 - k^3] = \sum_{k=1}^n [3k^2 + 3k + 1] = 3 \sum_{k=1}^n k^2 + 3 \cdot \sum_{k=1}^n k + \sum_{k=1}^n 1 = 3 \sum_{k=1}^n k^2 + \frac{3}{2}n(n+1) + n.$$

Máme tedy

$$(n+1)^3 - 1 = 3 \sum_{k=1}^n k^2 + \frac{3}{2}n(n+1) + n \implies \sum_{k=1}^n k^2 = \frac{1}{3}((n+1)^3 - 1 - \frac{3}{2}n(n+1) - n) = \frac{1}{6}n(n+1)(2n+1).$$

(iv): Obdobný trik. Všimněte si, že při nalezení součtu $\sum k^2$ jsme potřebovali znát součet $\sum k$ a součet $\sum 1$. Teď si budeme hrát s $(k+1)^4 - k^4$ a budeme potřebovat znát součty $\sum k^2$, $\sum k$ a $\sum 1$. Přenecháme to čtenáři. \square

Pro vyšší mocniny k se odvození vzorce stává nepříliš příjemným. V informatice ale často stačí jen přibližný vzorec. Ten se dá odvodit snáze a navíc je výrazně jednodušší, viz příklad 10b.n.

Snadno si rozmyslíme, že Gaussův trik funguje na všechny aritmetické posloupnosti, dokonce ani nemusíme začínat s indexem on nuly. Uvažujme nějakou posloupnost $(a_k)_{k=N}^n$, která je aritmetická s krokem d . Opět si můžeme představit členy napsané ve dvou řádcích pod sebou, ve druhém pozpátku.

$$\begin{array}{cccccc} a_N & a_{N+1} & \cdots & a_{n-1} & a_n & \\ & a_n & a_{n-1} & \cdots & a_{N+1} & a_N \end{array}$$

Vidíme celkem $n - N + 1$ dvojic pod sebou. Součet té první a poslední se shoduje. Jak je na tom druhá a předposlední? Máme $a_{N+1} = a_N + d$ a $a_{n-1} = a_n - d$, proto

$$a_{N+1} + a_{n-1} = a_N + d + a_n - d = a_N + a_n.$$

Obdobně ukážeme, že všechny dvojice mají stejný součet, celková suma je tedy $(n - N + 1)(a_N + a_n)$. Zároveň jsme ale sečetli všechny členy dvakrát.

Věta 8c.7. (součet aritmetické posloupnosti)

Předpokládejme, že $(a_k)_{k=N}^n$ pro $N \leq n$ je aritmetická posloupnost. Pak

$$\sum_{k=N}^n a_k = \frac{1}{2}(n - M + 1)(a_N + a_n).$$

Neboli sečteme první a poslední člen, vydělíme dvěma (čímž zjistíme, jaký je vlastně průměrný člen posloupnosti) a vynásobíme počtem členů. Dává to smysl. Někdy se hodí vzoreček pracující s parametry posloupnosti, uvedeme základní verzi.

Věta 8c.8. (součet aritmetické posloupnosti)

Uvažujme čísla $a, d \in \mathbb{R}$. Pak

$$\sum_{k=0}^n (a + dk) = (n + 1)a + \frac{1}{2}n(n + 1)d.$$

Důkaz (rutinní): Toto je snadné,

$$\sum_{k=0}^n (a + dk) = \sum_{k=0}^n a + d \sum_{k=0}^n k = (n + 1)a + \frac{1}{2}n(n + 1)d.$$

□

Alternativní způsob, jak najít uzavřené vzorce pro rozličné součty, čtenář najde v kapitole 10, viz příklad 10b.n a cvičení 10b.5.

V informatice také často potkáváme více sum vnořených do sebe. Vyhodnocujeme je postupným „rozbalováním“ součtů, někdy to jde lépe zevnitř, jindy zvenčí.

Příklad 8c.j: 1. U výrazu $\sum_{i=1}^2 \sum_{j=1}^3 i^2 j$ to vyjde v zásadě nastejno. Nejprve ukážeme postup, kdy začneme rozepisovat vnější sumu, pak postup, kdy začneme zevnitř.

$$\sum_{i=1}^2 \sum_{j=1}^3 i^2 j = \sum_{j=1}^3 1^2 j + \sum_{j=1}^3 2^2 j = (1^2 \cdot 1 + 1^2 \cdot 2 + 1^2 \cdot 3) + (2^2 \cdot 1 + 2^2 \cdot 2 + 2^2 \cdot 3) = 30,$$

$$\sum_{i=1}^2 \sum_{j=1}^3 i^2 j = \sum_{i=1}^2 (i^2 \cdot 1 + i^2 \cdot 2 + i^2 \cdot 3) = \sum_{i=1}^2 6i^2 = 6 \cdot 1^2 + 6 \cdot 2^2 = 30.$$

2. U následující sumy je rozvíjení zvenčí výrazně snazší, protože pak se dozvíme, jaké jsou vlastně meze vnitřní sumy. Pokud začneme zevnitř, budeme muset sčítat $\sum_j j$ s proměnnými mezemi.

$$\begin{aligned} \sum_{i=1}^3 \sum_{j=i}^3 (i + j) &= \sum_{j=1}^3 (1 + j) + \sum_{j=2}^3 (2 + j) + \sum_{j=3}^3 (3 + j) \\ &= [(1 + 1) + (1 + 2) + (1 + 3)] + [(2 + 2) + (2 + 3)] + [(3 + 3)] = 24 \\ \sum_{i=1}^3 \sum_{j=i}^3 (i + j) &= \sum_{i=1}^3 \left[i \cdot \sum_{j=i}^3 1 + \sum_{j=i}^3 j \right] = \sum_{i=1}^3 \left[i \cdot (3 - i + 1) + \frac{1}{2}(3 - i + 1)(i + 3) \right] = \frac{1}{2} \sum_{i=1}^3 (9i - 3i^2 + 12) \\ &= \frac{1}{2} \left[9 \sum_{i=1}^3 i - 3 \sum_{i=1}^3 i^2 + 12 \sum_{i=1}^3 1 \right] = \frac{1}{2} \left[9 \cdot \frac{1}{2} \cdot 3 \cdot 4 - 3 \cdot \frac{1}{6} \cdot 3 \cdot 4 \cdot 7 + 12 \cdot 3 \right] = \frac{1}{2} \cdot 48 = 24. \end{aligned}$$

3. Pokud ale vnější suma nemá konkrétní meze, pak rozvíjením zvenčí stejně nic nezískáme, ani to dokonce nejde (když nevíme konkrétně, jaké indexy vnější suma používá). Pak nezbyvá než se s tím poprat zevnitř.

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^i \sum_{k=1}^j 1 &= \sum_{i=1}^n \sum_{j=1}^i j = \sum_{i=1}^n \frac{1}{2} i(i + 1) = \frac{1}{2} \left[\sum_{i=1}^n i^2 + \sum_{i=1}^n i \right] \\ &= \frac{1}{2} \left[\frac{1}{6} n(n + 1)(2n + 1) + \frac{1}{2} n(n + 1) \right] = \frac{1}{6} n(n + 1)(n + 2). \end{aligned}$$

△

Cvičení

Cvičení 8c.1 (rutinní): Jsou dány následující posloupnosti. Najděte vždy prvních řekněme deset členů.

a) (0) $a_1 = 1, a_2 = -1, a_3 = 1, \dots$ (1) $a_{k+1} = a_k - a_{k-2}$ pro $k \geq 3$;

b) $a_k = \lfloor \sqrt{k} \rfloor, k \in \mathbb{N}$;

c) a_k je počet písmen v číslovce označující $k, k \in \mathbb{N}$;

d) a_k je největší celé číslo, jehož binární zápis má k bitů, $k \in \mathbb{N}$;

e) a_k je největší n takové, že $n! \leq k$ pro $k \in \mathbb{N}$.

Cvičení 8c.2 (dobré, poučné): Najděte alespoň tři různá pravidla pro definici posloupnosti tak, aby její první tři členy byly

a) 1, 2, 4;

b) 1, 2, 3.

Pro každé takové pravidlo dopočítejte další dva členy.

Cvičení 8c.3 (*dobré): Pro následující seznamy celých čísel najděte jednoduchý vzorec či pravidlo, který je generuje, a pomocí něj odhadněte další člen.

a) 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, ...;

i) 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, ...;

b) 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, ...;

j) 1, 8, 27, 125, 216, ...;

c) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, ...;

k)* 2, 3, 7, 25, 121, 721, 5041, 40321, ...;

d) 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, ...;

l)* 2, 16, 54, 128, 250, 432, 686, ...;

e) 1, -3, 9, -27, 81, -243, 729, ...;

m)* 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, ...;

f) 15, 8, 1, -6, -13, -20, -27, ...;

n)* 0, 2, 8, 26, 80, 242, 728, 2186, 6560, 19682, ...;

g) 3, 6, 12, 24, 48, 96, 192, ...;

o)* 1, 3, 15, 105, 945, 10395, 125125, 2027025, 34459425, ...;

h) 1, 4, 9, 16, 25, 36, 49, 64, ...;

p)* 2, 4, 16, 256, 65536, 4294967296, ...

Řešení:

8c.1: a) 1, -1, 1, 0, 1, 0, 0, -1, -1, -1, 0, 1, 2, 2, 1, -1, -3, -4, -3, 0, 4, 7, 7, 3, -4, -11, -14, -10, 1, 15.

Nevidím pro tohle nějaký rozumný vzoreček, je to zajímavá posloupnost. Vzorec ale určitě existuje, viz kapitola 10b.

b) 1, 1, 1, 2, 2, 2, 2, 3, 3. c) 5, 3, 3, 5, 3, 4, 4, 3, 5, 5.

d) 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.

e) 1, 2, 2, 2, 2, 3, 3, 3, 3, 3.

8c.2: a) Tak třeba A) $a_{k+1} = 2a_k$, pak 1, 2, 4, 8, 16; B) $a_{k+1} = 2^k$, pak 1, 2, 4, 8, 16;

C) $a_{k+1} = a_k + k$ pro $k \in \mathbb{N}$, pak 1, 2, 4, 7, 11; D) posloupnost všech přirozených čísel, která nejsou dělitelná třemi, pak 1, 2, 4, 5, 7; E) a_n je n -té prvočíslo mínus jedna;

F) $a_n = n$ pro n sudé, $a_n = \lceil \frac{1}{2}n \rceil^2$ pro n liché, vyjde 1, 2, 4, 4, 9, 6, 16, 8, 25, 10, ...

b) Tak třeba A) $a_k = k$ pro $k \in \mathbb{N}$, pak 1, 2, 3, 4, 5, vzorec $a_{k+1} = a_k + 1$ dává totéž;

B) $a_{k+1} = a_k + a_{k-1}$, pak 1, 2, 3, 5, 8; C) $a_k = k^3 + 2$ pro $k \geq -1$, pak 1, 2, 3, 10, 29.

D) posloupnost všech přirozených čísel, která nejsou složená, pak 1, 2, 3, 5, 7.

8c.3: a) 1. b) 9. c) 32. d) 47, $a_{k+1} = a_k + 4$. e) -2187, $a_{k+1} = a_k \cdot (-3)$ nebo $a_k = (-3)^k, k \geq 0$. f) -34, $a_{k+1} = a_k - 7$. g) 384, $a_{k+1} = 2a_k, a_k = 3 \cdot 2^{k-1}$. h) 81, $a_k = k^2$. i) 123, $a_{k+1} = a_k + 2k + 1$, tedy symbolicky +3, +5, +7, ... j) 343, $a_k = k^3$. k) 62881, $a_k = k! + 1$. l) 1024, $a_k = 2k^3$. m) 1100, $a_{k+1} = a_k + 1$, ale binárně!. n) 59048, $a_{k+1} = 3a_k + 2$. o) 654729075, $a_{k+1} = a_k \cdot (2k + 1)$, symbolicky $\cdot 3, \cdot 5, \cdot 7, \dots$ p) $1.844 \cdot 10^{19}, a_k = 2^{2^k}$.

8d. Asymptotická rychlost růstu

V řadě situací pracujeme s rozličnými výrazy, které jdou do nekonečna, a zajímá nás, které tam jdou rychleji a které pomaleji. Typickým příkladem je teorie algoritmů, kdy důležitým porovnávacím kritériem je jejich „výpočetní náročnost“. Algoritmus řeší určitý problém, přičemž vstupní data mohou přicházet v různých počtech či velikostech vyjádřených číslem $k \in \mathbb{N}$. Výpočetní náročnost algoritmu je funkce $f(k)$, která říká, kolik operací tento algoritmus musí provést k vyřešení úlohy při vstupu velikosti k . Obvykle se přitom bere ten nejpesimističtější případ. Co je to „operace“ závisí na kontextu, prakticky vzato výpočetní náročnost souvisí s tím, za jak dlouho nám algoritmus dá výsledek.

Známe to také z vlastní praxe. Když sčítáme dvě k -ciferná čísla, tak v hlavě sčítáme jednotlivé páry číslic, tedy potřebujeme provést přibližně k operací. Pokud je násobíme, tak v hlavě násobíme každou cifru prvního čísla s každou cifrou druhého čísla, což je k^2 operací. Víme, že k^2 roste do nekonečna rychleji než k , což souhlasí s intuitivní představou, že písemné sčítání jde lépe než násobení.

Ovšem $4k$ také roste rychleji než k , chvíli je dokonce větší než k^2 , ale k^2 nakonec vyhraje i nad $4k$. To ukazuje, že „roste rychleji“ může znamenat „trochu rychleji“, ale také „podstatně rychleji“. Praktický pohled ze světa algoritmizace to pěkně ilustruje.

Příklad 8d.a: Porovnáme několik algoritmů s rozdílnými výpočetními náročnostmi. Necháme algoritmy proběhnout na imaginárním počítači schopném zvládnout milion operací za vteřinu a zjistíme, jak dlouho jednotlivé algoritmy poběží, když se velikost dat zvětšuje. Poznamenejme, že velikost dat 10^8 není nijak výjimečná.

Čas je udáván v milisekundách „ms“, „s“ je sekunda, „m“ minuta, „h“ hodina, „d“ den a „r“ rok.

$k =$	10	100	1000	10000	10^5	10^6	10^7	10^8
• $\log_2(k)$:	0.0033ms	0.0066ms	0.010ms	0.013ms	0.017ms	0.020ms	0.023ms	0.027ms
• k :	0.01ms	0.1ms	1ms	10ms	0.1s	1s	10s	1.6m
$2k$:	0.02ms	0.2ms	2.0ms	20ms	0.2s	2s	20s	3.2m
$\frac{1}{100}k^2$:	0.001ms	0.01ms	10ms	1s	1.7m	2.8h	11.6d	3.2r
• k^2 :	0.1ms	10ms	1s	100s	167m	11.7d	3.2r	317r
$k^2 + 100k$:	1.1ms	20ms	1.1s	101s	167m	11.7d	3.2r	317r
• k^3 :	1ms	1s	16.7s	11.6d	31.7r	10^4 r	10^7 r	10^{10} r
• 2^k :	1ms	10^{16} r	10^{287} r					
• $\frac{1}{1000}k!$:	3ms	10^{141} r						

Řádky s tečkami představují typické výpočetní náročnosti. Logaritmicou náročnost má například binární vyhledávání v seřazeném seznamu, lineární pak vyhledávání v seznamu neseřazeném, ale třeba také sčítání velkých čísel. Kvadratickou náročnost má třeba seřazování položek podle abecedy nebo násobení velkých čísel. Náročnost k^3 pak vyžaduje násobení matic nebo jejich úprava Gaussovou eliminační metodou. Na závěr jsou dvě náročnosti, kterým se v praxi snažíme vyhnout. Exponenciální práci vyžaduje třeba lámání šifry RSA v závislosti na bitové délce klíče, ale také řešení problému obchodního cestujícího (viz kapitola 12c).

Faktoriál jsme vydělili tisícem, což se dá vnímat tak, že jsme tento algoritmus spustili na tisíckrát výkonnějším počítači. Chtěli jsme odložit nástup velkých výsledků, ale jak je vidět, moc to nepomohlo, délka běhu programu záhy překročí odhadované dosavadní trvání vesmíru. Exponenciální a faktoriální řádky pak nemělo smysl dokončovat.

Všechny tyto běhy se pro malé velikosti dat liší, ale nikterak masivně. Pro velká data je mezi nimi rozdíl propastný, dny versus roky versus miliardy let. Jde tedy o podstatný rozdíl v rychlosti jejich růstu do nekonečna. Budeme chtít zavést matematický pojem, který dokáže takovýto podstatný rozdíl v růstu dvou výrazů rozeznat.

Nyní se podívejme na řádek pod lineárním růstem. Výraz $2k$ odpovídá dvojnásobně náročnějšímu algoritmu, ale také to může být tentýž algoritmus spuštěný na dvakrát pomalejším stroji. Výpočty samozřejmě trvají déle než u náročnosti k , ale pořád je to srovnatelné, výrazně lepší než kvadratická náročnost. Pro srovnání jsme přidali také řádek odpovídající algoritmu kvadratické náročnosti spuštěnému na stonásobně výkonnější mašině. Pro malé množství dat je toto dražší řešení lepší, ale pro větší data se ukáže, že jsme investicí do železa ten kvadratický algoritmus nezachránili, lineární (i na pomalejším stroji) vychází lépe.

Z praktického pohledu to ukazuje, že pokud zvolíme výpočetně náročnější algoritmus, tak to pro velká data investicí do vybavení nezachráníme. Z pohledu této sekce nám to říká, že rozdíl v rychlosti růstu mezi nějakou $f(k)$ a $cf(k)$ (kde c je konstanta) sice existuje, ale není podstatný. Takže ten matematický pojem na rozpoznávání podstatného rozdílu v rychlosti růstu by měl ignorovat násobící konstanty.

Inspiruje nás to také k zavedení dalšího pojmu, který naopak rozpozná, že dva výrazy rostou v zásadě obdobně rychle, není mezi nimi podstatný rozdíl. I tento pojem by tedy měl ignorovat násobící konstanty.

Nyní porovnejme výraz k^2 s následujícím řádkem $k^2 + 100k$. Těch k jsme přidali docela hodně, což se pro malé hodnoty projeví nárůstem doby běhu. Ovšem pro větší k se rozdíl mezi k^2 a $k^2 + 100k$ zmenšuje, až nakonec zmizí. To znamená, že pro účely porovnávání lze u výrazu $k^2 + 100k$ tu lineární část vynechat, aniž by to ovlivnilo výsledek. Souvisí to s tím, že jsme před chvílí rozeznali, že k^2 jde do nekonečna podstatně rychleji než k , což také znamená, že pro velké hodnoty k je výraz k (i s případnou násobící konstantou) zanedbatelný ve srovnání s k^2 .

To znamená, že náš druhý nástroj rozpoznávající porovnatelné růsty bude ignorovat nejen násobící konstanty, ale také části výrazu, které jsou méně významné. S rozeznáním důležitého a nedůležitého nám pomůže ten první pojem, takže spolu budou souviset.

Alternativní pohled na podstatné a nepodstatné rozdíly v růstu nabídne otázka „škálovatelnosti“. Obvykle se systém (počítač a programové vybavení) připravují pro určitou situaci. Představme si, že obsluhujeme firmu, která se stará o deset zákazníků. Požaduje, abychom jim data zpracovali do jedné vteřiny, a my jsme takový systém připravili. Pak se stane, že firma je nečekaně úspěšná a počet jejich zákazníků se zdvojnásobí či dokonce zdesetinásobí. Co to udělá s naším systémem? V tabulce uvádíme různé možnosti podle výpočetní náročnosti použitého algoritmu, vzhledem k původnímu nastavení systému začínají všechny řádky v tabulce jednou vteřinou pro 10 zákazníků. Řádky k a $80k + \sqrt{k}$, respektive k^2 a $2k^2 + 5k$ ukazují, že násobící konstanty a přítomnost členů nižšího růstu nemají na škálovatelnost vliv a tedy nejsou podstatné.

△

$k =$	10	20	30	100
$\log_2(k):$	1s	1.3s	1.5s	2s
$k:$	1s	2s	3s	10s
$20k:$	1s	2s	3s	10s
$80k + \sqrt{k}:$	1s	2.0s	3.0s	9.9s
$k^2:$	1s	4s	9s	1m40s
$2k^2 + 5k:$	1s	3.6s	7.8s	1m22s
$k^3:$	1s	8s	27s	16m40s
$2^k:$	1s	17m4s	12d	4×10^{19} r
$k!:$	1s	21×10^3 r	2×10^{18} r	

Než zavedeme potřebné pojmy, vyjasníme otázku jazyka. Výpočetní náročnost je zobrazení či funkce z \mathbb{N} obvykle do \mathbb{N} . Mohla by to tedy také být posloupnost. Striktně vzato je pojem funkce vhodnější, protože výpočetní náročnost svazuje velikost vstupních dat s počtem operací, tedy vazba $n \mapsto f(n)$ je přímo v základech pojmu. Mnoho autorů proto pracuje s funkcemi. Na druhou stranu nás vlastně nezajímá, kolik operací potřebujeme na vynásobení dvou matic tisíc na tisíc; zajímá nás srovnání, jak rychle rostou náročnosti toho či jiného algoritmu pro tento úkol. Podstatné jsou tedy hodnoty, navíc nás ty první ani nezajímají, to důležité se děje pro velká čísla. To je chování typické pro posloupnosti, které používají zase jiní autoři.

Legitimní a používané jsou tedy oba přístupy, ostatně když prohlásíme, že k^2 roste řádově rychleji než k , tak nejde poznat, jestli se bavíme o funkci $f(k) = k^2$ nebo posloupnosti $a_k = k^2$. Nakonec jsem zvolil jazyk posloupností, protože a_k má polovinu znaků v porovnání s $f(k)$. Pokud čtenář preferuje jazyk funkcí, stačí v definicích a větách zaměnit značení a vznikne příslušná teorie.

Rozeznat mezi podstatným a nepodstatným rozdílem v rychlosti růstu nám pomůže otázka, kolikrát je jeden výraz větší než druhý. Takové porovnání se děje podílem. Srovnajme $2k^2 + 5k$ a k^2 :

$$\frac{2k^2 + 5k}{k^2} = 2 + \frac{5}{k}.$$

Pro velká k je $\frac{5}{k} \approx 0$, tedy lze říct, že $2k^2 + 5k$ je přibližně dvakrát větší než k^2 . To obvykle roli hraje, ale v této sekci to není podstatné. Teď porovnáme k^3 a k :

$$\frac{k^3}{k} = k^2.$$

Nás zajímá chování pro strašně velká k a pak lze nepřesně ale výmluvně říct, že k^3 je nekonečně krát větší než k , což už podstatné je. Někdy lze tutéž informaci vidět z výpočtu

$$\frac{k}{k^3} = \frac{1}{k^2} \approx 0.$$

Takže k^3 dominuje k tak masivně, že když jej vydělí, tak to k zmizí.

Protože nás zajímá chování pro velká k , nepotřebujeme znát začátky indexace a tedy nebudeme psát specifikaci pro indexy. A protože se nechceme omezovat, zavedeme tento pojem také pro posloupnosti, které do nekonečna nejdou.

!

Definice.

Nechť (a_k) , (b_k) jsou posloupnosti nenulových čísel.

Řekneme, že a_k je $o(b_k)$, psáno také $a_k = o(b_k)$, jestliže $\frac{|b_k|}{|a_k|} \rightarrow \infty$ neboli $\frac{a_k}{b_k} \rightarrow 0$.

Řekneme, že a_k je $\omega(b_k)$, psáno také $a_k = \omega(b_k)$, jestliže $\frac{|a_k|}{|b_k|} \rightarrow \infty$ neboli $\frac{b_k}{a_k} \rightarrow 0$.

Protože nás nezajímá počátek indexace, podmínka na nenulovost efektivně znamená, že se v posloupnostech nuly vyskytovat mohou, ale jen konečně mnoho.

Značení $a_k = o(b_k)$ se čte „ a_k je malé o b_k “, podobně s omegou. Značka $=$ zde neznamená klasickou rovnost, ale je to součástí specifického značení, je to jakási zkratka pro slovo „je“. Někteří autoři to vnímají jinak, berou $o(b_n)$ jako množinu všech posloupností (a_k) splňujících $\lim\left(\frac{a_k}{b_k}\right) = 0$. Pak namísto našeho značení s rovností píšou $a_k \in o(b_k)$.

Kromě oficiálního čtení je také rozšířena řada alternativ, které souvisejí s využitím v aplikacích. Nejen v diskrétní matematice je velmi rozšířená fráze „posloupnost (a_k) roste asymptoticky pomaleji než posloupnost (b_k) “, také by

šlo říct „asymptotický řád růstu a_k je menší než asymptotický řád růstu b_k “ a další obdobné formulace. Symetricky, lze říci „ b_k roste asymptoticky rychleji než a_k “, „ b_k má větší asymptotický řád růstu než a_k “ a podobně. Když se objeví slova „asymptoticky“, „rychlost růstu“ či „řád růstu“ v nějaké podobě, tak jde s vysokou pravděpodobností právě o vztah $a_k = o(b_k)$. Z pohledu vzájemné interakce jsou také užitečná vyjádření „ b_k dominuje a_k “, popřípadě „ a_k je zanedbatelné vzhledem k b_k “. Ten poslední pohled se ještě bude hodit.

Dá se říci, že je to jakási hodně silná nerovnost, v některých oblastech matematiky či aplikacích se také používá značení $a_k \ll b_k$. Podobně jako u běžné nerovnosti někdy lidé cítí potřebu mít i nerovnost opačnou, $a_k \gg b_k$, což nabízí druhý pojem $\omega(b_k)$. Již z definice je jasné, že pojmy o a ω jsou duální:

• $a_k = o(b_k)$ právě tehdy, když $b_k = \omega(a_k)$.

Tu omegu tedy opravdu nepotřebujeme a používá se zřídka. Oba pojmy se jako ostrá nerovnost také chovají.

!

Fakt 8d.1.

Uvažujme posloupnosti $(a_k), (b_k), (c_k)$ nenulových čísel.

(i) Nikdy neplatí $a_k = o(a_k)$.

(ii) Jestliže $a_k = o(b_k)$ a $b_k = o(c_k)$, pak $a_k = o(c_k)$.

(iii) Nemůže najednou platit $a_k = o(b_k)$ a $b_k = o(a_k)$.

Důkaz (poučný): (i) Posloupnost $\frac{|a_k|}{|a_k|} = 1$ nejde do ∞ .

(ii) Pomocí předpokladu spočítáme

$$\frac{|c_k|}{|a_k|} = \frac{|c_k|}{|b_k|} \cdot \frac{|b_k|}{|a_k|} \rightarrow \infty \cdot \infty = \infty.$$

(iii) Jestliže $a_k = o(b_k)$, pak $\frac{|b_k|}{|a_k|} \rightarrow \infty$. Proto $\frac{|a_k|}{|b_k|} \rightarrow 0$ a tedy nemůže zároveň platit $\frac{|a_k|}{|b_k|} \rightarrow \infty$. □

Jinak řečeno, pokud vnímáme vztah $a_k = o(b_k)$ jako relaci na množině posloupností, pak je antireflexivní, tranzitivní a antisymetrická neboli je to ostré uspořádání. Obdobně to platí pro vztah ω .

Chtěli jsme, aby pojem podstatného rozdílu v rychlosti růstu ignoroval násobící konstanty. Potvrdíme to.

!

Fakt 8d.2.

Nechť $(a_k), (b_k)$ jsou posloupnosti nenulových čísel. Jestliže $a_k = o(b_k)$, pak pro $A, B \neq 0$ platí $Aa_k = o(Bb_k)$.

Je to vlastně ekvivalence, protože když na předpoklad $Aa_k = o(Bb_k)$ aplikujeme tento fakt s konstantami $\frac{1}{A}, \frac{1}{B}$, dostaneme $a_k = o(b_k)$. Nejprve jej ovšem musíme dokázat.

Důkaz (rutinní): Předpoklad $a_k = o(b_k)$ dává $\frac{|a_k|}{|b_k|} \rightarrow \infty$. Pak díky $A \neq 0$ máme

$$\frac{|Aa_k|}{|Bb_k|} = \frac{|A|}{|B|} \cdot \frac{|a_k|}{|b_k|} \rightarrow \frac{|A|}{|B|} \cdot \infty = \infty.$$

□

Nyní potvrdíme dojem, který jsme získali z tabulky. Připomeňme, že logaritmy o různých základech se liší jen násobící konstantou, což by naše pojmy měly ignorovat. Budeme proto psát \log_2 s tím, že logaritmy o jiných základech (větších než 1) se chovají stejně.

!

Věta 8d.3.

(i) Nechť $a, b > 0$ a $q > 1$. Pak platí:

a) $[\log_2(k)]^a$ je $o(k^b)$,

b) k^b je $o(q^k)$,

c) q^k je $o(k!)$,

d) $k!$ je $o(k^k)$.

(ii) Jestliže $0 < a < b$, pak platí:

a) $[\log_2(k)]^a$ je $o([\log_2(k)]^b)$,

b) k^a je $o(k^b)$.

(iii) Jestliže $1 < q < r$, pak q^k je $o(r^k)$.

Symbolicky lze část (i) vyjádřit obrázkem

$$\log_2^a(k) \ll k^b \ll q^k \ll k! \ll k^k.$$

Každá položka zde reprezentuje celou skupinu výrazů, například k^b obsahuje všechny mocniny jako \sqrt{k} , k , k^7 a podobně, ale také jejich násobky. Každý výraz z jedné z těchto skupin dominuje jakémukoliv výrazu ze skupin jmenovaných dříve, třeba $2k!$ dominuje $13k^2$. Podle definice to znamená, že $\frac{2k!}{13k^2} \rightarrow \infty$, tedy pro velká k bude $2k!$ libovolněkrát větší než $13k^2$; pro malá k to neznamena nic.

Body (ii) a (iii) říkají, že v rámci každé skupiny o hierarchii rozhodují hodnoty parametru, třeba 3^k roste asymptoticky rychleji než e^k , což roste asymptoticky rychleji než 2^k , podobně k^7 roste asymptoticky rychleji než k^4 a to roste asymptoticky rychleji než \sqrt{k} .

Těmto vztahům se často říká „škála mocnin“ a její znalost umožní rychle porovnávat růsty různých výrazů.

Důkaz (náznak): Podle definice máme zkoumat podíly. Protože jsou všechny výrazy kladné, nemusíme psát absolutní hodnoty.

(i): a) Toto se dokazuje metodami matematické analýzy.

b) Nejprve odvodíme, že k je $o(q^k)$ pro libovolné $q > 1$. Zvolme tedy $K > 0$ a označme $d_k = q^k - Kk$. Protože $q > 1$, platí $q^k \rightarrow \infty$ a proto musí existovat takové n_0 , aby pro $k \geq n_0$ platilo $q^k \geq \frac{K+1}{q-1}$. Pak pro $k \geq n_0$ platí $(q-1)q^k > K+1$ neboli $q^{k+1} > q^k + K+1$, tedy

$$d_{k+1} = q^{k+1} - K(k+1) > q^k + K + 1 - Kk - K = q^k - Kk + 1 = d_k + 1.$$

S každým zvýšením k o jedničku se alespoň takto zvětší také d_k , tedy musí platit $d_k \rightarrow \infty$. To mimo jiné znamená, že existuje k_0 takové, že pro $k \geq k_0$ platí $d_k > 0$ neboli $q^k > Kk$ neboli $\frac{q^k}{k} > K$. Ověřili jsme podmínku z definice limity.

Pro libovolné $b > 0$ pak máme

$$\frac{q^k}{k^b} = \frac{(q^{k/b})^b}{k^b} = \left(\frac{(q^{1/b})^k}{k}\right)^b \rightarrow \infty^b = \infty.$$

c) Ve výrazu $\frac{k!}{q^k}$ máme pro $k \geq 1$ shodný počet členů v čitateli i jmenovateli a můžeme je spárovat.

$$\frac{k!}{q^k} = \frac{1}{q} \cdot \frac{2}{q} \cdot \frac{3}{q} \cdots \frac{k-1}{q} \cdot \frac{k}{q}.$$

Protože při výpočtu limity zvětšujeme k do nekonečna, dříve nebo později dojde k tomu, že $k > 2q$. Nechť K je nejmenší takové přirozené číslo. Označme $\frac{1}{q} \cdot \frac{2}{q} \cdots \frac{K-1}{q} \cdot \frac{K}{q} = A$. Pro $k > K$ pak máme

$$\begin{aligned} \frac{k!}{q^k} &= \frac{1}{q} \cdot \frac{2}{q} \cdots \frac{K}{q} \cdot \frac{K+1}{q} \cdots \frac{k-1}{q} \cdot \frac{k}{q} = A \cdot \frac{K+1}{q} \cdots \frac{k-1}{q} \cdot \frac{k}{q} \\ &> A \cdot 2 \cdots 2 = A \cdot 2^{k-K} = \frac{A}{2^K} \cdot 2^k \rightarrow \infty. \end{aligned}$$

d) Ve výrazu $\frac{k^k}{k!}$ máme pro $k \geq 1$ shodný počet členů v čitateli i jmenovateli a můžeme je spárovat.

$$\frac{k^k}{k!} = \frac{k \cdot k \cdot k \cdots k}{1 \cdot 2 \cdot 3 \cdots k} = \frac{k}{1} \frac{k}{2} \frac{k}{3} \cdots \frac{k}{k} \geq \frac{k}{1} \cdot 1 \cdot 1 \cdots 1 = k \rightarrow \infty.$$

(ii): $\frac{k^b}{k^a} = k^{b-a} \rightarrow \infty$, neboť $b - a > 0$. Podobně pro logaritmy.

(iii): $\frac{r^k}{q^k} = \left(\frac{r}{q}\right)^k \rightarrow \infty$, neboť $\frac{r}{q} > 1$, je to zase geometrická posloupnost. □

Tyto výrazy jsme už porovnávali ve cvičení 7a.4 a příkladech 7a.e a 7a.l, ale tam jsme dokazovali jen nerovnosti, třeba že $3^k > k^2$. Teď už víme, že 3^k je nejen větší, ale dokonce „nekonečněkrát“ větší.

Někdy se setkáváme také s kombinacemi výrazů ze škály mocnin, obvykle její znalost stačí k jejich analýze.

Příklad 8d.b: Chytré řadící algoritmy dokážou seřadit seznam k prvků s náročností $k \log_2(k)$. Protože $\frac{k \log_2(k)}{k} = \log_2(k) \rightarrow \infty$, platí $k = o(k \log_2(k))$. Výraz $k \log_2(k)$ tedy jde do nekonečna řádově rychleji než k , což nás asi nepřekvapuje. Na druhou stranu je oproti k navýšen o logaritmický člen, který je ve škále dominován libovolnou (kladnou) mocninou. To naznačuje, že $k \log_2(k) = o(k^a)$ pro libovolné $a > 1$. Důkaz:

$$\frac{k^a}{k \log_2(k)} = \frac{k^{a-1}}{\log_2(k)} \rightarrow \infty$$

díky $a - 1 > 0$. Výraz $k \log_2(k)$ je tedy na škále mocnin zasunut do skupiny mocnin k^a , a to těsně za k^1 . Totéž platí, pokud použijeme logaritmus o jiném základě větším než 1.

Teď uvažujme výraz $k2^k$. Ten je intuitivně k -krát neboli nekonečněkrát větší než 2^k , tedy očekáváme $2^k = o(k2^k)$. Snadno to potvrdíme vyhodnocením podílu. Je tedy nad skupinou všech geometrických posloupností? Nikoliv.

Uvažujme 6^k . To se dá napsat jako $6^k = 3^k \cdot 2^k$, což můžeme porovnat s $k \cdot 2^k$ a vidíme, jak se liší. Protože 3^k dominuje k , bude i 6^k dominovat $k2^k$, což opět snadno potvrdíme zkoumáním příslušného podílu. Výraz $k2^k$ je tedy vsunut do skupiny q^k . Kam přesně? Z libovolného $q > 2$ lze vzít stranou dvojku a něco zbude, podobně jako jsme to dělali s šestkou. Pak porovnáváme $(\frac{q}{2})^k 2^k$ versus $k2^k$ a díky $\frac{q}{2} > 1$ bude část $(\frac{q}{2})^k$ dominovat tomu k . Formálně lze například takto:

$$\frac{q^k}{k2^k} = \frac{(\frac{q}{2})^k}{k} \rightarrow \infty.$$

To ukazuje, že výraz $k2^k$ je do skupiny q^k zasunut hned za 2^k , následující geometrické posloupnosti (ty s $q > 2$) mu dominují.

△

Teď zavedeme pojmy pro přibližné porovnávání výrazů.

!

Definice.

Nechť (a_k) , (b_k) jsou posloupnosti nenulových čísel.

Řekneme, že a_k je $O(b_k)$, jestliže existují $K > 0$ a $k_0 \in \mathbb{N}$ takové, že $|a_k| \leq K|b_k|$ pro $k \geq k_0$.

Řekneme, že a_k je $\Omega(b_k)$, jestliže existují $L > 0$ a $k_0 \in \mathbb{N}$ takové, že $|a_k| \geq L|b_k|$ pro $\forall k \geq k_0$.

Řekneme, že a_k je $\Theta(b_k)$ nebo že $a_k \asymp b_k$, jestliže existují $K, L > 0$ a $k_0 \in \mathbb{N}$ takové, že $L|b_k| \leq |a_k| \leq K|b_k|$ pro $\forall k \geq k_0$.

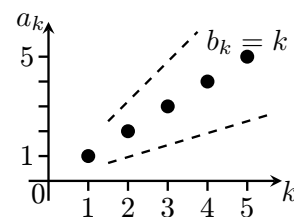
Vztah $a_k = O(b_k)$ čteme „ a_k je velké o b_k “. Říkáme také, že „ a_k má stejnou asymptotickou rychlost růstu jako b_k “.

Jako obvykle nás zajímá dění jen u ocasu posloupností, proto nám v definici to k_0 umožňuje ignorovat jejich začátky. Pro velká k pak vztah O vyžaduje $|a_k| \leq K|b_k|$, což znamená, že a_k mohou být větší než b_k , ale „ne o moc“. Je to taková „benevolentnější nerovnost“.

Pro zjednodušení předpokládejme a_k a b_k kladné, což u složitosti algoritmů máme. Graf posloupnosti (b_k) představuje jakési horní ohraničení a běžná nerovnost $a_k \leq b_k$ pak vybírá ty posloupnosti (a_k) , jejichž grafy jsou pod tímto ohraničením. Pojem $a_k = O(b_k)$ funguje obdobně, jen se jako horní ohraničení nebere pouze posloupnost (b_k) , ale také její kladné násobky. Například vztah $a_k = O(k)$ splní všechny posloupnosti, jejichž grafy se dají omezit shora nějakou přímkou. Takových je jistě mnoho, ale určitě mezi ně nepatří třeba $a_k = k^2$, protože parabola roste příliš rychle na to, aby se dala shora omezit nějakou přímkou.

Druhý pojem představuje opačnou „benevolentní nerovnost“ a jako obvykle jej nutně nepotřebujeme a také se moc nepoužívá.

Třetí pojem obě nerovnosti spojuje. Spojením nerovností \leq a \geq získáme rovnost, obdobně $a_k = \Theta(b_k)$ představuje „benevolentní rovnost“. Vezmeme graf posloupnosti (b_k) a vyrobíme z něj dva modifikované tvary vynásobením konstantami. Ty pak vytvoří jakýsi pás a všechny posloupnosti, jejichž grafy jsou v tomto pásu, splňují vztah $a_k = \Theta(b_k)$. Je intuitivně jasné, že pomocí pojmu $\Theta(b_k)$ dokážeme docela efektivně kontrolovat, jak rychle posloupnosti rostou.



Výraz $a_k = \Theta(b_k)$ čteme „ a_k je téta b_k “, ale v diskrétní matematice (a dalších aplikacích) často slyšíme také „asymptotická rychlost růstu a_k je b_k “, „ a_k je řádu b_k “ a podobně.

! **Příklad 8d.c:** Uvažujme $a_k = 13k$ a $b_k = 23k$. Pak pro všechna $k \geq 0$ platí $a_k = 13k \leq 23k = 1 \cdot b_k$ neboli $a_k \leq K b_k$ pro $K = 1$, proto $a_k = O(b_k)$.

Přepisem této nerovnosti na $b_k \geq 1 \cdot a_k$ se dozvíme, že také $b_k = \Omega(a_k)$. Jde tedy jen o jiný zápis stejného vztahu.

Obdobně můžeme pro všechna $k \geq 0$ odhadovat $b_k = 23k = \frac{23}{13} 13k = \frac{23}{13} a_k$ neboli $b_k \leq L a_k$ pro $L = \frac{23}{13}$, proto $b_k = O(a_k)$. I tuto nerovnost lze přepsat jako $a_k \geq \frac{1}{L} b_k$ a dostáváme $a_k = \Omega(b_k)$.

Zjistili jsme, že $a_k = O(b_k)$ a $b_k = O(a_k)$, tedy „benevolentní nerovnost“ platí v obou směrech.

Oba odhady a_k lze spojit do jednoho například takto: $\frac{13}{23} b_k \leq a_k \leq b_k$. To ukazuje, že $a_k = \Theta(b_k)$. Nebo je můžeme přepsat tak, abychom získali omezení pro b_k : $a_k \leq b_k \leq \frac{23}{13} a_k$. Takže také platí $b_k = \Theta(a_k)$.

Výsledky $13k = O(23k)$ a $13k = \Theta(23k)$ naznačují, že tyto relace splňují naše očekávání ohledně toho, že mají ignorovat násobící konstanty, viz cvičení 8d.5.

Nyní uvažujme $c_k = 13k + 23$. Evidentně platí $a_k \leq c_k$, proto $a_k = O(c_k)$. Ukážeme, že to platí i naopak.

Zvolme $k_0 = 23$. Pro $k \geq k_0$ pak platí $23 \leq k$, a tedy také

$$c_k = 13k + 23 \leq 13k + k = 14k = \frac{14}{13}13k = Ka_k, \text{ kde } K = \frac{14}{13}.$$

Proto $c_k = O(a_k)$.

Alternativně lze použít $k_0 = 1$ a pro $k \geq 1$ odhadovat

$$c_k = 13k + 23 \leq 13k + 23k = 36k = \frac{36}{13}13k = \frac{36}{13}a_k.$$

Spojením obou odhadů opět odvodíme, že $c_k = \Theta(a_k)$.

Zdá se, že tyto pojmy také umějí ignorovat nepodstatné části výrazů. Potvrdíme to ve větě 8d.6.

△

Přepisování nerovností na vhodné tvary lze provést i obecně a dokázat tak následující tvrzení o vztahu mezi porovnávacími pojmy.

!

Fakt 8d.4.

Pro libovolné posloupnosti $(a_k), (b_k)$ nenulových čísel platí následující:

- (i) $a_k = O(b_k)$ právě tehdy, když $b_k = \Omega(a_k)$
- (ii) $a_k = \Theta(b_k)$ právě tehdy, když $a_k = O(b_k)$ a $b_k = O(a_k)$,
což je právě tehdy, když $a_k = O(b_k)$ a $a_k = \Omega(b_k)$.

Obdobné vztahy spojují nerovnosti \leq, \geq a rovnost $=$. Ukážeme, že vlastnosti těchto známých relací platí v podstatě také pro jejich benevolentní verze.

!

Fakt 8d.5.

Uvažujme posloupnosti $(a_k), (b_k), (c_k)$ nenulových čísel.

- (i) $a_k = O(a_k), a_k = \Omega(a_k), a_k = \Theta(a_k)$.
- (ii) $a_k = \Theta(b_k)$ právě tehdy, když $b_k = \Theta(a_k)$.
- (iii) Jestliže $a_k = \Theta(b_k)$ a $b_k = \Theta(c_k)$, pak $a_k = \Theta(c_k)$.
Jestliže $a_k = O(b_k)$ a $b_k = O(c_k)$, pak $a_k = O(c_k)$.
Jestliže $a_k = \Omega(b_k)$ a $b_k = \Omega(c_k)$, pak $a_k = \Omega(c_k)$.

Důkazy necháme jako cvičení 8d.6.

Vidíme, že relace Θ je reflexivní, symetrická a tranzitivní, což jsou právě ty vlastnosti, které od rozumného pojmu shody očekáváme. Je to vlastně ekvivalence. Příklad 8d.c ukazuje, že tato relace na rozdíl od rovnosti není antisymetrická, ale to se od ní ani nečeká, u rovnosti je to taková kuriozita.

Relace O a Ω jsou reflexivní a tranzitivní. Na rozdíl od nerovnosti ale nejsou antisymetrické, jak jsme viděli v příkladě 8d.c. V praxi to ale nevádí, podstatné je, že nám fakt 8d.4 ukazuje „benevolentní“ období antisymetrie: Pokud jsou spolu dvě posloupnosti ve vztahu O neboli benevolentní nerovnosti v obou pořadích, pak jsou spolu také v relaci Θ neboli benevolentní rovnosti.

Přenášejí se i vztahy, které spojují běžnou ostrou nerovnost s nerovností a rovností.

!

Fakt 8d.6.

Uvažujme posloupnosti $(a_k), (b_k)$ nenulových čísel.

- (i) Jestliže $a_k = o(b_k)$, pak $a_k = O(b_k)$ a nemůže platit $a_k = \Omega(b_k)$ ani $a_k = \Theta(b_k)$.
- (ii) Jestliže $a_k = \omega(b_k)$, pak $a_k = \Omega(b_k)$ a nemůže platit $a_k = O(b_k)$ ani $a_k = \Theta(b_k)$.
- (iii) Jestliže $a_k = \Theta(b_k)$, pak nemůže platit $a_k = o(b_k)$ ani $b_k = o(a_k)$.

Důkaz (poučný): (i): Zvolme libovolné $K > 0$. Z předpokladu máme platnost $\frac{|b_k|}{|a_k|} \rightarrow \infty$ a podle definice limity musí existovat k_0 takové, aby pro $k \geq k_0$ platilo $\frac{|b_k|}{|a_k|} > K$. Pro tato k pak máme i $|a_k| < \frac{1}{K}|b_k|$, což dokazuje $a_k = O(b_k)$.

Pokud by zároveň platilo $a_k = \Omega(b_k)$ nebo $a_k = \Theta(b_k)$, tak pro nějaké $L > 0$ a k_0 máme $|a_k| \geq L|b_k|$ neboli $\frac{|b_k|}{|a_k|} \leq L$ pro všechna $k \geq k_0$, což ale znemožňuje splnění podmínky z definice $\frac{|b_k|}{|a_k|} \rightarrow \infty$ pro volbu hladiny L , spor.

(ii): Důkaz je obdobný.

(iii): Z definice $a_k = \Theta(b_k)$ najdeme $K, L > 0$ a k_0 takové, že pro všechna $k \geq k_0$ platí $L \leq \frac{|a_k|}{|b_k|} \leq K$. Jestliže ovšem pro všechna $k \geq k_0$ platí $\frac{|b_k|}{|a_k|} \leq L$, pak pro hladinu L není možné splnit podmínku z definice limity ∞ ,

tudíž neplatí, že $\frac{|b_k|}{|a_k|} \rightarrow \infty$ neboli neplatí, že $a_k = o(b_k)$. Z $\frac{|a_k|}{|b_k|} \leq K$ pro všechna k zase vyloučíme $\frac{|a_k|}{|b_k|} \rightarrow \infty$ a neplatí $b_k = o(a_k)$. □

Relace Θ coby ekvivalence může sloužit k tomu, abychom konstatovali, že dva dané výrazy se chovají stejně. V praxi ji ale obvykle používáme jinak. Zápisem $a_k = \Theta(b_k)$ sdělujeme, že nějaký zkoumaný a možná komplikovaný výraz a_k má stejnou asymptotickou rychlost růstu jako jednoduchý výraz b_k , který typicky vybíráme ze škály mocnin. Někdy nepotřebujeme znát přesnou rychlost růstu, stačí nám konstatování, že to není zase tak špatné. Pak bychom použili $a_k = O(b_k)$. Například $a_k = O(k^a)$ říká, že a_k jde do nekonečna v nejhorším jako polynom, což také může být docela rychle, ale rozhodně to není takový nárůst jako třeba u geometrických posloupností.

! Příklad 8d.d: Prozkoumáme asymptotickou rychlost růstu výrazu $4k^3 - 100k^2 + 15 \log_2(k)$.

Škála mocnin nám říká, že k^3 dominuje ostatním členům, tudíž by se chování daného výrazu mělo pro velká k řídit právě jím. Vliv násobící čtyřky bychom pro naše účely také měli ignorovat. Naše intuice tedy vede k následujícímu tvrzení.

$$1. \quad 4k^3 - 100k^2 + 15 \log_2(k) = \Theta(k^3).$$

Argumenty nám zjednoduší fakt, že (pro velká k) je daná posloupnost kladná, takže nebudeme psát absolutní hodnoty.

$$a) \quad \text{Nejprve dokážeme, že } 4k^3 - 100k^2 + 15 \log_2(k) = O(k^3).$$

Definice vyžaduje nalezení horního odhadu ve tvaru Kk^3 .

Podle škály mocnin $\log_2(k) = o(k^3)$, proto také $\log_2(k) = O(k^3)$ a tedy existuje $k_0 \in \mathbb{N}$ a $K_l > 0$ takové, že $\log_2(k) \leq K_l k^3$ pro $k \geq k_0$. Mimochodem, znalci elementárních funkcí vědí, že prostě $\log_2(k) \leq k^3$ pro všechna $k \in \mathbb{N}$. Každopádně pro $k \geq k_0$ můžeme odhadovat

$$4k^3 - 100k^2 + 15 \log_2(k) \leq 4k^3 + 15 \log_2(k) \leq 4k^3 + 15K_l k^3 = (4 + 15K_l)k^3.$$

Našli jsme požadované $K = 4 + 15K_l$.

$$b) \quad \text{Nyní dokážeme, že } 4k^3 - 100k^2 + 15 \log_2(k) = \Omega(k^3).$$

Zde narazíme na problém. Víme, že $k^2 \leq k^3$, což nabízí následující odhad:

$$4k^3 - 100k^2 + 15 \log_2(k) \geq 4k^3 - 100k^2 \geq 4k^3 - 100k^3 = -96k^3.$$

Bohužel, kandidát $L = -96$ je záporný a tedy nevyhovující. Musíme být opatrnější. Záměrně zvolíme zbytečně komplikovanou strategii, abychom ukázali, jak by se dalo postupovat v případě, že bychom místo $4k^3$ měli třeba $\frac{1}{2}k^3$.

Protože změna konstanty u k^3 neovlivní celkovou rychlost růstu, můžeme si z násobku 4 vypůjčit nějaký a -násobek pro $a < 4$ a využít jej k neutralizaci členu $100k^2$. Zvolíme $a = 2$ a máme

$$4k^3 - 100k^2 = 2k^3 + (2k^3 - 100k^2).$$

Víme, že $100k^2 = o(2k^3)$ neboli $\frac{2k^3}{100k^2} \rightarrow \infty$. Proto existuje $k_0 \in \mathbb{N}$ takové, že pro $k \geq k_0$ už máme $\frac{2k^3}{100k^2} \geq 1$ neboli $100k^2 \leq 2k^3$ neboli $2k^3 - 100k^2 \geq 0$. Pak také

$$4k^3 - 100k^2 + 15 \log_2(k) = 2k^3 + (2k^3 - 100k^2) + 15 \log_2(k) \geq 2k^3 + 0 + 0 = 2k^3.$$

Volba $L = 2$ tak potvrdí, že $4k^3 - 100k^2 + 15 \log_2(k) = \Omega(k^3)$.

Dokázali jsme, že „asymptotická rychlost růstu $4k^3 - 100k^2 + 15 \log_2(k)$ je k^3 “. Někdy bychom také řekli, že daný výraz roste řádově jako k^3 , nebo je typu k^3 , popřípadě že jeho dominantním členem je k^3 .

Tento výsledek ukazuje, že pojem Θ správně rozpoznal nedůležitost některých členů a také ignoroval násobící čtyřku u dominantního členu.

$$2. \quad 4k^3 - 100k^2 + 15 \log_2(k) = \Theta(13k^3).$$

Toto tvrzení není tak výmluvné, ale je také pravdivé. Vyplývá snadno z první části v cvičení 8d.5.

$$3. \quad 4k^3 - 100k^2 + 15 \log_2(k) = O(k^5).$$

Důkaz: Víme, že pro $k \geq 1$ je $k^3 \leq k^5$ a $\log_2(k) \leq k^5$, proto

$$4k^3 - 100k^2 + 15 \log_2(k) \leq 4k^3 + 15 \log_2(k) \leq 3k^5 + 15k^5 = 18k^5.$$

Výsledek jsme potvrdili. Je správný, nicméně není optimální (plýtvá). Podle první části už totiž víme, že také platí $4k^3 - 100k^2 + 15 \log_2(k) = O(k^3)$, což danou posloupnost omezí výrazněji.

Podle škály mocnin a tranzitivity relace O vyplývá, že jakmile jsme jednou pro daný výraz dokázali řád růstu $O(k^3)$, tak už platí také $O(k^a)$ pro libovolné $a \geq 3$, platí také $O(q^k)$ a podobně. Takové odhady ale nejsou optimální, obvykle se snažíme najít nejlepší variantu. Poznamenejme, že někdy v praxi takováto neoptimální omezení mají svou cenu, a to v případě, že zkoumaný výraz je natolik komplikovaný, že „správnou“ rychlost růstu nejsme schopni určit. Pak jsme rádi, když jej alespoň nějak omezíme shora.

△

! Všechny porovnávací pojmy spojuje otázka, co víme o $\frac{|b_k|}{|a_k|}$. Jsou tři hlavní možnosti. Pokud jde tento podíl do nekonečna, tak b_k dominuje a_k , popřípadě a_k je zanedbatelné vzhledem k b_k , a píšeme $a_k = o(b_k)$. Pokud $\frac{b_k}{a_k} \rightarrow 0$, tak $b_k = o(a_k)$, tedy b_k je zanedbatelné vzhledem k a_k . Pokud je tento podíl nějakým způsobem omezený, tak se dostáváme k pojmům O , Ω či Θ . V praxi bývá zajímavá zejména ta poslední možnost a vede k ní zajímavá cesta, vhodná zejména pro příznivce limity.

! **Věta 8d.7.**

Uvažujme posloupnosti $(a_k), (b_k)$ nenulových čísel.

Jestliže má $\frac{|a_k|}{|b_k|}$ nenulovou (a konečnou) limitu, tak $a_k = \Theta(b_k)$.

Důkaz je snadný přímo z definice limity, kterou jsme zde ovšem neprobrali.

Příklad 8d.e: Znovu dokážeme, že $4k^3 - 100k^2 + 15 \log_2(k) = \Theta(k^3)$.

Díky škále mocnin víme, že k^3 dominuje logaritmům a proto $\frac{\log_2(k)}{k^3} \rightarrow 0$. Odtud

$$\frac{4k^3 - 100k^2 + 15 \log_2(k)}{k^3} = 4 - 100 \frac{1}{k} + 15 \frac{\log_2(k)}{k^3} \rightarrow 4 - 100 \cdot 0 + 15 \cdot 0 = 4 > 0.$$

Hotovo.

△

Poznámka: Tento příklad vysvětluje, proč jsme zde zaváděli pojem nulové limity, když je převoditelný na limitu nekonečno. Formálně by nám pro studium dominance opravdu stačilo pracovat s limitou nekonečnou, ale výpočet výše by pak začal takto:

Ze škály mocnin víme, že $\frac{k^3}{\log_2(k)} \rightarrow \infty$. Odtud

$$\frac{k^3}{4k^3 - 100k^2 + 15 \log_2(k)} = ?$$

Namísto jednoduchého roznásobení zlomku máme problém. Je zvládnutelný trikem

$$\frac{k^3}{4k^3 - 100k^2 + 15 \log_2(k)} = \frac{1}{\frac{4k^3 - 100k^2 + 15 \log_2(k)}{k^3}} = \frac{1}{4 - 100 \frac{1}{k} + 15 \frac{1}{\frac{k^3}{\log_2(k)}}} \rightarrow \frac{1}{4 - 100 \cdot 0 + 15 \frac{1}{\infty}} = \dots,$$

ale je to zbytečná komplikace. Možnost vybrat si mezi $\frac{|b_k|}{|a_k|}$ a $\frac{|a_k|}{|b_k|}$ je velmi výhodná.

△

Poznámka: Zajímavá situace nastane, když podíl $\frac{b_k}{a_k}$ konverguje k jedné. Tato situace se obvykle značí $a_k \sim b_k$ a je to něco jako vyšší kvalita vztahu Θ . Pro velká k jsou takové posloupnosti nejen porovnatelné, ale prakticky stejné. To je velmi užitečné, když děláme výpočty s velkými čísly, stačí dosadit do něčeho pěkného namísto do komplikovaného vzorce.

Jako ukázkou dosadíme $k = 13 \cdot 10^6$ do výrazů $4k^3 - 100k^2 + 15 \log_2(k)$ a $4k^3$. Dostáváme $8.78798 \cdot 10^{21}$ a $8.78800 \cdot 10^{21}$, což je dost dobrá aproximace. Se zvyšujícím se k se přesnost aproximace dále zlepšuje.

Takovouto aproximaci najdeme snadno. Postupujeme jako při hledání dominantního zástupce pro Θ , u kterého ponecháme příslušný násobící koeficient.

△

! **Poznámka:** Vraťme se k otázce porovnávání rychlosti růstu dvou výrazů a_k a b_k . Podíváme se na chování podílu $\frac{|b_k|}{|a_k|}$ pro velká k a můžeme pozorovat následující:

Pokud máme štěstí, tak limita $\frac{|b_k|}{|a_k|}$ existuje. Protože $\frac{|b_k|}{|a_k|} > 0$, nemůže být záporná. Případy:

- Limita je nekonečná, pak $a_k = o(b_k)$.
- Limita je konečná a kladná, pak $a_k = \Theta(b_k)$.
- Limita je nula, pak $b_k = o(a_k)$.

Pokud limita neexistuje, pak je ještě šance, že ten zlomek umíme nějak omezit.

- Pokud najdeme K , aby pro velká k platilo $\frac{|b_k|}{|a_k|} \leq K$, tak $b_k = O(a_k)$.
- Pokud najdeme L , aby pro velká k platilo $\frac{|b_k|}{|a_k|} \geq L$, tak $a_k = \Omega(b_k)$.
- Pokud se povede obojí, tak $a_k = \Theta(b_k)$.
- Pokud se podíl nedá odříznout od nekonečna či mínus nekonečna, tak mezi a_k a b_k není žádný z hledaných vztahů.

V praxi se k tomuto postupu uchylujeme spíš v nouzi, pro běžné situace lépe funguje přístup, který záhy odvodíme.

△

Při zkoumání výrazu $4k^3 - 100k^2 + 15 \log_2(k)$ jsme ideálního zástupce k^3 našli ignorováním částí, které nám přišly nevýznamné. Vlastně tím propojujeme obě skupiny pojmů, které zde probíráme, tedy dominanci a přibližné porovnávání. Obecně to funguje takto:

!

Věta 8d.8.

Uvažujme posloupnosti $(a_k), (b_k)$ kladných čísel jdoucí do nekonečna. Jestliže $b_k = o(a_k)$, pak $a_k + b_k = \Theta(a_k)$.

Důkaz: Podle předpokladu platí $\frac{b_k}{a_k} \rightarrow 0$. Pak

$$\frac{|a_k + b_k|}{|a_k|} = \left| \frac{a_k + b_k}{a_k} \right| = \left| 1 + \frac{b_k}{a_k} \right| \rightarrow |1 + 0| = 1.$$

□

Indukcí to pak rozšíříme na více sčítanců, čímž dostaneme algoritmus pro hledání dominantního typu v kombinaci více členů.

! **Poznámka:** Je dobré si uvědomit, že vynechávání zanedbatelných členů funguje pouze v součtech (a rozdílech). Ve výrazu $k + \log_2(k)$ se k relativně velkému číslu k přidá relativně malé číslo $\log_2(k)$ (zde je důležité to vzájemné porovnání), čímž se výsledek příliš neovlivní.

Na druhou stranu ve výrazu $k \log_2(k)$ se velké číslo k násobí něčím, co je výrazně menší než k , ale pořad je to velké (logaritmus jde do nekonečna), tedy dojde k významnému navýšení výsledku oproti k a logaritmus ignorovat nelze.

Podobně ve výrazu $2^{k+\log_2(k)}$ by vynecháním logaritmu došlo jen k malé změně v součtu, ale exponenciála ten malý rozdíl zase nafoukne, čili nelze říct, že $2^{k+\log_2(k)}$ roste stejně rychle jako 2^k . Ve skutečnosti $2^{k+\log_2(k)} = 2^k 2^{\log_2(k)}$, tedy 2^k se násobí číslem jdoucím do nekonečna, rozhodně ten logaritmus nelze ignorovat.

Dobrá zpráva je, že v praxi obvykle čelíme právě součtům a někdy rozdílům, přičemž sčítáme základní výrazy ze škály mocnin násobené konstantami. Jinak řešeno, zajímají nás hlavně lineární kombinace výrazů ze škály mocnin.

△

S Algoritmus 8d.9.

pro určování asymptotické rychlosti růstu výrazu vhodného typu.

0. Předpoklad: Daný výraz a_k je lineární kombinace výrazů ze škály mocnin, popřípadě jejího rozšíření.

1. Jednotlivé členy rozdělíme do skupin, které mají následující pořadí dominance:

$$k! \gg k^k \gg q^k \gg k^b \gg \log_2^a(k) \gg c,$$

přičemž nás zajímají jen členy s $a > 0, b > 0$ a $q > 1$ (tedy jdoucí do nekonečna).

Předpokládejme, že tam alespoň jeden takový člen je. Pak lze členy q^k pro $|q| \leq 1$ a $k^b, \log_2^a(k)$ pro $a, b \leq 0$ ignorovat.

2. V tomto kroku uvažujeme jen ty členy, které patří do dominantní skupiny (podle škály mocnin) mezi těmi zastoupenými v kroku 1.

Vybereme z nich ten, který má největší konstantu a, b , popř. q . Pokud je jediný, stává se dominantním členem celého výrazu, označme jej b_k .

3. Platí $a_k = \Theta(b_k)$. Dokázat to lze například výpočtem limity $\frac{a_k}{b_k}$.

△

Často srovnáváme jen mocniny, z výsledků výše pak okamžitě plyne, že pro velká k je chování polynomu určeno jeho nejvyšší mocninou.

Příklad 8d.f:

1. $4k^2 + 257k = \Theta(k^2)$.

3. $k3^k + 20k^3 + 5 \cdot 3^k = \Theta(k3^k)$.

2. $3^k - 7k^{527} + 23 \cdot k2^k - 13 \log_2(k) = \Theta(3^k)$.

4. $20k! + 160k^{13} - 3^k = \Theta(k!)$.

△

Poznámka: Algoritmus dobře poslouží ve většině případů, ale mohou se objevit komplikace, se kterými nám pomůže dobrá znalost pojmů a myšlenek. Již jsme viděli, jak se vypořádat se smíšenými typy, například pro dané $b > 0$ výrazy $k^b \log_2^a(k)$ tvoří rodinu, která dominuje mocnině k^b , ale je dominována libovolnou mocninou k^B pro $B > b$. Skupina $q^k x^b$ pro jisté $q > 1$ zase dominuje geometrické posloupnosti (exponenciále) q^k , ale je dominována libovolným Q^k pro $Q > q$.

Při zkoumání výpočetní náročnosti se to nestává, ale v jiných oblastech se mohou ve výrazu objevit také q^k se základem $q < -1$. Protože pak $|q^k| = |q|^k \rightarrow \infty$, účastní se hry na dominanci a spadají do skupiny q^k . O dominanci mezi jednotlivými výrazy tohoto typu pak rozhoduje $|q|$.

Pokud se dominantním stane q^k pro $q < -1$, pak celý výraz nejde do nekonečna, ale jeho absolutní hodnota tam jde, a to rychlostí $|q|^k$. Chování výrazu samotného pak dobře vystihuje chování q^k , což je posloupnost, která střídavě utíká do $+\infty$ a $-\infty$, vidíme oscilaci s amplitudou rostoucí do nekonečna.

Může se také stát, že se objeví zástupci z jedné skupiny, mezi kterými neumíme rozhodnout. V zásadě se to týká právě exponenciál, kde se například ve výrazu objeví 2^k a také $(-2)^k$. Pak se pro sudé k tyto členy sčítají a dají dominantní hodnotu, ale pro k liché se odčítají a tím největším se ve výrazu stává někdo jiný. Celkové chování výrazu tak nelze popsat jednoduchým vzorcem, tedy nelze nějak jednoduše určit jeho řád. Viz například $13^k + (-13)^k + k^2$, které se pro sudá k rovná $2 \cdot 13^k + k^2$ rostoucí řádem 13^k , zatímco pro liché k se rovná k^2 . Při zkoumání výpočetní náročnosti algoritmů takovéto komplikace nečekáme.

Tam nečekáme také situaci, která se jinak stát může, a to případ, kdy žádný z členů výrazu nejde do nekonečna. Pak tam také nejde ani celá posloupnost a její dominantní člen je třeba hledat mezi těmi členy, které obvykle ignorujeme. To už se ale dostáváme mimo oblast diskrétní matematiky.

△

Ignorování zanedbatelných členů lze aplikovat nejen při hledání ideálního zástupce, ale také při porovnávání dvou složitějších výrazů. Pak stačí porovnávat jen jejich dominantní členy.

!

Fakt 8d.10.

Uvažujme posloupnosti $(a_k), (u_k), (b_k), (v_k)$ nenulových čísel. Předpokládejme, že $a_k = \Theta(u_k)$ a $b_k = \Theta(v_k)$. Pak platí:

- (i) $a_k = \Theta(b_k)$ právě tehdy, když $u_k = \Theta(v_k)$.
- (ii) $a_k = o(b_k)$ právě tehdy, když $u_k = o(v_k)$.

Na závěr se vrátíme k poznámce, že nám naše nástroje umožňují také zjednodušit výpočty tím, že pro komplikovaný výraz najdeme jednodušší aproximaci. To nám ale nemusí být moc platné, když ten zjednodušující výraz je faktoriál, jehož přesný výpočet zabere pro větší k dost času. Nabízí se nápad, že bychom jej také mohli aproximovat.

Začneme jednoduchým odhadem.

Fakt 8d.11.

Pro $k \geq 6$ platí $\frac{k^k}{3^k} < k! < \frac{k^k}{2^k}$.

Důkaz (rutinní s výjimkou): Tou výjimkou je netriviální fakt, že zlomek $(1 + \frac{1}{k})^k = (\frac{k+1}{k})^k$ je pro $k \in \mathbb{N}$ vždy mezi 2 a 3, na což jsou rozličné triky, které sem spíš nepatří, a dá se to najít v každé tlustší učebnici analýzy. Pro nás to znamená, že $\frac{1}{3} \leq (\frac{k}{k+1})^k \leq \frac{1}{2}$ neboli $3(\frac{k}{k+1})^k \geq 1$ a $2(\frac{k}{k+1})^k \leq 1$.

Dokážeme teď indukci, že $\frac{k^k}{3^k} < k!$.

(0) $k = 6$: Platí $\frac{6^6}{3^6} = 2^6 < 6!$, což určitě platí.

(1) Pro dané $k \geq 6$ předpokládejme, že $\frac{k^k}{3^k} < k!$. Pak

$$(k+1)! = (k+1) \cdot k! \stackrel{\text{IP}}{>} (k+1) \frac{k^k}{3^k} = \frac{3k^k}{(k+1)^{k+1}} \frac{(k+1)^k}{3^{k+1}} = 3 \left(\frac{k}{k+1} \right)^k \frac{(k+1)^{k+1}}{3^{k+1}} \geq \frac{(k+1)^{k+1}}{3^{k+1}}.$$

Důkaz hotov.

Teď dokážeme indukci, že $k! < \frac{k^k}{2^k}$.

(0) $k = 6$: $6! < 3^6 = \frac{6^6}{2^6}$ platí.

(1) Dáno $k \geq 6$, předpokládejme, že $k! < \frac{k^k}{2^k}$. Pak

$$(k+1)! = (k+1) \cdot k! \stackrel{\text{IP}}{<} (k+1) \frac{k^k}{2^k} = \frac{2k^k}{(k+1)^{k+1}} \frac{(k+1)^k}{2^{k+1}} = 2 \left(\frac{k}{k+1} \right)^k \frac{(k+1)^{k+1}}{2^{k+1}} \leq \frac{(k+1)^{k+1}}{2^{k+1}}.$$

□

Faktoriál je tedy někde mezi $\left(\frac{k}{3}\right)^k$ a $\left(\frac{k}{2}\right)^k$. Následující tvrzení říká, že když místo 2 nebo 3 v tomto odhadu dáme e , tak už víceméně dostaneme faktoriál.

Věta 8d.12. (Stirlingův vzorec)

Pro velká k platí $k! \sim \sqrt{2\pi k} \left(\frac{k}{e}\right)^k$.

Je to výsledek těžký, ale stojí za to, ta aproximace je opravdu vynikající. Dokonce až neuvěřitelně. Normálně když člověk slyší, že něco je aproximační vzorec, tak čeká dobré aproximace pro větší čísla, řekněme v řádu tisíců či milionů, někdy musí počkat ještě déle, ale tento vzorec se trefuje hodně blízko dokonce od začátku. Ukážeme to v tabulce, kde jsme dali i procentuální chybu vzhledem k základu, která o přesnosti vypovídá nejvíce.

k :	1	2	3	4	5	6	7	8	9	10	20	30
$k!$:	1	2	6	24	120	720	5040	40320	362880	3628800	$2.433 \cdot 10^{18}$	$2.653 \cdot 10^{32}$
Stirling :	0.92	1.9	5.8	23.5	118	710	4980	39902	359536	3598696	$2.423 \cdot 10^{18}$	$2.645 \cdot 10^{32}$
chyba % :	8	5	3.3	2	1.7	1.4	1.2	1	0.9	0.8	0.4	0.3

Pro inženýrské výpočty je chyba 0.3% moc, ale pro informatiku to bohatě stačí.

Cvičení

Cvičení 8d.1 (rutinní): Seřadte podle asymptotické rychlosti růstu (od nejméně k nejvíce dominantnímu) výrazy $5k + \log_2(k)$, $k^2 - 100k$, $k \log_2(k)$, $2k^3$, \sqrt{k} .

Cvičení 8d.2 (rutinní): Najděte asymptotické rychlosti růstu následujících výrazů.

- a) $\sqrt{k} + \log_2(k)$; c) $2^k + k^2 + 2k$;
 b) $k^3 + 13k^2 + 14$; d) $2^k + k!$.

Cvičení 8d.3 (poučné): Dokažte podle definice následující tvrzení:

- a) $100k^2 = O(k^4)$, $100k^2 = o(k^4)$; c) $k^4 = o(k!)$;
 b) $3k + 7 = \Theta(k)$; d) $k + 3 \sin(k) = \Theta(k)$.

Cvičení 8d.4 (poučné): Dokažte, že pro každé $a > 0$ platí $\frac{k!}{k^a} \rightarrow \infty$.

Nápověda: Nejprve dokažte, že pro $a > 0$ existuje K takové, že pro $k \geq K$ platí $\frac{k-a}{k} \geq \frac{1}{2}$. (Pomůže otázka, jaká je limita toho podílu.) Pak pro $a \in \mathbb{N}$ chytře zlomek rozdělte. Pro necelá a použijte srovnání pomocí nerovnosti.

Cvičení 8d.5 (poučné): Nechť (a_k) , (b_k) jsou posloupnosti nenulových čísel a $A, B \neq 0$. Dokažte následující:

- a) Jestliže $a_k = O(b_k)$, pak $Aa_k = O(Bb_k)$.
 b) Jestliže $a_k = \Theta(b_k)$, pak $Aa_k = \Theta(Bb_k)$.

Cvičení 8d.6 (poučné): Uvažujme posloupnosti (a_k) , (b_k) , (c_k) nenulových čísel. Dokažte následující:

- a) $a_k = O(a_k)$, $a_k = \Omega(a_k)$, $a_k = \Theta(a_k)$.
 b) $a_k = \Theta(b_k)$ právě tehdy, když $b_k = \Theta(a_k)$.
 c) Jestliže $a_k = O(b_k)$ a $b_k = O(c_k)$, pak $a_k = O(c_k)$.
 Jestliže $a_k = \Theta(b_k)$ a $b_k = \Theta(c_k)$, pak $a_k = \Theta(c_k)$.

Viz věta 8d.5.

Řešení:

8d.1: Pořadí je \sqrt{k} , $5k + \log_2(k)$, $k \log_2(k)$, $k^2 - 100k$, $2k^3$.

8d.2: a) $\Theta(\sqrt{k})$. b) $\Theta(k^3)$. c) $\Theta(2^k)$. d) $\Theta(k!)$.

8d.3: a) $100k^2 = o(k^4)$: $\frac{100k^2}{k^4} = \frac{100}{k^2} \rightarrow 0$. $100k^2 = O(k^4)$: plyne z předchozího nebo přímo: $K = 1$, $k_0 = 10$, pak $k \geq 10 \implies k^2 \geq 100 \implies 100k^2 \leq k^2 \cdot k^2 = 1 \cdot k^4$.

b) $L = 1$, $K = 4$, $k_0 = 7$, pak $k \geq 7 \implies 1 \cdot k \leq 3k + 7$ a $k \geq 7 \implies 3k + 7 \leq 3k + k = 4k$.

c) Předpoklad $k \geq 5$, pak $\frac{k!}{k^4} = 1 \cdot 2 \cdot \dots \cdot (k-5) \frac{k-4}{k} \frac{k-3}{k} \frac{k-2}{k} \frac{k-1}{k} k \geq \frac{k-4}{k} \frac{k-3}{k} \frac{k-2}{k} \frac{k-1}{k} k \rightarrow 1 \cdot 1 \cdot 1 \cdot 1 \cdot \infty = \infty$.

d) $L = \frac{1}{2}$, $K = 2$, $k_0 = 6$, pak $k \geq 6 \implies k + 3 \sin(k) \leq k + 3 \leq k + k = 2k$ a díky $3 \leq \frac{1}{2}k$ také $k \geq 6 \implies k + 3 \sin(k) \geq k - 3 \geq k - \frac{1}{2}k = \frac{1}{2}k$.

8d.4: Nechť $a \in \mathbb{N}$. Existence K plyne z $\frac{k-a}{k} \rightarrow 1$. Pro $k \geq K$ pak

$$\frac{k!}{k^a} = \frac{1 \cdot 2 \cdot \dots \cdot (k-a) \cdot \dots \cdot (k-1) \cdot k}{k \cdot \dots \cdot k} \geq \frac{k-a}{k} \dots \frac{k-1}{k} \cdot k \geq \frac{k-a}{k} \dots \frac{k-a}{k} \cdot k \geq \left(\frac{1}{2}\right)^a \cdot k \rightarrow \infty.$$

Pro obecné $a > 0$ je $k^a \leq k^{\lceil a \rceil}$.

8d.5: a) Máme $K > 0$ aby $|a_k| \leq K|b_k|$, pak $|Aa_k| = |A| \cdot |a_k| \leq |A|K|b_k| = \frac{|A|K}{|B|} \cdot |Bb_k|$. b) obdobně.

8d.6: a) $|a_k| \leq 1 \cdot |a_k|$. b) $L|b_k| \leq |a_k| \leq K|b_k| \iff \frac{1}{K}|a_k| \leq |b_k| \leq \frac{1}{L}|a_k|$. c) a d) $|a_k| \leq K_1|b_k| \leq K_1K_2|c_k|$, obdobně dolní odhad.