O relacích

Pavel Klavík

stručný textík ke cvičení z diskrétní matematiky

V tomto textu si zkusíme přiblížit, jak fungují relace. Zaměříme se například na jejich skládání, kterému není například v Kapitolách z diskrétní matematiky věnováno tolik prostoru, kolik by si zasloužilo. Relace jsou základním konceptem, který je při studiu matematiky velice důležité pochopit. V závěru textu také zmíníme několik hlubších věcí týkajících se ekvivalencí, v souvislostí s akcí grupy na množině.

Jako žádný text ani tento není bez chyb. Pokud nějakou objevíte, napište mi prosím na `pavel@klavik.cz`. Rád bych zde poděkoval Martině Vaváčkové, Lukáši Machovi a Dušanu Knopovi za četné připomínky k tomuto textu.

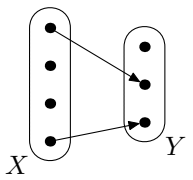
1 Seznámení s relacemi

Definice relace. *Relace* se definuje jako podmnožina kartézského součinu dvou nosných množin X a Y. Tedy relace je množina některých dvojic (x, y), kde $x \in X$ a $y \in Y$—říkáme, že takové dvojice jsou v relaci.

Příklad 1.1. *Nechť X je množina žen a Y je množina mužů. Příkladem relace ze života může být relace "být v manželství", tedy množina dvojic (x, y), že žena x a muž y jsou manželé.*

Pro relaci R se někdy $(x, y) \in R$ značí jako $x\,R\,y$. To má výhodu zejména pro relace jako $<$. Je zvykem spíše zapisovat $1 < 3$ než $(1, 3) \in <$.

Relace se dají znázorňovat grafem. Množinu X nakreslíme na jednu stranu, množinu Y na druhou stranu. Dvojice (x, y), které jsou v relaci, spojíme šipkou z x do y. Například grafické znázornění výše uvedené relace naleznete na obrázku 1.



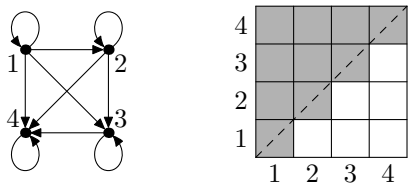
Obrázek 1: Jak vypadá relace "být v manželství" znázorněná grafem.

Často se používají relace, pro které jsou obě nosné množiny stejné, tedy podmnožiny $X \times X = X^2$. Ty popisují vztahy mezi některými dvojicemi prvků na množině X. Takovým relacím budeme říkat, že jsou *na množině* X.

Příklad 1.2. *Uvažme relaci $\leq$ na množině $\{1, 2, 3, 4\}$. Tato relace je následující podmnožina dvojic:*

$$\big\{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\big\}.$$

Existují další dva způsoby, jak graficky znázorňovat relace na množině X. První způsob je grafem. Jednotlivé prvky budeme reprezentovat puntíky (těm se říká *vrcholy*) a pokud dvojice (x, y) je v relaci, spojíme x šipkou s y. Zde je důležité, že šipka má orientaci. Šipkám, které vedou z x do x, se říká *smyčky*. Druhý způsob je maticí, kde políčko s indexy i, j zvýrazníme, právě když (i, j) leží v relaci. Obě znázornění pro relaci z výše uvedeného příkladu jsou na obrázku 2.



Obrázek 2: Znázornění relace $\leq$ na množině $\{1, 2, 3, 4\}$ grafem a maticí.

Jak brzy uvidíme, každé z těchto znázornění má svoje výhody i nevýhody. Proto se vždy hodí uvažovat to, které je pro daný problém nejpříhodnější.

Vlastnosti relací. Existuje několik vlastností, které jsou natolik důležité, že dostaly zvláštní jméno. Všimněte si, že tyto vlastnosti mají smysl jenom pro relace na množině. Říkáme, že relace R na množině X je

- **reflexivní**, pokud $\forall x \in X : (x, x) \in R$,
- **antireflexivní**, pokud naopak $\forall x \in X : (x, x) \notin R$,
- **symetrická**, pokud $\forall x, y \in X : (x, y) \in R \implies (y, x) \in R$, a
- **tranzitivní**, pokud $\forall x, y, z \in X : (x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R$.

Zda relace splňuje tyto vlastnosti, lze snadno nahlédnout ve znázornění grafem či matici.

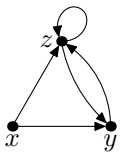
Relace je reflexivní, pokud má u každého vrcholu smyčku, naopak je antireflexivní, pokud nemá u žádného vrcholu smyčku. Například relace na obrázku 2 je reflexivní. V matici jsou smyčky reprezentované políčky na diagonále. Pokud je relace reflexivní, je celá diagonála zvýrazněna. Naopak antireflexivní relace nemá na diagonále zvýrazněné vůbec nic.

Relace je symetrická, pokud ke každé šipce z x do y existuje i šipka opačná. Zde si můžeme všimnout, že smyčky to splňují automaticky. V maticovém zápisu symetrické relace odpovídají maticím, které jsou symetrické podle vyznačené diagonály. Například relace na obrázku 2 symetrická není, neboť třeba šipka z 1 do 2 nemá šipku opačnou.

Tranzitivita je dobře vidět ve znázornění grafem. Říká, že pokud jdou šipky z x do y a z y do z, potom existuje i přímá šipka z x do z. Takže v grafu relace máme zkratky. Je snadné indukcí nahlédnout, že pokud mezi libovolnými dvěma vrcholy x a y existuje posloupnost šipek (říkejme jí *cesta*), potom v tranzitivní relaci existuje i přímá šipka z x do y.

I když se v definici tranzitivity vyskytují tři prvky x, y a z, neplatí, že by musely být různé. Například pokud máme dvojice (x, y) a (y, x) v relaci, potom tranzitivita říká, že také smyčky (x, x) a (y, y) jsou v relaci. Uvažme relaci nad jednoprvkovou množinou $\{x\}$ tvořenou jedinou dvojicí (x, x). Zkuste ověřit, že tato triviální relace je reflexivní, symetrická a tranzitivní. Druhým extrémním příkladem je prázdná relace, která neobsahuje ani jednu dvojici. Taková relace je vždy antireflexivní, symetrická a tranzitivní.

Příklad 1.3. *Uvažme relaci na množině $\{x, y, z\}$ definovanou následujícím grafem. Je tato relace reflexivní, antireflexivní, symetrická nebo tranzitivní?*



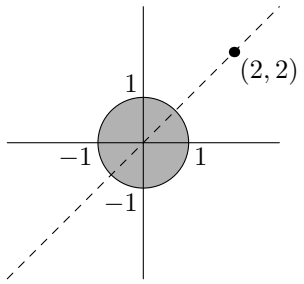
Řešení. Relace zjevně není ani reflexivní, ani antireflexivní, obsahuje totiž přesně jednu smyčku u vrcholu z. Relace není symetrická, neboť (x, y) leží v relaci, ale (y, x) v relaci neleží. Relace dokonce není ani tranzitivní, i když to na první pohled nemusí být patrné. Obsahuje totiž dvě opačné šipky (y, z) a (z, y). Z definice tranzitivity dostaneme, že i (y, y) a (z, z) by musely ležet v relaci. U vrcholu z je smyčka, ale u vrcholu y ji neobjevíme. □

Příklad 1.4. *Uvažme relaci R na množině $\mathbb{R}$. Dvojice $(x, y) \in R$, pokud*

$$x^2 + y^2 \leq 1.$$

Jak vypadá tato relace? Je reflexivní, antireflexivní, symetrická nebo tranzitivní?

Řešení. Prvky této relace jsou uspořádané dvojice reálných čísel, lze je tedy geometricky zobrazit jako body v rovině. Všechny body ležící v relaci R odpovídají kruhu o poloměru 1 se středem v počátku, viz obrázek 3.



Obrázek 3: Všechny body (x, y) splňujících $x^2 + y^2 \leq 1$.

Pokud by relace R měla být reflexivní, musela by obsahovat každý bod (x, x). Tyto body tvoří přímku $x = y$, vyznačenou čárkovaně na obrázku. Avšak celá přímka rozhodně v relaci R neleží, například $(2, 2) \notin R$, tedy relace R není reflexivní. Podobně relace není antireflexivní.

Symetrie říká, že pro každé $(x, y) \in R$ také $(y, x) \in R$. Zjevně, pokud $x^2+y^2 \leq 1$, z komutativity též platí $y^2 + x^2 \leq 1$. Geometricky symetrie říká, že relace R je symetrická podle vyznačené přímky $x = y$.

S tranzitivitou nám obrázek bohužel moc nepomůže. Naštěstí snadno objevíme protipříklad, $(1, 0)$ a $(0, 1)$ leží v relaci R, ale $(1, 1)$ neleží. Relace tedy není tranzitivní.

Připomíná vám toto geometrické uvažování vlastnosti, které má znázornění maticí? Toto není náhoda, protože body roviny si můžeme představit jako nekonečnou matici, která je nekonečně jemná. Vyznačená přímka $y = x$ je diagonálou této matice. □

Na závěr si ukážeme jedno na první pohled překvapivé tvrzení s poučným důkazem:

Tvrzení 1.5. *Pokud relace R na množině X je antireflexivní a tranzitivní, je také silně antisymetrická, tedy $\forall x, y \in X$ platí, že $(x, y) \in R \implies (y, x) \notin R$.*

Důkaz. Toto je typický příklad tvrzení, k jehož dokázání si stačí uvědomit, co znamenají jednotlivé vlastnosti. Tvrzení dokážeme sporem. Předpokládejme, že R je antireflexivní a tranzitivní relace a pro spor existuje $x, y \in X$, že $(x, y) \in R$ a $(y, x) \in R$. Z tranzitivity víme, že také $(x, x) \in R$. To je ale smyčka, a tedy relace R nemůže být antireflexivní—dostáváme spor. □

Všimněte si, že v důkazu nepotřebujeme vědět, že $x \neq y$. Samozřejmě důkaz by šel rozdělit na dvě možnosti, pro $x = y$ a pro $x \neq y$. Pokud $x = y$, hned dostáváme spor, že relace není antireflexivní. Výše uvedený důkaz ovšem funguje v obou případech. Pokud $x = y$, složíme smyčku (x, y) dvakrát a dostaneme smyčku (x, x) stejně jako předtím. Obecně platí, že čím méně možností musíme v důkazu rozebrat, tím je menší šance, že budeme mít nějaký krok chybně. Například velice snadno se může stát, že na některou z možností zapomeneme.

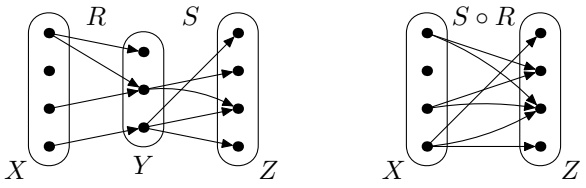
2 Skládání relací

Definice skládání. Mějme dvě relace R na $X \times Y$ a S na $Y \times Z$. Relace R *složeno* S, která se značí $S \circ R$,[1] je následující relace na $X \times Z$:

$$\big\{(x, z) \mid \exists y \in Y : (x, y) \in R \wedge (y, z) \in S\big\}.$$

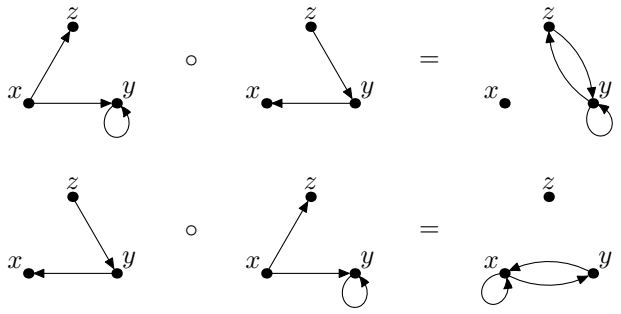
[1] Aby zmatků nebylo málo, někdy se skládání relací zapisuje také obráceně, jako $R \circ S$. Paradoxně pro zobrazení, což je speciální případ relací, se používá opačná forma, f složeno s g se zapisuje $g \circ f$. Toto je pravděpodobně jeden

Co definice znamená, je nejlépe pochopitelné z následujícího obrázku. Relace R a S položíme vedle sebe. Dvojice (x, z) je v relaci $S \circ R$, právě když existuje cestička z x do z využívající pouze šipek z R a S. Taková cesta nejprve musí využít šipku z x do nějakého $y \in Y$, která musí ležet v relaci R. Poté na ní musí v relaci S navazovat šipka z y do z. Je vidět, proč relace R musí být definována na $X \times Y$ a relace S na $Y \times Z$, jinak by na sebe totiž relace nepasovaly a složení by nebylo možné.



Obrázek 4: Pokud složíme relaci R s relací S, šipky vedou přímo z X do Z.

Pokud skládáme dvě relace na množině X, lze výsledek složení vyčíst přímo z grafu. To odpovídá tomu, že v grafu máme dva druhy šipek, šipky relace R a šipky relace S. Ve složení se potom budou vyskytovat ty šipky, které odpovídají cestičkám délky dva—použijeme nejprve šipku z R a na ni navazující šipku z S. Na obrázku 5 jsou relace R a S naznačeny pro přehlednost zvlášť. Navíc tento obrázek ilustruje veledůležitý fakt, že *skládání relací není komutativní*, tedy obecně neplatí, že by $S \circ R = R \circ S$. Zkuste objevit co nejmenší a nejjednodušší protipříklad.



Obrázek 5: Relace R a S na množině $\{x, y, z\}$ lze složit dvěma způsoby, vždy s jiným výsledkem.

Mocnění relací. Speciální příklad skládání je umocňování relace na množině. Nechť R je relace na množině X. Definujme $R^1 = R$ a induktivně $R^{n+1} = R \circ R^n$. Ukažme si, jak vypadá umocňování na příkladu, který se bude v dalším zkoumání skládání relací ještě hodit.

Příklad 2.1. *Nechť $R = (\mathbb{N}, <)$ a $S = (\mathbb{N}, \leq)$, kde $<$ a $\leq$ značí běžná uspořádání přirozených čísel. Jak vypadá R^n a S^n?*

Řešení. Začneme s relací R. Přirozené číslo x je v relaci s každým větším přirozeným číslem. Tedy šipky vedou do následujícího přirozeného čísla a všech větších. Aby dvojice (x, y) ležela v R^n, musí být x propojeno s y pomocí n navazujících šipek. To jde právě tehdy, pokud $x \leq y - n$.

U relace S si nejprve všimněme, že pokud $(x, y) \notin S$, neleží ani v libovolné její mocnině. Proč? Protože, pokud $(a, b) \in S$, platí $a \leq b$. Tedy žádná šipka nevede "doleva" v uspořádání přirozených čísel podle velikosti. Proto tam nemůže vést ani složení n šipek. Na druhou stranu pokud $(x, y) \in S$, (x, y) leží i v libovolné mocnině S^n. Stačí složit $(n-1)$-krát smyčku (x, x) s šipkou (x, y). Tedy platí $S = S^n$ pro každou mocninu S^n. □

Můžeme si všimnout, že pokud je množina X nekonečná, potom mohou být pro relaci na X každé dvě mocniny odlišné relace—například pro relaci R. Následující tvrzení ukazuje, že pro konečnou množinu X to není možné.

z historických neduhů matematiky, neboť kdysi byly relace a funkce zcela odlišné pojmy s jiným značení. V moderní matematice se propojily, ale historické značení zůstalo. V tomto textu si podobné zmatky odpustíme a skládání relací i zobrazení budeme značit stejně, tedy $S \circ R$. Čtenář by si měl vzít poučení, že kdykoliv se v nějakém textu setká se skládáním, měl by si dát pozor, které pořadí si autoři zvolili. Naštěstí taková věc se velice snadno pozná.

Tvrzení 2.2. *Nechť R je relace na konečné množině X. Potom existují dvě mocniny R^r a R^s, že $r \neq s$ a $R^r = R^s$.*

Důkaz. Na problém půjdeme od lesa. Položíme si na první pohled nesouvisející otázku: Kolik existuje různých relací na množině X? Pro každou dvojici (x, y), kde $x, y \in X$, si můžeme vybrat, zda v relaci bude, či nikoliv. Každou volbou získáme jinou relaci. Proto celkem existuje $2^{|X|^2}$ různých relací na množině X.

Pokud uvážíme $2^{|X|^2} + 1$ mocnin relace R, potom podle Dirichletova principu musí existovat dvě stejné mocniny. □

Poznamenejme na závěr, že takto získaný odhad je zbytečně velký, ve skutečnosti se budou mocniny opakovat mnohem dříve.

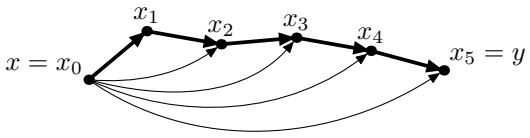
Relace S z příkladu 2.1 je zvláštní tím, že umocňování ji nemění. Platí pro ni totiž následující:

Tvrzení 2.3. *Pokud relace R na množině X je reflexivní, potom $R \subseteq R^n$ pro každé $n \in \mathbb{N}$.*

Důkaz. Stačí ukázat, že kdykoliv $(x, y) \in R$, také $(x, y) \in R^n$. Protože relace R je reflexivní, $(x, x) \in R$. Proto složíme $(n-1)$-krát smyčku s šipkou (x, y) a dostáváme, že $(x, y) \in R^n$. □

Tvrzení 2.4. *Pokud relace R na množině X je tranzitivní, potom $R^n \subseteq R$ pro každé $n \in \mathbb{N}$.*

Důkaz. Stačí ukázat, že kdykoliv $(x, y) \in R^n$, také $(x, y) \in R$. Aby $(x, y) \in R^n$, musí existovat $x_0, x_1, \ldots, x_n \in X$, že $(x_i, x_{i+1}) \in R$ pro každé $i \in \{0, 1, \ldots, n-1\}$, a navíc $x_0 = x$ a $x_n = y$.[2] Situace je naznačena na obrázku 6.



Obrázek 6: Tranzitivita na cestě z x do y zaručuje zkratky.

Víme, že relace R je tranzitivní. Tedy $(x_0, x_1) \in R$ a $(x_1, x_2) \in R$ zaručuje, že také $(x_0, x_2) \in R$. Dále $(x_0, x_2) \in R$ spolu s $(x_2, x_3) \in R$ implikuje, že $(x_0, x_3) \in R$. Pokud podobně aplikujeme indukci, zjistíme, že $(x_0, x_i) \in R$ pro každé $i \in \{1, \ldots, n\}$. V neposlední řadě tedy $(x_0, x_n) \in R$, neboli $(x, y) \in R$, což jsme chtěli dokázat. □

Obě tvrzení dohromady dávají následující důsledek, který například relace S z příkladu 2.1 splňuje:

Důsledek 2.5. *Pokud relace R na množině X je reflexivní a tranzitivní, potom $R = R^n$ pro každé $n \in \mathbb{N}$.*

3 Zobrazení

Definice zobrazení. Speciálním druhem relací jsou *zobrazení*. Zobrazení f je relace na $X \times Y$ taková, že pro každé $x \in X$ existuje právě jedno $y \in Y$, že $(x, y) \in f$. Jinými slovy, z každého prvku množiny X vede právě jedna šipka do množiny Y. Protože pro pevné x je y takové, že $(x, y) \in f$, určené jednoznačně, někdy se toto y označuje $f(x)$. Říká se, že f je zobrazení z X do Y, což se značí $f : X \to Y$. Poznamenejme, že pro zobrazení se někdy používá i pojem *funkce*, historicky byl termín funkce rezervován pro zobrazení do reálných nebo komplexních čísel. Pro nás budou oba pojmy totožné.

Skládání zobrazení funguje úplně stejně jako skládání relací obecně. Na druhou stranu jejich skládání má specifické vlastnosti, z nichž některé si v této kapitole předvedeme.

[2] Na $x_0, \ldots, x_n$ neklademe žádné další požadavky, například rozhodně neplatí, že by musely být po dvou různé.

Tvrzení 3.1. *Nechť f a g jsou libovolná zobrazení, $f : X \to Y$, $g : Y \to Z$. Potom $g \circ f$ je také zobrazení.*

Důkaz. Víme, že $g \circ f$ je relace na $X \times Z$. Potřebujeme ukázat, že je zobrazením. Nechť $(x, z) \in g \circ f$. Uvažme, proč vede šipka v $g \circ f$ z x do z. Musí existovat $y \in Y$, že $(x, y) \in f$ a $(y, z) \in g$. Protože ale f je zobrazení, je takové y určené jednoznačně jako $f(x)$. Protože g je zobrazení, y jednoznačně určuje z jako $g(y)$. Tedy z každého x vychází přesně jedna šipka do $g(f(x))$ a $g \circ f$ je zobrazení. □

Vlastnosti zobrazení. Zobrazení může mít jednu z následujících tří vlastností. Říkáme, že zobrazení $f : X \to Y$ je

- **prosté** (injektivní), pokud $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \implies x_1 = x_2$,
- **na** (surjektivní), pokud $\forall y \in Y\ \exists x \in X$, že $f(x) = y$, a
- **bijektivní**, pokud je zároveň prosté a na.

Jinými slovy, zobrazení je prosté, pokud do každého prvku $y \in Y$ vede nejvýše jedna šipka, a je na, pokud do každého vede alespoň jedna šipka.

Tvrzení 3.2. *Nechť f je zobrazení z X do X, kde X je konečná množina. Toto zobrazení je prosté, právě když je na.*

Důkaz. Pokud je f prosté, do každého $x \in X$ vede nejvýše jedna šipka. Protože ale šipek je stejně jako prvků v X, vede do každého z nich právě jedna šipka.[3] Tedy do každého $x \in X$ vede alespoň jedna šipka a f je zobrazení na. Druhá implikace se ukáže podobně. □

Naopak pokud je X nekonečná množina, tvrzení neplatí. Uvažme například zobrazení $f : \mathbb{N} \to \mathbb{N}$ a $g : \mathbb{N} \to \mathbb{N}$ definované $f : x \mapsto 2x$ a $g : x \mapsto \lfloor \frac{x}{2} \rfloor$.[4] Zobrazení f je prosté, ale není na. Naopak g je na, ale není prosté.

Velice důležité zobrazení *identita* $\mathrm{id} : X \to X$ je definované takto: $\forall x \in X : \mathrm{id}(x) = x$. Identita je neutrální zobrazení na skládání—tedy $\forall f$ platí $f \circ \mathrm{id} = f$ a $\mathrm{id} \circ f = f$, pokud složení dávají smysl. Výše uvedená zobrazení f a g jsou skoro inverzní. Složením z jedné strany jako $g \circ f$ dostaneme identitu. Při složení opačném však identitu nedostaneme. K zamyšlení: Jak vypadá $f \circ g$?

Na závěr si ukážeme, jaký vliv má skládání zobrazení na jejich vlastnosti.

Tvrzení 3.3. *Nechť $f : X \to Y$ a $g : Y \to Z$ jsou prostá zobrazení. Potom i zobrazení $g \circ f$ je prosté.*

Důkaz. Předpokládejme pro spor, že by existovala $x_1, x_2 \in X$ a $z \in Z$, že $x_1 \neq x_2$, $(x_1, z) \in g \circ f$ a $(x_2, z) \in g \circ f$. Tedy existují y_1 a y_2 (navíc určené jednoznačně), že $(x_i, y_i) \in f$ a $(y_i, z) \in g$ pro $i \in \{1, 2\}$, jinak by šipky (x_1, z) a (x_2, z) nebyly ve složení $g \circ f$. Protože f je prosté, nemůže být $y_1 = y_2$, jinak by do $y_1 = y_2$ vedly dvě šipky z f. Také g je prosté, a tedy nemůže být $y_1 \neq y_2$, jinak by dvě šipky vedly do z. Tyto dvě možnosti jsou naznačeny na obrázku 7. Dostáváme spor, a tedy $g \circ f$ je prosté. □

Je přirozené se ptát, zda platí opačné tvrzení, tedy zda prosté zobrazení $g \circ f$ říká, že by i f a g byla prostá zobrazení.

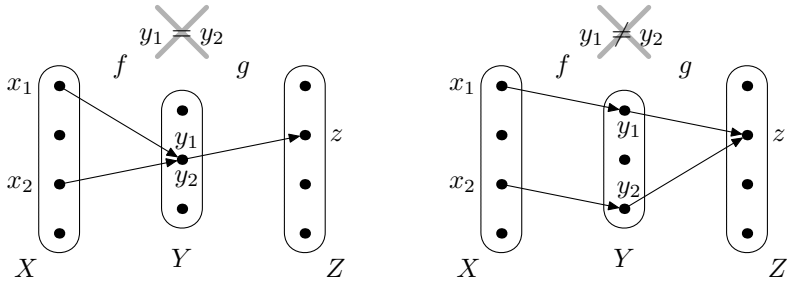
Tvrzení 3.4. *Nechť $f : X \to Y$ a $g : Y \to Z$ jsou zobrazení a $g \circ f$ je prosté. Potom i f je prosté.*

Důkaz. Dokážeme sporem. Pokud zobrazení f není prosté, existují $x_1, x_2 \in X$, že $x_1 \neq x_2$ a $f(x_1) = f(x_2) = y$. Ale zobrazení g zobrazí y na $g(y) = z$. Tedy ve složení dostaneme šipky (x_1, z) a (x_2, z) a zobrazení $g \circ f$ není prosté. To je hledaný spor. □

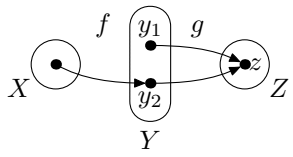
Na první pohled se může zdát, že výše uvedený důkaz lze snadno upravit a dokázat, že i g musí být prosté. Takový postup je však odsouzený selhat, neboť tvrzení pro g neplatí. Vyvrací ho například protipříklad na obrázku 8, $g \circ f$ je zjevně prosté, ale g není.

[3] Proč? Pokud by do nějakého prvku šipka nevedla, měli bychom $|X|$ šipek, které vedou do $|X| - 1$ prvků. Tedy podle Dirichletova principu by do jednoho z nich vedly alespoň dvě šipky, což nejde.

[4] Tento zápis v případě f říká: $\forall x \in \mathbb{N} : f(x) = 2x$.



Obrázek 7: Dvě situace v důkazu, z nichž ani jedna nemůže nastat.



Obrázek 8: Protipříklad, funkce g není prostá, ale $g \circ f$ prostá je.

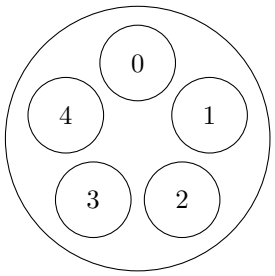
Protipříklad přesně ukazuje, kde je problém. Pokud zobrazení g není prosté, existují $y_1, y_2 \in Y$ a $z \in Z$, že $y_1 \neq y_2$, $(y_1, z) \in g$ a $(y_2, z) \in g$. Ovšem aby se tyto šipky ve složení projevily a způsobily, že $g \circ f$ nebude prosté, musí nějaká šipka v f vést z X do y_1 a nějaká do y_2. To ovšem nemusí obecně platit.

Z tohoto plyne následující poučení. Pokud něco dokazujeme, musíme dbát na detaily. Jinak totiž snadno dokážeme něco, co neplatí.

4 Ekvivalence

Definice ekvivalence. *Ekvivalence* jsou relace, které jsou současně reflexivní, symetrické a tranzitivní. V matematice se tento pojem vyskytuje velice často, a proto se s ním alespoň stručně seznámíme. Ekvivalence rozdělují prvky množiny X do skupin, kterým se říká *třídy ekvivalence*. Dva prvky ze stejné třídy jsou vždy v relaci, naopak dva prvky z různých tříd nikdy v relaci nejsou. Ekvivalence sdružuje prvky, které jsou nějakým způsobem podobné, neboli ekvivalentní.

Klasickým příkladem ekvivalence je relace R_k, kde $k \in \mathbb{N}$, na množině $\mathbb{Z}$, kde $(n, m) \in R_k$, právě když n a m mají stejný zbytek po dělení k. Uvažme $k = 5$. Tato ekvivalence je nakreslena na obrázku 9. Ekvivalence má pět tříd ekvivalence, podle zbytku čísla po dělení pěti.



Obrázek 9: Ekvivalence rozdělí čísla podle zbytků po dělení k na třídy ekvivalence.

Ukážeme si několik příkladů relací a pokusíme se určit, jestli to jsou ekvivalence.

Příklad 4.1. *Každé komplexní číslo lze zapsat v polárních souřadnicích ve tvaru* $r(\cos\varphi + i\sin\varphi) = r \cdot e^{\varphi i}$*, kde* r *je vzdálenost od počátku a* φ *je úhel (uvažujeme úhly v intervalu* $[0, 2\pi)$*. Definujme relace* R *a* S *na* $\mathbb{C}$ *jako:*

$$R = \big\{(a, b), \text{ že } |a| = |b|\big\}, \qquad S = \big\{(a, b), \text{ že } \varphi_a = \varphi_b\big\}.$$

Jsou tyto relace ekvivalence?

Řešení. Relace R je ekvivalence a její třídy jsou kružnice se středem v počátku. Všechna čísla, která leží na kružnici, mají stejnou vzdálenost od počátku. Tedy libovolná dvojice z nich je v relaci. Naopak pokud čísla leží na různých kružnicích, mají jiné vzdálenosti a v relaci nejsou. Proč je relace ekvivalence? Každému komplexnímu číslu $a \in \mathbb{C}$ přiřadíme jednoznačně reálné číslo $|a|$. Rovnost na reálných číslech je ekvivalence.

Relace S není ekvivalence, i když to není na první pohled patrné. Problémem je zde počátek, který svírá libovolný úhel φ. Počátek by proto musel ležet v každé ze tříd ekvivalence, ale to není možné. Selže tranzitivita a relace není ekvivalence. □

Příklad 4.2. *Zadefinujme relaci R_ε na $\mathbb{R}$, kde $\varepsilon > 0$, tak, že dvě čísla $x, y \in \mathbb{R}$ jsou v relaci R_ε, pokud jsou "skoro stejná", tedy formálně*

$$R_\varepsilon = \{(x, y), \text{ že } |x - y| < \varepsilon\}.$$

Je tato relace ekvivalence?

Řešení. Tato relace ekvivalencí samozřejmě není, protože nesplňuje tranzitivitu. Nechť $a, b, c \in \mathbb{R}$. To, že a je skoro stejné jako b a b je skoro stejné jako c, vůbec neznamená, že i a je skoro stejné jako c. Pokud by to totiž byla pravda, všechna reálná čísla by byla skoro stejná. Jako protipříklad proti tranzitivitě stačí zvolit a libovolně, $b := a + \frac{\varepsilon}{2}$ a $c := a + \varepsilon$. Potom $(a, b) \in R_\varepsilon$, $(b, c) \in R_\varepsilon$, ale $(a, c) \notin R_\varepsilon$. □

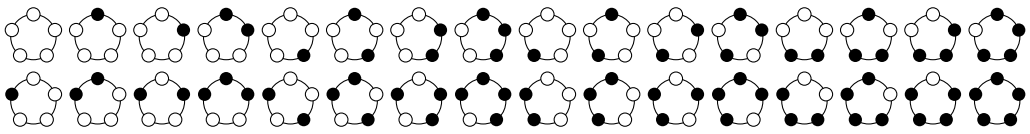
Poznamenejme, že na předcházející relaci je postavená prakticky celá analýza. Například definice limity posloupnosti říká toto: Číslo a je limita posloupnosti, pokud skoro všechna členy posloupnosti, tedy až na konečně mnoho, jsou skoro stejné jako limita a, kde skoro stejnost se definuje pro libovolné $\varepsilon > 0$ pomocí relace R_ε.

Překvapení na závěr. Na konci tohoto povídání si ukážeme jeden překvapivý trik, kterým dokážeme slavnou větu z teorie čísel. Jedná se o Malou Fermatovu větu a tento mistrný kousek objevil S. W. Golomb v roce 1956. Věta říká následující:

Věta 4.3 (Malá Fermatova)**.** *Nechť a je libovolné přirozené číslo a p je libovolné prvočíslo. Potom $a^p - a$ je dělitelné p, což se často zapisuje*

$$a^p - a \equiv 0 \pmod{p}.$$

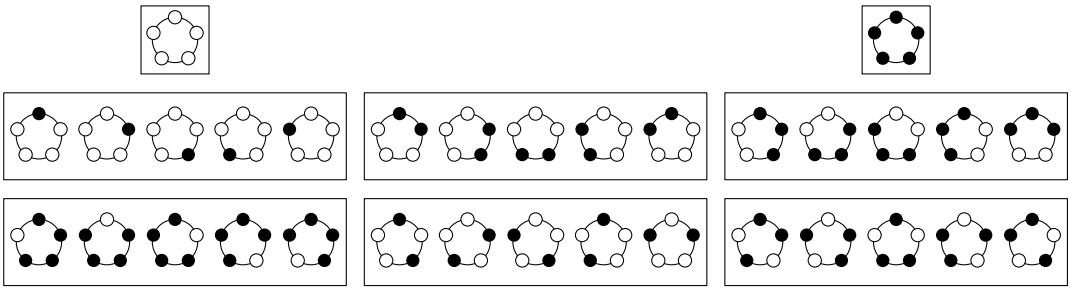
Důkaz. Na důkaz půjdeme kombinatoricky, budeme počítat náhrdelníky tvořené p korálky a různých barev. Nejprve si vysvětlíme myšlenku, až poté ukážeme, že opravdu funguje. Každý z náhrdelníků si můžeme představit jako posloupnost $a_1, \ldots, a_p$ čísel $1, \ldots, a$, tedy dohromady existuje a^p různých náhrdelníků. Pro $a = 2$ a $p = 5$ jsou všechny náhrdelníky zobrazeny na obrázku 10.



Obrázek 10: Existuje a^p různých náhrdelníků tvořených p korálky a různých barev.

Některé náhrdelníky jsou ale stejné, liší se pouze pootočením. Řekneme, že dva náhrdelníky jsou ekvivalentní, pokud jsou stejné až na pootočení. Rozmyslete si, že tato relace je to skutečně ekvivalence na náhrdelnících, tedy že je reflexivní, symetrická a tranzitivní. Na obrázku 11 jsou nakresleny třídy ekvivalence s příslušnými náhrdelníky.

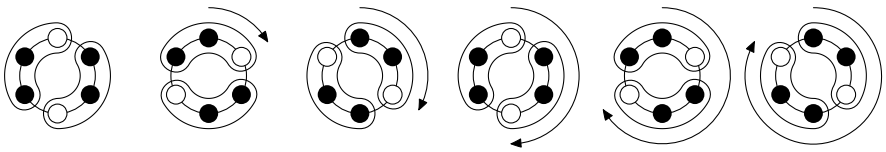
Všimněme si, že třídy jsou dvou druhů. Jednak nalezneme a jednoprvkových tříd, které jsou tvořeny jednobarevnými náhrdelníky. Ostatní třídy vždy obsahují p ekvivalentních náhrdelníků. Tvrdíme, že toto není náhoda a úplně stejně budou třídy vypadat pro libovolná a a p. Uvědomme si, že pokud bychom to uměli dokázat, je celá věta dokázaná. Existuje totiž $a^p - a$ nejednobarevných



Obrázek 11: Ekvivalence obsahuje dva druhy tříd, jednoprvkové a p-prvkové.

náhrdelníků. Pokud je umíme rozdělit do tříd ekvivalence po p prvcích, pak musí být jejich počet $a^p - a$ dělitelný p.

Uvažme jeden pevný náhrdelník délky k, což na chvíli nemusí být prvočíslo, a budeme zkoumat třídu ekvivalence, do které patří. Můžeme ho pootočit o $0, \ldots, k-1$ korálků, takže teoreticky může tato třída obsahovat až k odlišných náhrdelníků. Některá z pootočení však mohou dopadnout stejně, a tedy třída může být menší. Například pro $k = 6$ můžeme mít třídy obsahující teoreticky až šest náhrdelníků, ale v případě náhrdelníku na obrázku 12 bude třída jenom tříprvková, první tři natočení jsou stejná jako poslední tři.



Obrázek 12: Náhrdelník délky šest, který tvoří třídu ekvivalence velikosti tři. Náhrdelník se skládá ze dvou bloků délky tři, vyznačených na náhrdelnících.

Pokud se tak ale stane, náhrdelník se musí skládat z opakujících se bloků menší délky. Například náhrdelník na obrázku se skládá ze dvou bloků délky tři tvořených dvěma černými a jedním bílým korálkem. Třída ekvivalence bude potom obsahovat přesně tolik prvků, jaká je třída nejkratšího opakujícího se bloku, který tvoří celý náhrdelník.

Klíčový fakt je, že délka bloku musí dělit k. V našem případě je k prvočíslo p, které je dělitelné pouze 1 a p. Pokud je náhrdelník tvořený opakujícími se bloky délky jedna, potom je jednobarevný a má jednoprvkovou třídu ekvivalence. Ostatní náhrdelníky jsou tvořeny jediným blokem délky p, a proto je jejich třída ekvivalence velká přesně p. Tím je důkaz dokončen. □

Algebraický dodatek. Při studiu algebry se s ekvivalencemi setkáváme na každém kroku. Pokusíme se naznačit si pár myšlenek, které možná vnesou lepší světlo do předchozího důkazu. Zkoumáme-li například náhrdelníky, často nás nezajímají identické náhrdelníky, které se liší jenom pootočením nebo jinou symetrií, třeba zrcadlením. V algebře podobné symetrie množiny objektů souvisí s pojmem *akce grupy na množině*.

Vysvětlíme si význam jednotlivých pojmů. *Množina* je v našem případě množina všech náhrdelníků, bez ohledu na symetrie, tedy obsahuje a^p prvků. *Grupa* popisuje symetrie, které pro náhrdelníky uvažujeme. V našem případě to je grupa všech pootočení náhrdelníku o $0, \ldots, p-1$ korálků. *Akce* popisuje, jak se symetrie aplikují na prvky množiny. Tedy svazuje dva stejné prvky množiny (až na symetrii) s touto symetrií. Jestliže M je množina a $\mathbb{G} = (G, \cdot)$ je grupa, akce je zobrazení $\circ : M \times G \to M$. V našem případě akce vezme náhrdelník a pootočení z grupy a výsledkem bude pootočený náhrdelník.

Nejprve si vysvětlíme, proč $\mathbb{G}$ tvoří grupu. Jak jistě víte z hodin algebry, grupa je množina prvků spolu s grupovou operací, která se chová hezky.[5] V našem případě prvky grupy jsou symetrie,

[5] Co to znamená formálně? Grupa je uspořádaná dvojice $\mathbb{G} = (G, \cdot)$, kde $\cdot : G \times G \to G$. Navíc existuje neutrální prvek

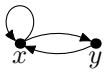
které na množině M uvažujeme. Grupová operace potom symetrie skládá, tedy složení dvou symetrií je zase symetrie. Skládání musí splňovat axiomy grupy, tedy existuje neutrální symetrie *identita*, která nic nemění. Dále ke každé operaci existuje inverzní symetrie, která změnu vrátí zpět. Formálně ještě musíme požadovat další vlastnosti od akce $\circ$.[6] V případě náhrdelníků je $\mathbb{G}$ aditivní grupa $\mathbb{Z}_p$.

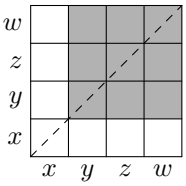
Grupa $\mathbb{G}$ nám definuje následující relaci R na množině M. Nechť $m_1, m_2 \in M$. Dvojice $(m_1, m_2) \in R$, právě když $\exists g \in G$, že $m_1 \circ g = m_2$. Jinými slovy, v relaci jsou ty dvojice, které jsou stejné až na nějakou symetrii danou grupou. Protože $\mathbb{G}$ je grupa, vzniklá relace R bude vždy ekvivalence. Zkuste si rozmyslet, proč tomu tak je. Třídy ekvivalence budou odpovídat jednotlivým prvkům, které jsou skutečně odlišné. Čím větší je grupa symetrií, tím jsou prvky množiny symetričtější a třídy ekvivalence větší.

V souvislosti s akcí grupy na množině si člověk může klást řadu otázek. Třeba: Kolik prvků obsahuje množina až na symetrie dané grupou? Tedy kolik tříd ekvivalence má relace R? Existuje Burnsidovo lemma, které umožní tyto otázky snadno zodpovědět, ale to už by bylo na jiné povídání.

5 Cvičení

1. Rozhodněte, zda následující relace jsou reflexivní, antireflexivní, symetrické a tranzitivní:





$$R = \{(x, y) \mid x^2 + 1 \geq y\}, \qquad S = \{(x, y) \mid |x| \geq y\}.$$

2. Uvažme relaci $<$ na množině $\mathbb{R}$. Jak vypadá mocnina $<^n$?

3. Relaci R na $X \times Y$ lze reprezentovat jako matici $|X| \times |Y|$, kde na pozici i, j je jednička, pokud $(i, j) \in R$ a nula jinak. Objevte souvislost mezi skládáním a násobením matic.

4. Nalezněte relaci R na konečné množině X, že $R^n \neq R^{n+1}$ pro každé $n \in \mathbb{N}$.

5. Ukázali jsme si, že skládání relací není obecně komutativní. Řekneme, že relace R na množině X *komutuje se vším*, pokud $R \circ S = S \circ R$ pro každou relaci S na množině X. Dokažte, že identita (relace, která má pouze smyčky u každého prvku) a prázdná relace (relace, která neobsahuje žádnou dvojici) komutují se vším. Dokažte, že žádná další taková relace neexistuje.

6. Nechť $f : X \to Y$ a $g : Y \to Z$ jsou zobrazení na. Platí, že i $g \circ f$ je na? Naopak, nechť $g \circ f$ je na. Vyplývá z toho, že f je na či g je na?

7. Nechť $f : X \to X$ je zobrazení, že $f \circ f = f$. Musí nutně platit, že $f = \mathrm{id}$? Charakterizujte všechna taková zobrazení.

8. Platí podobně jako u zobrazení, že by složení dvou ekvivalencí na množině X byla opět ekvivalence na množině X?

9. Dokažte, že relace R popisovaná v algebraickém dodatku je skutečně pro libovolnou akci grupy na množině ekvivalence.

$1 \in G$ vůči $\cdot$, tedy $\forall g \in G$ je $g \cdot 1 = 1 \cdot g = g$. Dále ke každému prvku existuje inverzní prvek, tedy $\forall g \in G\ \exists g^{-1} \in G$, že $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

[6] Třeba, že $\forall g_1, g_2 \in G$ a $\forall m \in M$ platí $(m \circ g_1) \circ g_2 = m \circ (g_1 \cdot g_2)$, nebo $\forall m \in M$ platí $m \circ 1 = m$.