Jakýsi úvod do diskrétní matematiky

Áďa Klepáčovic

28. listopadu 2022

Obsah

1 Zajímavé problémy **1**

1.1 Problém tří domů a tří studní 1

1.2 Hrátky s puntíky 2

2 Úvodní pojmy **3**

2.1 Logické spojky a kvantifikátory 3

2.2 Množiny 5

2.3 Relace 7

2.3.1 Kreslení relací 7

2.3.2 Skládání relací 9

2.4 Ekvivalence 10

1 | Zajímavé problémy

Jednou z hlavních a oblíbených podmnožin diskrétní matematiky a kombinatoriky je *teorie grafů*. Jednoduše řečeno, graf je množina bodů – vrcholů, mezi některýmiž vedou spojnice – hrany.

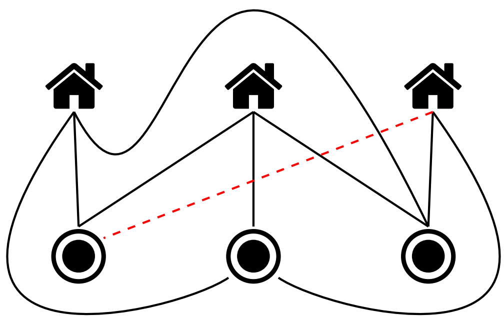
Představíme si pár úloh jako ze života, jak bývá v matematice zvykem, jejichž zdánlivá nevinnost je v rozporu s jejich významem pro rozvoj teorie.

1.1 Problém tří domů a tří studní

V zemi za sedmero horami a sedmero řekami žili byli tři sousedi. Každý z nich vlastnil rodinný domek a dělili se o vodu ze tří blízkých studní. Jednou se ale sousedi po sporu rozkmotřili a už se nechtěli ani vidět. Potřebovali ale pitnou vodu. Každý se odmítl vzdát nároku na nějakou ze studní, tak si jako poslední společný čin najali dvorního architekta, by nechal postavit cesty od každého domu ke každé studni. Cesty se nesměly nikde potkat, aby do sebe sousedi na cestě pro vodu náhodou nenarazili.

Dvorní architekt, probděv tři dny a tři noci hledaje způsob, jak nasupené sousedy uspokojit, klekl nakonec únavou a prohlásil, že cesty bez křížení vystavět nelze.

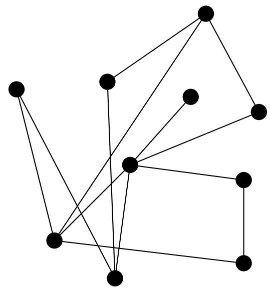
My s ním souhlasíme, ale není lehké najít způsob, jak úlohu matematicky formalizovat, a podat důkaz.



Obrázek 1: Tři domy a tři studně.

1.2 Hrátky s puntíky

Ukážeme si ještě dvě pěkné úlohy s puntíky a čarami. Mějme třeba deset puntíků v rovině a pár z nich spojme čarami, jako na obrázku 2.



Obrázek 2: Náhodný graf na deseti vrcholech.

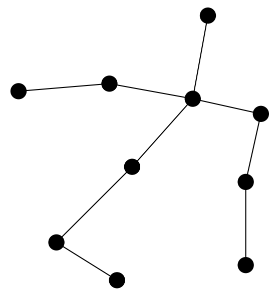
Otázka, kterou se budeme časem zabývat zní „Kolik maximálně mohu nakreslit spojnic, než mi vznikne trojúhelník?“ Trojúhelníkem zde myslíme trojici bodů, z nichž každé dva jsou spojeny. Do tohoto grafu se určitě ještě dají nějaké přikreslit, ale kolik přesně? A jak tuto úlohu řešit obecně pro jakýkoliv počet bodů?

Podobně zajímavá, ale už víc algoritmická otázka, by zněla „Jak poznám, jestli v nějakém grafu existuje trojúhelník?“. Samozřejmě by šlo se prostě podívat na každou jednu trojici bodů, ale jde to i líp?

Ještě na pár odstavců zůstaneme u spojených puntíků. Úloha, která se ukázala jako zásadní v teorii grafů má co dělat s cestami. *Cestou* v grafu nazveme posloupnost bodů – vrcholů, takovou, že mezi sousedními vrcholy na cestě vždycky vede spojnice. Jinak řečeno, mohu se v klidu projít od jednoho vrcholu k druhému, aniž bych musel skákat mezi vrcholy. Naším úkolem je najít takovou množinu spojnic – hran, že se mezi každými dvěma vrcholy dá projít po cestě.

Pro deset vrcholů jedno možné řešení vidíte na obrázku 3.

Je jednoduché si rozmyslet, kolik nejméně hran je třeba nakreslit. Ovšem, co když můžeme vybírat jen z nějaké předem dané množiny? Řešení pak nemusí vždycky existovat (může se totiž stát, že žádné hrany k dispozici nemáme). Dá se nějak efektivně poznat, kdy úlohu lze řešit a kdy ne? A co třeba otázka, kolik existuje řešení s minimálním počtem hran; co řešení, součet přes všechny jehož hrany je nejmenší? V této obecné podobě



Obrázek 3: Minimální kostra grafu na deseti vrcholech.

se úloze (i jejímu řešení) říká *minimální kostra* grafu a v budoucnu ji, stejně jako předchozí dvě úlohy, potkáme.

2 | Úvodní pojmy

Žádná matematická disciplína se neobejde bez pochopení základů logiky a teorie množin. Pro jistotu zde nejnutnější části připomeneme, ale tyto krátké úryvky nezamýšlejí naučit, leč osvěžit.

2.1 Logické spojky a kvantifikátory

Definice 2.1.1 (Výrok)**.** Výrokem nazveme jakoukoli větu, o které lze rozhodnout, zda je pravdivá, či nikoliv.

Příklad. Věty „Je mi zle.“ a „Sumec je drůbež.“ jsou výroky, zatímco „Tvoje máma.“ a „Cos' dostala z matiky?“ nikoliževěk.

Je též dlužno mít na paměti, že naše znalost pravdivosti věty nemění nic na tom, jestli daná věta je, nebo není výrokem. Třeba „Do pěti století kolonizujeme celou Sluneční soustavu.“ je zcela jistě výrok.

Další text vyžaduje znalost operátorů $\neg, \wedge, \vee, \Rightarrow$ a $\Leftrightarrow$. Je-li x výrok „Prší.“ a y výrok „Vezmu si deštník.“, pak

- výrok $\neg x$ znamená „**Ne**prší.“,

- výrok $x \wedge y$ znamená „Prší **a** vezmu si deštník.“,
- výrok $x \vee y$ znamená „Prší **nebo** si vezmu deštník.“,
- výrok $x \Rightarrow y$ znamená „**Když** prší, **tak** si vezmu deštník.“ a
- výrok $x \Leftrightarrow y$ znamená „Prší, **právě tehdy když** si vezmu deštník.“

Výstraha.

- Logická spojka $\vee$ **není výlučná**. Tedy $x \vee y$ platí v situaci, kdy
  - platí pouze x,
  - platí pouze y,
  - platí x i y.
- Výrok $x \Rightarrow y$ je vždy **pravdivý**, pokud x je **lživý**. Jinak řečeno, $x \Rightarrow y$ platí za situace, kdy
  - platí x i y,
  - neplatí x a platí y,
  - neplatí x a neplatí y.

Jako znalost logických spojek je kritická i znalost kvantifikátorů $\forall$ a $\exists$, které se čtou „pro všechny“ a „existuje“, resp.

Pokud je $p(x)$ výrok závislý na proměnné x (třeba „x je sudé.“), pak výrok

- $\forall x \in \mathbb{N} : p(x)$ zní „Všechna přirozená čísla jsou sudá.“ a
- $\exists x \in \mathbb{N} : p(x)$ zní „Existuje sudé přirozené číslo.“

Budeme rovněž užívat kvantifikátory $\exists!$ a $\nexists$, které znamenají „existuje přesně jeden“ a „neexistuje“.

Podáno intutivně: chci-li tvrdit, že $\forall x \in \mathbb{N} : p(x)$, musím dokázat, že ať mi nepřítel dá **jakékoliv** přirozené číslo x, tak $p(x)$ platí. Naopak, dokázat $\exists x \in \mathbb{N} : p(x)$ je obvykle zásadně jednodušší, neboť musím pouze najít **jedno** přirozené číslo x, pro které $p(x)$ platí.

2.2 Množiny

Požaduji znalost značek $\in, \cap, \cup, \setminus, \times$ a $\subseteq$. Pro připomenutí, jsou-li A, B dvě množiny, pak

- výrok $x \in A$ říká, že „x je prvkem A." nebo „ x patří do A.";
- $A \cap B$ je **průnik** A s B, čili množina obsahující prvky, které patří jak do A, tak do B;
- $A \cup B$ je **sjednocení** A s B, čili množina obsahující prvky, které patří do A nebo do B;
- $A \setminus B$ je **rozdíl** A s B, čili množina obsahující prvky, které patří do A a nepatří do B;
- $A \times B$ je **součin** A s B, čili množina **uspořádaných** dvojic (a, b), kde $a \in A$ a $b \in B$. Uspořádaná dvojice zde znamená, že $(a, b) \neq (b, a)$, tedy záleží na tom, který prvek je první a který druhý;
- výrok $A \subseteq B$ říká, že A je podmnožinou B, tedy, že každý prvek A je rovněž prvkem B.

Pro mnohonásobné a nekonečné verze budeme používat stejné symboly (s výjimkou součinu). Tedy, mám-li množiny $A_1, \ldots, A_n$, pak

- $\bigcap_{i=1}^{n} A_i$ je jejich průnik,
- $\bigcup_{i=1}^{n} A_i$ je jejich sjednocení a
- $\prod_{i=1}^{n} A_i$ je jejich součin.

Když jsou počáteční a koncový index známy z kontextu, budeme je vynechávat a psát pouze třeba $\bigcup A_i$. Součin množiny se sebou samou budeme často zkracovat mocninným zápisem, třeba $A \times A \times A = A^3$.

Příklad. Je-li $A = \{1, 3, 4\}$ a $B = \{2, 4, 5\}$, pak

- $A \cap B = \{4\}$,
- $A \cup B = \{1, 2, 3, 4, 5\}$,
- $A \setminus B = \{1, 3\}$ a

- $A \times B = \{(1,2),(1,4),(1,5),(3,2),(3,4),(3,5),(4,2),(4,4),(4,5)\}$.

Definice 2.2.1. Je-li A množina, pak

- $\#A$ značí **počet prvků** A neboli **velikost** A,
- 2^A značí **množinu všech podmnožin** A, čili

$$2^A := \{B \mid B \subseteq A\}.$$

Pro nekonečné množiny píšeme $\#A = \infty$.

Výstraha. Pojem velikosti takto zavedený není korektně definovaný. Není totiž jasné, co by měl „počet“ prvků znamenat. Pojem *bijekce* z podsekce o zobrazeních tento problém vyřeší.

Tvrzení 2.2.1 (Vlastnosti velikosti množiny)**.**

(1) $\#A \times B = \#A\#B$.

(2) $\#2^A = 2^{\#A}$.

Důkaz.

(1) Pro každý prvek $a \in A$ je v $A \times B$ právě $\#B$ dvojic (a,b), kde $b \in B$. Jelikož prvků $a \in A$ je z definice $\#A$ a každému odpovídá $\#B$ dvojic (a,b), je celkový počet uspořádaných dvojic v $A \times B$ právě $\#A\#B$.

(2) Pro nekonečné množiny tvrzení platí zřejmě. Předpokládejme, že A je konečná.

Očíslujeme si podmnožiny A binárními čísly délky $\#A$. Každá podmnožina A vznikne totiž tak, že procházíme postupně všechny prvky A a u každého se rozhodujeme, zda ho do ní zařadíme či nikoliv. Kladnému rozhodnutí bude odpovídat cifra 1 a zápornému 0. Má-li A řekněme 5 prvků, pak podmnožina očíslovaná číslem 00110 je podmnožina, která obsahuje pouze 3. a 4. prvek z A (při libovolném, **ale fixním**, očíslování samotné množiny A).

Odtud plyne, že A má tolik podmnožin, kolik je různých binárních čísel délky $\#A$. Těch je však $2^{\#A}$, jak jsme chtěli. □

2.3 Relace

Pojem *relace* zobecňuje věci jako zobrazení (se kterým jste se setkali, ale říkali jste mu bůhvíproč funkce) nebo uspořádání (které taky znáte, jen vám bůhvíproč neprozradili, oč jde).

Základní myšlenkou je to, že i relace – vztahy mezi objekty se dají pomocí množin (a jejich součinu) úspěšně definovat. Celá matematika, kterou jste dosud poznali, je založená na *teorii množin*, jinak řečeno, **všechno** je množina.

Definice 2.3.1 (Relace)**.** Jsou-li A, B množiny, pak **relací** mezi A a B nazveme *libovolnou* podmnožinu $A \times B$. Je-li $A = B$, pak R nazýváme relací na A.

Pojem relace v matematice je založen na konceptu, že vztah mezi množinami je dokonale popsán výpisem všech dvojic prvků, které v tom vztahu jsou. To se trochu liší od běžného chápání slova „vztah“. Asi byste nebyli úplně spokojení, kdybychom vám tvrdili, že vztah manželský na množině všech lidí je to samé, co výpis všech manželských párů. Z toho důvodu bude asi lepší se držet latinské verse, „relace“.

Protože nejstarší typy relací, mezi nimi třebas $<$ nebo $=$, lidé používali ještě před vznikem samotné teorie množin, značení je zde trochu matoucí. Fakt, že dvojice $(x, y) \in A \times B$ je v relaci R, nezapisujeme (jak by se čekalo) $(x, y) \in R$, ale spíš xRy. Podobně jako nepíšeme $(x, y) \in <$, ale $x < y$.

Jako spoustu věcí v matematice, relace je dobré si umět vizualizovat. Ukážeme si teď tři standardní způsoby, jak si lidé relace kreslí.

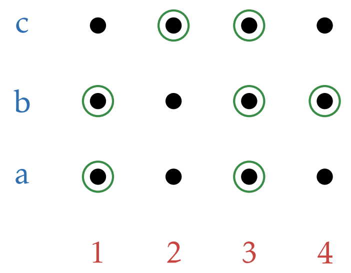
2.3.1 Kreslení relací

Po celou podsekci budeme předpokládat, že máme množiny $A = \{1, 2, 3, 4\}$ a množinu $B = \{a, b, c\}$.

Jedním ze způsobů, jak se dají kreslit relace, je *mříž*. Uvážíme relaci

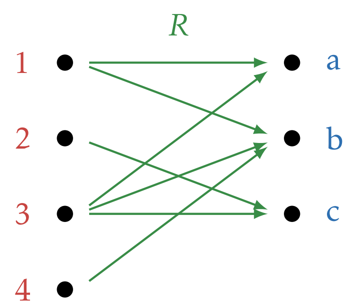
$$R = \{(1,a),(1,b),(2,c),(3,a),(3,b),(3,c),(4,b)\}$$

mezi A a B. Vizualizaci součinu $A \times B$ a relace R pomocí mříže vidíte na obrázku 4.



Obrázek 4: Kreslení relace $R \subseteq A \times B$ pomocí mříže.

Ještě jeden užitečný způsob kreslení, který funguje pro obecné relace, je kreslení pomocí šipek. V zásadě si člověk zobrazí obě množiny jako sloupce bodů a mezi příslušnými body kreslí šipky. Například jako na obrázku 5.



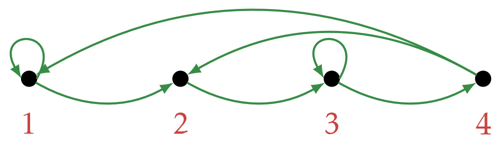
Obrázek 5: Kreslení relace $R \subseteq A \times B$ pomocí šipek.

Tenhle způsob se může zdát méně přehledný než mříž, ale má svoje nesporné využití, především v oblasti *skládání* relací, kterým se budeme zabývat za chvíli.

Ještě před tím si ale ukážeme způsob, jak přehledně kreslit relace na nějaké množině. Řekněme, že tentokrát je třeba

$$R := \{(1,1),(1,2),(2,3),(3,4),(3,3),(4,1),(4,2)\}$$

relace na množině A. Množinu A si nakreslíme jako body v rovině a relaci R jako šipky a smyčky. Vizte obrázek 6.



Obrázek 6: Kreslení relace R na A pomocí šipek a smyček.

2.3.2 Skládání relací

V této podsekci si řekneme, co znamená, že dvě (nebo více) relace složíme dohromady. Tato operace se dá vnímat jako jakési „zobecnění“ skládání zobrazení/funkcí. Jak si ale ukážeme, zobrazení jsou speciálním typem relací, takže tahle představa není úplně vhodná.

Pro jednoduchost se budeme soustředit na relace na nějaké množině A. Tohle ovšem není nutné; mám-li relaci $R \subseteq A \times B$ a relaci $S \subseteq B \times C$, vždy je mohu složit a dostat relaci mezi A a C.

Skládání relací není nijak divoká věc a vztahy (například mezi lidmi) v životě běžně skládáme, ale málokdy se na to asi díváme tímto způsobem. Například, řekněme, že Adéla má přítelkyni Simona a Simona má přítelkyni Terezu. Když složíme relace „býti přítelkyně Adély“ a „býti přítelkyně Simony“ dostaneme relaci, ve které je Tereza přítelkyně Adély. Na druhý příklad, třeba samotné přísloví „Nepřítel mého nepřítele je můj přítel.“, se dá vyložit jako skládání relací.

Teď formálně.

Definice 2.3.2 (Složení relací)**.** Mějme množinu A a relace $R, S \subseteq A \times A = A^2$. Složením relací R a S nazveme množinu

$$\{(x, z) \in A^2 \mid \exists y \in A : xRy \wedge yRz\}$$

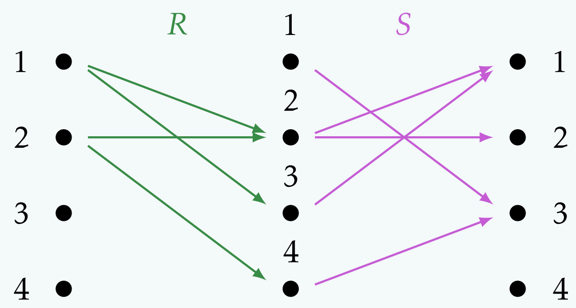
a značíme ji $R \circ S$.

Řečeno asi možná třeba trošku lidštěji, když pro dané $x, z \in A$ najdu takový prvek $y \in A$, že dvojice (x, y) je v relaci R a dvojice (y, z) je v relaci S, pak (x, z) je v relaci $R \circ S$. Vlastně (x, y) a (y, z) slepím dohromady skrze y.

Příklad. Řekněme, že je $A = \{1, 2, 3, 4\}$ a máme relace

$$R := \{(1,2),(1,3),(2,2),(2,4)\},$$
$$S := \{(1,3),(2,1),(2,2),(3,1),(4,3)\}$$

na A. V podsekci o kreslení relací jsme zmínili, že šipky jsou velmi užitečné při skládání. Teď uvidíte proč. Když si obě relace nakreslíme přímo vedle sebe, dostaneme obrázek 7.



Obrázek 7: Složení relací R a S.

V roli x z Definice 2.3.2 je zde první sloupec, v roli y druhý a v roli z třetí. Čili, prvek (x, z) bude v relaci $R \circ S$ jenom tehdy, když najdu v prostředním sloupci prvek y (aspoň jeden, ale klidně víc), přes který dokážu po šipkách dojít z x do z.

Z obrázku je teď už zřejmé, že

$$R \circ S = \{(1,1),(1,2),(2,1),(2,2),(2,3)\}.$$

2.4 Ekvivalence

Jedním speciálním typem relace na množině je tzv. *ekvivalence*. Důvodem pro tenhle název je fakt, že prvky, které jsou v relaci ekvivalence, jde za jisté interpretace považovat za „stejné". Asi nejobyčejnější příklad užití ekvivalence je při definici množiny racionálních čísel, $\mathbb{Q}$, jak si brzy ukážeme. Nejprve ale definice ekvivalence.

Definice 2.4.1 (Ekvivalence)**.** Relace $R \subseteq A^2$ je

- **reflexivní**, když je každý prvek v relaci sám se sebou, tj.
$$xRx \quad \forall x \in A;$$
- **symetrická**, když ke každé dvojici obsahuje i opačně uspořádanou, tj.
$$xRy \Rightarrow yRx \quad \forall x, y \in A;$$
- **transitivní**, když ke každým dvěma dvojicím, které jdou „slepit přes prostředníka“ (vizte definici skládání) obsahuje i tu slepenou dvojici. Formálně,
$$xRy \wedge yRz \Rightarrow xRz \quad \forall x, y, z \in A.$$

Relace, která je *reflexivní*, *symetrická* a *transitivní* se nazývá **ekvivalence**.

Vlastnosti reflexivity, symetrie a transitivity nejsou principiálně v žádném vztahu. Existují relace, které jsou jen reflexivní, ale nejsou ani symetrické ani transitivní apod. Jeden příklad za všechny.

Příklad. Položme $A := \{1, 2, 3, 4\}$. Relace

- $\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,3)\}$ je reflexivní, ale nikoli symetrická nebo transitivní;
- $\{(1,1),(2,2),(1,2),(2,1),(2,3),(3,2)\}$ je symetrická, ale není reflexivní ani transitivní;
- $\{(1,2),(2,3),(1,3),(3,4),(1,4),(2,4)\}$ je transitivní, ale není reflexivní ani symetrická.

Ekvivalence je velmi přirozený způsob, jak ztotožnit prvky, které bychom, často z technických důvodů, nechtěli považovat za různé. Vrátím-li se k příkladu zlomků, asi bychom nechtěli vidět třeba 1/5 a 2/10 jako dva různé zlomky. Zlomek 1/5 v tomto smyslu je vlastně množina všech zlomků, které jsou představují stejnou hodnotu. Tuto intuici zobecňuje pojem třídy ekvivalence.

Definice 2.4.2 (Třída ekvivalence)**.** Mějme ekvivalence $R \subseteq A^2$ a prvek $x \in A$. **Třídou ekvivalence** prvku x **vzhledem k R** myslíme množinu

$$[x]_R := \{y \in A \mid xRy\},$$

čili množinu všech prvků, které jsou s ním v relaci R. Dolní index R v zápisu $[x]_R$ budeme často vynechávat a psát jen $[x]$. Uvědomme si, že nezáleží na tom, jestli napíšu xRy nebo yRx v definici výše, protože R je symetrická.

Příklad (Racionální čísla)**.** Symbolem $\mathbb{N}$ značím množinu přirozených čísel $\{1, 2, 3, \ldots\}$ a symbolem $\mathbb{Z}$ množinu celých čísel, tj. množinu přirozených čísel, čísel k nim opačným a 0.

Racionální čísla se dají definovat jako všechny možné podíly celého čísla přirozeným. Když si zlomek a/b, kde $a \in \mathbb{Z}$ a $b \in \mathbb{N}$ představím jako uspořádanou dvojici (a, b), tj. (čitatel, jmenovatel), pak množina

$$A := \{(a, b) \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$$

je množina všech zlomků.

Ujasníme si, kdy dva zlomky považujeme za stejné. Snadno úpravou člověk dostane, že

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc,$$

což nám dává návod, jak definovat ekvivalenci na množině všech zlomků, A. Relaci $R \subseteq A^2$ definujeme tím způsobem, že $(a, b)R(c, d)$ právě tehdy, když $ad = bc$. Správně bychom měli dokázat, že to je opravdu ekvivalence, ale tím se nehodláme zdržovat.

Množina racionálních čísel, na kterou jste zvyklí, se pak nejelegantněji definuje jako množina tříd ekvivalence prvků z A vzhledem k R. Konkrétně,

$$\mathbb{Q} := \{[(a, b)]_R \mid a \in \mathbb{Z}, b \in \mathbb{N}\}.$$

Třídy ekvivalence jistým způsobem „parcelují“ množinu A na disjunktní (mající prázdný průnik) množiny. To je obsahem následujícího tvrzení, jehož důkaz je cvičení.

Tvrzení 2.4.1 (Vlastnosti tříd ekvivalence)**.** Nechť A je libovolná množina a R je ekvivalence na A. Pak

(1) $[x] \neq \emptyset$ pro všechna $x \in A$,

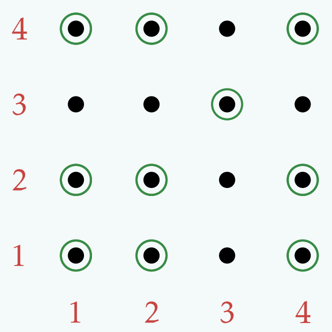
(2) Buď $[x] = [y]$, nebo $[x] \cap [y] = \emptyset$ pro všechna $x, y \in A$.

Důkaz. Cvičení. □

Příklad. Řekněme, že A je naše oblíbená množina $\{1, 2, 3, 4\}$. Snadno ověříme, že

$$R := \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(3,3),(4,1),(4,2),(4,4)\}$$

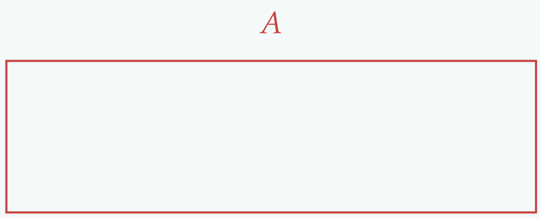
je ekvivalence na A. Její mříž vidíte na obrázku 8.



Obrázek 8: Mříž ekvivalence R na množině A.

Obecně, mříž každé ekvivalence má zaplněnou diagonálu z levého dolního rohu do pravého horního (kvůli reflexivitě) a je symetrická podle této diagonály (kvůli symetrii). Jak na první pohled poznat transitivitu nevím.

Všimněme si, že $1R2$ a $1R4$, takže $2 \in [1]$ a $4 \in [1]$. Podle tvrzení nahoře je $[1] = [2] = [4]$, protože tyto třídy ekvivalence nejsou disjunktní. Naopak, třída $[3]$ **je** disjunktní s každou z nich. Můžeme proto rozdělit množinu A na třídy ekvivalence třeba jako $A = [1] \cup [3]$. Náhled na obrázku



Obrázek 9: Množina A rozdělená na třídy ekvivalence R.