Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 1999/2000
Michal Marvan

0. Množiny, relace a zobrazení

Petitem (malým písmem) vyznačujeme části textu, které obsahují doplňující a rozšiřující výklad. Je možné (a někdy nutné) je při prvním čtení vynechat. Toto pravidlo neplatí pro příklady, cvičení a následující odstavec.

Matematika je deduktivní věda a algebra je její součást. Všechny pojmy jsou vymezeny *definicí*. Kriteriem pravdivosti matematického tvrzení je *důkaz*. To je potřeba brát smrtelně vážně.

Předpokládáme, že pojem *množina* je dostatečně znám ze střední školy. Tamtéž byly vyloženy základy výrokového počtu (negace $\neg$, konjunkce $\wedge$, disjunkce $\vee$, implikace $\Rightarrow$, ekvivalence $\Leftrightarrow$ výroků; obecný kvantifikátor $\forall$, existenční kvantifikátor $\exists$; důkaz přímý a důkaz sporem).

Ne všechny pojmy lze definovat a ne všechna tvrzení lze dokázat. Nejvíce takových mezer zeje právě v základech matematiky – evidentně nelze definovat definici, evidentně nelze dokázat správnost všech pravidel, podle kterých dokazujeme.

Ukázalo se, že nelze jednoduše definovat ani pojem „množina“ – naivní pokusy vedou ke sporům. Přesto v dnešní době převládá snaha zakotvit základy matematiky právě v teorii množin. Korektní zavedení pojmu množina představuje problém řešený v tzv. axiomatické teorii množin. Podrobný výklad je předmětem samostatné přednášky.

Dále budeme předpokládat, že jsou známy i pojmy přirozené, celé, racionální, reálné a komplexní číslo, základní aritmetické operace s nimi (včetně dělení přirozených čísel se zbytkem) a uspořádání reálných čísel podle velikosti.

1. Množiny

Buď M množina. Zápis $a \in M$ označuje, že a je prvek množiny M. Říkáme též, že a patří do množiny M. Zápis $a \notin M$ označuje, že a není prvek množiny M (nepatří do množiny M). Pro libovolné a nastává právě jedna z možností $a \in M$ nebo $a \notin M$.

Množiny A, B jsou si rovny, $A = B$, mají-li tytéž prvky, tj. platí-li ekvivalence $x \in A \Leftrightarrow x \in B$.

Intuitivní představa spojená s pojmem množina je stejná jako u slov „souhrn“ či „soubor.“ Mimo tento rámec jsou souhrny, které určují samy sebe (příklad: „množina všech množin“) – odkazy na sebe sama (logické kruhy), jak známo, mohou vést k logickým sporům (viz Russelův paradox níže).

Existuje právě jedna množina, která neobsahuje žádný prvek. Nazývá se *prázdná množina* a označuje se $\emptyset$. Konečnou množinu (množinu s konečným počtem prvků) lze zadat výčtem prvků, například $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$. Některé nekonečné množiny lze zadat neúplným výčtem, například $\mathbf{N} = \{1, 2, 3, 4, 5, \ldots\}$ je množina všech přirozených čísel.

Cvičení. Rozhodněte, zda platí $\{\clubsuit\} = \{\clubsuit, \clubsuit\}$.

Řekneme, že množina B je podmnožinou množiny A, jestliže každý prvek z množiny B náleží i množině A, tj. když platí implikace $x \in B \Rightarrow x \in A$. Zapisujeme $B \subseteq A$.

Zápis $B \subset A$ znamená, že $B \subseteq A$ a zároveň $B \neq A$. Například, $\{\heartsuit, \clubsuit\} \subset \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$.

Cvičení. Rozhodněte, zda platí a) $\{\clubsuit\} \in \{\{\clubsuit\}\}$; b) $\{\clubsuit\} \subset \{\{\clubsuit\}\}$; c) $\emptyset \in \{\emptyset\}$; d) $\emptyset \subset \{\emptyset\}$.

Příklad. Dokážeme, že pro libovolné dvě množiny A, B jsou následující výroky ekvivalentní: (1) $A = B$; (2) $A \subseteq B \wedge B \subseteq A$.

Víme, že výrok $\alpha \Leftrightarrow \beta$ je ekvivalentní s výrokem $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$. Dosadíme-li za α výrok „$x \in A$" a za β výrok „$x \in B$", dostáváme, že výrok $x \in A \Leftrightarrow x \in B$ je ekvivalentní s výrokem $(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)$, což bylo třeba dokázat.

Buď A libovolná množina. Buď ψ nějaká vlastnost taková, že o každém prvku $a \in A$ lze rozhodnout, zda vlastnost ψ má, což zapisujeme $\psi(a)$, či nemá, což zapisujeme $\neg\psi(a)$. Podmnožina množiny A tvořená všemi prvky $a \in A$ s vlastností ψ se označuje

$$\{ a \in A \mid \psi(a) \}.$$

Například, je-li $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$, pak $\{ a \in A \mid a \text{ je černé barvy} \} = \{\spadesuit, \clubsuit\}$.

Zápis $\{ a \mid \psi(a) \}$ (chybí „$\in A$", kde A je množina) je v principu také možný, ale nemusí označovat množinu.

Příklad (Russelův paradox): Nechť $N = \{ x \mid x \text{ je množina a } x \notin x \}$ (souhrn všech množin, které nejsou samy svým prvkem). Připustíme-li, že N je množina, pak mohou nastat dvě možnosti: Buď $N \notin N$, ale pak $N \in N$ podle definice souboru N, spor, anebo $N \in N$, ale pak $N \notin N$ podle definice souboru N, opět spor. Tudíž, N není množina.

Buď n přirozené číslo, buďte $A_1, \dots, A_n$ nějaké množiny. Sjednocení množin $A_1, \dots, A_n$ označíme $A_1 \cup \dots \cup A_n$; je to množina tvořená právě těmi prvky a, které leží v alespoň jedné z množin $A_1, \dots, A_n$. Například, $\{\heartsuit\} \cup \{\heartsuit, \spadesuit\} \cup \{\spadesuit, \clubsuit\} = \{\heartsuit, \spadesuit, \clubsuit\}$. Platí ekvivalence $a \in A \cup B \Leftrightarrow a \in A \vee a \in B$.

Průnik množin $A_1, \dots, A_n$ označíme $A_1 \cap \dots \cap A_n$; je to množina tvořená právě těmi prvky a, které leží v každé z množin $A_1, \dots, A_n$. Například, $\{\heartsuit, \spadesuit, \clubsuit\} \cap \{\heartsuit, \diamondsuit, \clubsuit\} = \{\heartsuit, \clubsuit\}$. Zřejmě $A \cap B = \{ x \in A \mid x \in B \} = \{ x \in B \mid x \in A \}$. Platí $a \in A \cap B \Leftrightarrow a \in A \wedge a \in B$.

Nakonec, rozdíl množin A, B je $A \setminus B = \{ a \in A \mid a \notin B \}$. Například: $\{\heartsuit, \spadesuit, \clubsuit\} \setminus \{\heartsuit, \diamondsuit\} = \{\spadesuit, \clubsuit\}$.

Sjednocení, průnik i rozdíl množin jsou vždy opět množiny. Platí rovnosti

$$\begin{aligned}
&A \cup B = B \cup A, && A \cap B = B \cap A,\\
&A \cup (B \cup C) = (A \cup B) \cup C && A \cap (B \cap C) = (A \cap B) \cap C\\
&\qquad\qquad\quad = A \cup B \cup C, && \qquad\qquad\quad = A \cap B \cap C,\\
&A \cap (B \cup C) = (A \cap B) \cup (A \cap C), && A \cup (B \cap C) = (A \cup B) \cap (A \cup C),\\
&A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C), && A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C).
\end{aligned}$$

Cvičení. Dokažte předchozí rovnosti dosazením do vhodných logických ekvivalencí.

2. Kartézský součin

Řekneme, že je dána *uspořádaná dvojice* (a, b) prvků množin A, B, jsou-li dány prvky $a \in A$ a $b \in B$. Uspořádané dvojice (a, b) a (a', b') jsou si rovny, $(a, b) = (a', b')$, právě když platí $a = a'$ a zároveň $b = b'$. Prvek a resp. b se nazývá první resp. druhý prvek dvojice (a, b). Uspořádaná dvojice (a, b) je určena svými dvěma prvky a jejich pořadím (na rozdíl od množiny $\{a, b\}$).

Shora uvedené vymezení pojmu uspořádaná dvojice lze považovat za jeho definici – umožnuje rozpoznat uspořádanou dvojici a rozhodnout, kdy jsou si dvě uspořádané dvojice rovny. Chceme-li však veškerou matematiku vybudovat z množin, můžeme uspořádanou dvojici (a, b) *definovat* předpisem $(a, b) = \{\{a\}, \{a, b\}\}$. Skutečně, $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$ právě tehdy, když $a = b \wedge a' = b'$ (dokažte).

Množinu všech uspořádaných dvojic (a, b) prvků množin A, B nazýváme *kartézský součin* množin A, B a označujeme $A \times B$.

Příklad. $\{\heartsuit, \diamondsuit\} \times \{\spadesuit, \clubsuit\} = \{(\heartsuit, \spadesuit),\ (\heartsuit, \clubsuit),\ (\diamondsuit, \spadesuit),\ (\diamondsuit, \clubsuit)\}$.

Příklad. Buďte A, B libovolné množiny, buďte $A' \subseteq A$, $B' \subseteq B$ jejich podmnožiny. Pak platí
$A' \times B' = (A \times B') \cap (A' \times B)$.
Proveďme důkaz tohoto tvrzení. Jde o rovnost množin; dokažme inkluze „$\subseteq$“ a „$\supseteq$“ zvlášť.

„$\subseteq$“: Buď $(a, b) \in A' \times B'$ libovolný prvek. To znamená, že $a \in A'$ a $b \in B'$ jsou dva libovolné prvky. Protože $A' \subseteq A$, je také $a \in A$, načež $(a, b) \in A \times B'$. Protože $B' \subseteq B$, máme podobně $b \in B$, načež $(a, b) \in A' \times B$. Tudíž, $(a, b) \in (A \times B') \cap (A' \times B)$. Příslušná inkluze je dokázána.

„$\supseteq$“: Buď (a, b) libovolný prvek průniku $(A \times B') \cap (A' \times B)$. Pak speciálně $(a, b) \in A \times B'$, načež $a \in A, b \in B'$. Podobně $(a, b) \in A' \times B$, načež $a \in A', b \in B$. Z $a \in A', b \in B'$ vyplývá $(a, b) \in A' \times B'$. Tím je dokázána i opačná inkluze.

Cvičení. Buďte A, B libovolné množiny, buďte $A', A'' \subseteq A$ podmnožiny. Dokažte, že platí
1. $(A' \cap A'') \times B = (A' \times B) \cap (A'' \times B)$;
2. $(A' \cup A'') \times B = (A' \times B) \cup (A'' \times B)$.

3. Relace

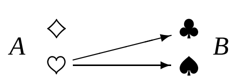
Definice. Buďte A, B libovolné množiny. *Relace* mezi množinami A, B je libovolná podmnožina kartézského součinu $A \times B$. Je-li $\rho \subseteq A \times B$ relace a jsou-li $a \in A$, $b \in B$ prvky takové, že $(a, b) \in \rho$, pak říkáme, že prvek a je v relaci ρ s prvkem b a stručně zapisujeme $a\rho b$.

Relace *na* množině A je zvláštní případ, kdy $A = B$.

Zadat relaci (neboli korespondenci) mezi množinami A, B je tedy totéž, co vybrat určitou množinu dvojic (a, b), kde $a \in A$ a $b \in B$.

Relace mezi množinami, zejména konečnými, můžeme znázorňovat grafem. Prvky množin A, B znázorníme body v rovině, body a a b znázorňující prvky jednotlivých množin spojíme šipkou tehdy a jen tehdy, jsou-li v relaci.

Příklady. 1. Nechť $A = \{\heartsuit, \diamondsuit\}$, $B = \{\spadesuit, \clubsuit\}$. Podmnožina $\rho = \{(\heartsuit, \spadesuit),\ (\heartsuit, \clubsuit)\}$ je relace mezi množinami A, B. Platí $\heartsuit\rho\spadesuit$ a $\heartsuit\rho\clubsuit$. Neplatí například $\diamondsuit\rho\clubsuit$. Graf:



2. Prázdná podmnožina $\emptyset \subseteq A \times B$ je relace mezi množinami A, B. Žádné dva prvky $a \in A$, $b \in B$ nejsou v této relaci.

3. Podmnožina $A \times B \subseteq A \times B$ je relace mezi množinami A, B. Každé dva prvky $a \in A$, $b \in B$ jsou v této relaci.

4. *Identická relace* na množině A je podmnožina $\mathrm{id}_A = \{(a, a) \mid a \in A\}$. Prvky $a, b \in A$ jsou v této relaci právě tehdy, když $a = b$.

5. Relace ostrého uspořádání podle velikosti „$<$“ na množině $\mathbf{R}$ reálných čísel.
6. Relace neostrého uspořádání podle velikosti „$\leq$“ na množině $\mathbf{R}$ reálných čísel.
7. Relace „$\lhd$“ sousedství zleva mezi celými čísly – řekneme, že číslo a sousedí zleva s číslem b, jestliže $b = a + 1$.

Cvičení. Nakreslete grafy relací 2. až 7.

Definice. Buď ρ relace mezi množinami A, B. Relace ρ^{-1} mezi množinami B, A definovaná předpisem

$$\rho^{-1} = \{ (b, a) \mid a\rho b \}$$

se nazývá *opačná relace* k relaci ρ.

Zřejmě v grafu relace ρ^{-1} vede šipka $b \to a$ právě tehdy, když v grafu relace ρ vede šipka $a \to b$. (Graf opačné relace vznikne obrácením všech šipek grafu původní relace.)

Příklady. 1. Relace ρ^{-1} mezi množinami $B = \{\spadesuit, \clubsuit\}$ a $A = \{\heartsuit, \diamondsuit\}$, opačná k relaci zavedené v předchozím příkladu č. 1, je podmnožina $\rho^{-1} = \{(\spadesuit, \heartsuit),\ (\clubsuit, \heartsuit)\}$. Graf:

$$\begin{tikzcd}
 & \diamondsuit & \clubsuit \arrow[dl] & \\
A & \heartsuit & \spadesuit \arrow[l] & B
\end{tikzcd}$$

2. Relace opačná k relaci „$<$“ uspořádání reálných čísel podle velikosti je relace „$>$“ opačného uspořádání podle velikosti.
3. Buď $H = \{ h_1, h_2 \}$ nějaká množina hochů, $D = \{ d_1, d_2 \}$ nějaká množina dívek. Někteří hoši chodí s dívkou; fakt, že hoch $h \in H$ chodí s dívkou $d \in D$ zapíšeme $h\chi d$. Vzniká tak relace $\chi \subseteq H \times D$. Relace χ^{-1} popisuje, která dívka chodí se kterým hochem.

Definice. Buď ρ relace mezi množinami A, B, buď σ relace mezi množinami B, C. Relace $\sigma \circ \rho$ (čti „σ po ρ“) mezi množinami A, C definovaná předpisem

$$\sigma \circ \rho = \{ (a, c) \mid \exists_{b \in B}(a\rho b \wedge b\sigma c) \}$$

se nazývá *složení relací* ρ a σ.

V grafu relace $\sigma \circ \rho$ vede šipka mezi prvky $a \in A$ a $c \in C$ právě tehdy, když v grafu relace ρ vede nějaká šipka $a \to b$ na niž v grafu relace σ navazuje šipka $b \to c$.

Příklady. 1. Pokračujme v předchozím příkladu č. 3. Některé dívky navíc chodí se svým psem; množinu všech takových psů označme P. Fakt, že dívka $d \in D$ chodí se psem $p \in P$ zapíšeme $d\pi p$. Vzniká tak relace $\pi \subseteq D \times P$. Pak $\pi \circ \chi$ je relace, která vyjadřuje, který hoch chodí se kterým psem. Vskutku, hoch h chodí se psem p právě tehdy, když existuje dívka d, se kterou chodí jak hoch h, tak pes p.

Například, nechť $H = \{ h_1, h_2 \}$, $D = \{ d_1, d_2 \}$, $P = \{ p_1, p_2 \}$. Nechť hoch h_2 chodí s dívkou d_1, hoch h_1 nechodí s nikým a dívka d_i chodí se psem p_i pro $i = 1, 2$. Máme

$$\begin{tikzcd}
 & h_1 \arrow[drr] & D & d_1 \arrow[r] & p_1 & \\
H & h_2 & \chi & d_2 \arrow[r, "\pi"'] & p_2 & P
\end{tikzcd}$$

a tedy $\pi \circ \chi = \{(h_1, p_2)\}$.
2. Uvažujme o relaci „$\lhd$“ sousedství zleva mezi celými čísly z příkladu č. 7. Pak $a(\lhd \circ \lhd)c$ právě tehdy, když $c = a + 2$.

Tvrzení. *Buď ρ relace mezi množinami A, B. Pak platí*

1°. $\rho \circ \mathrm{id}_A = \rho$;

1′. $\mathrm{id}_B \circ \rho = \rho$.

Buď navíc σ relace mezi množinami B, C. Pak platí

2. $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

Důkaz. 1° a 1′ jsou snadná; dokážeme tvrzení 2. Jde o rovnost množin, dokazujme každou inkluzi zvlášť.

„$\subseteq$“: Nechť $(c, a) \in (\sigma \circ \rho)^{-1}$. Pak $(a, c) \in \sigma \circ \rho$, načež existuje prvek $b \in B$ takový, že $a\rho b$ a $b\sigma c$. Potom ale $c\sigma^{-1}b$ a $b\rho^{-1}a$, takže $(c, a) \in \rho^{-1} \circ \sigma^{-1}$.

„$\supseteq$“: Cvičení (stačí postupovat obráceně).

Cvičení. 1. Ukažte, že $(\rho^{-1})^{-1} = \rho$.

2. Nechť $\rho \subseteq \rho'$, $\sigma \subseteq \sigma'$. Dokažte, že pak $\rho \circ \sigma \subseteq \rho' \circ \sigma'$.

4. Relace ekvivalence

Definice. Buď ρ relace na množině A. Relace ρ se nazývá
– *reflexivní*, jestliže pro každé $a \in A$ platí $a\rho a$;
– *symetrická*, jestliže platí implikace $a\rho b \Rightarrow b\rho a$;
– *tranzitivní*, jestliže platí implikace $(a\rho b \wedge b\rho c) \Rightarrow a\rho c$.

Příklady. 1. Identická relace id_A je reflexivní, symetrická i tranzitivní.

2. Relace „$\leq$“ neostrého uspořádání reálných čísel je tranzitivní a reflexivní.

3. Relace „$<$“ ostrého uspořádání reálných čísel je pouze tranzitivní.

Cvičení. Najděte chybu v následujícím „důkazu“ nepravdivého tvrzení, že každá symetrická a tranzitivní relace ρ je reflexivní: „Je-li $a\rho b$, pak ze symetrie plyne $b\rho a$, načež z tranzitivity plyne $a\rho a$.“

Cvičení. Graf relace na množině můžeme kreslit tak, že místo dvou kopií množiny A zobrazíme jen jednu a šipky vedeme mezi jejími prvky. Jak se pozná graf reflexivní resp. symetrické resp. tranzitivní relace?

Cvičení. Buď ρ relace na množině A.

1. Ukažte, že ρ je reflexivní právě tehdy, když platí $\mathrm{id}_A \subseteq \rho$.
2. Ukažte, že ρ je symetrická právě tehdy, když platí $\rho = \rho^{-1}$.
3. Ukažte, že ρ je tranzitivní právě tehdy, když platí $\rho \circ \rho \subseteq \rho$.

Definice. Reflexivní, symetrická a tranzitivní relace se nazývá *relace ekvivalence* (nebo prostě *ekvivalence*, pokud nemůže dojít k záměně s logickou ekvivalencí).

Příklady. 1. Identická relace id_A je ekvivalence na množině A.

2. Buď V nějaká množina vajec. Zaveďme relaci ς předpisem: $v_1 \varsigma v_2$ právě tehdy, když vejce v_1 a v_2 pocházejí od stejné slepice. Pak ς je ekvivalence.

Problém k řešení. Buďte ρ, σ relace ekvivalence na množině A. Dokažte, že $\sigma \circ \rho$ je relace ekvivalence právě tehdy, když $\sigma \circ \rho = \rho \circ \sigma$.

Relace ekvivalence se hojně vyskytují v matematice i v realitě. Jsou vždy spojeny s tak zvanými rozklady.

Definice. *Rozklad* na množině A je systém neprázdných podmnožin množiny A, zvaných *třídy* rozkladu, splňující podmínku, že každý prvek $x \in A$ leží v právě jedné z tříd. Třída rozkladu obsahující prvek x se obvykle označuje $[x]$.

Příklady. 1. Nechť $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$, $U = \{\heartsuit, \diamondsuit\}$, $V = \{\spadesuit, \clubsuit\}$. Pak $\{U, V\}$ je rozklad na množině A, protože každý z prvků $\heartsuit, \spadesuit, \diamondsuit, \clubsuit$ množiny A leží v právě jedné z množin U, V:

$$\begin{array}{cc} \overbrace{}^{U} & \overbrace{}^{V} \\ \hline \multicolumn{1}{|c|}{\heartsuit} & \multicolumn{1}{c|}{\spadesuit} \\ \multicolumn{1}{|c|}{\diamondsuit} & \multicolumn{1}{c|}{\clubsuit} \\ \hline \end{array}$$

Přitom $[\heartsuit] = U$, $[\spadesuit] = V$, $[\diamondsuit] = U$, $[\clubsuit] = V$.

2. Množinu všech obcí České republiky lze rozložit na třídy, tvořené obcemi jednotlivých okresů (za předpokladu, že každá obec v České republice leží v právě jednom okrese). Pak [Opava] označuje množinu všech obcí ležících v témže okrese jako Opava. Přitom [Opava] = [Vávrovice], ale [Opava] $\neq$ [Krnov].

3. Populace kura domácího může být rozložena na dvě třídy: kohouty a slepice.

Cvičení. 1. Nalezněte všechny rozklady na množině $A = \{1, 2, 3\}$ (je jich pět).

2. Dvě množiny A, B se nazývají disjunktní, je-li $A \cap B = \emptyset$. Ukažte, že každé dvě různé třídy rozkladu jsou disjunktní.

Tvrzení. *Buď dán rozklad na množině A na třídy $[a]$, $a \in A$. Buď ρ relace na množině A zadaná předpisem*

$$x \rho y \;\Leftrightarrow\; [x] = [y],$$

tj. $x \rho y$ právě když x, y leží v jedné a téže třídě rozkladu. Pak ρ je ekvivalence na A.

Důkaz. Relace ρ je reflexivní, protože $[x] = [x]$ pro každé $x \in A$. Relace ρ je symetrická, protože rovnost $[x] = [y]$ má za následek rovnost $[y] = [x]$. Relace ρ je tranzitivní, protože rovnosti $[x] = [y]$, $[y] = [z]$ mají za následek rovnost $[x] = [z]$.

Příklady. Ve stejně číslovaných předchozích příkladech platí:

1. $\heartsuit \rho \diamondsuit$, $\spadesuit \rho \clubsuit$.
2. Obec a je ekvivalentní obci b právě tehdy, když obě leží v témže okrese.
3. Dva exempláře kura domácího jsou ekvivalentní právě tehdy, když oba jsou kohouti nebo obě jsou slepice.

Každá ekvivalence pochází z rozkladu. Příslušný rozklad není těžké sestrojit.

Tvrzení. *Buď ρ ekvivalence na množině A. Pak je systém $\{[a] \mid a \in A\}$ podmnožin, definovaných předpisem*

$$[a] = \{x \in A \mid a \rho x\}, \qquad a \in A,$$

rozklad na A.

Důkaz. Ukažme, že každý prvek $x \in A$ leží v právě jedné třídě. Především každý prvek x leží v třídě $[x]$. Skutečně, $x \in [x]$, protože $x\rho x$ (reflexivita ekvivalence).

Ještě však musíme ukázat, že každá třída, v níž leží x, je rovna třídě $[x]$. Předpokládejme, že $x \in [y]$ a dokažme, že pak $[y] = [x]$.

Nejprve inkluzi $[x] \subseteq [y]$. Buď $u \in [x]$ libovolné, pak $u\rho x$. Máme ale $x \in [y]$, takže $x\rho y$. Potom z tranzitivity relace ρ plyne, že $u\rho y$, načež $u \in [y]$. Tudíž, $[x] \subseteq [y]$.

Inkluzi $[x] \supseteq [y]$ dokažte jako cvičení.

Vidíme, že prvky x, y leží v jedné a téže třídě rozkladu právě tehdy, když $x\rho y$.

Systém množin obecně je množina, jejíž prvky jsou zase množiny. Buď I nějaká množina (nazývá se *indexová množina*), pro každé $i \in I$ buď A_i zase nějaká množina. Pak $\{A_i \mid i \in I\}$ je systém množin. Značí se též $\{A_i\}_{i\in I}$.

Symbolem $\bigcup_{i\in I} A_i$ označujeme množinu všech prvků, které leží v alespoň jedné z množin A_i. Je to opět množina a nazývá se *sjednocení* systému množin $\{A_i\}_{i\in I}$.

Symbolem $\bigcap_{i\in I} A_i$ označujeme množinu všech prvků, které leží ve všech množinách A_i. Je to opět množina a nazývá se *průnik* systému množin $\{A_i\}_{i\in I}$.

Cvičení. Systém $\{ A_i \mid i \in I \}$ podmnožin množiny A je rozklad právě tehdy, když platí podmínky

(i) Každá podmnožina A_i je neprázdná;
(ii) $A = \bigcup_{i\in I} A_i$;
(iii) mají-li dvě třídy neprázdný průnik, $A_i \cap A_j \neq \emptyset$, pak se rovnají, $A_i = A_j$.

Problém k řešení. Buď ρ ekvivalence na množině A, buď σ ekvivalence na množině B. Zaveďme relaci τ na množině $C = A \times B$ předpisem

$$(a_1, b_1)\gamma(a_2, b_2) \;\Leftrightarrow\; a_1\rho a_2 \wedge b_1\sigma b_2.$$

Ukažte, že γ je relace ekvivalence. Ukažte, že třídy ekvivalence γ jsou právě množiny $U \times V$, kde U je třída ekvivalence ρ a V je třída ekvivalence σ.

5. Zobrazení

Jiný důležitý příklad relace mezi množinami představují zobrazení. Zde pojednáme jen o těch vlastnostech zobrazení, které dále použijeme. Další spřízněné definice a tvrzení jsou uvedeny v přednášce z matematické analýzy.

Buďte A, B množiny. *Zobrazení* f z množiny A do množiny B je relace $f \subseteq A \times B$, která splňuje podmínku:

($*$) Pro každý prvek $a \in A$ existuje právě jeden prvek $b \in B$ takový, že $(a, b) \in f$.

Prvek b se obvykle označuje $f(a)$, někdy také f_a. Nazývá se *hodnota* zobrazení f v prvku a nebo také *obraz* prvku a při zobrazení f.

Zápisem $f : A \to B$ vyjadřujeme, že f je zobrazení z množiny A do množiny B. Jiný zápis: $a \xrightarrow{f} b$. Místo $b = f(a)$ často píšeme $f : a \mapsto b$ nebo $a \overset{f}{\mapsto} b$.

Zobrazení $f : A \to B$ je jednoznačně určeno zadáním množin A, B a hodnot $f(a)$ pro každé $a \in A$. Zobrazení $f : A \to B$, $g : C \to D$ jsou si rovna právě tehdy, když $A = C$, $B = D$ a pro každé $a \in A$ platí $f(a) = g(a)$.

Příklady. 1. Nechť $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$, $B = \{\square, \blacksquare\}$. Pak následující zápisy definují jedno a to samé zobrazení $f : A \to B$:
(1) $f = \{(\heartsuit, \square), (\spadesuit, \blacksquare), (\diamondsuit, \square), (\clubsuit, \blacksquare)\}$.
(2) $f(\heartsuit) = \square$, $f(\spadesuit) = \blacksquare$, $f(\diamondsuit) = \square$, $f(\clubsuit) = \blacksquare$.
(3) $f : \heartsuit \mapsto \square$, $\spadesuit \mapsto \blacksquare$, $\diamondsuit \mapsto \square$, $\clubsuit \mapsto \blacksquare$.
2. Relace, která vejci přiřazuje slepici, která je snesla, je zobrazení z množiny všech slepičích vajec do množiny všech slepic.

Identická relace na množině A je zobrazení (*identické zobrazení*) z množiny A do ní samé a značí se $\mathrm{id}_A : A \to A$. Platí $\mathrm{id}_A(a) = a$ pro každé $a \in A$.

Tvrzení. *Buďte $f : A \to B$, $g : B \to C$ dvě zobrazení. Pak je relace $g \circ f$ zobrazení $A \to C$. Platí*

$$(g \circ f)(a) = g(f(a)) \quad \text{pro každé } a \in A. \tag{$**$}$$

Důkaz. Prvek $a \in A$ má za obraz $g(f(a)) \in C$. Dokažme jednoznačnost obrazu. Je-li $c \in C$ a $(a, c) \in g \circ f$, pak podle definice existuje $b \in B$ takové, že $(a, b) \in f$ a $(b, c) \in g$. Pak ovšem $b = f(a)$ a $c = g(b)$, protože f, g jsou zobrazení. Tudíž, $c = g(f(a))$.

Zobrazení $g \circ f$ se nazývá *kompozice* zobrazení f, g.

Tvrzení. (1) *Budiž $f : A \to B$ zobrazení. Pak*

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f.$$

(2) *Buďte $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení. Pak*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Důkaz. (1) Jde o zobrazení $A \to B$. Ukažme, že pro každé $a \in A$ nabývají stejných hodnot. Pro libovolné $a \in A$ ale máme $(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(a)) = f(a)$ a podobně $(\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a)$.
(2) Obě zobrazení $h \circ (f \circ g)$ a $(h \circ g) \circ f$ jsou zobrazení $A \to D$. Ukažme, že nabývají stejných hodnot pro každé $a \in A$. Pro libovolný prvek $a \in A$ máme $\big(h \circ (g \circ f)\big)(a) = h\big((g \circ f)(a)\big) = h(g(f(a))) = (h \circ g)\big(f(a)\big) = \big((h \circ g) \circ f\big)(a)$.

Cvičení. Proč platí každá z rovností uvedených v důkazu?
Například rovnost $\big(h \circ (g \circ f)\big)(a) = h\big((g \circ f)(a)\big)$ je výsledkem dosazení h za g, $g \circ f$ za f a a za a do formule $(**)$ definující skládání „$\circ$.“ Následující rovnost je důsledkem rovnosti $(g \circ f)(a) = (g(f(a))$; stejné prvky množiny B pak mají stejné obrazy při zobrazení $h : B \to C$. Vysvětlete zbývající rovnosti.

Buď dáno zobrazení $f : A \to B$. Je-li prvek $b \in B$ obrazem prvku $a \in A$, pak se prvek a nazývá *vzor prvku b při zobrazení f*. Množina všech vzorů prvku $b \in B$ při zobrazení f se značí $f^{-1}\{b\}$.
Zatímco obraz obecného prvku $a \in A$ vždy existuje a je jediný, vzor prvku $b \in B$ obecně existovat nemusí a nemusí být ani jediný. V souvislosti s tím uveďme další definice.
Zobrazení $f : A \to B$ se nazývá *surjektivní* (čili *surjekce*), jestliže platí

$$\forall_{b \in B} \exists_{a \in A}\, b = f(a).$$

Tudíž, zobrazení f je surjektivní právě tehdy, když má každý prvek $b \in B$ alespoň jeden vzor v A (je-li pro každé $b \in B$ množina $f^{-1}\{b\}$ neprázdná). Hovoříme též o zobrazení množiny A *na* množinu B.

Zobrazení $f : A \to B$ se nazývá *injektivní* (čili *injekce*) neboli *prosté*, jestliže platí

$$\forall_{a_1, a_2 \in A} \big(f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \big).$$

Jinak řečeno, zobrazení f je injektivní, má-li každý prvek $b \in B$ nejvýše jeden vzor v A (je-li pro každé $b \in B$ množina $f^{-1}\{b\}$ nejvýše jednoprvková).

Nakonec, zobrazení $f : A \to B$ se nazývá *bijektivní*, je-li injektivní a surjektivní současně Tudíž, zobrazení f je bijektivní tehdy a jen tehdy, má-li každý prvek $b \in B$ právě jeden vzor (je-li pro každé $b \in B$ množina $f^{-1}\{b\}$ jednoprvková).

Příklady. 1. $\{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\} \to \{\square, \blacksquare\}$, $f(\heartsuit) = \square$, $f(\spadesuit) = \blacksquare$, $f(\diamondsuit) = \square$, $f(\clubsuit) = \blacksquare$. Zobrazení f je surjektivní (oba prvky $\blacksquare, \square \in B$ mají vzor), ale není injektivní (např. $\blacksquare$ má dva vzory: $\spadesuit$ a $\clubsuit$). Není proto ani bijektivní.

2. Uvažujme o relaci „chodí“ mezi množinou H hochů a množinou D dívek. Tato relace je zobrazením, pokud každý hoch chodí s právě jednou dívkou. Toto zobrazení je bijektivní, pokud přitom každá dívka chodí s právě jedním hochem.

Tvrzení. *Buď $f : A \to B$ zobrazení. Následující podmínky jsou ekvivalentní*:

(1) *f je bijektivní*;

(2) *existuje zobrazení $g : B \to A$ takové, že*

$$g \circ f = \mathrm{id}_A, \qquad f \circ g = \mathrm{id}_B .$$

V pozitivním případě zobrazení g s vlastnostmi (2) *existuje jediné a je opět bijektivní.*

Zobrazení g z předchozího tvrzení se nazývá *inverzní* k f a značí se f^{-1}.

Důkaz. Dokažme implikaci „(1) $\Rightarrow$ (2).“ Buď f bijektivní. Definujme zobrazení $g : B \to A$ předpisem: pro libovolné $b \in B$ nechť $g(b) = a \Leftrightarrow b = f(a)$. Tento předpis definuje zobrazení, protože pro každý prvek $b \in B$ existuje právě jeden prvek a takový, že $b = f(a)$, totiž vzor prvku b při zobrazení f, a ten je jediný podle definice bijekce.

Ověřme rovnost $g \circ f = \mathrm{id}_A$. Zřejmě jde o dvě zobrazení $A \to A$. Pro každé $a \in A$ pak při označení $b = f(a)$ máme $(g \circ f)(a) = g(f(a)) = g(b) = a = \mathrm{id}_A(a)$, což se mělo dokázat. Podobně $f \circ g = \mathrm{id}_B$, protože obě jsou zobrazení $B \to B$ a pro každé $b \in B$ existuje jediné a takové, že $b = f(a)$, načež $g(b) = a$ a máme $(f \circ g)(b) = f(g(b)) = f(a) = b = \mathrm{id}_B(b)$.

Dokažme implikaci „(2) $\Rightarrow$ (1).“ Nechť existuje zobrazení $g : B \to A$ takové, že $g \circ f = \mathrm{id}_A$ a $f \circ g = \mathrm{id}_B$. Ukažme, že f je surjektivní. Buď $b \in B$ libovolné. Položme $a = g(b)$, potom $f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b$, takže a je vzor prvku b při zobrazení f a f je surjektivní. Ukažme, že f je injektivní. Buďte $a_1, a_2 \in A$ libovolné dva prvky takové, že $f(a_1) = f(a_2)$. Potom $g(f(a_1)) = g(f(a_2))$, ale $g(f(a_1)) = (g \circ f)(a_1) = \mathrm{id}_A(a_1) = a_1$ a podobně $g(f(a_2)) = a_2$, načež $a_1 = a_2$ a f je injektivní.

Dále je třeba dokázat jednoznačnost zobrazení $g : B \to A$ s vlastnostmi $g \circ f = \mathrm{id}_A$ a $f \circ g = \mathrm{id}_B$. Buď $g' : B \to A$ jiné zobrazení, pro něž platí $g' \circ f = \mathrm{id}_A$ a $f \circ g' = \mathrm{id}_B$.

Buď $b \in B$ libovolný prvek; ukažme, že $g(b) = g'(b)$. Máme ovšem $f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = (f \circ g')(b) = f(g'(b))$. Ale f je injektivní podle již dokázané implikace „(2) $\Rightarrow$ (1),“ načež $g(b) = g'(b)$. Vzhledem k libovolné volbě prvku b dostáváme rovnost $g = g'$.

Nakonec je třeba dokázat, že i zobrazení g je bijektivní. To ovšem plyne z již dokázané implikace „(2) $\Rightarrow$ (1),“ zaměníme-li mezi sebou $f \leftrightarrow g$ a $A \leftrightarrow B$.

Zapamatujte si formuli $f(a) = b \Leftrightarrow a = f^{-1}(b)$, $a \in A$, $b \in B$.

Cvičení. Ukažte, že je-li f bijekce, pak je inverzní zobrazení f^{-1} totožné s opačnou relací f^{-1}.

Příklad. Zobrazení $f : \{\heartsuit, \diamondsuit\} \to \{\spadesuit, \clubsuit\}$, $\heartsuit \mapsto \spadesuit$, $\diamondsuit \mapsto \clubsuit$, je bijekce. Inverzní je zobrazení $g = f^{-1} : \{\spadesuit, \clubsuit\} \to \{\heartsuit, \diamondsuit\}$, $\spadesuit \mapsto \heartsuit$, $\clubsuit \mapsto \diamondsuit$. (Invertování bijekce spočívá v obracení šipek.)

Tvrzení. *Buď $f : A \to B$ bijektivní zobrazení. Pak $(f^{-1})^{-1} = f$.*

Důkaz. Je potřeba dokázat, že f je inverzní zobrazení k f^{-1}. K tomu použijeme bod (2) předchozího tvrzení, kam dosadíme f za g a f^{-1} za f (a rovněž A za B a B za A). Obdržíme podmínku $f^{-1} \circ f = \mathrm{id}_A$ a $f \circ f^{-1} = \mathrm{id}_B$, která ovšem platí, protože f^{-1} je inverzní k f.

Tvrzení. *Buďte $f : A \to B$, $g : B \to C$ bijekce. Potom*
(1) *$g \circ f : A \to C$ je bijekce*;
(2) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Důkaz. Cvičení.

Cvičení. Buďte $f : A \to B$, $g : B \to C$ dvě zobrazení.
(1) Je-li zobrazení $g \circ f$ injektivní, pak je i zobrazení f injektivní.
(2) Je-li zobrazení $g \circ f$ surjektivní, pak je i zobrazení g surjektivní.
Dokažte.

Cvičení. Buďte $f : A \to B$, $g : A \to B$ dvě zobrazení. Dokažte, že platí:
(1) Buď $h : B \to C$ injektivní zobrazení takové, že $h \circ f = h \circ g$. Pak $f = g$. Jinými slovy, injektivním zobrazením lze krátit zleva.
(2) Buď $h : D \to A$ surjektivní zobrazení takové, že $f \circ h = g \circ h$. Pak $f = g$. Jinými slovy, surjektivním zobrazením lze krátit zprava.

Cvičení. Buďte A, B libovolné konečné množiny mající shodně po n prvcích. Buď $f : A \to B$ injektivní zobrazení. Ukažte, že f je bijektivní.

Návod: Dokazujte indukcí vzhledem k číslu n. Indukční krok: vyberte libovolně prvek $a \in A$ a uvažujte o množinách $A' = A \setminus \{a\}$ a $B' = B \setminus \{f(a)\}$.

Literatura

I. Bušek, L. Boček a E. Calda, *Matematika pro gymnázia* : *základní poznatky z matematiky* (Prométheus, Praha, 1995).