## 1. Množiny

Pojem množiny je základním pojmem matematiky. Množina je určena svými prvky, t.j., množinou rozumíme souhrn prvků. Teorii množin vybudoval německý matematik G.Cantor v roce 1872. Výše uvedené vymezení pojmu množiny není přesnou definicí. Vede také k rozporům neboť jsou "souhrny", které za množiny považovat nemůžeme. Později uvidíme, že nemůžeme vytvořit "množinu" všech množin. Nejjednodušší příklad takové zakázané "množiny" nalezl B.Russel v roce 1900. Je to souhrn $M = \{x \backslash x \notin x\}$ všech množin $x$, které neobsahují sebe jako prvek. Totiž, pokud by $M$ byla množina, můžeme si položit otázku, zda $M \in M$. Pokud ano, pak, podle definice $M$ platí $M \notin M$. Pokud ne, pak, opět podle definice $M$, platí $M \in M$. V obou případech dostáváme spor. Řešení problému definice pojmu množiny podává axiomatická teorie množin. My budeme pracovat v tzv. naivní teorii množin, t.j., na základě výše uvedené nepřesné "definice". Budeme však opatrní v jejím používání: ne všechny souhrny budeme považovat za množiny. Zároveň si naznačíme, jak vypadá axiomatická teorie množin.

Základní (a vlastně jedinou) vlastností množin je, že mají prvky. Píšeme $a \in A$, což znamená, že $a$ je prvkem množiny $A$. Malá a velká písmena používáme pro názornost; ve skutečnosti v teorii množin není nic jiného než množiny, t.j., i $a$ je množina. Fakt, že množina je určena svými prvky je vyjádřen následujícím axiomem (který je prvním axiomem axiomatické teorie množin):
*Axiom extensionality:* Dvě množiny jsou stejné, právě když mají stejné prvky.

Pomocí predikátové logiky (v jazyce s jediným binárním relačním symbolem $\in$, což je jazyk axiomatické teorie množin) se tento axiom zapíše následovně:

$$(\forall x, y)(x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y))$$

Pro množiny $A, B$ píšeme $A \subseteq B$ a říkáme, že množina $A$ je *podmnožina* množiny $B$, jestliže libovolný prvek množiny $A$ je prvkem množiny $B$. Zřejmě platí

$$A \subseteq A$$

$$A \subseteq B \text{ a } B \subseteq C \Rightarrow A \subseteq C$$

$$A = B \Leftrightarrow A \subseteq B \text{ a } B \subseteq A$$

Jsou-li $A, B$ množiny, můžeme z nich utvořit nové množiny

$$A \cup B = \{x \backslash x \in A \text{ nebo } x \in B\}$$

$$A \cap B = \{x \backslash x \in A \text{ a } x \in B\}$$

$$A - B = \{x \backslash x \in A \text{ a } x \notin B\}$$

které postupně nazýváme *sjednocení, průnik* a *rozdíl* množin $A$ a $B$.

Existuje množina, která se vyznačuje tím, že nemá žádné prvky. Nazývá se *prázdná* a označuje se $\emptyset$. Pro libovolnou množinu $A$ platí

$$\emptyset \subseteq A.$$

Množiny $A, B$ se nazývají *disjunktní*, jestliže $A \cap B = \emptyset$. Platí následující pravidla, která se postupně nazývají *komutativní, asociativní, idempotentní* a *distributivní* zákony:

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cup A = A$$

$$A \cap A = A$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Je-li $A$ podmnožinou množiny $M$, pak rozdíl $M - A$ se nazývá *doplněk* (nebo také *komplement*) podmnožiny $A$. Značíme jej $A'$. Platí následující pravidla, která se postupně nazývají zákony *jednotky, negace* a *de Morgana*:

$$A \cup M = M$$

$$A \cap M = A$$

$$A \cup \emptyset = A$$

$$A \cap \emptyset = \emptyset$$

$$A \cup A' = M$$

$$A \cap A' = \emptyset$$

$$M' = \emptyset$$

$$\emptyset' = M$$

$$A'' = A$$

$$(A \cap B)' = A' \cup B'$$

$$(A \cup B)' = A' \cap B'.$$

Obecněji, platí

$$A - (B \cup C) = (A - B) \cap (A - C)$$

$$A - (B \cap C) = (A - B) \cup (A - C).$$

Máme-li množiny $A, B$, můžeme utvořit novou množinu $\{A, B\}$, která má za prvky právě $A$ a $B$. Tento způsob tvorby množin se nazývá *axiom dvojice*. Jeho pomocí můžeme z prázdné množiny $\emptyset$ vytvořit nové množiny, např. $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}\}$, atd. Tímto způsobem můžeme definovat přirozená čísla: $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, atd. Vždy $n = \{0, 1, \cdots, n-1\}$. Tedy přirozená čísla jsou množiny. Rovněž můžeme utvořit množinu všech nezáporných celých čísel

$$\omega = \{0, 1, 2, \cdots, n, \cdots\}.$$

Nazýváme to *axiom nekonečna*.

Pro libovolnou množinu $A$ a libovolnou "množinovou vlastnost" $\varphi(x)$ můžeme utvořit novou množinu

$$\{a \in A \backslash \varphi(a) \text{ platí}\}.$$

Přesná definice množinové vlastnosti je, že se jedná o formuli predikátové logiky v jazyce s jediným binárním relačním symbolem $\in$. Tento způsob tvorby množin se nazývá *axiom vyčlenění*. Tímto způsobem vznikly množiny:

$$A \cap B = \{a \in A \backslash a \in B\}$$

$$A - B = \{a \in A \backslash a \notin B\}.$$

Pro libovolnou množinu $\mathcal{A}$ tak také můžeme utvořit množinu

$$\bigcap \mathcal{A} = \{a \backslash a \in A \text{ pro libovolné } A \in \mathcal{A}\}.$$

Psací písmo jsme opět použili pouze pro názornost. Obvyklé označení je pomocí indexů: máme množinu $I$ a množiny $A_i$ pro libovolné $i \in I$ a vytváříme množinu

$$\bigcap_{i \in I} A_i = \{a \backslash a \in A_i \text{ pro libovolné } i \in I\}.$$

Pro sjednocení množin potřebujeme nový způsob tvorby množin nazývaný *axiom sjednocení*. Říká, že pro libovolnou množinu $\mathcal{A}$ můžeme utvořit novou množinu

$$\bigcup \mathcal{A} = \{a \backslash \text{ existuje } A \in \mathcal{A} \text{ tak, že } a \in A\}.$$

Zejména

$$A \cup B = \bigcup \{A, B\}.$$

Obvyklé značení je

$$\bigcup_{i \in I} A_i = \{a \backslash a \in A_i \text{ pro nějaké } i \in I\}.$$

Platí následující pravidla:

$$A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i)$$

$$A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i)$$

$$(\bigcup_{i \in I} A_i)' = \bigcap_{i \in I} A_i'$$

$$(\bigcap_{i \in I} A_i)' = \bigcup_{i \in I} A_i'$$

*Uspořádaná dvojice* $(a, b)$ se definuje jako množina

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Tato definice je v duchu teorie množin: vše je množina, tedy i uspořádaná dvojice. Snadno se ověří, že platí

$$(a, b) = (c, d) \Leftrightarrow a = c \text{ a } b = d.$$

*Kartézský součin* množin $A, B$ nyní definujeme jako

$$A \times B = \{(a, b) \backslash a \in A, b \in B\}.$$

Platí

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

$$C \times (A \cup B) = (C \times A) \cup (C \times B)$$

$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$

$$C \times (A \cap B) = (C \times A) \cap (C \times B).$$

Tato pravidla lze rozšířit i na nekonečná sjednocení a průniky:

$$(\bigcup_{i \in I} A_i) \times C = \bigcup_{i \in I} (A_i \times C)$$

$$(\bigcap_{i \in I} A_i) \times C = \bigcap_{i \in I} (A_i \times C)$$

(a podobně z druhé strany). Všimněme si, že pro $A \neq B$ platí

$$A \times B \neq B \times A$$

Podobně

$$(A \times B) \times C \neq A \times (B \times C).$$

Je-li $A$ množina, můžeme utvořit množinu

$$\mathcal{P}(A) = \{X \backslash X \subseteq A\}$$

všech podmnožin množiny $A$. Nazýváme to *axiom množiny podmnožin.*

Dosud jsme se seznámili s následujícími axiomy teorie množin: axiom extensionality, axiom prázdné množiny, axiom vyčlenění, axiom dvojice, axiom sjednocení, axiom množiny podmnožin a axiom nekonečna. První udává, kdy jsou dvě množiny stejné, další popisují "povolené" způsoby tvorby množin. K úplné Zermelo-Fraenkelově teorii množin (což je standartní axiomatika teorie množin, označuje se ZF) nám chybí již jen dva dosti technické axiomy: axiom regularity a axiom nahrazení. (První z nich říká, že všechny množiny "vzniknou" z prázdné množiny.) Např. kartézský součin $A \times B$ vznikne vyčleněním z množiny $\mathcal{P}(\mathcal{P}(A \cup B))$; totiž uspořádané dvojice $(a, b)$ jsou prvky této množiny.

Ideální teorie množin by kromě axiomu extensionality obsahovala pouze axiom říkající, že pro libovolnou množinovou vlastnost $\varphi(x)$ je

$$\{a \backslash \varphi(a) \text{ platí}\}$$

množina. Russelův paradox však ukazuje, že tato teorie je sporná. Axiomy Zermelo-Fraenkelovy teorie množin uvádějí povolené případy výše uvedeného "ideálního" axiomu.

## 2. Zobrazení

**Definice.** *Zobrazení* $f : A \to B$ množiny $A$ do množiny $B$ je předpis přiřazující každému prvku množiny $A$ prvek množiny $B$.

Tato definice není, z hlediska teorie množin, přesná neboť obsahuje nedefinovaný pojem "předpis". Přesnou definici si uvedeme v příští kapitole.

Zobrazení $f : A \to B$ se nazývá *prosté* (nebo také *injektivní*), jestliže platí

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Nazývá se zobrazení množiny $A$ *na* množinu $B$ (nebo také *surjektivní*), jestliže pro libovolné $b \in B$ existuje $a \in A$ tak, že $f(a) = b$. Zobrazení, které je současně prosté i na se nazývá *bijektivní* (nebo také *bijekce*). Množiny $A, B$ se nazývají *isomorfní*, jestliže existuje bijekce $A \to B$. Značíme $A \cong B$.

Buď $f : A \to B$ bijektivní zobrazení. Položme

$$f^{-1}(b) = a \text{ právě když } f(a) = b.$$

Pak $f^{-1} : B \to A$ je zobrazení, které nazýváme *inverzní* k $f$. Zřejmě to je rovněž bijektivní zobrazení a platí

$$(f^{-1})^{-1} = f.$$

Předpis

$$id_A(a) = a$$

definuje zobrazení $id_A : A \to A$, které se nazývá *identické* (nebo rovněž *identita*) na $A$. Je to zřejmě bijekce a platí

$$(id_A)^{-1} = id_A.$$

Obecněji, je-li $A \subseteq B$, pak *zobrazení inkluze* $i : A \to B$ je definováno předpisem

$$i(a) = a$$

pro $a \in A$.

Buďte $f : A \to B$ a $g : B \to C$ zobrazení. Pak předpis

$$(g \circ f)(a) = g(f(a))$$

definuje zobrazení $g \circ f : A \to C$. Tento postup se nazývá *skládání* zobrazení a $g \circ f$ se nazývá *složené zobrazení*. Platí následující pravidla ($h : C \to D$ je další zobrazení):

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

$$f \circ id_A = f \qquad id_B \circ f = f$$

$$f \circ f^{-1} = id_B \qquad f^{-1} \circ f = id_A.$$

Jedná se o asociativní zákon, vlastnost jednotky a vlastnost inverzního zobrazení. V posledním pravidle je samozřejmě $f$ bijekce. Navíc, inverzní zobrazení je touto vlastností určeno jednoznačně. To znamená, že

$$f \circ g = id_B \text{ a } g \circ f = id_A \Rightarrow g = f^{-1}.$$

Symbolem $B^A$ označíme množinu všech zobrazení $A \to B$.

Pro libovolnou množinu $A$ existuje právě jedno zobrazení $\emptyset \to A$. Nazývá se prázdné zobrazení a označuje se $o_A$. Tedy $A^\emptyset = \{o_A\}$ je jednoprvková množina.

Zřejmě $(A^A, \circ)$ je monoid. Tento monoid není obecně komutativní. Například, označíme-li symbolem $k_a : A \to A$ konstantní zobrazení s hodnotou $a$, t.j. $k_a(x) = a$ pro všechna $x \in A$, pak platí

$$k_a \circ k_b = k_a \text{ a } k_b \circ k_a = k_b.$$

Bijektivní zobrazení množiny $A \to A$ se nazývá *permutace* množiny $A$. Symbolem $S(A)$ označíme množinu všech permutací množiny $A$. Pak $(S(A), \circ)$ je grupa. Tato grupa opět není obecně komutativní. Nazývá se *symetrická* grupa.

Zobrazení

$$p_1 : A \times B \to A \quad p_2 : A \times B \to B$$

daná předpisem

$$p_1(a, b) = a \quad p_2(a, b) = b$$

se nazývají *projekce*.

**Věta 2.1.** *Pro libovolné množiny $A, B, C$ platí následující pravidla:*
*(1)* $(A \times B)^C \cong A^C \times B^C$
*(2)* $(A^B)^C \cong A^{B \times C}$
*(3)* $A^{B \cup C} \cong A^B \times A^C$.
*V (3) musí množiny $B, C$ být disjunktní.*

*Důkaz.* (1) Bijekce $F : (A \times B)^C \to A^C \times B^C$ je dána předpisem

$$F(f) = (p_1 \circ f, p_2 \circ f),$$

kde $p_1 : A \times B \to A$ a $p_2 : A \times B \to B$ jsou projekce.

(2) Bijekce $F : (A^B)^C \to A^{B \times C}$ je dána předpisem

$$F(f)(b, c) = f(c)(b)$$

kde $f : C \to A^B$.

(3) Jsou-li $B, C$ disjunktní, pak bijekce $F : A^{B \cup C} \to A^B \times A^C$ je dána předpisem

$$F(f) = (f_1, f_2)$$

kde $f_1$ je zúžení $f : B \cup C$ na $B$ (t.j., $f_1(b) = f(b)$) a $f_2$ je zúžení $f$ na $C$. □

Kartézský součin můžeme pomocí pojmu zobrazení popsat následovně:

$$A \times B \cong \{f : \{1, 2\} \to A \cup B \backslash f(1) \in A, f(2) \in B\}.$$

To nás vede k následující definici kartézského součinu libovolného (i nekonečného) systému množin $A_i$, $i \in I$, kde $I$ je množina:

$$\prod_{i \in I} A_i = \{f : I \to \bigcup_{i \in I} A_i \backslash f(i) \in A_i \text{ pro libovolné } i \in I\}.$$

*Projekce*

$$p_i : \prod_{i \in I} A_i \to A_i$$

jsou definovány předpisem $p_i(f) = f(i)$.

Pro libovolnou podmnožinu $B$ množiny $A$ definujeme *charakteristickou funkci* $\chi_B : A \to 2$ této podmnožiny předpisem (zde $2 = \{0, 1\}$)

$$\chi_B(a) = 1 \Leftrightarrow a \in B.$$

Zobrazení $F : \mathcal{P}(A) \to 2^A$, $F(B) = \chi_B$ je zřejmě bijekce. Tedy

$$\mathcal{P}(A) \cong 2^A.$$

Je-li $f : A \to B$ zobrazení, pak množina

$$f(A) = \{f(a) \backslash a \in A\}$$

se nazývá *obraz* množiny $A$ v zobrazení $f$. Libovolné zobrazení $f : A \to B$ lze zapsat jako složení zobrazení na a prostého zobrazení

$$f : A \to f(A) \to B.$$

**Definice.** Řekneme, že množiny $A, B$ *mají stejnou mohutnost*, jestliže $A \cong B$.

Jedná se pouze o jiný název pro skutečnost, že množiny $A, B$ jsou isomorfní. Množina $A$ se nazývá *konečná*, pokud má stejnou mohutnost jako některá z množin $n = \{0, 1, \ldots, n - 1\}$, kde $n \in \omega$.

**Příklady 2.2.** (1) Dvě konečné množiny mají stejnou mohutnost, právě když mají stejný počet prvků.

(2) Množiny $\mathbb{Z}$ a $2\mathbb{Z}$ mají stejnou mohutnost neboť zobrazení $f : \mathbb{Z} \to 2\mathbb{Z}$, $f(x) = 2x$ je bijekce. Tedy vlastní podmnožina nekonečné množiny může mít stejný počet prvků jako celá množina.

(3) Množiny $\omega$, $\mathbb{N}$ a $\mathbb{Z}$ mají stejnou mohutnost. Stačí uvažovat bijekce $f : \omega \to \mathbb{N}$ a $g : \omega \to \mathbb{Z}$ dané předpisy

$$f(x) = x + 1$$

$$g(2n) = n \quad g(2n+1) = -(n+1).$$

(4) Ukážeme, že množina $\mathbb{Q}$ racionálních čísel má stejnou mohutnost jako $\omega$. Podobně jak pro $\mathbb{Z}$ stačí ukázat, že množina $\mathbb{Q}^+$ kladných racionálních čísel má stejnou mohutnost jako $\omega$. Napíšeme tato čísla jako vykrácené zlomky do řádků. Do prvního řádku dáme všechny vykrácené zlomky s čitatelem 1, do druhého řádku všechny vykrácené zlomky s čitatelem 2, atd. Vznikne čtvercová tabulka, která má spočetně mnoho řádků a spočetně mnoho sloupců. Vypíšeme-li její prvky po diagonálách (t.j., $1, \frac{1}{2}, 2, \frac{1}{3}, \dots$), seřadíme kladná racionální čísla do posloupnosti. Tedy $\mathbb{Q}^+$ má stejnou mohutnost jako $\omega$.

**2.3 Cantorova věta.** *Množiny $X$ a $\mathcal{P}(X)$ nikdy nemají stejnou mohutnost.*

*Důkaz.* Buď $f : X \to \mathcal{P}(X)$ zobrazení. Položme $Y = \{x \in X \setminus x \notin f(x)\}$. Předpokládejme, že existuje $z \in X$ tak, že $f(z) = Y$. Pak platí

$$z \in Y \Leftrightarrow z \notin Y,$$

což je spor.

□

Množina, která má stejnou mohutnost jako $\omega$ se nazývá *spočetná*. Nekonečná množina, která není spočetná se nazývá nespočetná. V předchozím příkladu jsme viděli, že $\mathbb{N}$, $\mathbb{Z}$ a $\mathbb{Q}$ jsou spočetné množiny.

**Věta 2.4.** *Podmnožina spočetné množiny je buď konečná nebo spočetná.*

*Důkaz.* Buď $X$ nekonečná podmnožina $\omega$. Uvažme zobrazení $f : \omega \to X$ takové, že $f(n)$ je nejmenší prvek v $X - \{f(0), \dots, f(n-1)\}$. Poněvadž $f$ je zřejmě bijektivní zobrazení, množina $X$ je spočetná. □

**Věta 2.5.** *Buď $f : \omega \to X$ zobrazení. Pak $f(\omega)$ je konečná nebo spočetná množina.*

*Důkaz.* Definujme zobrazení $g : f(\omega) \to \omega$ tak, že $g(x)$ je nejmenší prvek v $f^{-1}(x)$. Pak $g$ je prosté, takže tvrzení plyne z 2.4. □

**Věta 2.6.** *Množina $\mathbb{R}$ je nespočetná.*

*Důkaz.* Definujme zobrazení $f : 2^\omega \to \mathbb{R}$ desetinným rozvojem

$$f(h) = 0, h(0)h(1)h(2)\dots$$

kde $h : \omega \to 2$. Poněvadž $f$ je prosté zobrazení, z 2.3. a 2.4. plyne, že množina $\mathbb{R}$ není spočetná. □

Otázka, zda libovolná nekonečná podmnožina v $\mathbb{R}$ je buď spočetná nebo mohutnosti stejné jako $\mathbb{R}$, je nerozhodnutelná.

## 3. Relace

**Definice.** (Binární) *relací* $R$ (mezi množinami $A, B$) definujeme jako podmnožinu $R \subseteq A \times B$.

Obecně, můžeme definovat n-ární relaci jako podmnožinu $R \subseteq A_1 \times \cdots \times A_n$ pro $n = 1, 2, \cdots$. Například unární relace je podmnožina $R \subseteq A$.

Zobrazení $f : A \to B$ odpovídá relaci $R_f \subseteq A \times B$ s vlastností, že pro libovolné $a \in A$ existuje právě jedno $b \in B$ tak, že $(a, b) \in R_f$. Tím je podána slibovaná "množinová" definice pojmu zobrazení. Příslušná relace $R_f$ je vlastně graf zobrazení $f$.

Řadu pojmů o zobrazeních můžeme zobecnit na relace (relace je vlastně částečné, vícehodnotové zobrazení). Např. *definiční obor* relace $R \subseteq A \times B$ je

$$\{a \in A \backslash \text{ existuje } b \in B \text{ tak, že } (a, b) \in R\}$$

a *obor hodnot* je

$$\{b \in B \backslash \text{ existuje } a \in A \text{ tak,že } (a, b) \in R\}.$$

*Skládání relací* $R \subseteq A \times B$ a $S \subseteq B \times C$ se definuje předpisem

$$S \circ R = \{(a, c) \backslash \text{ existuje } b \in B \text{ tak, že } (a, b) \in R, (b, c) \in S\}$$

Platí $S \circ R \subseteq A \times C$. Dále (pro $T \subseteq C \times D$)

$$T \circ (S \circ R) = (T \circ S) \circ R$$

$$id_B \circ R = R = R \circ id_A.$$

*Inverzní relace* $R^{-1}$ k relaci $R \subseteq A \times B$ se definuje jako

$$R^{-1} = \{(b, a) \backslash (a, b) \in R\}.$$

Platí $R^{-1} \subseteq B \times A$. Zřejmě

$$R_{f^{-1}} = R_f^{-1}.$$

**Definice.** Pokud $R \subseteq A \times A$, pak říkáme, že $R$ je *relace na množině* $A$. Relace $R$ na množině $A$ se nazývá:

(1) *reflexivní*, pokud $id_A \subseteq R$
(t.j., pokud pro libovolné $a \in A$ platí $(a, a) \in R$)

(2) *symetrická*, pokud $R^{-1} = R$
(t.j., pokud $(a, b) \in R$ implikuje $(b, a) \in R$)

(3) *tranzitivní*, pokud $R \circ R \subseteq R$
(t.j., pokud $(a, b) \in R$ a $(b, c) \in R$, pak $(a, c) \in R$.

Relace $R$ na množině $A$ se nazývá *relace ekvivalence*, pokud je současně reflexivní, symetrická i tranzitivní.

Buď $f : A \to B$ zobrazení. Pak relace

$$J_f = \{(a_1, a_2) \backslash f(a_1) = f(a_2)\}$$

je relace ekvivalence na množině $A$. Nazývá se *jádro* zobrazení $f$. Ukážeme, že libovolná relace ekvivalence je jádrem nějakého zobrazení.

Buď $R$ relace ekvivalence na množině $A$. Pro $a \in A$ položíme

$$R_a = \{b \in A \backslash (a, b) \in R\}.$$

$R_a$ se nazývá *třída* relace ekvivalence $R$ určená prvkem $a$.

**Lemma 3.1.** *Buď $R$ relace ekvivalence na množině $A$ a $a, b \in A$. Pak platí*
*(1)* $a \in R_a$
*(2)* $R_a = R_b \Leftrightarrow (a, b) \in R$
*(3)* $R_a \cap R_b \neq \emptyset \Leftrightarrow R_a = R_b$.

*Důkaz.* (1) ihned plyne z reflexivity $R$.

(2) Nechť $R_a = R_b$. Poněvadž $a \in R_a = R_b$, platí $(b, a) \in R$, t.j., (dle symetrie) $(a, b) \in R$. Naopak, nechť $(a, b) \in R$. Pro libovolné $c \in R_b$ platí $(b, c) \in R$, t.j. $(a, c) \in R$ (podle tranzitivity), takže $c \in R_a$. Dokázali jsme, že $R_b \subseteq R_a$. Opačná inkluze plyne ze symetrie $R$.

(3) Nechť $R_a \cap R_b \neq \emptyset$. Pak existuje $c \in R_a \cap R_b$, takže platí $(a, c), (b, c) \in R$, t.j., $(a, c), (c, b) \in R$ a tedy $(a, b) \in R$. Podle (2) $R_a = R_b$. □

Množina

$$A \backslash R = \{R_a \backslash a \in A\}$$

se nazývá *faktorová množina* relace ekvivalence $R$ na množině $A$. Zobrazení

$$p_R : A \to A \backslash R$$

dané předpisem

$$p_R(a) = R_a$$

se nazývá *projekce* (příslušná k relaci ekvivalence $R$ na $A$).

**Věta 3.2.** *Pro libovolnou relaci ekvivalence $R$ na množině $A$ platí*

$$R = J_{p_R}.$$

*(T.j., relace ekvivalence je vždy jádrem své projekce.)*

*Důkaz.* Platí

$$p_R(a) = p_R(b) \Leftrightarrow R_a = R_b \Leftrightarrow (a, b) \in R.$$

□

**Věta 3.3.** *Buď $f : A \to B$ zobrazení. Pak*

$$A \backslash J_f \cong f(A).$$

*Důkaz.* Definujme zobrazení $g : A \backslash J_f \to f(A)$ vztahem

$$g((J_f)_a) = f(a). \tag{1}$$

Poněvadž

$$(J_f)_{a_1} = (J_f)_{a_2} \Leftrightarrow (a_1, a_2) \in J_f \Leftrightarrow f(a_1) = f(a_2)$$

$g$ je bijekce. □

**Poznámka 3.4.** Předpis (1) z předchozího důkazu definuje prosté zobrazení $g : A \backslash J_f \to B$. Platí $f = p_{J_f} \circ g$, takže libovolné zobrazení $f$ lze rozložit na složení zobrazení na $p_{J_f}$ následovaného prostým zobrazením $g$ .

Různá zobrazení mohou mít stejné jádro. Např., zobrazení $f$ je prosté, právě když $J_f = id_A$.

**Definice.** *Rozklad* $\mathcal{R}$ množiny $A$ je množina $\mathcal{R} \subseteq \mathcal{P}(A)$ neprázdných podmnožin množiny $A$ splňující
(1) $\bigcup \mathcal{R} = A$
(2) $X_1 \cap X_2 = \emptyset$ pro libovolná $X_1, X_2 \in \mathcal{R}, X_1 \neq X_2$.

Pro libovolnou relaci ekvivalence $R$ na množině $A$ je $A\backslash R$ rozklad množiny $A$. Ukážeme, že rozklady přesně odpovídají relacím ekvivalence.

**Věta 3.4.** *Buď $\mathcal{R}$ rozklad množiny $A$. Položme*

$$R_{\mathcal{R}} = \{(a,b)\backslash \text{ existuje } X \in \mathcal{R} \text{ tak, že } a, b \in X\}.$$

*Pak $R_{\mathcal{R}}$ je relace ekvivalence na $A$ a platí*

$$\mathcal{R} = A\backslash R_{\mathcal{R}}$$

.

*Důkaz.* Uvažujme zobrazení $r : A \to \mathcal{R}$ takové, že

$$a \in r(a).$$

Zřejmě $R_{\mathcal{R}} = J_r$, takže $R_{\mathcal{R}}$ je relace ekvivalence. Vztah $\mathcal{R} = A\backslash R_{\mathcal{R}}$ je zřejmý. □

Právě popsaná korespondence mezi rozklady a relacemi ekvivalence na množině $A$ je vzájemně jednoznačná:

$$\mathcal{R} = A\backslash R_{\mathcal{R}} \text{ a } R = R_{(A\backslash R)}.$$

Viděli jsme, že nezáporná celá čísla lze sestrojit pomocí množin, včetně (Peanovy) aritmetiky. Ukažeme, že totéž platí i pro celá a racionální čísla (v příští kapitole to provedeme i pro reálná čísla).

*Konstrukce celých čísel:* Definujme na množině $\omega \times \omega$ relaci $\sim$ vztahem

$$(a,b) \sim (c,d) \Leftrightarrow a + d = c + b.$$

Jedná se o relaci ekvivalence; reflexivita a symetrie jsou zřejmé, tranzitivita se ověří následovně: z $(a,b) \sim (c,d) \sim (e,f)$ plyne $a+d = c+b, c+f = e+d$, t.j., postupně $a+d+c+f = c+b+e+d$, $a+f = b+e$ a $(a,b) \sim (e,f)$.

Položíme

$$\mathbb{Z} = \omega \times \omega\backslash \sim .$$

Třídu ekvivalence $\sim$ určenou prvkem $(a,b)$ budeme značit symbolem $\overline{(a,b)}$ (tato třída hraje roli rozdílu $a - b$). Dále položíme

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$$

Přitom platí

$$-\overline{(a,b)} = \overline{(b,a)}.$$

Je třeba ověřit, že výše uvedené definice nezávisí na volbě reprezentantů. Ukážeme to pro sčítání (pro násobení to je analogické). Znamená to dokázat, že

$$(a,b) \sim (a',b'), (c,d) \sim (c'd') \Rightarrow (a+c, b+d) \sim (a'+c', b'+d').$$

Skutečně, $a + b' = a' + b, c + d' = c' + d$ implikuje $a + c + b' + d' = a' + c' + b + d$.

Přirozenému číslu $n$ odpovídá celé číslo $\overline{(n,0)}$. Zejména $0 = \overline{(0,0)}$.

*Konstrukce racionálních čísel:* Definujme na množině $\mathbb{Z} \times \mathbb{Z}^*$ (zde $\mathbb{Z}^*$ označuje množinu nenulových celých čísel) relaci $\sim$ vztahem

$$(a,b) \sim (c,d) \Leftrightarrow ad = cb.$$

Podobně, jak výše se ověří, že se jedná o relaci ekvivalence. Položíme

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*) \backslash \sim .$$

Třídu ekvivalence prvku $(a,b)$ opět značíme symbolem $\overline{(a,b)}$ (tato třída nyní hraje roli zlomku $\frac{a}{b}$). Položíme

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$$

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}.$$

Opět musíme ověřit nezávislost na volbě reprezentantů.

Celému číslu $a$ odpovídá racionální číslo $\overline{(a,1)}$. Zejména $1 = \overline{(1,1)}$. Pro $a, b \neq 0$ platí

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

## 4. Uspořádané množiny

Relace $R$ na množině $A$ se nazývá *antisymetrická*, jestliže

$$R \cap R^{-1} \subseteq id_A$$

t.j., pokud pro libovolné prvky $a, b \in A$ platí

$$(a,b) \in R, (b,a) \in R \Rightarrow a = b.$$

**Definice.** Relace $R$ na množině $A$, která je reflexivní, antisymetrická a tranzitivní se nazývá *uspořádání*.

Řekneme, že $(A, \leq)$ je *uspořádaná množina*, jestliže $\leq$ je relace uspořádání na $A$.

Uspořádaná množina $(A, \leq)$ se nazývá *lineárně uspořádaná* (nebo také *řetězec*), jestliže pro libovolná $a, b \in A$ platí buď $a \leq b$ nebo $b \leq a$.

V uspořádané množině $(A, \leq)$ symbolem $a < b$ rozumíme $a \leq b$, $a \neq b$.

**Příklady.** (1) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ jsou lineárně uspořádané množiny (vzhledem k uspořádání podle velikosti).

(2) Pro libovolnou množinu $A$ je $=$ uspořádání na $A$. Vzniklá uspořádaná množina se nazývá *protiřetězec* (samozřejmě se nejedná o lineární uspořádání, má-li $A$ aspoň dva prvky).

(3) Často můžeme uspořádanou množinu $(A, \leq)$ znázornit graficky. Prvky množiny $A$ nakreslíme jako body a úsečkou spojíme sousední prvky. Tím rozumíme prvky $a, b \in A$ takové, že $a \leq b$, přičemž neexistuje $c \in A$ takové, že $a < c < b$. Píšeme $a \prec b$. Body $a, b \in A$ takové, že $a \prec b$ přitom kreslíme tak, že $a$ je níže než $b$. Tyto obrázky se nazývají *Hasseovy diagramy.*

(4) Pro libovolnou množinu $X$ je $(\mathcal{P}(X), \subseteq)$ uspořádaná množina, která není lineárně uspořádaná (pokud $A$ má aspoň dva prvky).

V dalším budeme uspořádanou množinu většinou stručně označovat pouze symbolem $A$. Prvky $a, b \in A$ se nazývají *nesrovnatelné*, pokud neplatí ani $a \leq b$ ani $b < a$. Značíme je $a \parallel b$. *Nejmenší prvek* uspořádané množiny $A$ je prvek $a$ takový, že pro libovolné $x \in A$ platí $a \leq x$. *Minimální prvek* $a$ je definován tím, že neexistuje prvek $x \in A$ tak, že $x < a$. Nejmenší prvek je, pokud existuje, jediný a je zároveň minimální. Minimálních prvků může být víc a nemusí být nejmenší (např. v protiřetězci). Analogicky definujeme *největší prvek* a *maximální prvek.*

Je-li $(A, \leq)$ uspořádaná množina, pak $(A, \geq)$ je rovněž uspořádaná množina; nazývá se *duálně uspořádaná.* Označujeme-ji $A^{op}$. Největší (maximální) prvek uspořádané množiny $A$ je vlastně nejmenší (minimální) prvek duálně uspořádané množiny $A^{op}$. Takové pojmy nazýváme *duální.* Podobně k libovolnému tvrzení o uspořádaných množinách existuje duální tvrzení (a platí-li výchozí tvrzení pro libovolnou uspořádanou množinu, pak duální tvrzení platí rovněž pro libovolnou uspořádanou množinu). Např., uspořádaná množina obsahuje nejvýše jeden největší prvek.

Relace, která je reflexivní a tranzitivní se nazývá *předuspořádání. Předuspořádaná množina* je dvojice $(A, \sqsubseteq)$, kde $\sqsubseteq$ je předuspořádání na množině $A$.

Příklady předuspořádaných množin, které nejsou uspořádané, jsou

(1) $(\mathbb{Z}^*, |)$, kde $|$ je relace dělitelnosti.

(2)$(Form_P, \sqsubseteq)$, kde $Form_P$ označuje množinu všech formulí výrokové logiky jazyka $P$ a

$$A \sqsubseteq B \quad \Leftrightarrow \quad \models A \to B.$$

**Věta 4.1.** *Buď $(A, \sqsubseteq)$ předuspořádaná množina. Pro $a, b \in A$ klademe*

$$a \sim b \Leftrightarrow a \sqsubseteq b \text{ a zároveň } b \sqsubseteq a.$$

*Pak $\sim$ je relace ekvivalence na $A$. Položíme-li pro $\bar{a}, \bar{b} \in A \setminus \sim$*

$$\bar{a} \leq \bar{b} \Leftrightarrow a \sqsubseteq b,$$

*pak $(A \setminus \sim, \leq)$ je uspořádaná množina.*

*Důkaz.* Snadno se ověří, že $\sim$ je relace ekvivalence na $A$. Definice relace $\leq$ na faktorové množině je korektní (t.j., nezávisí na volbě reprezentantů) neboť

$$a_1 \sim a_2, b_1 \sim b_2, a_1 \sqsubseteq b_1 \Leftrightarrow a_2 \sqsubseteq b_2.$$

Reflexivita a tranzitivita relace $\leq$ okamžitě plyne z reflexivity a tranzitivity výchozí relace $\sqsubseteq$. Zbývá ověřit, že $\leq$ je antisymetrická. Avšak

$$\bar{a} \leq \bar{b}, \bar{b} \leq \bar{a} \Leftrightarrow a \sqsubseteq b, b \sqsubseteq a \Leftrightarrow a \sim b \Leftrightarrow \bar{a} = \bar{b}.$$

□

Aplikujeme-li Větu 4.1. na předuspořádanou množinu $(\mathbb{Z}, |)$, platí

$$a \sim b \Leftrightarrow a = b \text{ nebo } a = -b.$$

Tedy indukovaná uspořádaná množina je vlastně totéž jako $(\mathbb{Z}^+, |)$. V případě předuspořádané množiny $(Form_P, \sqsubseteq)$ platí

$$A \sim B \Leftrightarrow \quad \vdash A \leftrightarrow B$$

.

**Definice.** Buďte $A, B$ uspořádané množiny a $f : A \to B$ zobrazení. Řekneme, že $f$ je *izotonní*, pokud platí

$$a_1 \leq a_2 \Rightarrow f(a_1) \leq f(a_2).$$

Jsou-li $A, B$ uspořádané množiny a $f : A \to B$ bijektivní zobrazení takové, že $f$ i $f^{-1}$ jsou isotonní, pak říkáme, že f je *izomorfismus*. Uspořádané množiny $A, B$ se v tom případě nazývají *isomorfní* a značíme $A \cong B$.

**Definice.** Buď $A$ uspořádaná množina a $X \subseteq A$. Řekneme, že prvek $a \in A$ je *horní závora* podmnožiny $X$, jestliže platí $x \leq a$ pro libovolné $x \in X$.

Řekneme, že $a$ je *supremum* podmnožiny $X$, jestliže je horní závorou $X$ a pro libovolnou horní závoru $b$ množiny $X$ platí $a \leq b$.

Tedy supremum $X$ je nejmenší horní závora $X$. Označujeme ho $\sup X$. Duálně se definuje *dolní závora* podmnožiny $X$ a *infimum* podmnožiny $X$ (t.j., největší dolní závora $X$). Značíme jej $\inf X$.

Uvědomme si, že $\sup\emptyset$ je nejmenší prvek uspořádané množiny $A$ (pokud existuje) a $\inf\emptyset$ je největší prvek $A$.

V uspořádané množině $(\mathcal{P}(A), \subseteq)$ platí

$$\sup\mathcal{X} = \bigcup \mathcal{X}$$

$$\inf\mathcal{X} = \bigcap \mathcal{X}.$$

**Věta 4.2.** *Buď $A$ uspořádaná množina, v níž libovolná podmnožina má supremum. Pak libovolná podmnožina v $A$ má infimum.*

*Důkaz.* Nechť $X \subseteq A$. Buď $X^-$ množina dolních závor $X$ v $A$. Ukážeme, že platí

$$\inf X = \sup X^-.$$

Zřejmě platí, že $\inf X$, jestliže existuje, je $\sup X^-$. Je třeba ukázat, že $\sup X^-$ je $\inf X$. K tomu stačí ukázat, že $\sup X^- \in X^-$. Avšak pro libovolná $x \in X$ a $y \in X^-$ platí $y \leq x$, takže $\sup X^- \leq x$. Tedy $\sup X^- \in X^-$. □

**Definice.** Uspořádaná množina, jejíž libovolná podmnožina má supremum i infimum se nazývá *úplný svaz.*

Duální věta k Větě 2. říká, že pokud libovolná podmnožina uspořádané množiny $A$ má infimum, pak $A$ je úplný svaz.

Doplňme, že uspořádaná množina $A$ se nazývá *svaz*, pokud libovolná její neprázdná konečná podmnožina má supremum i infimum (což je totéž jako požadavek, že libovolná dvouprvková podmnožina má supremum a infimum).

**Věta 4.3.** *(Tarski) Buď $A$ úplný svaz a $f : A \to A$ isotonní zobrazení. Pak $f$ má pevný bod, t.j., existuje $a \in A$ s vlastností $f(a) = a$.*

*Důkaz.* Položme

$$M = \{x \backslash x \leq f(x)\}.$$

Pro libovolný prvek $x \in M$ platí $f(x) \in M$. Skutečně, z $x \in M$ plyne $x \leq f(x)$, tedy $f(x) \leq f(f(x))$ a proto i $f(x) \in M$.

Položme $a = \sup M$. Tedy pro libovolné $x \in M$ platí $x \leq f(x)$, tedy $f(x) \leq f(a)$, takže $x \leq f(x) \leq f(a)$. Tedy $f(a)$ je horní závora podmnožiny $M$. Poněvadž $a$ je supremum $M$, máme $a \leq f(a)$. Tedy $a \in M$ a již jsme ověřili, že to znamená $f(a) \in M$. Tedy $f(a) \leq a$, jelikož $a$ je supremum $M$. Dokázali jsme, že platí $f(a) = a$. Tedy $a$ je hledaný pevný bod. □

Pevný bod sestrojený v předešlém důkazu je zřejmě největším pevným bodem zobrazení $f$. Duálně,

$$\inf\{x \backslash f(x) \leq x\}$$

je nejmenším pevným bodem $f$.

Ukážeme, že za zesílených předpokladů lze pevný bod získat "konstruktivně". Řekneme, že zobrazení $f : A \to B$ úplných svazů *zachovává suprema*, jestliže pro libovolnou podmnožinu $X \subseteq A$ platí

$$f(\sup X) = \sup f(X).$$

Takové zobrazení je vždy isotonní:

$$a \leq b \Rightarrow b = \sup\{a, b\} \Rightarrow f(b) = \sup\{f(a), f(b)\} \Rightarrow f(a) \leq f(b).$$

Poznamenejme, že pro libovolné izotonní zobrazení $f : A \to B$ platí

$$\sup f(X) \leq f(\sup X).$$

**Věta 4.4.** *Buď $A$ úplný svaz a $f : A \to A$ zobrazení, které zachovává suprema. Pak $f$ má pevný bod.*

*Důkaz.* Buď $a_0$ nejmenší prvek v $A$, jenž existuje neboť $A$ je úplný svaz. Pro libovolné $n = 0, 1, 2, \ldots$ položíme $a_{n+1} = f(a_n)$. Pak pro $a = \sup\{a_n \backslash n = 1, 2, \ldots\}$ platí

$$f(a) = f(\sup\{a_n \backslash n \in \omega\}) = \sup\{f(a_n) \backslash n \in \omega\} = \sup\{a_{n+1} \backslash n \in \omega\} = a.$$

Tedy $a$ je pevný bod $f$. □

**Poznámka 4.5.** Právě sestrojený pevný bod je zřejmě nejmenším pevným bodem $f$. Ve Větě 4.4. by stačilo předpokládat, že $f$ zachovává suprema řetězců. Význam tohoto obecnějšího tvrzení je vidět z následujícího příkladu.

**Příklad 4.6.** Buď $X$ množina a $\mathcal{P}(X \times X)$ množina všech podmnožin množiny $X \times X$ (t.j., relací na množině $X$) uspořádaná inkluzí. Buď $R \in \mathcal{P}(X \times X)$ relace na $X$ a $A$ podmnožina uspořádané množiny $\mathcal{P}(X \times X)$ tvořená všemi relacemi obsahujícími $R$

$$A = \{S \in \mathcal{P}(X \times X) \backslash R \subseteq S\}.$$

Definujme zobrazení $f : A \to A$ předpisem

$$f(S) = S \cup S \circ S.$$

Snadno se ověří, že $f$ zachovává suprema řetězců. Nejmenší pevný bod zobrazení $f$ (sestrojený v důkaze věty 4.4) je nejmenší tranzitivní relace na množině $X$ obsahující relaci $R$. Nazývá se *tranzitivní obal* relace $R$.

Poznamenejme, že $f$ nezachovává všechna suprema.

Buď $A$ uspořádaná množina, $a, b \in A$. Budeme označovat $a \vee b = \sup\{a, b\}$ a $a \wedge b = \inf\{a, b\}$. Často také budeme značit $\bigvee X = \sup X$ a $\bigwedge X = \inf X$. Připomeňme, že uspořádaná množina $A$ se nazývá *svaz*, pokud pro libovolné prvky $a, b \in A$ existují $a \vee b$ i $a \wedge b$.

**Lemma 4.7.** *Buď $A$ svaz, $a, b, c \in A$. Pak platí*

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

.

*Důkaz.* Nechť $a, b, c \in A$. Platí $a \leq (a \vee b)$, $a \leq (a \vee c)$, $b \wedge c \leq b \leq (a \vee b)$ a $b \wedge c \leq c \leq (a \vee c)$. Tedy platí $a \vee (b \wedge c) \leq (a \vee b)$ a $a \vee (b \wedge c) \leq (a \vee c)$. Odsud plyne tvrzení lemmatu. □

Rovnost v 4.5 obecně neplatí. Svazy, v nichž tato rovnost platí, se nazývají distributivní.

Podobně jak v 4.5 se ukáže, že pro libovolnou množinu $I$ platí

$$a \wedge \bigvee_{i \in I} b_i \geq \bigvee_{i \in I} (a \wedge b_i).$$

Dokonce, pro libovolné množiny $I$, $J_i$, $i \in I$ platí

$$\bigwedge_{i \in I} \bigvee_{j \in J_i} a_{ij} \geq \bigvee_{f \in F} \bigwedge_{i \in I} a_{if(i)} \tag{1}$$

kde $F$ je množina všech zobrazení $f : I \to \bigcup_{i \in I} J_i$ takových, že $f(i) \in J_i$ pro libovolné $i \in I$.

Důkaz je následující: pro libovolné $f \in F$ a libovolné $i \in I$ platí

$$\bigwedge_{i \in I} a_{if(i)} \leq a_{if(i)} \leq \bigvee_{j \in J_i} a_{ij}.$$

Tedy pro libovolné $f \in F$ platí

$$\bigwedge_{i\in I} a_{if(i)} \leq \bigwedge_{i\in I} \bigvee_{j\in J_i} a_{ij}.$$

Odsud však již plyne dokazovaná nerovnost (1).

**Konstrukce reálných čísel**: V teorii množin již umíme sestrojit racionální čísla. Nyní ukážeme, jak lze sestrojit čísla reálná. Především však musíme definovat uspořádání na množinách $\mathbb{Z}$ a $\mathbb{Q}$.

V $\mathbb{Z}$ položíme

$$\overline{(a,b)} \leq \overline{(c,d)} \Leftrightarrow a+d \leq c+b$$

(odpovídá to tomu, že $a-b \leq c-d$). V $\mathbb{Q}$

$$\overline{(a,b)} \leq \overline{(c,d)}, \quad b,d>0 \Leftrightarrow ad \leq cb$$

(odpovídá to tomu, že $ab^{-1} \leq cd^{-1}$).

*Řez* v množině $\mathbb{Q}$ racionálních čísel definujeme jako dvojici $(X,Y)$ neprázdných podmnožin množiny $\mathbb{Q}$ splňující

(1) $X \cap Y = \emptyset$

(2) $X \cup Y = \mathbb{Q}$

(3) $x \in X, y \in Y \Rightarrow x < y$.

Řezy v $\mathbb{Q}$ jsou jednoho z následujících tří typů:

(a) *mezera*: $X$ neobsahuje největší prvek a $Y$ neobsahuje nejmenší prvek

(b) *dedekindovský řez 1.druhu*: $X$ obsahuje největší prvek a $Y$ neobsahuje nejmenší prvek

(b) *dedekindovský řez 2.druhu*: $X$ neobsahuje největší prvek a $Y$ obsahuje nejmenší prvek.

(Čtvrtá možnost, že $X$ obsahuje největší prvek a $Y$ obsahuje nejmenší prvek (takový řez by se nazýval *skok*) nemůže v $\mathbb{Q}$ nastat.)

Nyní $\mathbb{R}$ definujeme jako množinu všech řezů, které jsou buď mezery nebo dedekindovské řezy 1.druhu. (Přitom mezery odpovídají iracionálním číslům a dedekindovské řezy 1.druhu číslům racionálním.) Uspořádání a aritmetické operace definujeme pro reálná čísla následovně:

$$(X,Y) \leq (X',Y') \Leftrightarrow X \subseteq X'$$

$$(X,Y)+(X',Y') = (\quad, Y+Y')$$

$$(X,Y)\cdot(X',Y') = (\quad, Y\cdot Y').$$

Zde

$$X+Y = \{x+y \backslash x \in X, y \in Y\}$$

$$X\cdot Y = \{x\cdot y \backslash x \in X, y \in Y\}.$$

Platí

$$\sup(X_i,Y_i) = (\bigcup X_i, \bigcap Y_i)$$

## 5. Kombinatorika

Buď $S$ konečná množina. *Variace* definujeme jako uspořádané výběry prvků množiny $S$ a *kombinace* jako neuspořádané výběry. Má-li množina $S$ $n$ prvků, mluvíme o variacích (kombinacích) n prvků. Má-li příslušný výběr $k$ prvků, mluvíme o variacích (kombinacích) k-té třídy. Variace i kombinace mohou být jak bez opakování, tak s opakováním. Variace k-té třídy z n prvků s opakováním jsou právě zobrazení k-prvkové množiny $X$ do n-prvkové množiny $S$. Z 4.1. (3) ihned plyne, že počet variací s opakováním k-té třídy z n prvků je $n^k$. Variace (tím se rozumí bez opakování) k-té třídy z n prvků jsou právě prostá zobrazení $X \to S$.

**Věta 5.1.** *Počet variací k-té třídy z n prvků je roven* $\frac{n!}{(n-k)!}$ *(kde* $k \leq n$*).*

*Důkaz.* Indukcí vzhledem ke $k$. Variace $s_1 \dots s_{k-1}$ dává právě $n-k+1$ variací $s_1 \dots s_{k-1} s_k$. Tedy počet variací k-té třídy je $n(n-1)\dots(n-k+1)$. □

Bijektivní zobrazení $S \to S$ jsou právě *permutace* množiny $S$. Z 5.1. ihned plyne, že počet permutací n-prvkové množiny je $n!$.

Kombinace k-té třídy z n prvků jsou právě k-prvkové podmnožiny množiny o $n$ prvcích.

**Věta 5.2.** *Pro* $k \leq n$ *je počet kombinací k-té třídy z n prvků roven*

$$\frac{n!}{(n-k)!k!}$$

*Důkaz.* Každá kombinace k-té třídy určuje $k!$ variací. Tvrzení tedy plyne z 5.1. □

Čísla

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

se nazývají *kombinační*. Mají následující vlastnosti; lze je odvodit přímo z definice nebo pomocí binomického rozvoje.

(1) $\binom{n}{k} = \binom{n}{n-k}$

(2) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

(3) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

(4) $\sum_{k=1}^{n} (-1)^k k \binom{n}{k} = 0$

(9) $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

(vztah (4) odvodíme derivováním binomického rozvoje $(1+x)^n$ podle $x$ a dosazením $x = -1$).

**Věta 5.3.** *Počet kombinací k-té třídy z n prvků s opakováním je roven*

$$\binom{n+k-1}{k}$$

*Důkaz.* Buď $s_1 \dots s_k$ kombinace s opakováním k-té třídy vybraná z množiny $S$ o $n$ prvcích. Doplňme ji všemi prvky množiny $S$. Tedy pro $S = \{a, b, c, d, e\}$ a kombinaci s opakováním $bbd$ dostaneme $abbbcdde$. Navzájem různé prvky oddělíme svislou čarou. V našem příkladě dostaneme $a|bbb|c|dd|e$. V obecném případě dostaneme $n + k$ prvků rozdělených $n - 1$ čarami. Poněvadž počet možných míst pro svislé čáry je $n + k - 1$, počet možností je $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$. To je však právě počet kombinací s opakováním. □

Mějme nyní n-prvkovou množinu $S$ a vlastnosti $P_1, \dots, P_k$. Buď $n_i$ počet prvků množiny $S$ s vlastností $P_i$ a obecněji $n_{i_1 \dots i_r}$ počet prvků množiny $S$ s vlastnostmi $P_{i_1}, \dots, P_{i_r}$. Nechť $n(0)$ označuje počet prvků množiny $S$, které nemají žádnou z vlastností $P_i$.

**Věta 5.4. (princip inkluze a exkluze).**

$$n(0) = n - \sum_i n_i + \sum_{i_1 < i_2} n_{i_1 i_2} - \dots + (-1)^s \sum_{i_1 < \dots < i_s} n_{i_1 \dots i_s} \dots + (-1)^k n_{1 \dots k}$$

*Důkaz.* Prvek, který nemá žádnou z uvažovaných vlastností se počítá jednou ve sčítanci $n$ a v dalších sčítancích se neobjeví. Prvek, který má právě vlastnost $P_j$ se objeví jednou ve sčítanci $n$ a jednou ve druhém sčítanci $\sum_i n_i$, takže jeho příspěvek k pravé straně je 0. Stačí, když ukážeme, že totéž nastane pro pro libovolný prvek mající právě vlastnosti $P_{j_1}, \dots, P_{j_r}$. Takový prvek přispívá jedničkou do každého součtu

$$\sum_{i_1 < \dots < i_s} n_{i_1 \dots i_s}$$

pro $s \leq r$ a pro libovolný výběr $i_1 < \dots < i_s$ z $j_1, \dots, j_r$. Takových výběrů je právě $\binom{r}{s}$. Tedy celkový příspěvek našeho prvku k součtu vpravo v principu inkluze a exkluze je

$$1 - \binom{r}{1} + \binom{r}{2} - \dots + (-1)^s \binom{r}{s} + \dots + (-1)^r \binom{r}{r} = (1-1)^r = 0$$

□

Jako aplikaci principu inkluze a exkluze si uvedeme následující tvrzení.

**Věta 5.5.** *Pro $k \leq m$ je počet všech zobrazení m-prvkové množiny na k-prvkovou množinu roven*

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^m$$

*Důkaz.* Za výchozí množinu $S$ vezmeme množinu všech zobrazení m-prvkové množiny do k-prvkové množiny $a_1, \dots, a_k$. Za vlastnost $P_i$ vezmeme, že prvek $a_i$ nepatří do obrazu daného zobrazení $f \in S$. Pak $n(0)$ je rovno hledanému počtu surjektivních zobrazení. Dále $n = k^m$ a $n_{i_1 \dots i_s}$ je rovno počtu zobrazení m-prvkové množiny do množiny $\{a_i \backslash i \neq i_1, \dots, i_s\}$, t.j., $(k-s)^m$. Tedy

$$\sum_{i_1 < \dots < i_s} n_{i_1 \dots i_s} = \binom{k}{s} (k-s)^m$$

Odsud plyne tvrzení věty. □

Eulerova funkce $\varphi$ přiřazuje přirozenému číslu $n$ počet všech čísel $0 < k \leq n$ nesoudělných s $n$.

**Věta 5.6.** *Platí*

$$\varphi(n) = n \prod_p (1 - \frac{1}{p})$$

*kde $p$ probíhá všechna prvočísla dělící $n$.*

*Důkaz.* Položíme $S = \{1, \ldots, n\}$. $P_p$ bude znamenat, že $p$ dělí $i$. Pak $n(0) = \varphi(n)$ a zřejmě

$$n_{p_1 \ldots p_s} = \frac{n}{p_1 \ldots p_s}$$

Tedy

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i_1 < i_2} \frac{n}{p_{i_1} p_{i_2}} - \cdots =$$

$$n(1 - \sum_i \frac{1}{p_i} + \sum_{i_1 < i_2} \frac{1}{p_{i_1} p_{i_2}} - \ldots) = n \prod_p (1 - \frac{1}{p})$$

□

## 6. Základy teorie grafů

Relace $R$ na množině $A$ se nazývá *ireflexivní*, jestliže platí $(a, a) \notin R$ pro libovolný prvek $a \in A$.

**Definice.** *Graf* $(G, R)$ definujeme jako konečnou množinu $G$ spolu s ireflexivní symetrickou relací $R$ na $G$.

Grafy v našem smyslu jsou právě konečné neorientované grafy bez smyček. Jsou rovněž grafy nekonečné, orientované (relace $R$ není nutně symetrická) a grafy se smyčkami (připouští se i relace, které nejsou ireflexivní).

Námi definovaný graf je právě množina $G$ spolu s množinou $E$ dvouprvkových podmnožin množiny $G$:

$$\{a, b\} \in E \Leftrightarrow (a, b) \in R.$$

Prvky množiny $G$ se nazývají *vrcholy* grafu a prvky množiny $E$ *hrany* grafu. *Stupeň* $s(a)$ vrcholu $a$ grafu $(G, R)$ definujeme jako počet vrcholů $b$ takových, že $(a, b) \in R$.

**Věta 6.1.** $\sum_{a \in G} s(a) = |R|$.

*Důkaz.* Je zřejmý.

**Důsledek 6.2.** *V libovolném grafu je počet vrcholů lichého stupně vždy sudý.*

*Důkaz.* Plyne z 6.1 neboť $|R| = 2|E|$ je sudé číslo. □

*Cesta* v grafu se definuje jako posloupnost $a_1, a_2, \ldots, a_n$ navzájem různých vrcholů taková, že $(a_i, a_{i+1}) \in R$ pro $i = 1, \ldots, n-1$. Říkáme, že tato cesta *spojuje* vrcholy $a_1$ a $a_n$. Pokud nepředpokládáme, že vrcholy $a_i$, $i = 1, \ldots, n-1$ jsou navzájem různé, říkáme, že máme definován *sled* v grafu.

Graf se nazývá *souvislý*, jestliže libovolné dva navzájem různé vrcholy lze v něm spojit cestou. *Kružnice* v grafu $(G,R)$ je posloupnost $a_1, a_2, \ldots, a_n, a_{n+1} = a_1$ vrcholů taková, že $a_1, a_2, \ldots, a_n$ jsou navzájem různé, $n > 2$ a $(a_i, a_{i+1}) \in R$ pro $i = 1, \ldots, n$. *Strom* je souvislý graf bez kružnic.

**Věta 6.3.** *Libovolný strom $(G,R)$ mající aspoň dva vrcholy obsahuje aspoň dva vrcholy stupně 1.*

*Důkaz.* Buď $a_1, \ldots, a_n$ nejdelší cesta v $(G,R)$. Pak $s(a_1) = s(a_n) = 1$ neboť v opačném případě by cesta šla prodloužit. □

**Věta 6.4.** *Souvislý graf $(G,R)$ je strom, právě když $|G| = |E| + 1$.*

*Důkaz.* Buď $(G,R)$ strom. Rovnost $|G| = |E| + 1$ dokážeme indukcí. Pro $|G| = 1$ tvrzení platí. Předpokládejme, že platí pro každý graf o $n$ vrcholech a uvažujme graf $(G,R)$ o $n+1$ vrcholech. Podle 6.3 $G$ obsahuje vrchol $v$ stupně 1. Pak graf $(G' = G - \{v\}, R' = R \cap (G' \times G'))$ je strom. Podle indukčního předpokladu platí $|G'| = |E'| + 1$. Avšak $|G| = |G'| + 1$ a $|E| = |E'| + 1$, takže tvrzení platí i pro graf $(G,R)$.

Opačnou implikaci rovněž dokážeme indukcí. Tvrzení platí pro $|G| = 1$ a předpokládejme, že platí pro všechny grafy o $n$ vrcholech. Buď $(G,R)$ graf o $n+1$ vrcholech takový, že $|G| = |E| + 1$. Pokud $G$ obsahuje vrchol stupně 1, jeho odebráním opět dostaneme graf $(G',R')$ splňující rovnost $|G'| = |E'| + 1$. Podle indukčního předpokladu je tento graf strom, takže stromem je i výchozí graf $(G,R)$. Pokud $G$ neobsahuje vrchol stupně 1, pak platí

$$2|E| = |R| = \sum_{a \in G} s(a) \geq 2|G| = 2|E| + 2,$$

což není možné. □

*Kostra* grafu $(G,R)$ je strom $(G,R')$ takový, že $R' \subseteq R$.

**Věta 6.5.** *Libovolný souvislý graf obsahuje kostru.*

*Důkaz.* Udáme algoritmus nalezení kostry v souvislém grafu $(G,E)$ (pro jeho zadání je výhodnější popsat graf pomocí vrcholů a hran). Postupně volíme hrany $e_1, \ldots, e_n$ tak, že vzniklý graf neobsahuje kružnici. Postup se zastaví, pokud hranu $e_{n+1}$ již nelze přidat. Ukážeme, že vzniklý graf $(G,E_1)$, $E_1 = \{e_1, \ldots, e_n\}$ je strom, t.j., je hledanou kostrou. Podle konstrukce, tento graf neobsahuje kružnici. Musíme ukázat, že je souvislý. Předpokládejme, že tomu tak není, t.j., existují vrcholy $a, b \in G$, které nelze spojit cestou v $(G,E_1)$. Existuje cesta $a = a_1, \ldots, a_k = b$ v $(G,E)$. Buď $i$ nejmenší číslo $i = 1, \ldots, k$ takové, že $a, a_i$ lze spojit cestou v $(G,E_1)$ (nebo $i = 1$) a $a, a_{i+1}$ nelze spojit cestou v $(G,E_1)$. Pak $E_1 \cup \{a_i, a_{i+1}\}$ neobsahuje kružnici, což není možné. □

*Podgraf* grafu $(G,R)$ definujeme jako graf $(G',R')$ takový, že $G \subseteq G'$ a $R \subseteq R'$. Pokud $R' = R \cap (G' \times G')$, pak podgraf $(G',R')$ se nazývá úplný a značíme jej stručně $G'$.

*Komponenta* grafu $(G,R)$ se definuje jako maximální souvislý podgraf $(G',R')$ grafu $(G,R)$. Zřejmě se musí jednat o úplný podgraf.

**Věta 6.6.** *Dvě různé komponenty grafu $(G,R)$ jsou disjunktní.*

*Důkaz.* Tvrzení plyne ze skutečnosti, pokud $G_1$ a $G_2$ jsou úplné souvislé podgrafy grafu $(G,R)$ a $G_1 \cap G_2 \neq \emptyset$, pak podgraf $G_1 \cup G_2$ je souvislý.

**Důsledek 6.7.** *Komponenty grafu $(G,R)$ tvoří rozklad množiny vrcholů $G$.*

*Důkaz.* Plyne z 6.6. a skutečnosti, že libovolný vrchol grafu patří do nějaké komponenty.

Vrchol $v$ souvislého grafu $(G,R)$ se nazývá *artikulace*, pokud úplný podgraf $G - \{v\}$ je nesouvislý. Hrana $\{u,v\}$ souvislého grafu $(G,R)$ se nazývá *most*, pokud graf $(G, E - \{u,v\})$ je nesouvislý.

Graf se nazývá *eulerovský* pokud stupeň libovolného jeho vrcholu je sudé kladné číslo. Sled $a_1,\ldots,a_n$ v grafu se nazývá *tah*, pokud pro libovolnou hranu $e$ grafu existuje nejvýše jedna dvojice $a_i, a_{i+1}$ taková, že $\{a_i, a_{i+1}\} = e$. Tah se nazývá *uzavřený*, pokud $a_1 = a_n$. Řekneme, že graf lze *sestrojit jedním tahem*, pokud v něm existuje tah, v němž se libovolná hrana vyskytuje právě jednou.

**Věta 6.8.** *Graf lze sestrojit jedním uzavřeným tahem, právě když je souvislý a eulerovský.*

*Důkaz.* Jestliže graf lze setrojit jedním tahem, pak musí být souvislý. Navíc nemůže obsahovat vrchol lichého stupně neboť tah do daného vrcholu vstupuje přesně tolikrát, kolikrát z něho vystupuje. Tedy graf je eulerovský.

Naopak, buď $(G,R)$ souvislý eulerovský graf. Zvolme vrchol $v \in G$. Poněvadž graf je souvislý, existuje hrana $\{v,w\}$. Je-li tato hrana most, pak jejím odstraněním dostaneme nesouvislý graf $(G, E - \{v,w\})$, jehož komponenta obsahující $v$ obsahuje právě jeden uzel lichého stupně. To odporuje 6.2. Tedy $\{v,w\}$ není most, takže vrcholy $v$ a $w$ jsou spojeny cestou v grafu $(G, E - \{v,w\})$. Tedy vrchol $v$ leží na kružnici grafu $(G,R)$.

Sestrojená kružnice tvoří uzavřený tah začínající a končící ve vrcholu $v$. Buď $T$ nejdelší uzavřený tah grafu $(G,R)$ začínající a končící ve vrcholu $v$. Buď $(G',E')$ podgraf grafu $(G,R)$ složený ze všech hran grafu $(G,R)$ nepatřících do tahu $T$ a všech uzlů, na nich ležících. Zřejmě $(G',E')$ je eulerovský graf. Poněvadž graf $(G,R)$ je souvislý, existuje vrchol $u$ patřící do $G'$ i do $T$. Poněvadž jsme dokázali, že v eulerovském grafu leží libovolný vrchol na kružnici, existuje kružnice grafu $(G',E')$ obsahující vrchol $u$. Přidáním této kružnice k tahu $T$ dostáváme delší tah, což není možné. Tedy $G' = \emptyset$, čímž je důkaz ukončen. □

Graf se nazývá *rovinný*, jestliže jej lze nakreslit v rovině tak, že hrany se neprotínají (pouze se dotýkají ve vrcholech).