1. Výroková logika

Buď P neprázdná množina symbolů, které nazýváme *atomické výrokové formule.* Symboly *jazyka* L_P výrokové logiky (nad množinou P) jsou prvky množiny P, logické spojky $\neg$ (*negace*), $\rightarrow$ (*implikace*), $\vee$ (*disjunkce*), $\wedge$ (*konjunkce*) a závorky $(,)$.

Výrokové formule jazyka L_P definujeme následovně :

(1) Každá atomická výroková formule je výroková formule.
(2) Je-li A výroková formule, pak $(\neg A)$ je výroková formule.
(3) Jsou-li A, B výrokové formule, pak $(A \vee B)$, $(A \wedge B)$ a $(A \rightarrow B)$ jsou výrokové formule.
(4) Konečná posloupnost symbolů jazyka L_P je výroková formule, právě když vznikne konečným počtem užití pravidel (1)-(3).

Přejděme nyní k definici pravdivosti výrokových formulí.

Pravdivostní ohodnocení atomických výrokových formulí se definuje jako zobrazení $v : P \rightarrow \{0,1\}$. Jeho rozšíření $\overline{v}$ na množinu všech výrokových formulí definujeme následovně :

(1) $\overline{v}(A) = v(A)$ pro libovolné $A \in P$
(2) $\overline{v}(\neg A) = 1$ pokud $v(A) = 0$ a $\overline{v}(A) = 0$ pokud $v(A) = 1$
(3) $\overline{v}(A \rightarrow B) = 0$ pokud $v(A) = 1$ a $v(B) = 0$, ve všech zbývajících případech $\overline{v}(A \rightarrow B) = 1$
(4) $\overline{v}(A \wedge B) = 1$ pokud $v(A) = 1$ a $v(B) = 1$, ve všech zbývajících případech $\overline{v}(A \wedge B) = 0$
(5) $\overline{v}(A \vee B) = 0$ pokud $v(A) = 0$ a $v(B) = 0$; ve všech zbývajících případech $\overline{v}(A \vee B) = 1$.

Výroková formule A se nazývá *pravdivá při ohodnocení* v, jestliže $\overline{v}(A) = 1$. Výroková formule se nazývá *pravdivá*, jestliže je pravdivá při všech ohodnoceních. Píšeme $\models A$.

Budeme rovněž používat výrokovou spojku $\leftrightarrow$ (*ekvivalence*) takovou, že $A \leftrightarrow B$ označuje formuli

$$(A \rightarrow B) \wedge (B \rightarrow A).$$

Symbol T bude označovat vždy pravdivou formuli (t.j., $\overline{v}(T) = 1$ pro libovolné ohodnocení v) a symbol F vždy nepravdivou formuli (t.j., $\overline{v}(F) = 0$ pro libovolné ohodnocení v). Formule A, B se nazývají *ekvivalentní*, pokud formule $A \leftrightarrow B$ je pravdivá. Značíme $A \sim B$.

Algebra výroků (Booleova algebra)

$$A \wedge B \sim B \wedge A$$

$$A \vee B \sim B \vee A$$

$$A \wedge (B \wedge C) \sim (A \wedge B) \wedge C$$

$$A \vee (B \vee C) \sim (A \vee B) \vee C$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

$$A \wedge A \sim A$$
$$A \vee A \sim A$$

$$A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \sim (A \vee B) \wedge (A \vee C)$$

$$A \wedge T \sim A$$
$$A \vee T \sim T$$
$$A \wedge F \sim F$$
$$A \vee F \sim A$$

$$\neg\neg A \sim A$$
$$A \wedge \neg A \sim F$$
$$A \vee \neg A \sim T$$
$$\neg T \sim F$$
$$\neg F \sim T$$

$$\neg(A \wedge B) \sim \neg A \vee \neg B$$
$$\neg(A \vee B) \sim \neg A \wedge \neg B$$

Jedná se o *komutativní*, *asociativní*, *idempotentní* a *distributivní* zákon, vlastnosti jednotky, negace a *de Morganův* zákon.

Výroková formule je v *disjunktivním normálním tvaru*, je-li disjunkcí formulí, v nichž platí:

(a) každá je konjunkcí atomických formulí a jejich negací

(b) v žádné se nevyskytuje žádná atomicka formule současně se svou negací.

Disjunktivní normální tvar se nazýva *úplný* pokud se ve všech konjunkcích vyskytují stejné atomické formule.

Věta 1.1. *Libovolná výroková formule je ekvivalentní formuli v úplném disjunktivním normálním tvaru.*

Důkaz. Mějme výrokovou formuli závisející na atomických výrokových formulích $A_1, \ldots, A_n$. Tato formule určuje zobrazení $f : 2^n \to 2$, kde $2 = \{0, 1\}$. Pro $a = (a_1, \ldots, a_n) \in 2^n$ položíme $A_i^a = A_i$ pokud $a_i = 1$ a $A_i^a = \neg A_i$ pokud $a_i = 0$. Snadno se ověří, že

$$\bigvee\{A_1^a \wedge \ldots A_n^a \backslash a \in 2^n, f(a) = 1\}$$

je hledaný disjunktivní normální tvar. $\square$

Poznámka. Úplný disjunktivní normální tvar formule je určen jednoznačně až na volbu a pořadí proměnných. Za disjunktivní tvar formule F považujeme prázdnou disjunkci (t.j., disjunkci prázdné množiny konjunkcí).

2. Základy predikátové logiky

Jazyk predikátové logiky se skládá z následujících symbolů:
$x_1, x_2 \ldots, x_n, \ldots$ (proměnné)
$\neg, \rightarrow, \vee, \wedge, \leftrightarrow$ (logické spojky)
$\forall, \exists$ (kvantifikátory)
$=$ (rovnost)
$($, $)$ (závorky)
$R_1, \ldots$ (symboly pro relace)

Každému symbolu pro relace je přiřazeno kladné celé číslo, které se nazývá *arita* (nebo také četnost) příslušného symbolu. Podobně jak jazyk výrokové logiky závisí na zadané množině P atomických výrokových formulí, jazyk predikátové logiky závisí na zadání množiny symbolů pro relace.

Atomické formule predikátové logiky jsou výrazy tvaru

$$x_i = x_j$$

kde x_i, x_j jsou proměnné nebo

$$R(x_{i_1}, \ldots x_{i_n})$$

kde R je relační symbol arity n a $x_{i_1}, \ldots x_{i_n}$ jsou proměnné.

Formule predikátové logiky definujeme následovně:

(1) Každá atomická formule je formule.
(2) Jsou-li φ, ψ formule, pak $\neg\varphi, \varphi \rightarrow \psi, \varphi \vee \psi, \varphi \wedge \psi, \varphi \leftrightarrow \psi$ jsou formule.
(3) Je-li x_i proměnná a φ formule, pak $(\forall x_i)\varphi, (\exists x_i)\varphi$ je formule.
(4) Konečná posloupnost symbolů jazyka predikátové logiky je formule, právě když vznikne konečným počtem užití pravidel (1)-(3).

Volné proměnné formule φ definujeme jako formule, na které nepůsobí žádný z kvantifikátorů. (Přitom kvantifikátor $\forall x_i$ nebo $\exists x_i$ působí na libovolný výskyt proměnné x_i ve formuli φ v (3)).

Realizací $\mathcal{M}$ jazyka L predikátové logiky rozumíme neprázdnou množinu M, na níž je zadána n-ární relace $R_{\mathcal{M}}$ pro libovolný relační symbol R arity n jazyka L.

Buď $\varphi(x_{i_1}, \ldots, x_{i_n})$ formule jazyka L predikátové logiky (to znamená, že volné proměnné formule φ jsou $x_{i_1}, \ldots, x_{i_n}$). Buď $\mathcal{M}$ realizace jazyka L a $a_1, \ldots, a_n$ prvky množiny M. Pak lze přirozeným způsobem definovat, že formule φ je *pravdivá* v $\mathcal{M}$ pro prvky $a_1, \ldots, a_n$. Pro atomické formule to je dáno interpretací relačních symbolů jako relací, spojka $\vee$ znamená "nebo", $\wedge$ znamená "a", $\neg$ negaci, $\rightarrow$ implikaci, $\leftrightarrow$ ekvivalenci, $\forall$ "pro všechna" a $\exists$ "existuje".

Predikátová formule $\varphi(x_{i_1}, \ldots, x_{i_n})$ se nazývá pravdivá v realizaci $\mathcal{M}$, jestliže je pravdivá pro všechny prvky $a_1, \ldots, a_n$ v M. Predikátová formule se nazývá pravdivá, je-li pravdivá ve všech realizacích.

Příkladem pravdivé predikátové formule je

$$\neg(\forall x_1)\varphi(x_1) \leftrightarrow (\exists x_1)\neg\varphi(x_1)$$

3. 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*:

$$A \cup M = M$$
$$A \cap M = A$$
$$A \cup \emptyset = A$$
$$A \cap \emptyset = \emptyset$$

$$A \cup A' = M$$
$$A \cap A' = \emptyset$$
$$M' = \emptyset$$
$$\emptyset' = M$$

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

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.

4. 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 4.1. *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. $\square$

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 4.2. (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 ω, $\mathbb{N}$ 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 ω. Podobně jak pro $\mathbb{Z}$ stačí ukázat, že množina $\mathbb{Q}^+$ kladných racionálních čísel má stejnou mohutnost jako ω. 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 ω.

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

Důkaz. Buď $f : X \to \mathcal{P}(X)$ zobrazení. Položme $Y = \{x \in X \backslash x \notin f(x)\}$. 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 ω 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 4.4. *Podmnožina spočetné množiny je buď konečná nebo spočetná.*

Důkaz. Buď X nekonečná podmnožina ω. 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 4.5. *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 4.4. □

Věta 4.6. *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 $h : 2 \to \omega$. Poněvadž f je prosté zobrazení, z 4.3. a 4.4. 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.

5. Relace

Definice. (Binární) *relaci* 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 $f : A \to B$ je odpovídá jako 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 5.1. *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 5.2. *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 5.3. *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
$$g((J_f)_a) = f(a).$$
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. □

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 5.4. *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 $a+d+c+f = c+b+e+f$, $a+f = b+e$ 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

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

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

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

6. 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 $a < b$ 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 *přeuspořádání. 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 6.1. *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 $\bar{a}, \bar{b} \in A \backslash \sim$
$$\bar{a} \leq \bar{b} \Leftrightarrow a \sqsubseteq b,$$

pak $(A\backslash \sim, \leq)$ 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

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

$\square$

Aplikujeme-li Větu 6.1. 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 *isotonní*, 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 *isomorfismus*. 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

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

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

Věta 6.2. *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

$$\mathrm{inf}X = \mathrm{sup}X^-.$$

Zřejmě platí, že inf$X$, jestliže existuje, je supX^-. Je třeba ukázat, že supX^- 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$X^- \in X^-$. $\square$

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 6.3. *(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 $X \in A$ 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 6.4. *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 6.5. Právě sestrojený pevný bod je zřejmě nejmenším pevným bodem f. Ve Větě 6.4. by stačilo předpokládat, že f zachovává suprema řetězců. Význam tohoto obecnějšího tvrzení je vidět z následujícího příkladu.

Příklad 6.6. 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 6.4) 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 6.7. *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 6.5 obecně neplatí. Svazy, v nichž tato rovnost platí, se nazývají distributivní.

Podobně jak v 6.5 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 $\mathbb{Q}$

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

(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

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

7. 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 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 7.1. *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 7.1. ihned plyne, že počet permutací n-prvkové množiny je n^n.

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

Věta 7.2. *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 7.1. □

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) $\sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$

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

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

(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 7.3. *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. $\square$

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

Věta 7.4. (princip inkluze a exkluze).

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

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 $\sum\limits_i n_i$, takže jeho příspěvek k pravé straně je 0. Stačí, když ukážeme, že totéž nastane pro pro libovolný prvek mající právě vlastnosti $P_{j_1}, \ldots, P_{j_r}$. Takový prvek přispívá jedničkou do každého součtu

$$\sum_{i_1 < \cdots < i_s} n_{i_1 \ldots i_s}$$

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

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

$\square$

Jako aplikaci principu inkluze a exkluze si uvedeme následující tvrzení.

Věta 7.5. *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 $a_1, \ldots, a_k$. 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 $n_{i_1 \ldots i_s}$ je rovno počtu zobrazení m-prvkové množiny do množiny $\{a_i \backslash i \neq i_1, \ldots, i_s\}$, t.j., $(k-s)^m$. Tedy

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

Odsud plyne tvrzení věty. $\square$

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

Věta 7.6. *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

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

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

□