Matematická logika

Rostislav Horčík

horcik@math.feld.cvut.cz
horcik@cs.cas.cz
www.cs.cas.cz/~horcik

Informace k předmětu

- Osnova + požadavky: `math.feld.cvut.cz` -> Seznam předmětů -> Matematická logika
- Informace k přednášce: `www.cs.cas.cz/~horcik`

Literatura

- M. Demlová, B. Pondělíček: Matematická logika. Skripta ČVUT FEL.
- J. Velebil: Velmi jemný úvod do matematické logiky. Ke stažení na `math.feld.cvut.cz/velebil/teaching/y01mlo.html`

Množiny

- Množina je “souhrn, nebo soubor” navzájem rozlišitelných objektů, kterým říkáme prvky. Fakt, že prvek x patří do množiny A značíme $x \in A$. Opak značíme $x \notin A$.

Množiny

- Množina je "souhrn, nebo soubor" navzájem rozlišitelných objektů, kterým říkáme prvky. Fakt, že prvek x patří do množiny A značíme $x \in A$. Opak značíme $x \notin A$.
- Množinu můžeme zadat výčtem, tj. vypíšeme (naznačíme) její prvky, např.

$$A = \{3, 6, w, \{\pi\}\}, \qquad S = \{0, 2, 4, 6, 8, \ldots\}.$$

Množiny

- Množina je “souhrn, nebo soubor” navzájem rozlišitelných objektů, kterým říkáme prvky. Fakt, že prvek x patří do množiny A značíme $x \in A$. Opak značíme $x \notin A$.
- Množinu můžeme zadat výčtem, tj. vypíšeme (naznačíme) její prvky, např.

$$A = \{3, 6, w, \{\pi\}\}, \qquad S = \{0, 2, 4, 6, 8, \dots\}.$$

- Je-li V vlastnost, pak množinu C všech prvků x s vlastností V (a žádných jiných) zapisujeme

$$C = \{x \mid x \text{ má vlastnost } V\}.$$

Např. množina všech lichých přirozených čísel

$$L = \{m \mid m = 2k + 1,\ k \in \mathbb{N}\}.$$

Princip extensionality

Množiny S a T jsou si rovny ($S = T$) právě tehdy, když každý prvek množiny S je prvkem T a naopak každý prvek T je prvkem S.

$$A = \{\alpha, \beta, \gamma\} = \{\gamma, \alpha, \beta\} = \{\beta, \beta, \gamma, \alpha, \alpha, \alpha\}.$$

Princip extensionality

Množiny S a T jsou si rovny ($S = T$) právě tehdy, když každý prvek množiny S je prvkem T a naopak každý prvek T je prvkem S.

$$A = \{\alpha, \beta, \gamma\} = \{\gamma, \alpha, \beta\} = \{\beta, \beta, \gamma, \alpha, \alpha, \alpha\}.$$

Definice

Mějme dvě množiny S a T. Jestliže každý prvek množiny S je také prvkem množiny T, říkáme, že S je podmnožina T a píšeme $S \subseteq T$.

Princip extensionality

Množiny S a T jsou si rovny ($S = T$) právě tehdy, když každý prvek množiny S je prvkem T a naopak každý prvek T je prvkem S.

$$A = \{\alpha, \beta, \gamma\} = \{\gamma, \alpha, \beta\} = \{\beta, \beta, \gamma, \alpha, \alpha, \alpha\}\,.$$

Definice

Mějme dvě množiny S a T. Jestliže každý prvek množiny S je také prvkem množiny T, říkáme, že S je podmnožina T a píšeme $S \subseteq T$.

Pozorování

$S = T$ právě tehdy, když $S \subseteq T$ a současně $T \subseteq S$.

Operace s množinami

- $\emptyset$ značí prázdnou množinu. $\emptyset \subseteq A$ pro každou množinu A.

Operace s množinami

- $\emptyset$ značí prázdnou množinu. $\emptyset \subseteq A$ pro každou množinu A.
- Mějme množiny A, B.

$$
\begin{aligned}
A \cup B &= \{x \mid x \in A \text{ nebo } x \in B\} && \text{sjednocení,}\\
A \cap B &= \{x \mid x \in A \text{ a } x \in B\} && \text{průnik,}\\
A - B &= \{x \mid x \in A \text{ a } x \notin B\} && \text{rozdíl.}
\end{aligned}
$$

Operace s množinami

- $\emptyset$ značí prázdnou množinu. $\emptyset \subseteq A$ pro každou množinu A.
- Mějme množiny A, B.

$$\begin{array}{ll} A \cup B = \{x \mid x \in A \text{ nebo } x \in B\} & \text{sjednocení,} \\ A \cap B = \{x \mid x \in A \text{ a } x \in B\} & \text{průnik,} \\ A - B = \{x \mid x \in A \text{ a } x \notin B\} & \text{rozdíl.} \end{array}$$

- Kartézský součin množin A, B

$$A \times B = \{(a, b) \mid a \in A, b \in B\},$$
$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Když $A_1 = \cdots = A_n$ pak $A_1 \times \cdots \times A_n$ značíme A^n.

Operace s množinami

- $\emptyset$ značí prázdnou množinu. $\emptyset \subseteq A$ pro každou množinu A.
- Mějme množiny A, B.

$$
\begin{array}{ll}
A \cup B = \{x \mid x \in A \text{ nebo } x \in B\} & \text{sjednocení,} \\
A \cap B = \{x \mid x \in A \text{ a } x \in B\} & \text{průnik,} \\
A - B = \{x \mid x \in A \text{ a } x \notin B\} & \text{rozdíl.}
\end{array}
$$

- Kartézský součin množin A, B

$$
\begin{aligned}
A \times B &= \{(a, b) \mid a \in A, b \in B\}\,, \\
A_1 \times \cdots \times A_n &= \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}\,.
\end{aligned}
$$

Když $A_1 = \cdots = A_n$ pak $A_1 \times \cdots \times A_n$ značíme A^n.

- Potenční množina $P(A)$ množiny A

$$P(A) = \{B \mid B \subseteq A\}\,. \quad \text{(jiné značení: } 2^A, \exp(A))$$

Relace

Definice

Nechť $A_1, \ldots, A_n$ jsou množiny a $R \subseteq A_1 \times \cdots \times A_n$. Pak R nazýváme *n-ární relací*. Pro $n = 1, 2, 3$ říkáme, že R je *unární, binární, ternární* relace. Jestliže $A_1 = \cdots = A_n$, mluvíme o relaci R *na množině A*.

Relace

Definice

Nechť $A_1, \ldots, A_n$ jsou množiny a $R \subseteq A_1 \times \cdots \times A_n$. Pak R nazýváme n-ární relací. Pro $n = 1, 2, 3$ říkáme, že R je unární, binární, ternární relace. Jestliže $A_1 = \cdots = A_n$, mluvíme o relaci R na množině A.

Konvence

Mějme binární relaci R. Fakt, že $(a, b) \in R$, budeme také zapisovat zkráceně jako $a\ R\ b$.

Příklady - relační databáze

- $L =$ množina jmen lidí v ČR, $T =$ množina jejich telefonních čísel, $A =$ množina jejich adres.
- Označme $M = L \cup T \cup A$.
- Pak telefonní seznam je ternární relace $R \subseteq M^3$ taková, že

$$(x, y, z) \in R \text{ p.t.k. člověk jména } x \text{ má telefonní číslo } y \text{ a adresu bydliště } z.$$

jméno	tel.	adresa
$\vdots$	$\vdots$	$\vdots$
x	y	z
$\vdots$	$\vdots$	$\vdots$

- Množiny L, T, A jsou příklady unárních relací na M.

Příklady binárních relací

- Být menší nebo rovno. Jedná se např. o relaci $\leq$ na množině všech přirozených čísel $\mathbb{N}$, kde $(m, n) \in \leq$ (tj. $m \leq n$) právě tehdy, když m je menší nebo rovno n.

Příklady binárních relací

- Být menší nebo rovno. Jedná se např. o relaci $\leq$ na množině všech přirozených čísel $\mathbb{N}$, kde $(m, n) \in \leq$ (tj. $m \leq n$) právě tehdy, když m je menší nebo rovno n.

- Být podmnožinou. Jedná o relaci $\subseteq$ na potenční množině $P(U)$ pro nějakou množinu U. Pro dvě množiny $X, Y \in P(U)$ platí: $(X, Y) \in \subseteq$ (tj. $X \subseteq Y$) právě tehdy, když množina X je podmnožinou množiny Y.

Příklady binárních relací

- Být menší nebo rovno. Jedná se např. o relaci $\leq$ na množině všech přirozených čísel $\mathbb{N}$, kde $(m, n) \in \leq$ (tj. $m \leq n$) právě tehdy, když m je menší nebo rovno n.

- Být podmnožinou. Jedná o relaci $\subseteq$ na potenční množině $P(U)$ pro nějakou množinu U. Pro dvě množiny $X, Y \in P(U)$ platí: $(X, Y) \in \subseteq$ (tj. $X \subseteq Y$) právě tehdy, když množina X je podmnožinou množiny Y.

Definice

Relace $f \subseteq A \times B$ se nazývá zobrazení z množiny A do množiny B, pokud pro každé $a \in A$ existuje právě jedno $b \in B$ takové, že $(a, b) \in f$. Toto jedno b značíme $f(a)$.

Znázornění relací

Nechť

$$A = \{a, b, c\}\,, \qquad B = \{0, 1, 2, 3\}\,,$$

$$R = \{(a, 0), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1))\}\,.$$

- Charakteristickou funkcí

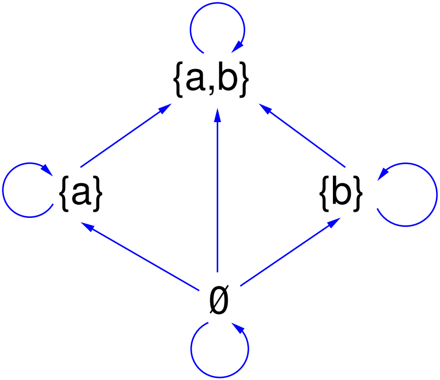
	0	1	2	3
a	1	0	0	1
b	0	1	1	1
c	0	1	0	0

- Orientovaným grafem

Příklad - podmnožiny dvouprvkové množiny

- $A = \{a, b\}$, $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

$$\begin{aligned}\subseteq \quad = \quad & \{(\emptyset,\emptyset),(\emptyset,\{a\}),(\emptyset,\{b\}),(\emptyset,\{a,b\}),(\{a\},\{a\}),(\{a\},\{a,b\}),\\ & (\{b\},\{b\}),(\{b\},\{a,b\}),(\{a,b\},\{a,b\})\}\,.\end{aligned}$$



Operace s relacemi

- Množinové operace. Sjednocení, průnik, doplněk.

Operace s relacemi

- Množinové operace. Sjednocení, průnik, doplněk.
- Inversní relace. Mějme binární relaci $R \subseteq A \times B$. Pak inversní relací k relaci R je relace $R^{-1} \subseteq B \times A$ definovaná takto:

$$x \; R^{-1} \; y \quad \text{právě tehdy, když} \quad y \; R \; x \, .$$

Operace s relacemi

- Množinové operace. Sjednocení, průnik, doplněk.
- Inversní relace. Mějme binární relaci $R \subseteq A \times B$. Pak inversní relací k relaci R je relace $R^{-1} \subseteq B \times A$ definovaná takto:

$$x \; R^{-1} \; y \quad \text{právě tehdy, když} \quad y \; R \; x\,.$$

- Skládání relací. Mějme binární relace $R \subseteq A \times B$ a $S \subseteq B \times C$. Pak složená relace $R \circ S \subseteq A \times C$ definovaná předpisem:

$$a \; R \circ S \; c \quad \text{právě tehdy, když existuje } b \in B \text{ takové, že}$$

$$a \, R \, b \quad \text{a} \quad b \, S \, c\,.$$

Příklad - skládání binárních relací

- Nechť A je množina nějakých obcí.

Příklad - skládání binárních relací

- Nechť A je množina nějakých obcí.
- Definujme binární relaci R na A takto:

$a\ R\ b$ právě tehdy, když obce a, b jsou spojeny přímou cestou nebo $a = b$.

Příklad - skládání binárních relací

- Nechť A je množina nějakých obcí.
- Definujme binární relaci R na A takto:

  $a\ R\ b$ právě tehdy, když obce a, b jsou spojeny přímou cestou nebo $a = b$.
- $R \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes jednu obec.

Příklad - skládání binárních relací

- Nechť A je množina nějakých obcí.
- Definujme binární relaci R na A takto:

  $a\ R\ b$ právě tehdy, když obce a, b jsou spojeny přímou cestou nebo $a = b$.

- $R \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes jednu obec.
- $(R \circ R) \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes dvě obce.

Příklad - skládání binárních relací

- Nechť A je množina nějakých obcí.
- Definujme binární relaci R na A takto:

  $a\ R\ b$ právě tehdy, když obce a, b jsou spojeny přímou cestou nebo $a = b$.
- $R \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes jednu obec.
- $(R \circ R) \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes dvě obce.
- $R \circ (R \circ R) = (R \circ R) \circ R$.

Příklad - skládání binárních relací

- Nechť A je množina nějakých obcí.
- Definujme binární relaci R na A takto:

  $a\ R\ b$ právě tehdy, když obce a, b jsou spojeny přímou cestou nebo $a = b$.

- $R \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes jednu obec.
- $(R \circ R) \circ R$ dává do relace obce, které jsou spojeny cestou maximálně přes dvě obce.
- $R \circ (R \circ R) = (R \circ R) \circ R$.
- $\underbrace{R \circ \cdots \circ R}_{n-\text{krát}}$ dává do relace obce, které jsou spojeny cestou maximálně přes $n - 1$ obcí.

Vlastnosti skládání

Tvrzení

Skládání relací je asociativní. Přesněji, je-li $R \subseteq A \times B$, $S \subseteq B \times C$ a $T \subseteq C \times D$, pak platí

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

Vlastnosti skládání

Tvrzení

Skládání relací je asociativní. Přesněji, je-li $R \subseteq A \times B$, $S \subseteq B \times C$ a $T \subseteq C \times D$, pak platí

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

Pozorování

Skládání relací není komutativní.

Např. pro $R = \{(a, a), (b, a)\}$ a $S = \{(a, b), (b, a)\}$ relace na $\{a, b\}$ máme $R \circ S \neq S \circ R$.

Vlastnosti relací na množině

Řekneme, že binární relace R na množině A (tj. $R \subseteq A^2$) je

- reflexivní, jestliže pro všechna $a \in A$ platí $a\,R\,a$;

Vlastnosti relací na množině

Řekneme, že binární relace R na množině A (tj. $R \subseteq A^2$) je

- reflexivní, jestliže pro všechna $a \in A$ platí $a \mathrel{R} a$;

- symetrická, jestliže pro všechna $a, b \in A$ platí:

  je-li $a \mathrel{R} b$, pak také $b \mathrel{R} a$;

Vlastnosti relací na množině

Řekneme, že binární relace R na množině A (tj. $R \subseteq A^2$) je

- reflexivní, jestliže pro všechna $a \in A$ platí $a \, R \, a$;
- symetrická, jestliže pro všechna $a, b \in A$ platí:

  je-li $a \, R \, b$, pak také $b \, R \, a$;
- antisymetrická, jestliže pro všechna $a, b \in A$ platí:

  je-li $a \, R \, b$ a $b \, R \, a$, pak $a = b$;

Vlastnosti relací na množině

Řekneme, že binární relace R na množině A (tj. $R \subseteq A^2$) je

- reflexivní, jestliže pro všechna $a \in A$ platí $a \, R \, a$;
- symetrická, jestliže pro všechna $a, b \in A$ platí:

  je-li $a \, R \, b$, pak také $b \, R \, a$;
- antisymetrická, jestliže pro všechna $a, b \in A$ platí:

  je-li $a \, R \, b$ a $b \, R \, a$, pak $a = b$;
- tranzitivní, jestliže pro všechna $a, b, c \in A$ platí:

  je-li $a \, R \, b$ a $b \, R \, c$, pak $a \, R \, c$.

Ekvivalence a uspořádání

Definice

Binární relace R na množině A se nazývá:

- ekvivalence na A, pokud je reflexivní, symetrická a tranzitivní,
- (částečné) uspořádání na A, pokud je reflexivní, antisymetrická a tranzitivní.

Ekvivalence a uspořádání

Definice

Binární relace R na množině A se nazývá:

- ekvivalence na A, pokud je reflexivní, symetrická a tranzitivní,
- (částečné) uspořádání na A, pokud je reflexivní, antisymetrická a tranzitivní.

Příklad

- Mějme rovinu bodů $\mathbb{R}^2$. Pak relace definovaná $(x, y)\ E\ (u, v)$ pokud $x^2 + y^2 = u^2 + v^2$ je ekvivalence na $\mathbb{R}^2$.

Ekvivalence a uspořádání

Definice

Binární relace R na množině A se nazývá:

- ekvivalence na A, pokud je reflexivní, symetrická a tranzitivní,
- (částečné) uspořádání na A, pokud je reflexivní, antisymetrická a tranzitivní.

Příklad

- Mějme rovinu bodů $\mathbb{R}^2$. Pak relace definovaná $(x, y)\ E\ (u, v)$ pokud $x^2 + y^2 = u^2 + v^2$ je ekvivalence na $\mathbb{R}^2$.
- Nechť A je množina. Pak relace $\subseteq$ na $P(A)$ je uspořádání.

Ekvivalence a uspořádání

Definice

Binární relace R na množině A se nazývá:

- ekvivalence na A, pokud je reflexivní, symetrická a tranzitivní,
- (částečné) uspořádání na A, pokud je reflexivní, antisymetrická a tranzitivní.

Příklad

- Mějme rovinu bodů $\mathbb{R}^2$. Pak relace definovaná $(x, y)\ E\ (u, v)$ pokud $x^2 + y^2 = u^2 + v^2$ je ekvivalence na $\mathbb{R}^2$.
- Nechť A je množina. Pak relace $\subseteq$ na $P(A)$ je uspořádání.
- Nechť A je množina. Pak relace $I_A = \{(x, x) \mid x \in A\}$ je ekvivalence i uspořádání.

Třídy ekvivalence

Definice

Je dána relace ekvivalence R na množině A. Třídou ekvivalence R odpovídající prvku $a \in A$ nazýváme množinu

$$R[a] = \{b \in A \mid a\ R\ b\}\,, \quad \text{(jiná značení: } [a]_R,\ a/R)$$

Množinu všech tříd dané ekvivalence, tj. množinu $\{R[a] \mid a \in A\}$ často nazýváme faktorovou množinou podle ekvivalence R a značíme A/R.

Třídy ekvivalence

Tvrzení

Nechť R je ekvivalence na množině A. Množina tříd ekvivalence $\{R[a] \mid a \in A\}$ má tyto vlastnosti:

- Každý prvek $a \in A$ leží v $R[a]$ a platí rovnost $\bigcup\{R[a] \mid a \in A\} = A$.
- Třídy ekvivalence $R[a]$ jsou po dvou disjunktní, tj. jestliže $R[a] \cap R[b] \neq \emptyset$, pak $R[a] = R[b]$.

Rozklad

Definice

Mějme neprázdnou množinu A. Množina $\mathcal{S}$ neprázdných podmnožin množiny A se nazývá rozklad množiny A, jestliže jsou splněny následující podmínky:

- Každý prvek $a \in A$ leží v některé podmnožině z $\mathcal{S}$, tj. $\bigcup \mathcal{S} = A$.
- Prvky množiny $\mathcal{S}$ jsou po dvou disjunktní; tj. jestliže $X \cap Y \neq \emptyset$, pak $X = Y$ pro všechna $X, Y \in \mathcal{S}$.

Rozklad

Tvrzení

Nechť $\mathcal{S}$ je rozklad množiny A. Pak relace $R_{\mathcal{S}}$ definovaná:

$$a\ R_{\mathcal{S}}\ b \quad \text{právě tehdy, když } a, b \in X \text{ pro nějaké } X \in \mathcal{S}$$

je ekvivalence na množině A.

Rozklad

Tvrzení

Nechť $\mathcal{S}$ je rozklad množiny A. Pak relace $R_{\mathcal{S}}$ definovaná:

$$a \, R_{\mathcal{S}} \, b \quad \text{právě tehdy, když } a, b \in X \text{ pro nějaké } X \in \mathcal{S}$$

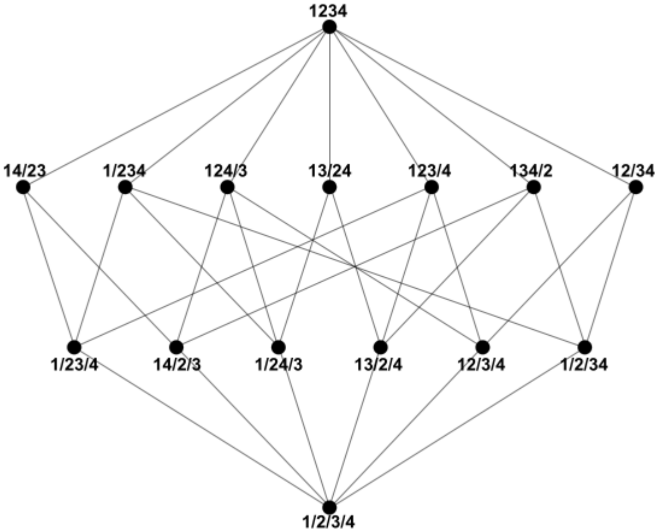
je ekvivalence na množině A.

Poznámka

$$R \longrightarrow A/R \longrightarrow R_{A/R} = R$$

$$\mathcal{S} \longrightarrow R_{\mathcal{S}} \longrightarrow A/R_{\mathcal{S}} = \mathcal{S}$$

Příklad - rozklady množiny $\{1, 2, 3, 4\}$



Největší a maximální prvek

Definice

Mějme množinu A a na ní relaci uspořádání $\preceq$.

- Řekneme, že prvek $a \in A$ je největší prvek množiny A, jestliže pro všechny prvky $x \in A$ platí $x \preceq a$.
- Řekneme, že prvek $b \in A$ je maximální prvek množiny A, jestliže neexistuje prvek $y \in A$, $y \neq b$, takový, že $b \preceq y$.

Největší a maximální prvek

Definice

Mějme množinu A a na ní relaci uspořádání $\preceq$.

- Řekneme, že prvek $a \in A$ je největší prvek množiny A, jestliže pro všechny prvky $x \in A$ platí $x \preceq a$.
- Řekneme, že prvek $b \in A$ je maximální prvek množiny A, jestliže neexistuje prvek $y \in A$, $y \neq b$, takový, že $b \preceq y$.

Tvrzení

Mějme množinu A a na ní uspořádání. Množina A má nejvýše jeden největší prvek; navíc, je-li a největší prvek množiny A, pak je jediným maximálním prvkem množiny A. Nemá-li množina A největší prvek, může mít několik maximálních prvků, anebo žádný.

Nejmenší a minimální prvek

Definice

Mějme množinu A a na ní relaci uspořádání $\preceq$.

- Řekneme, že prvek $a \in A$ je nejmenší prvek množiny A, jestliže pro všechny prvky $x \in A$ platí $a \preceq x$.
- Řekneme, že prvek $b \in A$ je minimální prvek množiny A, jestliže neexistuje prvek $y \in A$, $y \neq b$, takový, že $y \preceq b$.

Nejmenší a minimální prvek

Definice

Mějme množinu A a na ní relaci uspořádání $\preceq$.

- Řekneme, že prvek $a \in A$ je nejmenší prvek množiny A, jestliže pro všechny prvky $x \in A$ platí $a \preceq x$.
- Řekneme, že prvek $b \in A$ je minimální prvek množiny A, jestliže neexistuje prvek $y \in A$, $y \neq b$, takový, že $y \preceq b$.

Tvrzení

Mějme množinu A a na ní uspořádání. Množina A má nejvýše jeden nejmenší prvek; navíc, je-li a nejmenší prvek množiny A, pak je jediným minimálním prvkem množiny A. Nemá-li množina A nejmenší prvek, může mít několik minimálních prvků, anebo žádný.