Úvod do teoretické informatiky

Zdeněk Sawa

Katedra informatiky, FEI,
Vysoká škola báňská – Technická universita Ostrava
17. listopadu 15, Ostrava-Poruba 708 33
Česká republika

8. února 2012

Přednášející

Garant předmětu:

Jméno: Ing. Zdeněk Sawa, Ph.D.

E-mail: zdenek.sawa@vsb.cz

Místnost: A1024

Další přednášející:

- Mgr. Marek Menšík, Ph.D. (logika)

WWW stránky

Webové stránky k předmětu naleznete na adrese:

http://www.cs.vsb.cz/sawa/uti

Na těchto stránkách najdete:

- Informace o předmětu
- Učební texty
- Slidy z přednášek
- Zadání příkladů na cvičení
- Aktuální informace
- Animace

Požadavky

- **Zápočet** (22 bodů):
  - Zápočtová písemka (22 bodů) — bude se psát na přednášce (pravděpodobně na 9. přednášce).

  Minimum pro získání zápočtu je 7 bodů.

- **Zkouška** (78 bodů)
  - Písemná zkouška skládající se ze tří částí po 26 bodech, přičemž z každé části je nutné získat nejméně 10 bodů.

Uznané zápočty

- Studenti, kteří předmět opakují a mají nárok na uznání zápočtu, ale **nemají** ho dosud v Edisonu zapsaný a **chtějí** ho uznat, musí v průběhu prvních dvou týdnů semestru požádat svého cvičícího o uznání zápočtu.
- Podobně studenti, kteří mají nárok na uznání zápočtu, **mají** v Edisonu zapsaný, ale **nechtějí** ho uznat, musí v průběhu prvních dvou týdnů semestru požádat svého cvičícího o jeho zrušení.
- Studenti, kteří mají uznaný zápočet, nebudou psát zápočtovou písemku.

Náplň předmětu

Cílem tohoto předmětu je poskytnout studentům stručný úvod do následujících oblastí:

- **Logika**
- **Formální jazyky a automaty**
- **Vyčíslitelnost a složitost**

Výukové materiály

Hlavními výukovými texty jsou:

- prof. RNDr. Petr Jančar, CSc.
  Úvod do teoretické informatiky (učební text),
  VŠB-TU Ostrava, 2007.

  Poznámka: Pro zájemce s hlubším zájmem o problematiku je k dispozici i rozšířená verze tohoto textu určená pro studenty magisterského studia (pro předmět Teoretická informatika).

- doc. RNDr. Marie Duží, CSc.
  Matematická logika (učební text),
  VŠB-TU Ostrava, 2003.

Výukové materiály

Kromě výukových textů jsou k dispozici:

- **Slidy** z přednášek (na web budou doplňovány aktuální verze)
- **Animace** vytvořené M. Kotem, Z. Sawou a některými studenty v rámci diplomových prací
- **Zadání příkladů do cvičení**

Další literatura (pro zájemce)

- M. Sipser: *Introduction to the Theory of Computation*, PWS Publishing Company, 1997.
- D. Kozen: *Automata and Computability*, Undergraduate Text in Computer Science, Springer Verlag, 1997.
- Ch. Papadimitriou: *Computational Complexity*, Addison-Wesley, 1993.
- J. E. Hopcroft, R. Motwani, J. D. Ullman: *Introduction to Automata Theory, Languages, and Computation* (3rd Edition), Addison Wesley, 2006.
- H.D. Ebbinghaus, J. Flum, W. Thomas: *Mathematical Logic* (2nd edition), Springer, 1994.
- M. Huth, M. Ryan.: *Logic in Computer Science: Modelling and Reasoning about Systems*, Cambridge University Press, 2004.
- V. Švejdar: *Logika - neúplnost, složitost a nutnost*, Academia, 2002.

Další literatura (pro zájemce)

- Ding-Zhu Du, Ker-I Ko: *Problem Solving in Automata, Languages, and Complexity*, Wiley, 2001. Pozn.: v rámci sítě VŠB je tato publikace dostupná v elektronické podobě (jako PDF) na adrese `http://knihovna.vsb.cz/sluzby/e-knihy-wiley.htm`

Cvičení

- Zadání příkladů budou zveřejňována předem.
- Očekává se, že se studenti předem pokusí je sami vyřešit.
- Na cvičení se budou řešit především problémy a nejasnosti, na které při řešení narazí.
- Studenti jsou povinni si zadání předem vytisknout a donést na cvičení.
- Cvičení nejsou náhradou přednášek a samostudia.

Základní pojmy

Množiny

Množina – kolekce vzájemně odlišitelných objektů, které nazýváme jejími **prvky**.

- $x \in S$ – objekt x je prvkem množiny S
- $x \notin S$ – objekt x není prvkem množiny S

Jednou z možností, jak popsat množinu, je explicitně vyjmenovat všechny její prvky, např.:

$$S = \{1, 2, 3\}$$

Množina nemůže obsahovat prvek více než jednou a prvky množiny nejsou nijak seřazeny.

Množiny

Množiny A a B jsou si **rovny** ($A = B$), jestliže obsahují tytéž prvky.

Například

$$\{1, 2, 3\} = \{2, 1, 3\} = \{3, 2, 1\}$$

Množina neobsahující žádné prvky se nazývá **prázdná množina** a označuje se symbolem $\emptyset$.

Poznámka: Kromě množin se také někdy používají **multimnožiny**. Na rozdíl od množiny může multimnožina obsahovat více výskytů jednoho prvku.

$$M = \{1, 1, 1, 2, 3, 3, 3, 3, 3\}$$

Množiny

Příklady některých důležitých množin:

- $\mathbb{N}$ – množina všech **přirozených** čísel, tj. $\mathbb{N} = \{0, 1, 2, \ldots\}$,
- $\mathbb{N}_+$ – množina všech **kladných přirozených** čísel, tj. $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$,
- $\mathbb{Z}$ – množina všech **celých** čísel, tj. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
- $\mathbb{Q}$ – množina všech **racionálních** čísel (zlomky),
- $\mathbb{R}$ – množina všech **reálných** čísel.

Množiny

- $A \subseteq B$ – označuje, že A je **podmnožinou** B, tj.

$$\forall x(x \in A \Rightarrow x \in B)$$

(každý prvek množiny A patří rovněž do množiny B).

- $A \subset B$ – označuje, že A je **vlastní podmnožinou** B, tj.

$$A \subseteq B \ \wedge \ \exists x(x \in B \wedge x \notin A)$$

(tj. $A \subseteq B$, ale $A \neq B$).

Poznámka: Někdy se též používá zápis $A \subset B$ pro označení, že A je podmnožinou B (tj. připouští i možnost $A = B$), a zápis $A \subsetneq B$ pro označení, že A je vlastní podmnožinou B.

Množiny

Pro danou množinu A můžeme definovat množinu $B \subseteq A$ tvořenou těmi prvky množiny A, které mají určitou vlastnost (splňují nějakou podmínku) $\varphi(x)$.

$$B = \{x \in A \mid \varphi(x)\}$$

Příklad: Podmnožina X množiny přirozených čísel $\mathbb{N}$ tvořená těmi čísly, která dávají po dělení pěti zbytek dvě.

$$X = \{x \in \mathbb{N} \mid x \bmod 5 = 2\}$$

Množiny

Množinové operace:

- **Průnik** množin A a B je množina

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

- **Sjednocení** množin A a B je množina

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

- **Rozdíl** množin A a B je množina

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Poznámka: Pro rozdíl množin se též používá zápis $A \setminus B$.

Příklad: Jestliže $A = \{a, b, c, d\}$ a $B = \{b, c, e, f\}$, pak

$$A \cap B = \{b, c\}, \qquad A \cup B = \{a, b, c, d, e, f\}, \qquad A - B = \{a, d\}.$$

Množiny

Někdy jsou všechny množiny, které uvažujeme, podmnožinami nějaké jedné množiny U nazývané **universum**.

Příklad: Pokud se například bavíme o množinách přirozených čísel, pak je universem množina $\mathbb{N}$.

Pro dané universum U definujeme **doplněk** množiny A jako

$$\overline{A} = U - A$$

Pro libovolné množiny $A, B \subseteq U$ platí de Morganova pravidla:

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \qquad \overline{A \cup B} = \overline{A} \cap \overline{B}$$

Množiny A a B jsou **disjunktní**, jestliže nemají žádný společný prvek, tj. jestliže $A \cap B = \emptyset$.

Množiny

Velikost dané množiny S se nazývá její **kardinalita** a označuje se $|S|$.

- V případě **konečné** množiny, je její kardinalita přirozené číslo odpovídající počtu jejích prvků, např. $|\emptyset| = 0$.
- Dvě (obecné) množiny mají stejnou kardinalitu, jesliže existuje bijekce (tj. vzájemně jednoznačné zobrazení) mezi jejich prvky.
- Množina S se nazývá **spočetná**, jestliže existuje bijekce mezi S a $\mathbb{N}$. Spočetné množiny jsou „nejmenší“ mezi nekonečnými množinami.
- Nekonečná množina, která není spočetná, se nazývá **nespočetná**.

Příklad: Množiny $\mathbb{N}$, $\mathbb{Z}$ a $\mathbb{Q}$ jsou spočetné, množina $\mathbb{R}$ je nespočetná.

Množiny

Množina všech podmnožin množiny S se nazývá **potenční množina** množiny S a označuje se zápisem $\mathcal{P}(S)$.

Příklad: Pokud $S = \{a, b, c\}$, pak

$$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Pokud je množina S konečná, pak $|\mathcal{P}(S)| = 2^{|S|}$.

Poznámka: Často se také používá pro označení potenční množiny místo $\mathcal{P}(S)$ výraz 2^S.

Množiny

Uspořádaná dvojice prvků a a b se označuje (a, b).

Na rozdíl od množiny u uspořádané dvojice záleží na pořadí prvků, (a, b) je něco jiného než (b, a).

Poznámka: Formálně je možno uspořádanou dvojici (a, b) pomocí množin např. takto:

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

Analogicky můžeme definovat uspořádané trojice, čtveřice atd.

Kartézský součin množin A a B, označovaný $A \times B$, je množina všech uspořádaných dvojic, kde první prvek z dvojice patří do množiny A a druhý do množiny B:

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

Příklad: $\{a, b\} \times \{a, b, c\} = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c)\}$

Množiny

Jestliže A a B jsou konečné množiny, pak $|A \times B| = |A| \cdot |B|$.

Kartézský součin n množin $A_1, A_2, \ldots, A_n$ je množina ***n*-tic**

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ i = 1, 2, \ldots, n\}$$

Jestliže všechna A_i jsou konečné množiny, platí

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$$

Místo kartézského součinu $A \times A \times \cdots \times A$, kde se množina A vyskytuje n krát, píšeme A^n.

Pro konečnou množinu A platí $|A^n| = |A|^n$.

Relace

Relace na množinách $A_1, A_2, \ldots, A_n$ je libovolná podmnožina kartézského součinu $A_1 \times A_2 \times \cdots \times A_n$.

Relace na n množinách se nazývá **n-ární** relace.

Jestliže $n = 2$, jedná se o **binární** relaci.
Jestliže $n = 3$, jedná se o **ternární** relaci.

V případě, že $A_1 = A_2 = \cdots = A_n$, hovoříme o **homogenní** relaci, v opačném případě o relaci **heterogenní**.

Když říkáme, že R je n-ární relace na množině A, máme tím na mysli, že $R \subseteq A^n$.

Relace

Příklad: Relace „menší než“ na množině přirozených čísel je množina

$$\{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a < b\}$$

Poznámka: Jestliže $R \subseteq A \times B$ je binární relace, někdy místo $(a, b) \in R$ používáme infixový zápis a píšeme $a\ R\ b$.

Relace

Binární relace $R \subseteq A \times A$ je:

- **reflexivní**, jestliže pro všechna $a \in A$ platí $(a, a) \in R$,
- **ireflexivní**, jestliže pro všechna $a \in A$ platí $(a, a) \notin R$,
- **symetrická**, jestliže pro všechna $a, b \in A$ platí, že pokud $(a, b) \in R$, pak $(b, a) \in R$,
- **asymetrická**, jestliže pro všechna $a, b \in A$ platí, že pokud $(a, b) \in R$, pak $(b, a) \notin R$,
- **antisymetrická**, jestliže pro všechna $a, b \in A$ platí, že pokud $(a, b) \in R$ a $(b, a) \in R$, pak $a = b$,
- **tranzitivní**, jestliže pro všechna $a, b, c \in A$ platí, že pokud $(a, b) \in R$ a $(b, c) \in R$, pak $(a, c) \in R$.

Relace

Příklad:

- Relace "$=$" na $\mathbb{N}$ je reflexivní, symetrická, antisymetrická a tranzitivní, ale není ireflexivní ani asymetrická.
- Relace "$\leq$" na $\mathbb{N}$ je reflexivní, antisymetrická a tranzitivní, ale není ireflexivní, symetrická ani asymetrická.
- Relace "$<$" na $\mathbb{N}$ je ireflexivní, asymetrická, antisymetrická a tranzitivní, ale není reflexivní ani symetrická.

Relace

- **Reflexivní uzávěr** relace $R \subseteq A \times A$ je nejmenší reflexivní relace $R' \subseteq A \times A$ taková, že $R \subseteq R'$.

  Poznámka: Pojmem „nejmenší“ zde máme na mysli to, že neexistuje žádná reflexivní relace R'' taková, že $R \subseteq R'' \subset R'$.

- **Symetrický uzávěr** relace $R \subseteq A \times A$ je nejmenší symetrická relace $R' \subseteq A \times A$ taková, že $R \subseteq R'$.

- **Tranzitivní uzávěr** relace $R \subseteq A \times A$ je nejmenší tranzitivní relace $R' \subseteq A \times A$ taková, že $R \subseteq R'$.

- **Reflexivní a tranzitivní uzávěr** relace $R \subseteq A \times A$ je nejmenší relace $R' \subseteq A \times A$ taková, že $R \subseteq R'$ a R' je současně reflexivní i tranzitivní.

Ekvivalence

Binární relace R na množině A je **ekvivalence** právě tehdy, když je reflexivní, symetrická a tranzitivní.

Příklad: Následující relace $\equiv_5$ je ekvivalence

$$\equiv_5 = \{(a, b) \in \mathbb{Z}^2 \mid (a \bmod 5) = (b \bmod 5)\}$$

obecně pro libovolné $n > 0$ je relace $\equiv_n$ ekvivalence

$$\equiv_n = \{(a, b) \in \mathbb{Z}^2 \mid (a \bmod n) = (b \bmod n)\}$$

Ekvivalence

Jestliže R je ekvivalence na množině A, pak **třídou ekvivalence** prvku $a \in A$ je množina $[a]_R = \{b \in A \mid (a, b) \in R\}$, tj. množina všech prvků s ním ekvivalentních.

Mějme množinu A. Množina jejích podmnožin $\mathcal{A} = \{A_i \mid i \in I\}$ (pro nějakou indexovou množinu I) tvoří **rozklad** na množině A, jestliže:

- všechny množiny A_i jsou vzájemně disjunktní, tj. jestliže pro libovolné $A_i, A_j \in \mathcal{A}$ platí $A_i \cap A_j = \emptyset$ pokud $i \neq j$, a
- sjednocení množin z $\mathcal{A}$ je množina A, tj.

$$A = \bigcup_{A_i \in \mathcal{A}} A_i$$

Ekvivalence

Ekvivalence $R \subseteq A \times A$ definuje na A rozklad $\{\, [a]_R \mid a \in A \,\}$.

Naopak rozklad $\mathcal{A} = \{A_i \mid i \in I\}$ na množině A definuje ekvivalenci

$$R = \{(a, b) \subseteq A \times A \mid a, b \in A_i \text{ pro nějaké } A_i \in \mathcal{A}\}\,.$$

Příklad: Ekvivalence $\equiv_5$ definuje rozklad $\mathcal{A} = \{A_0, A_1, A_2, A_3, A_4\}$ na $\mathbb{N}$, kde

- $A_0 = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$
- $A_1 = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$
- $A_2 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$
- $A_3 = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$
- $A_4 = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$

Uspořádání

Binární relace R na množině A je **(částečné a neostré) uspořádání**, jestliže je reflexivní, tranzitivní a antisymetrická.

Binární relace R na množině A je **(částečné) ostré uspořádání**, jestliže je asymetrická a tranzitivní.
(Pozn.: Z toho, že je R asymetrická plyne, že je také ireflexivní a antisymetrická.)

Pro neostrá uspořádání se obvykle používají symboly jako $\leq$ a jemu podobné, pro ostrá uspořádání pak symboly jako $<$ a jemu podobné.

Uspořádání (ať už neostré či ostré) $R \subseteq A \times A$ je **úplné** (nebo také **lineární**), jestliže pro všechna $a, b \in A$ platí buď $(a, b) \in R$, $(b, a) \in R$ nebo $a = b$ (tj. pokud neexistují vzájemně nesrovnatelné prvky).

Uspořádání

Příklady:

- Relace "$\leq$" je úplné (neostré) uspořádání na množině $\mathbb{N}$ ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$).
- Relace "$<$" je ostré úplné uspořádání na množině $\mathbb{N}$ ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$).
- Relace "$\subseteq$" je částečné (neostré) uspořádání na množině $\mathcal{P}(X)$ (pro libovolnou množinu X).
- Relace "je dělitelem" je částečné (neostré) uspořádání na množině $\mathbb{N}_+$.
- Relace "$=$" je částečné (neostré) uspořádání na množině $\mathbb{N}$.

Ke každému neostrému uspořádání R na množině A existuje odpovídající ostré uspořádání $R' = R - \{(a, a) \mid a \in A\}$.

Naopak ke každému ostrému uspořádání S na množině A existuje odpovídající neostré uspořádání $S' = S \cup \{(a, a) \mid a \in A\}$

Uspořádání

Mějme libovolné neostré uspořádání $\leq$ na množině A.

- Prvek $a \in A$ je **minimální prvek** množiny A, jestliže v A neexistuje menší prvek než a (tj. z $x \leq a$ plyne $x = a$).
- Prvek $a \in A$ je **maximální prvek** množiny A, jestliže v A neexistuje větší prvek než a (tj. z $a \leq x$ plyne $a = x$).
- Prvek $a \in A$ je **nejmenší prvek** množiny A, jestliže je menší než všechny ostatní prvky v A (tj. pro každé $x \in A$ platí $a \leq x$).
- Prvek $a \in A$ je **největší prvek** množiny A, jestliže je větší než všechny ostatní prvky v A (tj. pro každé $x \in A$ platí $x \leq a$).

Uspořádání

- Prvek $a \in A$ je **infimum** množiny B (píšeme $a = \inf B$), jestliže a je největší ze všech prvků, které jsou menší než všechny prvky z B, tj. platí

$$(\forall x \in B)(a \leq x) \ \wedge \ (\forall b)((\forall x \in B)(b \leq x) \Rightarrow b \leq a)$$

- Prvek $a \in A$ je **supremum** množiny B (píšeme $a = \sup B$), jestliže a je nejmenší ze všech prvků, které jsou větší než všechny prvky z B, tj. platí

$$(\forall x \in B)(x \leq a) \ \wedge \ (\forall b)((\forall x \in B)(x \leq b) \Rightarrow a \leq b)$$

Funkce

Funkce f z množiny A do množiny B je binární relace $f \subseteq A \times B$ taková, že pro každé $a \in A$ existuje právě jedno $b \in B$ takové, že $(a, b) \in f$.

Množina A se nazývá **definiční obor** funkce f,

množina B se nazývá **obor hodnot** funkce f.

To, že f je funkce z množiny A do množiny B obvykle zapisujeme jako

$$f : A \to B$$

Místo $(a, b) \in f$ obvykle píšeme $b = f(a)$, neboť volbou prvku a je prvek b jednoznačně určen.

Funkce $f : A \to B$ tedy každému prvku z A přiřazuje právě jeden prvek z B.

Jestliže $b = f(a)$, říkáme, že a je **argumentem** funkce f a že b je **hodnotou** funkce f v bodě a.

Funkce

Výše uvedená definice se týká tzv. **totální** funkce, tj. funkce, jejíž hodnota je definovaná pro každou hodnotu argumentu.

Někdy má smysl uvažovat také tzv. **částečné (parciální) funkce**, tj. funkce, jejichž hodnota není pro některé hodnoty argumentu definována.

Formálně je částečná funkce $f : A \to B$ definována jako relace $f \subseteq A \times B$ taková, že pro každé $a \in A$ existuje nejvýše jedno $b \in B$ takové, že $(a, b) \in f$.

Poznámka: Pokud budeme mluvit o funkci a neuvedeme jinak, budeme mít vždy na mysli funkci totální.

Funkce

Konečná posloupnost (sekvence) délky n je funkce, jejímž definičním oborem je množina $\{0, 1, \ldots, n-1\}$.

Konečnou posloupnost obvykle zapisujeme tak, že vypíšeme její hodnoty:

$$f(0), f(1), \ldots, f(n-1)$$

Nekonečná posloupnost (sekvence) je funkce, jejímž definičním oborem je $\mathbb{N}$.

Nekonečnou posloupnost někdy zapisujeme tak, že uvedeme několik prvních prvků, za kterými následují tři tečky:

$$f(0), f(1), f(2), \ldots$$

Funkce

Jestliže definičním oborem funkce f je kartézský součin, obvykle vynecháváme jeden pár závorek v zápise argumentu funkce f.

Pokud například máme funkci $f : A_1 \times A_2 \times \cdots \times A_n \to B$, pak místo $b = f((a_1, a_2, \ldots, a_n))$ píšeme $b = f(a_1, a_2, \ldots, a_n)$.

Místo o funkci někdy též mluvíme o **operaci**.

n-ární operace je funkce f typu

$$f : A_1 \times A_2 \times \cdots \times A_n \to B$$

V případě, že $n = 2$, mluvíme o **binární** operaci.

- $f : A^n \to A$ – n-ární operace na množině A,
- $f : A \to A$ – unární operace na množině A,
- $f : A \times A \to A$ – binární operace na množině A.

Funkce

Mějme funkci $f : A^n \to A$. Množina $B \subseteq A$ je **uzavřená na operaci** f, jestliže z $a_1, a_2, \ldots, a_n \in B$ plyne, že $f(a_1, a_2, \ldots, a_n) \in B$.

Jestliže $f : A \to B$ je funkce a $b = f(a)$, pak někdy také říkáme, že b je **obrazem** a. Obrazem množiny $A' \subseteq A$ je množina

$$f(A') = \{b \in B \mid b = f(a) \text{ pro nějaké } a \in A'\}.$$

Funkce $f : A \to B$ je:

- **surjektivní** (je surjekcí, je zobrazením na), jestliže $f(A) = B$,
- emphinjektivní (je injekcí, je prostá), jestliže z $a \neq a'$ plyne $f(a) \neq f(a')$,
- **bijektivní** (je bijekcí, je vzájemně jednoznačným zobrazením), jestliže je současně surjektivní i injektivní.

Jestliže funkce f je bijekcí, pak funkce **inverzní** k funkci f, označovaná f^{-1}, je definována takto: $f^{-1}(b) = a$ právě když $f(a) = b$.

Funkce

Předpokládejme nyní funkci $f : A \times A \to A$.

- Funkce f je **asociativní**, jestliže pro libovolné prvky $a, b, c \in A$ platí
$$f(f(a, b), c) = f(a, f(b, c)) .$$
- Funkce f je **komutativní**, jestliže pro libovolné prvky $a, b \in A$ platí
$$f(a, b) = f(b, a) .$$
- Prvek $z \in A$ je **nulovým prvkem** vzhledem k funkci f, jestliže pro libovolné $a \in A$ platí
$$f(z, a) = f(a, z) = z .$$
- Prvek $e \in A$ je **jednotkovým prvkem** vzhledem k funkci f, jestliže pro libovolné $a \in A$ platí
$$f(e, a) = f(a, e) = a .$$

Poznámka: Dá se ukázat, že ke každé funkci existuje nejvýše jeden nulový a nejvýše jeden jednotkový prvek.

Jestliže k funkci f existuje jednotkový prvek e, pak $b \in A$ je **inverzním prvkem** k prvku $a \in A$ právě tehdy, když

$$f(a, b) = f(b, a) = e$$

Funkce

Pro funkce typu $f : A \times A \to A$ je často vhodnější používat infixovou notaci a používat jako název funkce nějaký speciální symbol.

Mějme například funkci

$$\otimes : A \times A \to A$$

Pak místo $\otimes(a, b)$ píšeme $a \otimes b$.

- Asociativita $\otimes$ pak znamená, že pro libovolné $a, b, c \in A$ platí

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

- a komutativita $\otimes$ znamená, že pro libovolné $a, b \in A$ platí

$$a \otimes b = b \otimes a$$

Příklad: Místo $+(x, y)$ píšeme $x + y$.