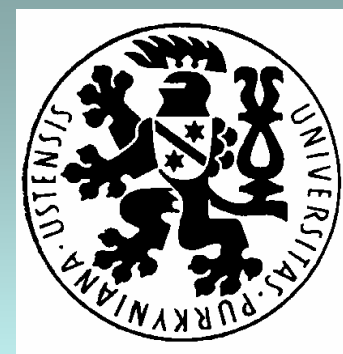




**Katedra matematiky
PF UJEP**



Aritmetika s didaktikou I.

KM1 / 0001

Přednáška 04

Struktury s jednou binární operací

O čem budeme hovořit:

- pojem matematické struktury
- struktury s jednou binární operací

Matematické struktury

Definice matematické struktury

Uspořádanou n -tici $[M; R_1; R_2; \dots ; O_1; O_2; \dots]$ budeme nazývat matematickou strukturou právě tehdy, když M je množina (tzv. nosič struktury), $R_1; R_2; \dots$ jsou binární relace v množině M a $O_1; O_2; \dots$ jsou binární operace v množině M .

Příklady matematických struktur:

- $[N_0; = ; < ; + ; \cdot],$
- $[Z; +],$
- $[\text{Pot}(A) ; \subseteq ; \cap ; \cup ; -],$

atd.

Poznámky ke strukturám

Jednou z relací ve struktuře bývá vždy rovnost, pro ni jsou samozřejmě splněny **požadavky reflexivnosti, symetrie a tranzitivnosti**. Tato relace se v zápise struktury vynechává.

Kromě toho se vyžaduje, aby **relace** (tedy i rovnost) **byly invariantní vzhledem k operacím**.

To znamená, že:

- pro binární relaci **R** a binární operaci **O** platí
$$(\forall x, y, z \in M) x R y \Rightarrow (x O z) R (y O z) \quad \wedge$$
$$\wedge x R y \Rightarrow (z O x) R (z O y)$$
- resp. pro binární relaci **R** a unární operaci **O** platí
$$(\forall x, y, z \in M) x R y \Rightarrow (O x) R (O y)$$

Příklady invariance

- Ve struktuře $[\mathbf{N}_0; < ; +]$ jsou binární relace $=$ a $<$ invariantní vzhledem k binární operaci $+$, tj. platí

$$(\forall x, y, z \in \mathbf{N}_0) x = y \Rightarrow x + z = y + z \quad \wedge$$

$$\wedge x = y \Rightarrow z + x = z + y$$

$$\text{a } (\forall x, y, z \in \mathbf{N}_0) x < y \Rightarrow x + z < y + z \quad \wedge$$

$$\wedge x < y \Rightarrow z + x < z + y$$

- Ve struktuře $[\mathbf{Pot}(\mathbf{Z}) ; \subseteq ; \cap]$ je binární relace $\subseteq$ invariantní vzhledem k binární operaci $\cap$, tj. platí

$$(\forall A, B, C \subseteq \mathbf{Z}) A \subseteq B \Rightarrow A \cap C \subseteq B \cap C \quad \wedge$$

$$A \subseteq B \Rightarrow C \cap A \subseteq C \cap B$$

atd.

Struktury s jednou binární operací

Definice (komutativního) grupoidu

Strukturu $[M; O]$ budeme nazývat (komutativním) grupoidem právě tehdy, když binární operace O je (komutativní a) úplná v M .

Příklady:

- $[\mathbb{N}_0; +]$ a $[\mathbb{N}_0; \cdot]$ jsou komutativní grupoidy,
 - $[\mathbb{N}_0; -]$ není grupoid
 - $[\mathbb{Z}; -]$ je nekomutativní grupoid,
 - $[\text{Pot}(A) ; \cup]$ je komutativní grupoid,
- atd.

Poznámka k neutrálnímu prvku

Uvažujme grupoid $[M; \square]$ a budeme předpokládat, že v množině existují M dva různé neutrální prvky n_1 a n_2 operace $\square$.

Platí tedy, že:

$$(\forall x \in M) \quad x \square n_1 = x \quad \wedge \quad n_1 \square x = x, \quad (1)$$

a současně $(\forall x \in M) \quad x \square n_2 = x \quad \wedge \quad n_2 \square x = x. \quad (2)$

Z druhé části (1) plyne, že $n_1 \square n_2 = n_2,$

a z první části (2) plyne, že $n_1 \square n_2 = n_1.$

Z těchto rovností vyplývá, že $n_1 = n_2,$

oba neutrální prvky tedy splynou.

Závěr: Grupoid má nejvýše jeden neutrální prvek.

Definice (komutativní) plogrupy

(Komutativní) grupoid $[M; O]$ budeme nazývat (komutativní) plogrupou právě tehdy, když binární operace O je navíc asociativní v M .

Příklady:

- $[\mathbb{N}_0; +]$ a $[\mathbb{N}_0; \cdot]$ jsou komutativní plogrupy,
 - $[\mathbb{Z} ; -]$ není plogrupa,
 - $[\text{Perm}(A) ; \bullet]$ je nekomutativní plogrupa,
 - $[\text{Pot}(A) ; \cup]$ je komutativní plogrupa,
- atd.

Definice (komutativního) monoidu

(Komutativní) pologrupu $[M; O]$ budeme nazývat (komutativním) monoidem právě tehdy, když navíc v M existuje neutrální prvek operace O .

Příklady:

- $[N_0; \cdot]$ je komutativní monoid,
 - $[N; +]$ není monoid,
 - $[\text{Perm}(A); \bullet]$ je nekomutativní monoid,
 - $[\text{Pot}(A); \cup]$ je komutativní monoid,
- atd.

Poznámka k inverzním prvkům

Uvažujme monoid $[M; \square]$ s neutrálním prvkem n a budeme předpokládat, že k nějakému prvku $x \in M$ existují v M dva inverzní prvky x_1' a x_2' .

Operace $\square$ je tedy asociativní a platí současně:

$$x \square x_1' = n \quad \wedge \quad x_1' \square x = n$$

$$x \square x_2' = n \quad \wedge \quad x_2' \square x = n$$

$$\begin{aligned} \text{Pak: } x_1' &= x_1' \square n = x_1' \square (x \square x_2') = \\ &= (x_1' \square x) \square x_2' = n \square x_2' = x_2', \end{aligned}$$

a oba inverzní prvky tedy splynou.

Závěr: V monoidu existuje ke každému prvku nejvýše jeden inverzní prvek.

Definice (komutativní) grupy

(Komutativní) monoid $[M; O]$ budeme nazývat (komutativní) grupou právě tehdy, když navíc ke každému prvku $x \in M$ existuje v M inverzní prvek.

Příklady:

- $[Z; +]$ je komutativní grupa,
 - $[N_0; +]$ není grupa,
 - $[\text{Perm}(A); \bullet]$ je nekomutativní grupa,
 - $[\text{Pot}(A); \cup]$ není grupa,
- atd.

Poznámka o krácení v grupě

Uvažujme grupu $[M; \square]$ s neutrálním prvkem n .

Rovnost je vzhledem k operaci $\square$ invariantní, tedy platí:

$$(\forall x, y, z \in N_0) \quad x = y \Rightarrow x \square z = y \square z \quad \wedge \\ \wedge \quad x = y \Rightarrow z \square x = z \square y .$$

Lze dokázat i obrácená tvrzení, tedy že platí (tzv. krácení):

$$(\forall x, y, z \in N_0) \quad x \square z = y \square z \Rightarrow x = y \quad \wedge \\ \wedge \quad z \square x = z \square y \Rightarrow x = y .$$

Důkaz: Z předpokladu

$$x \square z = y \square z$$

pomocí invariance

$$(x \square z) \square z' = (y \square z) \square z'$$

a pomocí asociativity

$$x \square (z \square z') = y \square (z \square z')$$

získáme

$$x \square n = y \square n$$

a tedy

$$x = y$$

Závěr: V grupě lze krátit (zprava i zleva).

Závěrečné shrnutí

Název struktury [M; O]	Vlastnosti operace O
(komutativní) grupoid	(K) Ú
(komutativní) pologrupa	(K) Ú A
(komutativní) monoid	(K) Ú A N
(komutativní) grupa	(K) Ú A N I

Jaké vlastnosti by měly **uspořádané** struktury?

Děkuji za pozornost

