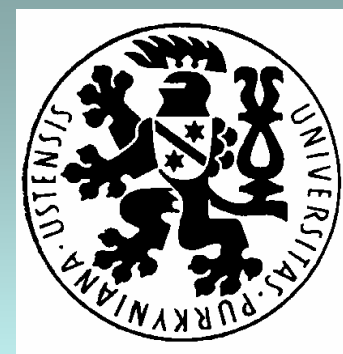




**Katedra matematiky
PF UJEP**



Aritmetika s didaktikou I.

KM1 / 0001

Přednáška 05

Struktury se dvěma binárními operacemi

O čem budeme hovořit:

- opakování struktur s jednou operací
- struktury se dvěma operacemi

Struktury s jednou binární operací

Opakování

Přehled vlastností struktur s jednou binární operací

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

Matematické struktury se dvěma binárními operacemi

Definice (komutativního) polookruhu

Strukturu $[M; O_1 ; O_2]$ budeme nazývat (komutativním) polookruhem právě tehdy, když

- struktura $[M; O_1]$ je komutativní pologrupa,
- struktura $[M; O_2]$ je (komutativní) pologrupa,
- operace O_2 je distributivní vzhledem k O_1 .

Příklady:

- $[\mathbf{N} ; + ; \cdot]$ je komutativní polookruh,
 - $[\mathbf{Pot}(A) ; \cup ; \cap]$ je komutativní polookruh,
- atd.

Definice (komutativního) okruhu

Strukturu $[M; O_1 ; O_2]$ budeme nazývat (komutativním) okruhem právě tehdy, když

- struktura $[M; O_1]$ je komutativní grupa,
- struktura $[M; O_2]$ je (komutativní) pologrupa,
- operace O_2 je distributivní vzhledem k O_1 .

Příklady:

- $[\mathbb{Z} ; + ; \cdot]$ je komutativní okruh,
 - $[\text{Pot}(A) ; \cup ; \cap]$ není okruh,
- atd.

Poznámka k významům znaménka „minus“ v okruhu $[\mathbb{Z} ; + ; \cdot]$

Celá čísla zapisujeme takto:

$\dots, -3, -2, -1, 0, +1, +2, +3, \dots$

Znaménko „minus“ se užívá ve třech významech:

- 1) jako součást označení **záporných** čísel,
například -3 nebo -14 ,
- 2) jako označení pro unární operaci, která číslu přiřazuje **inverzní prvek** vzhledem ke sčítání (tzv. **opačný prvek**),
například $-(+3) = -3$ nebo $-(-9) = +9$
- 3) jako označení pro binární operaci **odčítání**, která je
definována pomocí opačných prvků: $a - b = a + (-b)$,
například $-3 - (-9) = -3 + (-(-9)) = -3 + (+9) = +6$

Poznámka o nulovém prvku

Uvažujme libovolný okruh $[M; \square; \#]$ a označme neutrální prvek první operace $\square$ symbolem **n**.

Tomuto prvku se říká **nulový prvek**.

Jak se nulový prvek n chová při druhé operaci?

Pro libovolné $x \in M$ jistě platí:

$$(x \# n) \square n = x \# n = x \# (n \square n) = (x \# n) \square (x \# n),$$

a odtud krácením

$$x \# n = n.$$

Podobně platí

$$n \# x = n.$$

Nulový prvek je tedy „oboustranně agresivní“.

#	n	a	b	c	...
n	n	n	n	n	...
a	n				
b	n				
c	n				
...	...				

Definice „dělitelů nuly“ a oboru integrity

Necht' je dán okruh $[M; +; \cdot]$ s nulovým prvkem 0 .

Pak jsou dvě logické možnosti:

bud' $(\exists a, b \in M) a \cdot b = 0 \wedge a \neq 0 \wedge b \neq 0$, (1)

anebo $(\forall a, b \in M) a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$. (2)

V prvním případě, když platí (1), nazýváme čísla a , b **děliteli nuly**, a okruh $[M; +; \cdot]$ **okruhem s děliteli nuly**.

V druhém případě, když platí (2), v okruhu $[M; +; \cdot]$ neexistují dělitelé nuly a okruh $[M; +; \cdot]$ nazýváme **oborem integrity**.

Příklady oborů integrity

1) Okruh $[\mathbb{Z}_3; + ; \cdot]$ s operacemi sčítání a násobení, které jsou definovány těmito tabulkami, je obor integrity.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2) Okruh $[\mathbb{Z}; + ; \cdot]$ je také obor integrity.

Podmínku pro obor integrity lze přeformulovat do tvaru

$$(\forall a, b \in M) \quad a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0.$$

Příklad okruhu s děliteli nuly

Necht' je dán okruh $[Z_6; +; \cdot]$, operace sčítání a násobení jsou dány těmito tabulkami:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Děliteli nuly v okruhu $[Z_6; +; \cdot]$ jsou prvky 2, 3 a 4.

Druhá poznámka o nulovém prvku

Uvažujme libovolný okruh $[M; \square; \#]$ s nulovým prvkem n . Již víme, že platí:

$$(\forall x \in M) \quad n \# x = x \# n = n.$$

Předpokládejme, že v M existuje neutrální prvek i druhé operace $\#$ (budeme mu říkat jednotkový prvek a budeme ho označovat e). Předpokládejme ještě, že $n \neq e$.

O inverzních prvcích u druhé operace obecně víme, že

$$x \# x^{-1} = x^{-1} \# x = e,$$

pro inverzní prvek k nulovému prvku by tedy muselo být

$$n \# n^{-1} = n^{-1} \# n = e, \text{ což není možné.}$$

Nulový prvek n tedy nemá inverzní prvek vzhledem k $\#$.

Definice (komutativního) tělesa

Strukturu $[M; O_1 ; O_2]$ budeme nazývat (komutativním) tělesem právě tehdy, když

- struktura $[M; O_1]$ je komutativní grupa (s neutrálním prvkem n)
- struktura $[M - \{n\}; O_2]$ je (komutativní) grupa,
- operace O_2 je distributivní vzhledem k O_1 .

Příklady:

- $[\mathbb{Q} ; + ; \cdot]$ je komutativní těleso,
- $[\mathbb{Z}_3 ; + ; \cdot]$ je komutativní těleso,
- $[\mathbb{D} ; + ; \cdot]$ není těleso,

atd.

Vztah mezi tělesy a obory integrity

Dokažme, že **každé těleso je oborem integrity**.

Musíme tedy prokázat, že v žádném tělese neexistují dělitelé nuly. Dokážeme to sporem.

Předpokládejme tedy (na chvíli), že v tělese $[M; +; \cdot]$ s nulovým prvkem 0 existují prvky a, b takové, že platí

$$a \cdot b = 0 \wedge a \neq 0 \wedge b \neq 0.$$

Protože $b \neq 0$, existuje inverzní prvek b^{-1} , a pak

$$(a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1}$$

$$a \cdot (b \cdot b^{-1}) = 0$$

$a = 0$, což je spor !!!

Přehled vlastností struktur se dvěma binárními operacemi

Název struktury [M; □ ; #]	Vlastnosti [M; □]	Vlastnosti [M; #]	Další vlastnosti
(komutativní) polookruh	komutativní pologrupa	(komutativní) pologrupa	distributivita
(komutativní) okruh	komutativní grupa	(komutativní) pologrupa	distributivita
(komutativní) obor integrity	komutativní grupa	(komutativní) pologrupa	distributivita, neexistence dělitelů nuly
(komutativní) těleso	komutativní grupa	(komutativní) grupa (!!)	distributivita

Děkuji za pozornost

