Algebraické struktury se dvěma operacemi

motivace: Ve školské matematice jsou situace, kdy jsou na jedné množině definovány dvě neomezeně definované operace. Např. sčítání a násobení přirozených čísel. Odtud plyne nutnost zavést alg. struktury se dvěma alg. operacemi

$$(M, \oplus, \odot)$$

Obě operace musí být svázány distributivním zákonem. Jinak nemá smysl o takové struktuře mluvit.

$\odot \, D \, \oplus$

Př: $(\mathbb{C}, \oplus, \odot)$ $\quad a \oplus b = a+b-1$

$a \odot b = a+b-3ab$

dokazujeme $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

$L = a \odot (b+c+1) = a + (b+c+1) - 3a(b+c+1) = a+b+c+1-3ab-3ac-3a$

$P = (a+b-3ab) \oplus (a+c-3ac) = a+b-3ab+a+c-3ac-1 =$
$= 2a+b+c-1-3ab-3ac$

$L \neq P$ není distributivní

Př, $(\mathbb{R}, \oplus, \odot)$ $\quad a \oplus b = a^2+b^2$

$a \odot b = ab$

dokazujeme $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

$L = a \odot (b^2+c^2) = a \cdot (b^2+c^2) = ab^2+ac^2 = a(b^2+c^2)$

$P = (a \cdot b) \oplus (ac) = a^2b^2 + a^2c^2 = a^2(b^2+c^2)$

$L \neq P$ není distributivní

Algebraické struktury se dvěma operacemi

$(M, \oplus, \odot)$

$\oplus$ - sčítání, EN - nulový prvek, 0 ; $\bar{a} = -a$ opačný prvek k prvku a

$\odot$ - násobení, EN - jednotkový prvek, 1 ; $\bar{a} = a^{-1} = \frac{1}{a}$ převrácený prvek k a

$(M, \oplus, \odot)$

polookruh (kom.) $\oplus$: $ND \wedge A \wedge K$
$\odot$: $ND \wedge A\ (\wedge K)$
$\odot D \oplus$

okruh (kom.) $\oplus$: $ND \wedge A \wedge K \wedge \overset{0}{EN} \wedge EI \wedge ZR$
$\odot$: $ND \wedge A (\wedge K)$
$\odot D \oplus$

obor integrity - kom. okruh, ve kterém neexistují vlastní dělitelé nulového prvku
$(a \neq 0,\ b \neq 0,\ a \odot b = 0)$

těleso (kom.) $\oplus$: $ND \wedge A \wedge K \wedge \overset{0}{EN} \wedge EI \wedge ZR$
$\odot$: $ND \wedge A (\wedge K)$, $\odot D \oplus$
$(M - \{0\}, \odot)$ - grupa, tj. operace $\odot$ má na mn. $M - \{0\}$ vlastnosti $ND, A, \underset{1}{EN}, EI, ZR$

Př. $(\mathbb{N}, +, \cdot)$ - komutat. polookruh s oběma neutrálními prvky, který není okruhem

$(\mathbb{C}, +, \cdot)$ - obor integrity, není tělesem

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ - tělesa, obory integrity

$(M, \oplus, \odot)$ - polookruh; Ex.-li prvek x takový, že $a = b \oplus x = x \oplus b$, pak x se nazývá <u>rozdíl</u> prvků a, b. $x = a \ominus b$

Ex.-li prvek x takový, že $a = b \odot x = x \odot b$, pak x se nazývá <u>podíl</u> prvků a, b. $x = a \oslash b$

~~Okruh $(M, \oplus, \odot)$~~ $x = a \ominus b$ def. $x = a \ominus b = a \oplus (-b)$

Těleso $(M, \oplus, \odot)$ $x = a \oslash b$, $b \neq 0$ def. $x = a \oslash b = a \odot \frac{1}{b}$

Příklady ze školské matematiky

$(N, +, \cdot)$ komutativní polookruh s jedničkou

$(C, +, \cdot)$ komutativní obor integrity s jedničkou

$$a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0$$

neboli $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

$(Q, +, \cdot)$ komutativní těleso ; $(Q - \{0\}, \cdot)$ je grupa

$(R, +, \cdot)$ komutativní těleso

$(Q_0^+, +, \cdot)$ komutativní polookruh s jedničkou

$M = \{a, b\}$ $(P(M), \cup, \cap)$ komutativní polookruh s jedničkou

$\cup$: ND, K, A, EN, ~~EI~~, ~~ZR~~ $\cap D \cup$ nula … $\emptyset$

$\cap$: ND, K, A, EN, ~~EI~~, ~~ZR~~ jednička … M

lze řešit tabulkou,

např. víme, že platí $A \cup (B \cup C) = (A \cup B) \cup C$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Př. $M = \{a, b, c\}$

$x \oplus y = x$

$x \odot y = y$

$\oplus$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

$\odot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

$\oplus$ ND, ~~K~~, A, ~~EN~~, ~~EI~~, ~~ZR~~ $\odot D \oplus$ nekomutativní polookruh

$\odot$ ND, ~~K~~, A, ~~EN~~, ~~EI~~, ~~ZR~~

A: $x \oplus (y \oplus z) = x \oplus y = x$; $(x \oplus y) \oplus z = x \oplus z = x$

$x \odot (y \odot z) = x \odot z = z$; $(x \odot y) \odot z = y \odot z = z$

D: $x \odot (y \oplus z) = x \odot y = y$; $(x \odot y) \oplus (x \odot z) = y \oplus z = y$

$(x \oplus y) \odot z = x \odot z = z$; $(x \odot z) \oplus (y \odot z) = z \oplus z = z$

Příklad z učebnice 124/21:

$\mathbb{C}$ celá čísla: operace $\oplus$ $\quad x \oplus y = x + y + 1$

operace $\odot$ $\quad x \odot y = x + y + xy$

Určete typ struktury $(\mathbb{C}, \oplus, \odot)$

Už jsme vyřešili: $(\mathbb{C}, \oplus)$ je komutativní grupa $(e = -1)$

$(\mathbb{C}, \odot)$ je komutativní pologrupa $(e = 0)$

Tedy podle terminologie: (-1) je prvek nulový,

0 je prvek jednotkový

ověříme $\odot D \oplus$, tedy $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

$$L = x \odot (y \oplus z) = x \odot (y + z + 1) = x + (y + z + 1) + x \cdot (y + z + 1) =$$
$$= 2x + y + z + xy + xz + 1$$

$$P = (x \odot y) \oplus (x \odot z) = (x + y + xy) \oplus (x + z + xz) = \qquad L = P$$
$$= x + y + xy + x + z + xz + 1 = 2x + y + z + xy + xz + 1$$

Víme už, že množina $(\mathbb{C} - \{-1\}, \odot)$ netvoří grupu (-1 je nulový prvek).

Proto $(\mathbb{C}, \oplus, \odot)$ nemůže být těleso. Ověříme existenci dělitelů nuly: (nulový prvek je -1)

$$x \odot y = -1$$
$$x + y + xy = -1$$
$$x + y + xy + 1 = 0$$
$$(x+1) + y(x+1) = 0$$
$$(x+1) \cdot (y+1) = 0 \implies x = -1 \text{ nebo } y = -1$$

Ukázali jsme, že z předpokladu $x \odot y = -1$ platí buďto $x = -1$ nebo $y = -1$. Dělitelé nuly tedy neexistují.

Závěr: $(\mathbb{C}, \oplus, \odot)$ je obor integrity.

Př. $(\mathbb{Q}, \oplus, \odot)$ $\quad x \oplus y = x + y$ $\quad$ určete typ struktury

$x \odot y = \frac{1}{2} xy$

$\cdot D +$ $\quad x \odot (y \oplus z) = x \odot (y+z) = \frac{1}{2} x \cdot (y+z) = \frac{xy}{2} + \frac{xz}{2}$

$(x \odot y) \oplus (x \odot z) = \frac{1}{2} xy \oplus \frac{1}{2} xz = \frac{xy}{2} + \frac{xz}{2}$ $\quad$ platí

$\oplus$ ND, K, A, EN, EI, ZR $\quad$ „obyčejné" sčítání $\quad (e=0)$

$\odot$ ND, K, zřejmé

A $\quad (x \odot y) \odot z = \frac{1}{2} xy \odot z = \frac{1}{2} \cdot \left(\frac{1}{2} xy \cdot z\right) = \frac{xyz}{4}$

$x \odot (y \odot z) = x \odot \frac{1}{2} yz = \frac{1}{2} \left(x \cdot \frac{1}{2} yz\right) = \frac{xyz}{4}$

EN $\quad x \odot e = x$

$\frac{1}{2} xe = x$

$xe = 2x \quad | : x \ (x \neq 0)$

$\underline{e = 2}$

zk. pro $e = 2, x = 0$

$0 \odot 2 = \frac{1}{2} 0 \cdot 2 = 0$

EI $\quad x \odot \overline{x} = 2$

$\frac{1}{2} x \overline{x} = 2$

$x \overline{x} = 4$

$\underline{\overline{x} = \frac{4}{x}} \quad , x \neq 0$

ZR: $\quad a \odot x = b$

$\frac{1}{2} ax = b$

$\underline{x = \frac{2b}{a}} \quad , a \neq 0$

tedy $(\mathbb{Q}, \odot)$ je pologrupa,

ale $(\mathbb{Q} - \{0\}, \odot)$ je komutativní grupa

$(\mathbb{Q}, \oplus, \odot)$ je komutativní těleso.

Pravidla pro počítání v polookruhu:

$$(a \ominus b) \oplus b = a \qquad (a \oplus b) \ominus b = a$$

$$(a \oplus b) \ominus c = (a \ominus c) \oplus b = a \oplus (b \ominus c)$$

$$a \ominus (b \ominus c) = (a \oplus c) - b \qquad a \ominus (b \oplus c) = (a \ominus b) \ominus c$$

$$(a \oplus c) \ominus (b \oplus c) = a \ominus b \qquad (a \ominus c) \ominus (b \ominus c) = a \ominus b$$

$$(a \oslash b) \odot b = a \qquad (a \odot b) \oslash b = a$$

$$(a \odot b) \oslash c = (a \oslash c) \odot b = a \odot (b \oslash c)$$

$$a \oslash (b \oslash c) = (a \odot c) \oslash b \qquad a \oslash (b \odot c) = (a \oslash b) \oslash c$$

$$(a \odot c) \oslash (b \odot c) = a \oslash b \qquad (a \oslash c) \oslash (b \oslash c) = a \oslash b$$

Tato pravidla odpovídají pravidlům pro počítání v oboru přirozených čísel za předpokladu, že všechny zapsané rozdíly a podíly existují. V polookruhu $(N, +, \cdot)$ nelze převádět odčítání na přičítání opačného prvku $(A - B = A + (-B))$ ani dělení nelze převádět na násobení prvkem převráceným $(A : B = A \cdot \frac{1}{B})$. Proto je nutno tato pravidla dokázat jako věty.

Př.: $a \ominus (b \ominus c) = (a \oplus c) \ominus b$, pokud existují $b \ominus c$, $a \ominus (b \ominus c)$

označme $a \ominus (b \ominus c) = x$, potom $a = x \oplus (b \ominus c)$. Podle předch. věty je $a = (x \oplus b) \ominus c$, odtud $a \oplus c = x \oplus b$, tedy $x = (a \oplus c) \ominus b$. Po dosazení za x $a \ominus (b \ominus c) = (a \oplus c) \ominus b$

DŮKAZY V KOMUTATIVNÍM OKRUHU $(M, +, \cdot)$

připomenutí: $+$ ND, K, A, EN, EI, ZR

$\cdot$ ND, K, A, EN, $\cancel{EI}$, $\cancel{ZR}$

$\cdot D +$

$a+(-b) = a-b$

① $D: a \cdot 0 = 0 \cdot a = a$

místo $+[-(a \cdot a)]$ píšeme $-(a \cdot a)$

$$0 + a = a \quad | \cdot a$$

$$a \cdot (0+a) = a \cdot a$$

$$(a \cdot 0) + (a \cdot a) = a \cdot a \quad | -(a \cdot a)$$

$$[(a \cdot 0) + (a \cdot a)] - (a \cdot a) = (a \cdot a) - (a \cdot a) \qquad A$$

$$(a \cdot 0) + \underbrace{[(a \cdot a) - (a \cdot a)]}_{0} = \underbrace{(a \cdot a) - (a \cdot a)}_{0}$$

$$(a \cdot 0) + 0 = 0$$

$$a \cdot 0 = 0$$

$0 \cdot a = 0$ plyne z komutativnosti násobení.

② $D: a \cdot (-b) = -(a \cdot b)$

$$(a \cdot b) + [-(a \cdot b)] = 0$$

$$(a \cdot b) + [a \cdot (-b)] \overset{D}{=} a \cdot [b + (-b)] = a \cdot 0 = 0$$

opačný prvek je určen jednoznačně, tedy platí $a \cdot (-b) = -(a \cdot b)$.

③ $D: a \cdot (-1) = -a$ (v tělese existuje prvek 1, tedy také -1)

$$a \cdot (-1) = -(a \cdot 1) = -a$$