Algebraické struktury – základní struktury s jednou a dvěma operacemi, výskyt struktur na ZŠ, využití distributivnosti násobení ke sčítání

Algebraická struktura je v matematice každá neprázdná množina M, na které jsou definované nějaké operace a daná množina je vzhledem k těmto operacím uzavřená (výsledkem operace nad prvky této množiny je vždy také prvek této množiny).

Def. (**Grupoid**) Algebraická struktura s jednou binární operací se nazývá grupoid a značí se $(M; \bullet)$.

Def. (**Asociativní grupoid**) Grupoid $(M, \bullet)$ se nazývá asociativní, právě tehdy když platí:

$$\forall x, y, z \in M; (x \bullet y) \bullet z = x \bullet (y \bullet z)$$

Def. (**Grupoid s neutrálním prvkem**) Grupoid $(M, \bullet)$ se nazývá Grupoid s neutrálním prvkem, právě tehdy když platí

$$\exists e \in M \forall x \in M; e \bullet x = x \bullet e = x.$$

Každý prvek e, pro který platí

$$\forall x \in M; e \bullet x = x \bullet e = x,$$

se nazývá **neutrální prvek**.

Věta. Grupoid $(M; \bullet)$ má nejvýše jeden neutrální prvek.
vyvozují.

Důkaz:
Nechť e_1 a e_2 jsou jednotkové prvky grupoidu M, pak $e_1 = e_1 \bullet e_2 = e_2$.

Def. (**Grupoid s inverzními prvky**) Grupoid $(M; \bullet)$ se nazývá Grupoid s inverzními prvky, právě tehdy když platí

$$e \in M \wedge \forall x \in M \exists y \in M; x \bullet y = y \bullet x = e.$$

Jestliže $x \in M$, pak každý prvek $y \in M$ pro který platí, že

$$x \bullet y = y \bullet x = e$$

se nazývá **inverzní prvek** k prvku x.

Věta. Jestliže $(M; \bullet)$ je asociativní grupoid, pak ke každému jeho prvku existuje nejvýše jeden prvek inverzní.

Důkaz:
Nechť x a z jsou inverzní prvky k prvku x v asociativním grupoidu $(M, \bullet)$, pak platí:

$$z = (y \bullet x) \bullet z = y \bullet (x \bullet z) = y$$
$$z = e \bullet z = (y \bullet x) \bullet z = y \bullet (x \bullet z) = y \bullet e = y$$

Def. (**Komutativní grupoid**) Grupoid $(M;\bullet)$ se nazývá komutativní, právě tehdy když platí:

$$\forall x,y \in M; x \bullet y = y \bullet x$$

*Def. (**Grupoid s krácením**) Grupoid $(M,\bullet)$ se nazývá grupoid s krácením, právě tehdy když platí*

$$\forall x,y,z \in M; (x \bullet z = y \bullet z \Rightarrow x = y) \wedge (z \bullet x = z \bullet y \Rightarrow x = y).$$

Říkáme, že prvkem $z \in M$ lze v grupoidu $(M;\bullet)$ krátit, právě tehdy když

$$\forall x,y \in M; (x \bullet z = y \bullet z \Rightarrow x = y) \wedge (z \bullet x = z \bullet y \Rightarrow x = y).$$

První část formule popisuje krácením prvkem z zprava, druhá část krácením prvkem z zleva.

*Def. (**Grupoid s dělením**) Grupoid $(M,\bullet)$ se nazývá grupoid s dělením, právě tehdy když platí*

$$\forall x,y \in M \exists u \in M \exists v \in M; x \bullet u = y \wedge v \bullet x = y.$$

*Def. (**Grupoid s jednoznačným dělením**) Grupoid $(M,\bullet)$ se nazývá Grupoid s jednoznačným dělením, právě tehdy když platí*

$$\forall x,y \in M \exists! u \in M \exists! v \in M; x \bullet u = y \wedge v \bullet x = y.$$

Základní typy grupoidů

*Def. (**Zúžení operace**) Nechť $(G,\bullet)$ je grupoid a nechť neprázdná množina $A \subseteq G$ je uzavřená vzhledem k operaci $\bullet$. Operace $*$ pro níž platí*

$$\forall x,y \in A; x * y = x \bullet y,$$

se nazývá zúžením operace $\bullet$ na množinu A.

*Def. (**Podgrupoid**) Nechť $(G,\bullet)$ a $(H,*)$ jsou grupoidy. Grupoid $(H;*)$ se nazývá podgrupoidem grupoidu $(G;\bullet)$, právě tehdy když*

1. *$H \subseteq G$*
2. *Operace $*$ je zúžením operace $\bullet$ na množinu H.*

*Def. (**Izomorfní obraz**) Nechť $(G,\bullet)$ a $(G',*)$ jsou grupoidy. Grupoid $(G',*)$ se nazývá izomorfním obrazem grupoidu $(G,\bullet)$, právě tehdy když existuje prosté zobrazení f množiny G na množinu G´, které zachovává operaci, tzn pro něž platí*

$$\forall x,y \in G; f(x \bullet y) = f(x) * f(y).$$

Zobrazení f se nazývá izomorfní zobrazení nebo izomodfismus rgupoidu G na grupoid G´.

Def. (**Pologrupa**) Grupoid $(G,\bullet)$ se nazývá **pologrupa**, právě tehdy když je asociativní. Pokud je grupoid ještě komutativní nebo s neutrálním prvkem nebo s krácením, pak se nazývá komutativní pologrupa nebo pologrupa s neutrálním prvkem nebo pologrupa s krácením.

Def. (**Grupa**) Grupoid $(G,\bullet)$ se nazývá **grupa**, právě tehdy když je asociativní má neutrálním prvek a má inverzní prvky. Jestliže je tento grupoid ještě komutativní, nazývá se **komutativní** nebo **Abelova** grupa.

Příklad:

- $(\boldsymbol{N}, +)$ je komutativní pologrupa s neutrálním (nulovým) prvkem a s krácením.
- $(\boldsymbol{N}, \cdot)$ je komutativní pologrupa s neutrálním (jednotkovým) prvkem.
- $(\boldsymbol{Z}, +)$ je Abelova grupa s krácením a s jednoznačným odčítáním.
- $(\boldsymbol{Z}_4, +)$ je Abelova (celých čísel modulo 4) s krácením a s jednoznačným odčítáním.

Příklad: Sestrojte Cayleyho tabulku pro $(\boldsymbol{Z}_4, +)$.

$$c = \{0, 1, 2, 3\}$$

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- *Uzavřenost operace vzhledem k množině poznáme tak, že každé pole tabulky je vyplněno prvky množiny* $\boldsymbol{Z}_4$. *Žádné pole tabulky není prázdné a v žádném poli tabulky se nevyskytuje jiné číslo než* $0, 1, 2, 3$.

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- *Struktura má neutrální prvek v případě, že řádek vedle něj (respektive sloupec pod ním) je vyplněn stejně, jako záhlaví tabulky. (V tomto případě je neutrálním prvkem* 0.*)*

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- *Struktura má inverzní prvky v případě, že se neutrální prvek vyskytuje v každém řádku a sloupci tabulky právě jednou. (V tomto případě jsou dvojicemi navzájem inverzních prvků:* $\{0;0\},\{1;3\},\{3;1\},\{2;2\}$*.)*

$+$	***0***	***1***	***2***	***3***
0	*0*	*1*	*2*	*3*
1	*1*	*2*	*3*	*0*
2	*2*	*3*	*0*	*1*
3	*3*	*0*	*1*	*2*

- *Komutativitu operace na množině poznáme tak, že vyplněná tabulka je „souměrná" podle hlavní diagonály (v tabulce vyznačené žlutou barvou).*
- *Asociativitu operace na množině z tabulky přímo nepoznáme. Tu je třeba ověřit pro každé tři prvky množiny.*

Struktury se dvěma operacemi

Def. (**Distributivita**) Nechť jsou na neprázdné množině M definovány dvě binární operace, plus $(+)$ a krát $(\cdot)$. Říkáme, že operace krát $(\cdot)$ je distributivní vzhledem k operaci plus $(+)$ v M, právě tehdy když platí:

$$\forall x,y,z \in M; (x+y)\cdot z = x\cdot z + y\cdot z \wedge z\cdot(x+y) = z\cdot x + z\cdot y.$$

Def. (**Okruh**) Struktura $(M,+,\cdot)$ se nazývá **okruh**, právě tehdy když je $(+,\cdot)$ distributivní, grupoid $(M,+)$ je komutativní grupa a $(M,\cdot)$ je pologrupa.
Jestliže je pologrupa $(M,\cdot)$ komutativní, popř. s jednotkovým prvkem atd., nazývá se M komutativní okruh, popř. okruh s jednotkovým prvkem atd. Grupoidy $(M,+)$ a $(M,\cdot)$ nazýváme aditivní grupa a multiplikativní pologrupa okruhu M.

Def. (**Dělitele nuly**) Nechť $(M,+,\cdot)$ je okruh. Pak nenulový prvek $x \in M$ se nazývá dělitel nuly, právě tehdy když existuje alespoň jeden nenulový prvek $y \in M$ takový, že $x\cdot y = 0$ nebo $y\cdot x = 0$. Pravá část definice symbolicky:

$$\exists y \in M, y \neq 0 \wedge (x\cdot y = 0 \vee y\cdot x = 0).$$

*Def. (**Podokruh**) Nechť $(M,+,\cdot)$ a $(K,\oplus,\odot)$ jsou okruhy. Pak říkáme, že okruh $(K,\oplus,\odot)$ je podokruhem okruhu $(M,+,\cdot)$, právě tehdy když*

1. $K \subseteq M$
2. *Operace $\oplus,\odot$ jsou po řadě zúžením operací $+,\cdot$ na množinu K.*

Operace v okruhu M i v jeho podokruhu K se obecně značí stejně.

*Def. (**Izomorfní obraz**) Nechť $(M,+,\cdot)$ a $(M',\oplus,\odot)$ jsou okruhy. Pak říkáme, že okruh $(M',\oplus,\odot)$ je izomorfním obrazem okruhu $(M,+,\cdot)$, právě tehdy když existuje prosté zobrazení f množiny M na množinu M´, které zachovává obě operace, tzn., pro nějž platí*

$$\forall x,y \in M; f(x*y) = f(x) \oplus f(y) \wedge f(x\cdot y) = f(x) \odot f(y).$$

Zobrazení f se nazývá izomorfní zobrazení nebo izomodfismus okruhů M a M´.

*Def. (**Homomorfní obraz**) Nechť $(M,+,\cdot)$ a $(M',\oplus,\odot)$ jsou okruhy. Pak říkáme, že okruh $(M',\oplus,\odot)$ je homomorfním obrazem okruhu $(M,+,\cdot)$, právě tehdy když existuje zobrazení f množiny M na množinu M´, které zachovává obě operace, tzn., pro nějž platí*

$$\forall x,y \in M; f(x*y) = f(x) \oplus f(y) \wedge f(x\cdot y) = f(x) \odot f(y).$$

Zobrazení f se nazývá homomorfní zobrazení nebo homomorfismus okruhů M a M´.

Def. (**Obor Integrity**) Okruh $(I,+,\cdot)$ se nazývá **obor integrity**, právě tehdy když $(I,\cdot)$má neutrální prvek a neobsahuje dělitele nuly.
Protože v oboru integrity $(I,+,\cdot)$ neexistují dělitele nuly, platí v něm formule:

$$\forall x,y \in I; x \neq 0 \wedge y \neq 0 \Rightarrow x\cdot y \neq 0$$

Def. (**Těleso**) Okruh $(T,+,\cdot)$ se nazývá **těleso**, právě tehdy když struktura $(T\setminus\{0\},\cdot)$ je grupa. Pokud je $(T\setminus\{0\},\cdot)$ Abelova grupa, říkáme, že $(T,+,\cdot)$ je komutativní těleso nebo pole.

Uvažujme strukturu $(M,+,\cdot)$. Jestliže v definici okruhu, oboru integrity a tělesa nahradíme podmínku „$(M,+)$ je Abelova grupa“ podmínkou „$(M,+)$ je komutativní pologrupa“, pak obdržíme po řadě definice polookruhu, polooboru integrity a polotělesa.

Příklad:

- $(\boldsymbol{Z},+,\cdot)$ je obor integrity.
- $(\boldsymbol{Q},+,\cdot)$ je komutativní těleso.
- $(\boldsymbol{R},+,\cdot)$ je komutativní těleso.
- $(\boldsymbol{Z}_4,+,\cdot)$ okruh s neutrálním prvkem (existují dělitele nuly).
- $(\boldsymbol{Z}_5,+,\cdot)$ je obor integrity.

Cayleyho tabulka pro $(\boldsymbol{Z}_4,\cdot)$

+	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- *Oranžově podbarvená buňka ukazuje na existence dělitelů nuly. Součin dvou nenulových čísel dá nulový výsledek, tedy $2\cdot 2 = 0$.*

Na ZŠ využíváme distributivnosti násobení ke sčítání přímo i při pamětném počítání.

$$(2\ +3)\cdot 4=(2\cdot 4)+(3\cdot 4)=20$$