1 Binární operace na množině

Obsah

Obsah

Binární operace

Definice 3.1
Nechť $A \neq \emptyset$. Každé zobrazení $f : A^n \to A$ nazýváme *n-ární operace na množině A*. Pokud $n = 1$, pak mluvíme o *unární operaci*, jestliže $n = 2$, pak jde o tzv. *binární operaci na množině A*.

Příklad 3.1

- Odmocňování není unární operací na $\mathbf{C}$.
- Odčítání není binární operací na $\mathbf{N}$, ale na $\mathbf{R}$ ano.
- Aritmetický průměr je obecně n-ární operace např. na $\mathbf{R}$, ale ne na $\mathbf{N}$.

Binární operace, Cayleyho tabulky

Příklad 3.2

- Uvažujme zbytkové třídy "modulo 4", tedy množiny $[0]_4 = \{\ldots, -4, 0, 4, \ldots\}$, $[1]_4 = \{\ldots, -3, 1, 5, \ldots\}$, $[2]_4 = \{\ldots, -2, 2, 6, \ldots\}$, $[3]_4 = \{\ldots, -1, 3, 7, \ldots\}$.
- Definujme dále na množině $\mathbf{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ binární operace "$\oplus$" (sčítání na zbytkových třídách) a "$\odot$" (násobení na zbytkových třídách) takto:

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Binární operace

Definice 3.2
Nechť $\triangle$ je binární operace na množině $A \neq \emptyset$. Říkáme, že $\triangle$ je na A

- *komutativní*, jestliže $\forall a, b \in A: \; a \triangle b = b \triangle a$;
- *asociativní*, jestliže $\forall a, b, c \in A: \; (a \triangle b) \triangle c = a \triangle (b \triangle c)$.

Příklad 3.3

- Násobení na množině $\mathbf{C}$ je komutativní i asociativní binární operace.
- Odčítání není komutativní, ani asociativní binární operací $\mathbf{R}$.

2 Algebraické struktury s jednou binární operací

Obsah

Obsah

Pologrupy

Definice 3.3
Nechť " $\triangle$ " je binární operace na $A \neq \emptyset$. Pak dvojici $(A\ ;\ \triangle\ )$ nazýváme *grupoid*. Je-li operace " $\triangle$ " asociativní, pak mluvíme o *pologrupě* $(A\ ;\ \triangle\ )$.

Příklad 3.4

- $(Rel(A)\ ;\ \circ\ )$, kde $Rel(A)$ je množina všech binárních relací na množině A a " $\circ$ " je skládání relací, je pologrupou.
- $(2^A\ ;\ \cup\ )$ a $(2^A\ ;\ \cap\ )$ jsou pologrupy.

Neutrální prvky

Definice 3.4
Jestliže v grupoidu $(A\ ;\ \triangle\ )$ existuje prvek e takový, že $\forall a \in A$ platí

$$a \triangle e = a = e \triangle a,$$

pak e se nazývá *jednotka* (nebo *neutrální prvek*) grupoidu $(A\ ;\ \triangle\ )$.

Věta 3.1
Každý grupoid má nejvýše jednu jednotku.

Monoidy

Definice 3.5
Jestliže v pologrupě $(A\ ;\ \triangle\ )$ existuje jednotka e, pak $(A\ ;\ \triangle\ )$ se nazývá *monoid.*

Příklad 3.5

- $(Rel(A)\ ;\ \circ\ )$ je monoid.
- $(2^A\ ;\ \cup\ )$ a $(2^A\ ;\ \cap\ )$ jsou monoidy.

Inverzní prvky

Definice 3.6
Nechť $(A\ ;\ \triangle\ )$ je monoid s jednotkou e. Jestliže pro každý prvek $a \in A$ existuje prvek $b \in A$ tak, že

$$a \triangle b = b \triangle a = e,$$

pak prvek b se nazývá *inverzní prvek k prvku* a a píšeme $b = a^{-1}$.

Zřejmě naopak prvek a je inverzní k prvku b, tedy $a = b^{-1}$. Je navíc patrné, že $(a^{-1})^{-1} = a$.

Grupy

Definice 3.7
Nechť $(A\ ;\ \triangle\ )$ je monoid s jednotkou e, ve kterém ke každému prvku a existuje prvek inverzní. Pak $(A\ ;\ \triangle\ )$ se nazývá *grupa.* Je-li operace " $\triangle$ " komutativní na A, pak mluvíme o tzv. *abelovské grupě.*

Příklad 3.6

- $(Rel(A)\ ;\ \circ\ )$ je nekomutativní grupa.
- $(\mathbf{R}\ ;\ \cdot\ )$ je komutativní monoid, který není grupou.
- $(2^A\ ;\ \cup\ )$ a $(2^A\ ;\ \cap\ )$ jsou monoidy, ale ne grupy.
- $(\mathbf{Z}_4\ ;\ \oplus\ )$ je abelovská grupa.

3 Algebraické struktury se dvěma binárními operacemi

Obsah

Obsah

Okruhy

Definice 3.8
Okruhem rozumíme trojici $(A\ ;+,\ \cdot\ )$ takovou, že " $+$ " a " $\cdot$ " jsou binární operace na množině $A \neq \emptyset$ a platí:

1. $(A\ ;+)$ je abelovská grupa s jednotkou, kterou značíme 0 (tzv. *nula okruhu* A);
2. $(A\ ;\ \cdot\ )$ je pologrupa;
3. $\forall a, b, c \in A$: $$\begin{aligned} a \cdot (b+c) &= a \cdot b + a \cdot c, \\ (b+c) \cdot a &= b \cdot a + c \cdot a. \end{aligned}$$

Je-li navíc operace " $\cdot$ " komutativní na A, pak se okruh A nazývá *komutativní*. Jestliže pologrupa $(A \setminus \{0\}\ ;\ \cdot\ )$ obsahuje neutrální prvek, pak se okruh A nazývá *unitární*. Tuto jednotku značíme 1.

Okruhy

Příklad 3.7

- $(\mathbf{Z}\ ;+,\ \cdot\ )$, $(\mathbf{Q}\ ;+,\ \cdot\ )$, $(\mathbf{R}\ ;+,\ \cdot\ )$, $(\mathbf{C}\ ;+,\ \cdot\ )$ jsou komutativní, unitární okruhy.
- $(C[a,b]\ ;\oplus,\odot)$, kde $C[a,b]$ je množina spojitých funkcí na intervalu $[a,b]$ a kde
$$\forall f, g \in C[a,b],\ \forall x \in [a,b]: \quad \begin{aligned} (f \oplus g)(x) &\stackrel{def}{=} f(x) + g(x), \\ (f \odot g)(x) &\stackrel{def}{=} f(x) \cdot g(x), \end{aligned}$$
je komutativní, unitární okruh.

Tělesa

Definice 3.9
Okruh $(A\ ;+,\ \cdot\ )$ se nazývá *těleso*, jestliže množina jeho nenulových prvků tvoří spolu s operací " $\cdot$ " grupu. Těleso $(A\ ;+,\ \cdot\ )$ se nazývá *komutativní*, je-li grupa $(A \setminus \{0\}\ ;\ \cdot\ )$ abelovská.

Příklad 3.8

- $(\mathbf{Z}\ ;+,\ \cdot\ )$ je kom., unit. okruh, který není tělesem.
- $(\mathbf{Z}_4\ ;\ \oplus\ ,\ \odot\ )$ z Př. 2 je kom., unit. okruh, který není tělesem.
- $(\mathbf{Q}\ ;+,\ \cdot\ )$, $(\mathbf{R}\ ;+,\ \cdot\ )$, $(\mathbf{C}\ ;+,\ \cdot\ )$ jsou komutativní tělesa.
- $(C[a,b]\ ;\oplus,\odot)$ je kom., unit. okruh., který není tělesem.