

Binární operace v množině

Definice 1: Necht' M je libovolná neprázdná množina. **Binární operací** \circ v množině M rozumíme zobrazení z množiny kartézského součinu $M \times M$ do množiny M .

- Jestliže v binární operaci je vzoru $[x,y] \in M \times M$ přiřazen obraz $z \in M$, píšeme:
 1. $x \circ y = z$; prvek $z \in M$ se nazývá **výsledek operace** \circ .
 2. $\circ: M \times M \rightarrow M$.

Poznámka 1. Zápisu $[[x,y], z] \in \circ$, odpovídá zápis $x \circ y = z$ (tj. z je výsledek operace \circ).

Příklad 1. a) Zápisu $[[1,2], 3] \in +$, odpovídá $1 + 2 = 3$ (tj. 3 je výsledek operace sčítání čísel 1 a 2).

binární operace sčítání součet

b) Zápisu $[[2,3], 6] \in \cdot$, odpovídá $2 \cdot 3 = 6$ (tj. 6 je výsledek operace násobení čísel 2 a 3).

binární operace násobení součin

Poznámka 2. Označení binárních operací: $+$, \cdot , \circ , $*$, \square , ..

Příklady binárních operací ve školské matematice:

- 1) Sčítání ($+$), odčítání ($-$), násobení (\cdot), dělení ($:$), umocňování, ... (pracujeme s nimi v číselných množinách).
- 2) Sjednocení (\cup), průnik (\cap), rozdíl ($-$), symetrický rozdíl (Δ) množin, ... (pracujeme s nimi v systémech množin).

Vlastnosti binárních operací:

Označení:

- \mathbb{N} - $\{1, 2, 3, 4, \dots\}$ - množina všech přirozených čísel
- \mathbb{N}_0 - $\{0, 1, 2, 3, 4, \dots\}$ - množina všech přirozených čísel s nulou (množina všech nezáporných celých čísel)
- \mathbb{C} - $\{\dots, -2, -1, 0, 1, 2, 3, 4, \dots\}$ - množina všech celých čísel
- \mathbb{Q} - množina všech racionálních čísel (zlomky)
- \mathbb{R} - množina všech reálných čísel

Definice 2: Binární operace \circ v množině M , která má vlastnost, že je definována pro každou uspořádanou dvojici $[x,y] \in M \times M$, se nazývá operace **neomezeně definovaná** v množině M (zkráceně operace **definovaná na** množině M). Značíme **ND**.

Symbolicky: $(\forall x, y \in M)(\exists z \in M)[x \circ y = z]$.

Příklad 2:

- operace sčítání ($+$).....v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ **je ND**
- operace odčítání ($-$).....v množině \mathbb{N} **není ND**
v množině $\mathbb{C}, \mathbb{Q}, \mathbb{R}$ **je ND**
- operace násobení (\cdot)..... v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ **je ND**

- operace dělení ($:$)..... v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ není ND
v množině $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ je ND

Definice 3: Binární operace \circ definovaná na množině M (je ND), se nazývá **komutativní** právě tehdy, když platí:

$$(\forall x, y \in M)[x \circ y = y \circ x].$$

Značíme **K**.

Příklad 3:

- operace sčítání (+).....na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ je K
- operace odčítání (-).....na množině $\mathbb{C}, \mathbb{Q}, \mathbb{R}$ není K
- operace násobení (\cdot)..... na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ je K
- operace dělení ($:$)..... na množině $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ není K

Definice 4: Binární operace \circ definovaná na množině M , se nazývá **asociativní** právě tehdy, když platí:

$$(\forall x, y, z \in M)[(x \circ y) \circ z = x \circ (y \circ z)].$$

Značíme **A**.

Příklad 4:

- operace sčítání (+).....na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ je A
- operace odčítání (-).....na množině $\mathbb{C}, \mathbb{Q}, \mathbb{R}$ není A
- operace násobení (\cdot)..... na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ je A
- operace dělení ($:$)..... na množině $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ není A

Definice 5: Necht' v množině M je definována binární operace \circ . Existuje-li prvek $e \in M$, pro který platí:

$$(\forall x \in M)[x \circ e = e \circ x = x].$$

Pak se prvek $e \in M$ nazývá **neutrálním prvkem** množiny M vzhledem k operaci \circ .

Značíme **EN**.

Příklad 5:

- operace sčítání (+).....na množině \mathbb{N} nemá vlastnost EN (tj. neexistuje neutrální prvek v množině \mathbb{N} vzhledem ke sčítání)
- operace sčítání (+).....na množině $\mathbb{N}_0, \mathbb{C}, \mathbb{Q}$ má vlastnost EN (tj. existuje neutrální prvek vzhledem ke sčítání $e = 0$, tj. $x + 0 = 0 + x = x$ platí pro každé $x \in M$)
- operace odčítání (-).....v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ nemá vlastnost EN (tj. neexistuje neutrální prvek vzhledem k odčítání)
- operace násobení (\cdot)..... na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ má vlastnost EN (tj. existuje neutrální prvek vzhledem k násobení $e = 1$, tj. $x \cdot 1 = 1 \cdot x = x$ platí pro každé $x \in M$)
- operace dělení ($:$).....v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ nemá vlastnost EN (tj. neexistuje neutrální prvek vzhledem k dělení)

Poznámka 3. Je-li operace \circ komutativní, pak v zápisu vlastnosti **EN** lze vynechat jedna ze dvou stran rovnosti $x \circ e$ nebo $e \circ x$.

Definice 6: Necht' v množině M je definována binární operace \circ a necht' e je neutrální prvek množiny M vzhledem k operaci \circ . Prvek $\bar{a} \in M$ nazýváme **inverzním prvkem** k prvku $a \in M$ v operaci \circ v množině M právě tehdy, když platí:

$$\bar{a} \circ a = a \circ \bar{a} = e.$$

Jestliže $(\forall a \in M)(\exists \bar{a} \in M)[\bar{a} \circ a = a \circ \bar{a} = e]$, řekneme, že ke každému prvku množiny M existuje prvek inverzní vzhledem k operaci \circ . Značíme **EI**.

Příklad 6:

- operace sčítání (+).....na množině \mathbb{N}_0 nemá vlastnost EI
- operace sčítání (+).....na množině \mathbb{C}, \mathbb{Q} má vlastnost EI (tj. existuje inverzní prvek ke každému prvku z dané množiny vzhledem ke sčítání tak, aby platilo $\bar{a} + a = a + \bar{a} = 0$. Inverzní prvek k prvku a vzhledem ke sčítání se nazývá **prvek opačný** a značíme jej $\bar{a} = -a$)
- operace odčítání (-).....v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ nemá vlastnost EI (neboť nemá vlastnost **EN**)
- operace násobení (\cdot)..... na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ nemá vlastnost EI
- operace násobení (\cdot)..... na množině $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ má vlastnost EI (tj. existuje inverzní prvek ke každému prvku z dané množiny vzhledem k násobení tak, aby platilo $\bar{a} \cdot a = a \cdot \bar{a} = 1$. Inverzní prvek k prvku a vzhledem k násobení se nazývá **prvek převrácený** a značíme jej $\bar{a} = \frac{1}{a} = a^{-1}$.)
- operace dělení ($:$).....v množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ nemá vlastnost EI (neboť nemá vlastnost **EN**)

Poznámka 4. Je-li operace \circ komutativní, pak v zápisu vlastnosti **EI** lze vynechat jedna ze dvou stran rovnosti $\bar{a} \circ a = a \circ \bar{a}$.

Definice 7: Necht' v množině M je definována binární operace \circ . Existuje-li prvek $g \in M$, pro který platí:

$$(\forall x \in M)[x \circ g = g \circ x = g].$$

Pak se prvek $g \in M$ nazývá **agresivním prvkem** množiny M vzhledem k operaci \circ . Značíme **AG**.

Příklad 7:

- operace sčítání (+).....na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}$ nemá vlastnost AG (tj. neexistuje agresivní prvek vzhledem ke sčítání)
- operace násobení (\cdot)..... na množině $\mathbb{N}_0, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ má vlastnost AG (tj. existuje agresivní prvek vzhledem k násobení $g=0$: $x \cdot 0 = 0 \cdot x = 0$)

Poznámka 5. Je-li operace \circ komutativní, pak v zápisu vlastnosti **AG** lze vynechat jedna ze dvou stran rovnosti $x \circ g$ nebo $g \circ x$.

Definice 8: Říkáme, že binární operace \circ definovaná na množině M má vlastnost **řešitelnost základních rovnic** právě tehdy, když platí:

$$(\forall a, b \in M)(\exists x, y \in M)[a \circ x = b \wedge y \circ a = b].$$

Značíme **ZR**.

Poznámka 5. Je-li operace \circ komutativní, pak v zápisu vlastnosti **ZR** lze vynechat jedna z výrokových forem $a \circ x = b$ nebo $y \circ a = b$.

Příklad 8:

- operace sčítání (+).....na množině \mathbb{N} , nemá vlastnost **ZR** (tj. rovnice $a + x = b$ není pro všechny prvky množiny \mathbb{N} řešitelná)
- operace sčítání (+).....na množině $\mathbb{C}, \mathbb{Q}, \mathbb{R}$ má vlastnost **ZR** (tj. rovnice $a + x = b$ je pro všechny prvky uvažovaných množin řešitelná: $x = b - a$)
- operace násobení (\cdot)..... na množině $\mathbb{N}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ nemá vlastnost **ZR** (tj. rovnice $a \cdot x = b$ není pro všechny prvky uvažovaných množin řešitelná)
- operace násobení (\cdot)..... na množině $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ má vlastnost **ZR** (tj. rovnice $a \cdot x = b$ je pro všechny prvky uvažovaných množin řešitelná: $x = \frac{b}{a}$)

Určení vlastností binárních operací podle tvaru operační tabulky

Uvažujme binární operaci \circ v množině M zapsané pomocí operační tabulky, viz příklad:

Příklad 9: Je dána množina $M = \{a, b, c\}$ a operace \circ v množině M daná tabulkou. Určete vlastnosti operace \circ . Pokud existuje neutrální nebo agresivní prvek, určete je. K jednotlivým prvkům stanovte prvky inverzní, pokud existují.

\circ	a	b	c
a	b	c	a
b	c	c	b
c	a	b	c

Vysvětlivky k tabulce: $a \circ a = b$
 $b \circ c = b$
 $c \circ a = a$

Řešení: **ND** \wedge **K** \wedge ~~**A**~~ \wedge **EN** \wedge **EI** \wedge ~~**ZR**~~ \wedge ~~**AG**~~

Pravidla pro určování vlastností operace v množině dané tabulkou:

ND: Tabulka je celá vyplněná prvky množiny M

K: Prvky tabulky, která je celá vyplněná prvky množiny M , jsou souměrně rozloženy podle hlavní diagonály

- A:** Z tabulky obvykle nepoznáme - určujeme z definice nebo ze vztahu $A \Rightarrow (ZR \Leftrightarrow EI)$
- EN:** Alespoň jeden řádek a jeden sloupec jsou stejné jako záhlaví tabulky
- EI:** Každý řádek i sloupec tabulky obsahuje neutrální prvky tak, že ve všech řádcích a sloupcích existují takové, že jsou souměrně rozloženy podle hlavní diagonály.
- ZR:** Každý řádek i sloupec obsahuje všechny prvky množiny M
- AG:** Agresivní prvek $g \in M$ má v celém jemu příslušejícím řádku i sloupci prvek g .

Algebraické struktury s jednou operací

Definice 9: Uspořádaná dvojice (M, \circ) , kde M je neprázdná množina, ve které je definována binární operace \circ , se nazývá **algebraická struktura s jednou operací**.

Příklad 9: Příklad algebraických struktur: $(\mathbb{N}, +)$, $(\mathbb{C}, -)$, $(\mathbb{Q} - \{0\}, :)$, (\mathbb{R}, \cdot) ; (M, \circ) , kde množina $M = \{a, b, c\}$ a operace \circ jsou z *Příkladu 9*.

Definice 10:

- I. Algebraická struktura (M, \circ) se nazývá **grupoid** právě tehdy, když operace \circ je neomezeně definovaná v množině M (ND).
- II. Grupoid (M, \circ) , jehož operace \circ je asociativní, se nazývá **podgrupa** (ND, A).
- III. Pologrupa (M, \circ) taková, že v M existuje neutrální prvek vzhledem k operaci (M, \circ) a ke každému prvku $a \in M$ existuje prvek inverzní $\bar{a} \in M$, se nazývá **grupa** (ND, A, EN, EI).

Poznámka 6. Jestliže v případech I., II., III. je operace \circ komutativní, pak hovoříme o

- I. Komutativním grupoidu
- II. Komutativní pologrupě
- III. Komutativní grupě

Schéma k *Definici 10:*

	Vlastnost operace \circ	Algebraická struktura
(M, \circ)	ND	Grupoid
	ND \wedge K	Komutativní grupoid
	ND \wedge A	Pologrupa
	ND \wedge A \wedge K	Komutativní pologrupa
	ND \wedge A \wedge EN \wedge EI	Grupa
	ND \wedge A \wedge EN \wedge EI \wedge K	Komutativní grupa

Příklady algebraických struktur s jednou operací

1. $(\mathbb{N}, +)$... komutativní pologrupa

sčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

rovnice $a + x = b$ není pro libovolné $a, b \in \mathbb{N}$ řešitelná

2. $(\mathbb{N}_0, +)$... komutativní pologrupa s neutrálním prvkem $e = 0$

sčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

3. $(\mathbb{N}_0, -)$... není ani grupoid

odčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

hledáme neutrální prvek, pro který platí: $a - e = e - a = a$

$$a - e = a \wedge e - a = a$$

$$e = 0 \wedge e = 2a \text{ (vlastnost EN není splněna)}$$

4. (\mathbb{N}_0, \cdot) ... komutativní pologrupa s neutrálním prvkem $e = 1$

násobení ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

5. $(\mathbb{N}_0, :)$... není ani grupoid

dělení ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

6. $(\mathbb{C}, +)$... komutativní grupa s neutrálním prvkem $e = 0$

sčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

$$\bar{a} = -a$$

rovnice $a + x = b$ je pro libovolné $a, b \in \mathbb{C}$ řešitelná

7. $(\mathbb{C}, -)$... grupoid s vlastností ZR

odčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

operace odčítání není K: $a - x = b \wedge y - a = b$

obě rovnice jsou pro lib. $a, b \in \mathbb{C}$ řešitelné

8. (\mathbb{C}, \cdot) ... komutativní pologrupa s neutrálním prvkem $e = 1$

násobení ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

rovnice $a \cdot x = b$ není pro libovolné $a, b \in \mathbb{C}$ řešitelná

9. $(\mathbb{C}, :)$... není ani grupoid

dělení ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

10. $(\mathbb{Q}, +), (\mathbb{R}, +)$... komutativní grupy s neutrálním prvkem $e = 0$

sčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

$$\bar{a} = -a$$

rovnice $a + x = b$ je pro libovolné $a, b \in \mathbb{Q}, \mathbb{R}$ řešitelná

11. $(\mathbb{Q}, -), (\mathbb{R}, -)$... grupoid s vlastností ZR

odčítání ... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

12. $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$... komutativní pologrupy s neutrálním prvkem $e = 1$

násobení... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EH~~ \wedge ~~ZR~~

$$\text{EH: } \bar{a} \cdot a = 1$$

$$\bar{a} = \frac{1}{a}$$

pro $a = 0$ však neexistuje \bar{a} , neboť výraz $\frac{1}{0}$ není definován

$$\text{ZR: } a \cdot x = b$$

$$x = \frac{b}{a}$$

pro $a = 0 \wedge b \neq 0$ však neexistuje $x \in \mathbb{Q}, \mathbb{R}$ tak, aby platilo $0 \cdot x = b$. 13.

$(\mathbb{Q}, :), (\mathbb{R}, :)$... není ani grupoid

dělení... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EH~~ \wedge ~~ZR~~

14. $(\mathbb{Q} - \{0\}, \cdot), (\mathbb{R} - \{0\}, \cdot)$... komutativní grupa s neutrálním prvkem $e = 1$

násobení... ~~ND~~ \wedge ~~K~~ \wedge ~~A~~ \wedge ~~EN~~ \wedge ~~EI~~ \wedge ~~ZR~~

$$\bar{a} = \frac{1}{a}$$