# Binární operace v množině

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

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

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

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

**binární operace sčítání** **součet**

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

**binární operace násobení** **součin**

*Poznámka 2.* <u>Označení binárních operací</u>: $+$, $\cdot$, $\circ$, $*$, $\square$,..

<u>Příklady binárních operací ve školské matematice</u>:

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

## <u>Vlastnosti binárních operací:</u>

Označení:

- $\mathbb{N}$ - {1, 2, 3, 4, ...} - množina všech přirozených čísel
- $\mathbb{N}_0$ - {0, 1, 2, 3, 4, ...} - množina všech přirozených čísel s nulou (množina všech nezáporných celých čísel)
- $\mathbb{C}$ - {..., -2, -1, 0, 1, 2, 3, 4, ...} - 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 x M, se nazývá operace **neomezeně definovaná** v množině M (zkráceně operace **definovaná na** množině M). Značíme **ND**.

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

*Příklad 2*:

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

- operace dělení (**:**)……. v množině $\mathbb{N}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$ <u>není</u> **ND**
  v množině $\mathbb{Q}$ - {0}, $\mathbb{R}$ - {0} <u>je</u> **ND**

---

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

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

Značíme **K**.

*Příklad 3*:

- operace sčítání (+)…….na množině $\mathbb{N}$, $\mathbb{C}$, $\mathbb{Q}$ <u>je</u> **K**
- operace odčítání (**-**)……na množině $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$ <u>není</u> **K**
- operace násobení (·)….. na množině $\mathbb{N}$, $\mathbb{C}$, $\mathbb{Q}$ <u>je</u> **K**
- operace dělení (**:**)…….. na množině $\mathbb{Q}$ - {0}, $\mathbb{R}$ - {0} <u>není</u> **K**

---

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

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

Značíme **A**.

*Příklad 4*:

- operace sčítání (+)…….na množině $\mathbb{N}$, $\mathbb{C}$, $\mathbb{Q}$ <u>je</u> **A**
- operace odčítání (**-**)……na množině $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$ <u>není</u> **A**
- operace násobení (·)….. na množině $\mathbb{N}$, $\mathbb{C}$, $\mathbb{Q}$ <u>je</u> **A**
- operace dělení (**:**)…….. na množině $\mathbb{Q}$ - {0}, $\mathbb{R}$ - {0} <u>není</u> **A**

---

*Definice 5:* Nechť v množině M je definována binární operace ○. Existuje-li prvek $e \in$ M, pro který platí:

$$(\forall\, x \in \mathrm{M})[\, x \circ e = e \circ x = x].$$

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

*Příklad* 5:

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

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

---

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

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

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

*Příklad* 6:

- operace sčítání (+)…….na množině $\mathbb{N}_0$ nemá vlastnost **EI**
- operace sčítání (+)…….na množině ℂ, 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 ℕ, ℂ, ℚ, ℝ nemá vlastnost **EI** (neboť nemá vlastnost **EN**)
- operace násobení (·)….. na množině ℕ, ℂ, ℚ nemá vlastnost **EI**
- operace násobení (·)….. na množině ℚ - {0}, 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 ℕ, ℂ, ℚ, ℝ nemá vlastnost **EI** (neboť nemá vlastnost **EN**)

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

---

*Definice 7:* Nechť v množině M je definována binární operace ○. Existuje-li prvek $g \in$ M, pro který platí:

$$(\forall\, x \in \mathrm{M})[x \circ g = g \circ x = g].$$

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

*Příklad* 7:

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

*Poznámka 5*. Je-li operace ○ 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 ○ definovaná na množině M má vlastnost **řešitelnost základních rovnic** právě tehdy, když platí:

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

Značíme **ZR**.

*Poznámka 5*. Je-li operace ○ 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 ℕ, <u>nemá vlastnost</u> **ZR** (tj. rovnice $a + x = b$ <u>není pro všechny prvky množiny ℕ řešitelná</u>)
- operace sčítání (+)…….na množině ℂ, ℚ, ℝ <u>má vlastnost</u> **ZR** (tj. rovnice $a + x = b$ <u>je pro všechny prvky uvažovaných množin řešitelná</u>: $x = b - a$)
- operace násobení (·)….. na množině ℕ, ℂ, ℚ, ℝ <u>nemá vlastnost</u> **ZR** (tj. rovnice $a \cdot x = b$ <u>není pro všechny prvky uvažovaných množin řešitelná</u>)
- operace násobení (·)….. na množině ℚ - {0}, ℝ - {0} <u>má vlastnost</u> **ZR** (tj. rovnice $a \cdot x = b$ <u>je pro všechny prvky uvažovaných množin řešitelná</u>: $x = \frac{b}{a}$ )

## <u>Určení vlastností binárních operací podle tvaru operační tabulky</u>

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

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

| ○ | a | b | c |
|---|---|---|---|
| a | b | c | a |
| b | c | c | b |
| c | a | b | c |

<u>Vysvětlivky k tabulce</u>: a ○ a = b
b ○ c = b
c ○ a = a

Řešení: <u>**ND**</u> ∧ <u>**K**</u> ∧ ~~**A**~~ ∧ <u>**EN**</u> ∧ <u>**EI**</u> ∧ ~~**ZR**~~ ∧ ~~**AG**~~

<u>Pravidla pro určování vlastností operace v množině dané tabulkou:</u>

**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, ○), kde M je neprázdná množina, ve které je definována binární operace ○, se nazývá **algebraická struktura s jednou operací.**

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

*Definice 10:*

I. Algebraická struktura (M, ○) se nazývá **grupoid** právě tehdy, když operace ○ je neomezeně definovaná v množině M (ND).

II. Grupoid (M, ○), jehož operace ○ je asociativní, se nazývá **podgrupa** (ND, A).

III. Pologrupa (M, ○) taková, že v M existuje neutrální prvek vzhledem k operaci (M, ○) 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 ○ komutativní, pak hovoříme o

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

Schéma k *Definici 10*:

| | **Vlastnost operace ○** | **Algebraická struktura** |
|---|---|---|
| (M, ○) | ND | Grupoid |
| | ND ∧ K | Komutativní grupoid |
| | ND ∧ A | Pologrupa |
| | ND ∧ A ∧ K | Komutativní pologrupa |
| | ND ∧ A ∧ EN ∧ EI | Grupa |
| | ND ∧ A ∧ EN ∧ EI ∧ K | Komutativní grupa |

## Příklady algebraických struktur s jednou operací

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

sčítání … <u>ND</u> ∧ <u>K</u> ∧ <u>A</u> ∧ ~~EN~~ ∧ ~~EI~~ ∧ ~~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 … <u>ND</u> ∧ <u>K</u> ∧ <u>A</u> ∧ <u>EN</u> ∧ ~~EI~~ ∧ ~~ZR~~

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

odčítání …~~ND~~ ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ ~~ZR~~

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

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

$e = 0 \;\wedge\; e = 2a$ (vlastnost EN není splněna)

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

násobení …<u>ND</u> ∧ <u>K</u> ∧ <u>A</u> ∧ <u>EN</u> ∧ ~~EI~~ ∧ ~~ZR~~

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

dělení… ~~ND~~ ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ ~~ZR~~

---

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

sčítání…<u>ND</u> ∧ <u>K</u> ∧ <u>A</u> ∧ <u>EN</u> ∧ <u>EI</u> ∧ <u>ZR</u>

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

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

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

odčítání …<u>ND</u> ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ <u>ZR</u>

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

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

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

násobení …ND ∧ K ∧ A ∧ EN ∧ ~~EI~~ ∧ ~~ZR~~

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

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

dělení… ~~ND~~ ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ ~~ZR~~

---

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

sčítání…<u>ND</u> ∧ <u>K</u> ∧ <u>A</u> ∧ <u>EN</u> ∧ <u>EI</u> ∧ <u>ZR</u>

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

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 …<u>ND</u> ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ <u>ZR</u>

12. (ℚ, ·), (ℝ, ·)… komutativní pologrupy s neutrálním prvkem $e = 1$

násobení …ND ∧ K ∧ A ∧ EN ∧ ~~EI~~ ∧ ~~ZR~~

~~EI~~: $\bar{a} \cdot a = 1$

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

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

~~ZR~~: $a \cdot x = b$

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

pro $a = 0 \wedge b \neq 0$ však neexistuje x ∈ ℚ, ℝ tak, aby platilo $0 \cdot x = b$.

13. (ℚ, :), (ℝ, :)… není ani grupoid

dělení… ~~ND~~ ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ ~~ZR~~

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

násobení…ND ∧ K ∧ A ∧ EN ∧ EI ∧ ZR

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