

- **Binárna operácia** na množine A je zobrazenie množiny $A \times A$ do A .

- **Binárna operácia** na množine A je zobrazenie množiny $A \times A$ do A .
- Hovoríme, že binárna operácia \circ na množine A je **komutatívna**, ak

$$\forall x, y \in A; \quad x \circ y = y \circ x.$$

- **Binárna operácia** na množine A je zobrazenie množiny $A \times A$ do A .
- Hovoríme, že binárna operácia \circ na množine A je **komutatívna**, ak

$$\forall x, y \in A; \quad x \circ y = y \circ x.$$

- Hovoríme, že binárna operácia \circ na množine A je **asociatívna**, ak

$$\forall x, y, z \in A; \quad (x \circ y) \circ z = x \circ (y \circ z).$$

- Nech \circ je binárna operácia na množine A . Ak existuje taký prvok $e \in A$, o ktorom platí

$$\forall a \in A; \quad a \circ e = e \circ a = a,$$

tak prvok e nazývame **neutrálnym prvkom** operácie \circ .

Definícia-Inverzný prvok operácie

- Nech \circ je binárna operácia na množine A a nech e je neutrálny prvok tejto operácie. Ak o prvkoch $a, a' \in A$ platí

$$a \circ a' = a' \circ a = e,$$

tak prvok a' nazývame **inverzným prvkom k prvku a** (vzhľadom na operáciu \circ .)

Budeme pracovať na množine prirodzených čísel (počítame aj s nulou).

- Klasické sčítanie

\mathbb{N}	+	-	*	/
UZ.	Ano	Ano	Ano	Ne
AS.	Ano	Ne	Ano	
N.P.	0	Ne	1	
IN.P.	Ano	Ne	Ne (R bez nuly by fungovalo)	
KOM.	Ano	Ne	Ano	

\mathbb{N}	+	-	*	/
UZ.	Ano	Ne	Ano	Ne
AS.	Ano		Ano	
N.P.	0		1	
IN.P.	Ne		Ne	
KOM.	Ano		Ano	

$\mathbb{R} \setminus \{0\}$	+	-	*	/
UZ.	Ne	Ne	Ano	Ano
AS.			Ano	Ne
N.P.			1	Ne
IN.P.			Ano	Ne
KOM.			Ano	Ne

Budeme pracovať na množine prirodzených čísel (počítame aj s nulou).

- Klasické sčítanie je operácia na N , navyše je komutatívna, asociatívna a má neutrálny prvok 0. K prvkom množiny N neexistujú inverzné (opačné) prvky, iba k 0, tá si je sama sebe inverzná.

Budeme pracovať na množine prirodzených čísel (počítame aj s nulou).

- Klasické sčítanie je operácia na N , navyše je komutatívna, asociatívna a má neutrálny prvok 0. K prvkom množiny N neexistujú inverzné (opačné) prvky, iba k 0, tá si je sama sebe inverzná.
- Klasické odčítanie

Budeme pracovať na množine prirodzených čísel (počítame aj s nulou).

- Klasické sčítanie je operácia na N , navyše je komutatívna, asociatívna a má neutrálny prvok 0. K prvkom množiny N neexistujú inverzné (opačné) prvky, iba k 0, tá si je sama sebe inverzná.
- Klasické odčítanie nie je operáciou na N . Napr. $1 \in N, 2 \in N$, ale $1 - 2 \notin N$.

Budeme pracovať na množine prirodzených čísel (počítame aj s nulou).

- Klasické sčítanie je operácia na N , navyše je komutatívna, asociatívna a má neutrálny prvok 0. K prvkom množiny N neexistujú inverzné (opačné) prvky, iba k 0, tá si je sama sebe inverzná.
- Klasické odčítanie nie je operáciou na N . Napr. $1 \in N, 2 \in N$, ale $1 - 2 \notin N$.
- Klasické násobenie

Budeme pracovať na množine prirodzených čísel (počítame aj s nulou).

- Klasické sčítanie je operácia na N , navyše je komutatívna, asociatívna a má neutrálny prvok 0. K prvkom množiny N neexistujú inverzné (opačné) prvky, iba k 0, tá si je sama sebe inverzná.
- Klasické odčítanie nie je operáciou na N . Napr. $1 \in N, 2 \in N$, ale $1 - 2 \notin N$.
- Klasické násobenie je operácia na N , navyše je komutatívna, asociatívna a ak "vyhodíme 0", tak má aj neutrálny prvok 1. K prvkom množiny N neexistujú inverzné prvky, iba k 1, tá si je sama sebe inverzná.

- Binárna operácia (na množine A) má najviac jeden neutrálny prvok.

Tvrdenie-Inverzný prvok operácie

- Nech \circ je asociatívna operácia na množine A a nech e je neutrálny prvok tejto operácie. Potom ku každému prvku $a \in A$ existuje najviac jeden inverzný prvok.

- Usporiadanú dvojicu (G, \circ) , kde G je neprázdna množina a \circ je binárna operácia na množine G , nazývame **grupoidom**. Množinu G nazývame nosičom a operáciu \circ operáciou grupoidu.

- Usporiadanú dvojicu (G, \circ) , kde G je neprázdna množina a \circ je binárna operácia na množine G , nazývame **grupoidom**. Množinu G nazývame nosičom a operáciu \circ operáciou grupoidu.
- Hovoríme, že grupoid (H, \circ) je **podgrupoidom** grupoidu (G, \circ) , ak platí:
 - $H \subseteq G$,
 - $\forall a, b \in H; a \circ b \in H$.

- Usporiadanú dvojicu (G, \circ) , kde G je neprázdna množina a \circ je asociatívna operácia na množine G , nazývame **pologrupou**. Množinu G nazývame nosičom a operáciu \circ operáciou pologrupy.

- Usporiadanú dvojicu (G, \circ) , kde G je neprázdna množina a \circ je asociatívna operácia na množine G , nazývame **pologrupou**. Množinu G nazývame nosičom a operáciu \circ operáciou pologrupy.
- Pologrupa s neutrálnym prvkom sa nazýva **monoid**.

- Usporiadanú dvojicu (G, \circ) , kde G je neprázdna množina a \circ je asociatívna operácia na množine G , nazývame **pologrupou**. Množinu G nazývame nosičom a operáciu \circ operáciou pologrupy.
- Pologrupa s neutrálnym prvkom sa nazýva **monoid**.
- Monoid, v ktorom ku každému prvku existuje inverzný prvok, sa nazýva **grupa**.

- Usporiadanú dvojicu (G, \circ) , kde G je neprázdna množina a \circ je asociatívna operácia na množine G , nazývame **pologrupou**. Množinu G nazývame nosičom a operáciu \circ operáciou pologrupy.
- Pologrupa s neutrálnym prvkom sa nazýva **monoid**.
- Monoid, v ktorom ku každému prvku existuje inverzný prvok, sa nazýva **grupa**.
- Grupa s komutatívnou operáciou sa nazýva **komutatívna** alebo **Abelova grupa**.

- Ak je podgrupoid grupy G grupou, nazývame ho **podgrupou** grupy G .

- Ak je podgrupoid grupy G grupou, nazývame ho **podgrupou** grupy G .
- Rozklady podľa podgrupy:
 - **Ľavý rozklad** grupy G podľa podgrupy H je množina

$$\{aH : a \in G\},$$

kde množiny $aH = \{a \cdot h : h \in H\}$ sa nazývajú **ľavé triedy** rozkladu.

- **Pravý rozklad** grupy G podľa podgrupy H je množina

$$\{Ha : a \in G\}$$

kde množiny $Ha = \{h \cdot a : h \in H\}$ sa nazývajú **pravé triedy** rozkladu.

- **Lagrangeova veta.** Počet prvkov podgrupy je deliteľom počtu prvkov grupy.

- **Lagrangeova veta.** Počet prvkov podgrupy je deliteľom počtu prvkov grupy.
- Nech H je neprázdna podmnožina množiny G . (H, \circ) je podgrupou grupy (G, \circ) vtedy a len vtedy, keď platí:

$$\forall a, b \in H; \quad a \circ b^{-1} \in H.$$

- Podgrupa (H, \circ) grupy (G, \circ) sa nazýva **normálna podgrupa**, ak pre ľubovoľné $a \in G, h \in H$ platí: $a \circ h \circ a^{-1} \in H$.
- Ak je ľavý a pravý rozklad grupy G podľa podgrupy H rovnaký, tak H je normálna podgrupa.
- **Poznámka.** Každá podgrupa komutatívnej grupy je normálna. Podgrupy nekomutatívnych grúp nemusia byť normálne.

Homomorfizmy

Nech (A, \star) , (B, \circ) sú algebry rovnakého typu. Nech $h: A \rightarrow B$ je také zobrazenie, že pre ľubovoľné $a, b \in A$ platí

$$h(a \star b) = h(a) \circ h(b),$$

tak h sa nazýva **homomorfizmus** algebry A do algebry B .

- Ak h je injektívny homomorfizmus, hovoríme, že h je **monomorfizmus**.
- Ak h je surjektívny homomorfizmus, hovoríme, že h je **epimorfizmus**.
- Ak h je bijektívny homomorfizmus, hovoríme, že h je **izomorfizmus**.
- Ak h je homomorfizmus algebry A do A , hovoríme, že h je **endomorfizmus**.
- Ak h je izomorfizmus A na A , hovoríme, že h je **automorfizmus**.

Relácia kongruencie alebo kongruencia je ekvivalencia na algebre (napr. grupe), ktorá je zlučiteľná so všetkými operáciami na tejto algebre (teda napríklad, ak sú tri páry prvkov ekvivalentné a výsledky nejakej operácie na týchto pároch sú tiež ekvivalentné, potom existuje pre tieto páry zhodnosť). Teda ak sú operandy na rovnakom mieste po dvoch ekvivalentné, potom musia aj výsledky operácie byť ekvivalentné.

- Nech (X, \circ) je algebra, R je ekvivalencia na X . Potom R je **kongruencia** na X ak platí:
 $[a, b] \in R \wedge [c, d] \in R \Rightarrow [a \circ c, b \circ d] \in R.$

Relácia kongruencie alebo kongruencia je ekvivalencia na algebre (napr. grupe), ktorá je zlučiteľná so všetkými operáciami na tejto algebre (teda napríklad, ak sú tri páry prvkov ekvivalentné a výsledky nejakej operácie na týchto pároch sú tiež ekvivalentné, potom existuje pre tieto páry zhodnosť). Teda ak sú operandy na rovnakom mieste po dvoch ekvivalentné, potom musia aj výsledky operácie byť ekvivalentné.

- Nech (X, \circ) je algebra, R je ekvivalencia na X . Potom R je **kongruencia** na X ak platí:
 $[a, b] \in R \wedge [c, d] \in R \Rightarrow [a \circ c, b \circ d] \in R$.
- Hovoríme, že dve čísla $a, b \in \mathbb{Z}$ sú kongruentné, ak ich rozdiel je deliteľný číslom m , ktoré nazývame **modulo** ($m|(a - b)$).
Formálne

$$a \equiv b \pmod{m}.$$

- Zrejme

$$\left. \begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array} \right\} \Rightarrow a + c \equiv b + d \pmod{m}.$$

teda \equiv je kongruencia na $(\mathbb{Z}, +)$.

- Zrejme

$$\left. \begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array} \right\} \Rightarrow a + c \equiv b + d \pmod{m}.$$

teda \equiv je kongruencia na $(\mathbb{Z}, +)$.

- Ale aj

$$\left. \begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array} \right\} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}.$$

teda \equiv je kongruencia aj na (\mathbb{Z}, \cdot) .

- Nech (G, \circ) je grupa, R je kongruencia na G . Nech $1 \in G$ je jednotkový prvok v G . Potom $H = [1]_R = \{x; x \in G \wedge [x, 1] \in R\}$ je normálna podgrupa grupy G .
- Nech (G, \circ) je grupa, $H \subseteq G$ je jej normálna podgrupa. Potom relácia $R = \{[x, y]; x, y \in G \wedge y^{-1} \circ x \in H\}$ je kongruencia na G .

- Nech (G, \circ) je grupa, $H \subseteq G$ je jej normálna podgrupa. Nech relácia $R = \{[x, y]; x, y \in G \wedge y^{-1} \circ x \in H\}$ je kongruencia na G . (to už vieme, že je kongruencia). Potom grupa tried grupy G vzhľadom na normálnu podgrupu H sa nazýva **faktorovou grupou** a označuje sa G/H .