

# Grupy a polia

5. októbra 2010

# Definícia binárnej operácie

## Definícia

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

Namiesto  $*(a, b)$  budeme používať označenie  $a * b$ , tento zápis budeme niekedy skracovať ako  $ab$ .

## Príklady binárnych operácií

 $+ \cdot$  na  $\mathbb{R}$  $a \oplus b = (a + b) \bmod 5$  a  $a \odot b = (a \cdot b) \bmod 5$  na  $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ 

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

# Príklady binárnych operácií

Pre konečnú množinu môžeme binárnu operáciu zadať tabuľkou.

$\triangle$	0	1	2
0	0	1	2
1	0	1	2
2	0	2	1

# Vlastnosti binárnych operácií

## Definícia

Nech  $*$  je binárna operácia na množine  $M$ .

- ▶  $e \in M$  je *neutrálny prvok* operácie  $*$ , ak  $(\forall m \in M)$  platí

$$e * m = m * e = m.$$

- ▶ Operácia  $*$  je *komutatívna*, ak  $(\forall x, y \in M)$  platí

$$x * y = y * x.$$

- ▶ Operácia  $*$  je *asociatívna*, ak  $(\forall x, y, z \in M)$  platí

$$(x * y) * z = x * (y * z).$$

Ak existuje neutrálny prvok, tak je jednoznačne určený.

# Asociatívnosť

Asociatívnosť vlastne znamená, že nezáleží na uzátvorkovaní:

$$\begin{array}{c} (x * y) * z \\ \swarrow \quad \searrow \\ x * (y * z) \end{array}$$

# Vlastnosti binárnych operácií

## Definícia

Nech  $*$  je binárna operácia na množine  $M$  a  $e \in M$  je jej neutrálny prvok.

- ▶ Prvok  $b \in M$  je *inverzný* k prvku  $a$ , ak platí

$$a * b = b * a = e.$$

Pre asociatívnu binárnu operáciu platí jednoznačnosť inverzného prvku. Inverzný prvok označujeme  $a^{-1}$ .

# Definícia grupy

## Definícia

Dvojica  $(G, *)$ , kde  $G$  je množina a  $*$  je binárna operácia na  $G$ , sa nazýva *grupa*, ak

- (i) operácia  $*$  je asociatívna,
- (ii) operácia  $*$  má neutrálny prvok, (neutrálny prvok budeme spravidla označovať  $e$ )
- (iii) ku každému prvku  $g \in G$  existuje inverzný prvok vzhľadom na operáciu  $*$ . (Tento inverzný prvok budeme označovať  $g^{-1}$ .)

Ak  $*$  je navyše komutatívna, tak aj grupa  $(G, *)$  sa nazýva komutatívna (abelovská).

Príklady grúp:  $(\mathbb{R}, +)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\mathbb{Z}_5, \oplus)$



# Definícia grupy

Grupa:  $*$  je binárna operácia na  $G$  a platí

$$(\forall a, b, c \in G) a * (b * c) = (a * b) * c$$

$$(\exists e \in G)(\forall a \in G) e * a = a * e = a$$

$$(\forall a \in G)(\exists b \in G) a * b = b * a = e$$

Komutatívna grupa:

$$(\forall a, b \in G) a * b = b * a$$

# Vlastnosti grúp

## Veta (Zákony o krátení)

Ak  $(G, *)$  je grupa, tak pre ľubovoľné  $a, b, c \in G$  platí

$$a * b = a * c \quad \Rightarrow \quad b = c$$

$$b * a = c * a \quad \Rightarrow \quad b = c$$

## Veta

Nech  $(G, *)$  je grupa. Potom pre ľubovoľné  $a, b \in G$  platí

$$(a^{-1})^{-1} = a$$

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

# Definícia poľa

## Definícia

Nech  $F$  je množina,  $+$  a  $\cdot$  sú binárne operácie na  $F$ . Hovoríme, že trojica  $(F, +, \cdot)$  je *pole*, ak

- (i)  $(F, +)$  je komutatívna grupa, jej neutrálny prvok budeme označovať  $0$ ;
- (ii)  $(F \setminus \{0\}, \cdot)$  je komutatívna grupa, jej neutrálny prvok budeme označovať  $1$ ;
- (iii) pre ľubovoľné  $a, b, c \in F$  platí

$$a(b + c) = ab + ac,$$

$$(a + b)c = ac + bc.$$

(Túto vlastnosť nazývame *distributívnosť*.)

## Označenia

Pre inverzný prvok v grupe  $(F, +)$  budeme používať označenie  $-a$ , t.j. pre túto grupu používame aditívny zápis. Prvok  $-a$  nazývame *opačný prvok* k prvku  $a$ . Inverzný prvok k prvku  $a \neq 0$  pol'a  $F$  vzhľadom na operáciu  $\cdot$  budeme značiť  $a^{-1}$ .

Namiesto  $b + (-c)$  budeme používať stručnejší zápis  $b - c$ .

Príklady polí:  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{Z}_5, \oplus, \odot)$

# Ekvivalentná definícia poľa

## Definícia

Pole je množina  $F$ , na ktorej sú definované 2 binárne operácie  $+$  a  $\cdot$  spĺňajúce:

- (i) pre všetky  $a, b, c \in F$  platí  $a + (b + c) = (a + b) + c$ ,
- (ii) pre všetky  $a, b \in F$  platí  $a + b = b + a$ ,
- (iii) existuje prvok  $0 \in F$  taký, že pre každé  $a \in F$  sa  $a + 0 = a$ ,
- (iv) ku každému  $a \in F$  existuje  $b \in F$  tak, že  $a + b = 0$ ,
- (v) pre všetky  $a, b, c \in F$  platí  $a.(b.c) = (a.b).c$ ,
- (vi) pre všetky  $a, b \in F$  platí  $a.b = b.a$ ,
- (vii) existuje prvok  $1 \in F$  taký, že  $1 \neq 0$  a pre každé  $a \in F$  sa  $a.1 = a$ ,
- (viii) ku každému  $a \in F$ ,  $a \neq 0$  existuje  $b \in F$  tak, že  $a.b = 1$ ,
- (ix) pre všetky  $a, b, c \in F$  sa  $a.(b + c) = a.b + a.c$ .

## Základné vlastnosti poľa

## Tvrdenie

Nech  $(F, +, \cdot)$  je pole. Potom pre  $a, b, c \in F$  platí

- (i)  $a \cdot 0 = 0, 0 \cdot a = 0,$
- (ii)  $a \cdot b = b \cdot a,$
- (iii)  $(-a) \cdot b = -a \cdot b,$
- (iv)  $(-a) \cdot (-b) = a \cdot b,$
- (v)  $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0,$
- (vi)  $a \cdot b = a \cdot c \wedge a \neq 0 \Rightarrow b = c,$
- (vii)  $a \cdot a = a \Rightarrow a = 0 \vee a = 1.$

Pole  $\mathbb{Z}_p$ 

$$\mathbb{Z}_n := \{0, 1, \dots, n - 1\}$$

$$a \oplus b = (a + b) \bmod n,$$

$$a \odot b = (ab) \bmod n,$$

## Veta

Ak  $p$  je prvočíslo, tak  $(\mathbb{Z}_p, \oplus, \odot)$  je pole.

Dôkaz využíva vlastnosť, že pre každé prvočíslo  $p$  platí  $p \mid m \cdot n \Rightarrow p \mid m$  alebo  $p \mid n$ .

$$n \times a \quad a a a^n$$

## Definícia

Ak  $n \in \mathbb{Z}$  a  $a, b$  sú prvky pol'a  $F$ , tak definujeme  $n \times a$  takto:

$$0 \times a = 0,$$

$$(n + 1) \times a = n \times a + a,$$

Ak  $n > 0$  tak definujeme  $(-n) \times a = -(n \times a)$ .

Podobne definujeme pre  $a \neq 0$ :

$$a^0 = 1,$$

$$a^{n+1} = a^n \cdot a,$$

$$a^{-n} = (a^n)^{-1} \quad (n > 0).$$

$$n \times a = \underbrace{a + a + \cdots + a}_{n\text{-krát}}$$

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{-krát}}$$