Binárne operácie a grupy

Lineárna algebra

Barbora Pokorná

KAG, FMFI UK

2020

Binárna operácia

DEFINÍCIA

Nech množina $M \neq \emptyset$. Binárna operácia na M je zobrazenie $\star\colon M \times M \to M$.

- namiesto $\star(x, y)$ budeme písať $x \star y$

PRÍKLADY

- $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $n + m = n + m$ je binárna operácia na $\mathbb{N}$
- $-\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $n - m = n - m$ nie je binárna operácia na $\mathbb{N}$
- $+$ a $\cdot$ na množine $\mathbb{R}$ sú binárne operácie

Zápis do tabuľky

Ak je množina M konečná (a dosť malá), binárnu operáciu na nej môžeme zapísať do tabuľky.
Na množine $M = \{a, b, c\}$ zapíšeme výsledky binárnej operácie $\triangle$ takto:

$\triangle$	a	b	c
a	$a \triangle a$	$a \triangle b$	$a \triangle c$
b	$b \triangle a$	$b \triangle b$	$b \triangle c$
c	$c \triangle a$	$c \triangle b$	$c \triangle c$

PRÍKLAD: Na množine $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ máme binárne operácie $\oplus$ a $\odot$ definované

$\oplus$	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

$a \oplus b = (a + b) \mod 5$

$\odot$	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

$a \odot b = (a.b) \mod 5$

Neutrálny prvok

DEFINÍCIA

Neutrálnym prvkom binárnej operácie $\star$ na množine M rozumieme taký prvok $e \in M$, že pre každé $x \in M$ platí $x \star e = e \star x = x$.

- čiže ide o prvok, ktorý je vzhľadom na operáciu v „neutrálnom vzťahu“ ku všetkým prvkom množiny
- binárna operácia nemusí mať neutrálny prvok
- ak ho má, tak je jediný
  dôkaz sporom: nech $e_1, e_2 \in M$ sú neutrálne prvky, potom $e_1 = e_1 \star e_2 = e_2$
- v tabuľkovom zápise ho vieme ľahko nájsť (kandidáta hľadáme na diagonále + overíme príslušný riadok a stĺpec)

PRÍKLADY

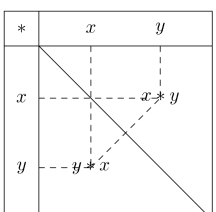
- binárna operácia $+$ na $\mathbb{N}$ nemá neutrálny prvok
- binárna operácia $\odot$ na $\mathbb{Z}_5$ má neutrálny prvok 1

Asociatívnosť a komutatívnosť binárnej operácie

DEFINÍCIA

Nech $\star\colon M \times M \to M$ je binárna operácia na množine M.
Hovoríme, že $\star$ je asociatívna, ak pre každé $a, b, c \in M$ platí $a \star (b \star c) = (a \star b) \star c$.
Hovoríme, že $\star$ je komutatívna, ak pre každé $a, b \in M$ platí $a \star b = b \star a$.

- komutatívnosť binárnej operácie v tabuľkovom zápise vieme rozhodnúť podľa toho, či je tabuľka symetrická podľa uhlopriečky



Obr. 1: $x \star y = y \star x$

Inverzný prvok

DEFINÍCIA

Nech $\star\colon M \times M \to M$ je binárna operácia na množine M taká, že existuje jej neutrálny prvok $e \in M$. Ak pre nejaký prvok $x \in M$ existuje $y \in M$ taký, že $x \star y = y \star x = e$, hovoríme, že y je inverzný prvok k prvku x a označíme ho x^{-1}.

PRÍKLAD

Binárna operácia $\cdot\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definovaná obyčajným násobením

- je asociatívna
- je komutatívna
- má neutrálny prvok $1 \in \mathbb{R}$
- inverzný prvok k prvku $a \in \mathbb{R} \setminus \{0\}$ je prvok $a^{-1} = \frac{1}{a}$
- inverzný prvok k prvku 0 neexistuje

Jednoznačnosť inverzného prvku

VETA

Nech $\star\colon M \times M \to M$ je asociatívna binárna operácia na množine M taká, že existuje jej neutrálny prvok $e \in M$. Potom pre každé $x \in M$ existuje najviac jeden inverzný prvok x^{-1}.

DÔKAZ

- nech pre $x \in M$ existujú $y, y' \in M$ také, že
  $x \star y = y \star x = e$
  $x \star y' = y' \star x = e$
- potom $y = y \star e = y \star (x \star y') = (y \star x) \star y' = e \star y' = y'$
- a teda $y = y'$

Grupa

DEFINÍCIA

Nech $G \neq \emptyset$ je množina a nech $\circledast\colon G \times G \to G$ je binárna operácia na G. Hovoríme, že dvojica $(G, \circledast)$ je grupa, ak sú splnené tri podmienky:

1. operácia $\circledast$ je asociatívna
   $\forall x, y, z \in G:\ (x \circledast y) \circledast z = x \circledast (y \circledast z)$
2. v G existuje neutrálny prvok operácie $\circledast$
   $\exists e \in G:\ \forall x \in G$ platí $x \circledast e = e \circledast x = x$
3. ku každému prvku z G existuje v G inverzný prvok vzhľadom na $\circledast$
   $\forall x \in G\ \exists y \in G:\ x \circledast y = y \circledast x = e$

DEFINÍCIA

Grupu $(G, \circledast)$ nazývame komutatívna (abelovská), ak binárna operácia $\circledast$ je komutatívna.

Aditívny a multiplikatívny zápis

PRÍKLADY abelovských grúp

- $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_m, \oplus)$ pre $m \in \mathbb{N}$

Multiplikatívny zápis $(G, \cdot)$

- ak binárna operácia nemusí byť komutatívna, ozn. ju symbolom $\cdot$
- hovoríme potom o „násobení“, resp. multiplikatívnej grupe
- neutrálny prvok ozn. 1
- inverzný prvok k prvku $x \in G$ ozn. x^{-1}

Aditívny zápis $(G, +)$

- ak binárna operácia je komutatívna, ozn. ju symbolom $+$
- hovoríme potom o „sčitovaní“, resp. aditívnej grupe
- neutrálny prvok ozn. 0
- inverzný prvok k prvku $x \in G$ ozn. $-x$ (opačný prvok)
- potom $x + (-y)$ môžeme písať $x - y$

Vlastnosti grúp

VETA (Zákony o krátení): Ak $(G, \cdot)$ je grupa, tak pre ľubovoľné $x, y, z \in G$ platí

$$x \cdot y = x \cdot z \;\Rightarrow\; y = z$$
$$y \cdot x = z \cdot x \;\Rightarrow\; y = z$$

VETA: Nech $(G, \cdot)$ je grupa. Potom pre ľubovoľné $x, y \in G$ platí

1. $(x^{-1})^{-1} = x$
2. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

DÔKAZ

Prvého tvrdenia:

- prvok $(x^{-1})^{-1}$ je inverzný k x^{-1}
- zároveň $x \cdot x^{-1} = x^{-1} \cdot x = 1$, takže aj x je inverzný k prvku x^{-1}
- pri asociatívnej bin. op. nemôžu existovať dva rôzne inverzné prvky k x^{-1}, preto $(x^{-1})^{-1} = x$

Druhého tvrdenia:

- $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1$
- podobne sa ukáže $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = 1$, a teda $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

Podgrupa

DEFINÍCIA

Nech $(G, \cdot)$ je grupa a nech $U \neq \emptyset$ je podmnožina množiny G. Ak $*\colon U \times U \to U$ je binárna operácia na U taká, že $x * y = x \cdot y$ pre $\forall (x, y) \in U \times U$ a $(U, *)$ je grupa, tak $(U, *)$ sa nazýva podgrupa grupy $(G, \cdot)$.

Pozn.: Zobrazenie $*$ sa rovná hodnotovému zúženiu zúženia $\cdot|_{U \times U}\colon U \times U \to G$.

PRÍKLAD

Grupa $(\mathbb{Z}, +)$ je podrupou grupy $(\mathbb{R}, +)$.

VETA (kritériá podgrupy)

Nech $(G, \cdot)$ je grupa. Množina $U \neq \emptyset$, $U \subset G$ je podgrupou grupy G práve vtedy, keď je splnená hociktorá z týchto dvoch navzájom ekvivalentných podmienok:

1. pre $\forall x, y \in U$ je $x \cdot y^{-1} \in U$
2. pre $\forall x, y \in U$ je $x \cdot y \in U$ a zároveň $y^{-1} \in U$.

VETA: Podgrupa komutatívnej grupy je komutatívna.

Pole

DEFINÍCIA

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

- $(F, +)$ je komutatívna grupa
- $(F \setminus \{0\}, \cdot)$ je komutatívna grupa
- vzťah sčitovania a násobenia určujú distributívne zákony

  $x \cdot (y + z) = x \cdot y + x \cdot z$

  $(x + y) \cdot z = x \cdot z + y \cdot z$

PRÍKLADY polí:

- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}_p, \oplus, \odot)$ pre $p-$prvočíslo

Základné vlastnosti poľa

VETA

Pre pole $(F, +, \cdot)$ platí:

- $x \cdot 0 = 0 \cdot x = 0$ pre $\forall x \in F$
- $(-y) \cdot x = -(y \cdot x) = y \cdot (-x)$ pre $\forall x, y \in F$
- $(-x) \cdot (-y) = x \cdot y$ pre $\forall x, y \in F$
- $x \cdot y = 0 \;\Rightarrow\; x = 0 \vee y = 0$
- $x \cdot y = x \cdot z \wedge x \neq 0 \;\Rightarrow\; y = z$
- $a \cdot a = a \;\Rightarrow\; a = 0 \vee a = 1$

Dôkaz základných vlastností poľa

- $x \cdot 0 = 0 \cdot x = 0$ pre $\forall x \in F$
  Máme $0 \cdot x + x \cdot x = (0 + x) \cdot x = x \cdot x$, a teda $0 \cdot x = 0$.
  Podobne $x \cdot 0 + x \cdot x = x \cdot (0 + x) = x \cdot x$, čiže $x \cdot 0 = 0$.

- $(-y) \cdot x = -(y \cdot x) = y \cdot (-x)$ pre $\forall x, y \in F$
  Máme $y + (-y) = 0$ a vďaka predošlému dostávame $0 = (y + (-y)) \cdot x = y \cdot x + (-y) \cdot x$, čiže $-(y \cdot x) = (-y) \cdot x$.
  Podobne $0 = y \cdot (x + (-x)) = y \cdot x + y \cdot (-x)$, a teda $-(y \cdot x) = y \cdot (-x)$.

- $(-x) \cdot (-y) = x \cdot y$ pre $\forall x, y \in F$
  Platí $(-x) \cdot (-y) + (-(x \cdot y)) = (-x) \cdot (-y) + (-x) \cdot y = (-x) \cdot ((-y) + y) = (-x) \cdot 0 = 0$.
  Teda prvok $(-x) \cdot (-y)$ je opačný prvok k prvku $-(x \cdot y)$. Lenže aj prvok $x \cdot y$ je opačný k prvku $-(x \cdot y)$, lebo $x \cdot y + (-(x \cdot y)) = 0$. Keďže $+$ je z predpokladu asociatívna operácia, inverzný prvok je jednoznačne určený. Teda máme $(-x) \cdot (-y) = x \cdot y$.

Dôkaz základných vlastností poľa

- $x \cdot y = 0 \;\Rightarrow\; x = 0 \vee y = 0$
  Ukážeme sporom: nech $x \neq 0 \wedge y \neq 0 \wedge x \cdot y = 0$.
  Keďže prvky x, y sú nenulové, tak $x, y \in F \setminus \{0\}$, lenže $(F, +, \cdot)$ je pole, takže $(F \setminus \{0\}, \cdot)$ je grupa a teda súčin prvkov $x \cdot y \in F \setminus \{0\}$, čiže $x \cdot y \neq 0$ a to je spor s predpokladom.

- $x \cdot y = x \cdot z \wedge x \neq 0 \;\Rightarrow\; y = z$
  Keďže $x \neq 0$, tak $\exists\, x^{-1}$ a potom
  $y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot z) = (x^{-1} \cdot x) \cdot z = 1 \cdot z = z$.

- $a \cdot a = a \;\Rightarrow\; a = 0 \vee a = 1$
  Nech $a \cdot a = a$. Ak $a = 0$, tak $0.0 = 0$.
  Ak $a \neq 0$, tak existuje $a^{-1} \in F \setminus \{0\}$, že
  $1 = a \cdot a^{-1} = (a \cdot a) \cdot a^{-1} = a \cdot (a \cdot a^{-1}) = a \cdot 1 = a$, čiže $a = 1$.

Zoznam použitých obrázkov

- obr. 1: Martin Sleziak