

# Osnovne algebrske strukture

## Algebrska struktura

### Definicija 1.1

Naj bo  $\mathbb{S}$  poljubna neprazna množica.

Vsaki preslikavi  $\varphi : \mathbb{S} \times \mathbb{S} \rightarrow \mathbb{S}$  rečemo DVOMESTNA NOTRANJA OPERACIJA ali okrajšano DNO na množici  $\mathbb{S}$ .

Sliko urejenega para  $(a, b) \in \mathbb{S} \times \mathbb{S}$  pišemo  $a\varphi b$  (namesto običajnega zapisa  $\varphi(a, b)$ ) in jo imenujemo KOMPOZITUM (SESTAV) ELEMENTOV  $a$  in  $b$  iz  $\mathbb{S}$ .

Dvomestno notranjo operacijo označujemo z znaki:  $+, \cdot, \circ, \triangle, \heartsuit, \dots$

### Zgled 1.2

a)  $\mathbb{S} = \mathbb{N}$

o je običajno seštevanje naravnih števil.

Sledi, je DNO, saj  $\forall a, b \in \mathbb{N}$  je  $a \circ b \in \mathbb{N}$ .

b)  $\mathbb{S} = \mathbb{N}$

o je običajno odštevanje naravnih števil.

Sledi, ni DNO, npr.: za  $1 \circ 2 = 1 - 2 = -1 \notin \mathbb{N}$ .

### Definicija 1.3

DNO  $\circ$  na množici  $\mathbb{S} \neq \emptyset$  je ASOCIATIVNA če za vse elemente  $a, b, c \in \mathbb{S}$  velja

$$(a \circ b) \circ c = a \circ (b \circ c)$$

KOMUTATIVNA, če za vsaka elementa  $a, b \in \mathbb{S}$  velja

$$a \circ b = b \circ a$$

### Zgled 1.4.

a)  $\mathbb{S} = \mathbb{Z}$

o je običajno seštevanje celih števil.

Sledi, je DNO.

Sledi,  $\circ$  je komutativna, in je asociativna.

b)  $\mathbb{S} = \mathbb{Z}$

o je odštevanje celih števil.

Sledi, je DNO.

Preverimo komutativnost:

$$a = 1, b = 0$$

$$a \circ b = 1 - 0 = 1$$

$$b \circ a = 0 - 1 = -1$$

Sledi, ni komutativno.

Preverimo, asociativnost:

$$\begin{aligned}a &= 1, b = 2, c = 3 \\(a \circ b) \circ c &= (1 - 2) - 3 = -4 \\a \circ (b \circ c) &= 1 - (2 - 3) = 2\end{aligned}$$

Sledi, ni asociativno.

c)  $\mathbb{S} = \mathbb{R}^{n \times n}$  (kvadratne matrice z realnimi koeficienti)

$\circ$  je običajno množenje matrik.

Sledi, je DNO, ker je rezultat zmnožka spet kvadratna matrika velikosti  $n \times n$  z realnimi koeficienti.

Preverimo asociativnost:

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$\begin{aligned}(A \circ B) \circ C &= \left( \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\&= \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\&= \begin{bmatrix} (a_1 a_2 + b_1 c_2) a_3 + (a_1 b_2 + b_1 d_2) c_3 & (a_1 a_2 + b_1 c_2) b_3 + (a_1 b_2 + b_1 d_2) d_3 \\ (c_1 a_2 + d_1 c_2) a_3 + (c_1 b_2 + d_1 d_2) c_3 & (c_1 a_2 + d_1 c_2) b_3 + (c_1 b_2 + d_1 d_2) d_3 \end{bmatrix} \\&= \begin{bmatrix} a_1 a_2 a_3 + b_1 a_3 c_2 + a_1 c_2 c_3 + b_1 c_3 d_2 & a_1 a_2 b_3 + b_1 b_2 d_3 + a_1 b_2 c_3 + b_1 c_2 d_3 \\ c_1 a_2 a_3 + d_1 a_3 c_2 + c_1 c_2 c_3 + d_1 c_3 d_2 & c_1 a_2 b_3 + d_1 b_2 d_3 + c_1 b_2 c_3 + d_1 c_2 d_3 \end{bmatrix}\end{aligned}$$

$$\begin{aligned}A \circ (B \circ C) &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \left( \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right) \\&= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 a_3 + b_2 c_3 & a_2 b_3 + b_2 d_3 \\ c_2 a_3 + d_2 c_3 & c_2 b_3 + d_2 d_3 \end{bmatrix} \\&= \begin{bmatrix} a_1(a_2 a_3 + b_2 c_3) + b_1(c_2 a_3 + d_2 c_3) & a_1(a_2 b_3 + b_2 d_3) + b_1(c_2 b_3 + d_2 d_3) \\ c_1(a_2 a_3 + b_2 c_3) + d_1(c_2 a_3 + d_2 c_3) & c_1(a_2 b_3 + b_2 d_3) + d_1(c_2 b_3 + d_2 d_3) \end{bmatrix} \\&= \begin{bmatrix} a_1 a_2 a_3 + b_1 a_3 c_2 + a_1 c_2 c_3 + b_1 c_3 d_2 & a_1 a_2 b_3 + b_1 b_2 d_3 + a_1 b_2 c_3 + b_1 c_2 d_3 \\ c_1 a_2 a_3 + d_1 a_3 c_2 + c_1 c_2 c_3 + d_1 c_3 d_2 & c_1 a_2 b_3 + d_1 b_2 d_3 + c_1 b_2 c_3 + d_1 c_2 d_3 \end{bmatrix}\end{aligned}$$

Sledi, je asociativno.

Preverimo komutativnost:

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$A \circ B = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$B \circ A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 0 & 0 \end{bmatrix}$$

**Trditev 1.5.**

Če je DNO  $\circ$  na  $\mathbb{S} \neq \emptyset$  asociativna, potem je produkt (kompozitum) elementov  $a_1, a_2, \dots, a_n \in \mathbb{S}$  ( $n \in \mathbb{N}$ ) natančno določen z vrstnim redom teh elementov.

Tak produkt označimo z  $a_1 \circ a_2 \circ \dots \circ a_n$ .

Dokaz: izpustimo!

**Trditev 1.6.**

Če je  $\circ$  asociativna in komutativna DNO na  $\mathbb{S} \neq \emptyset$ , potem je naš produkt elementov  $a_1, a_2, \dots, a_n \in \mathbb{S}$  ( $n \in \mathbb{N}$ ) enolično določen ne glede na vrstni red naših elementov.

Dokaz: izpustimo!

**Definicija 1.7.**

Naj bo  $\mathbb{S} \neq \emptyset$  z DNO  $\circ$ .

Element  $l \in \mathbb{S}$  je LEVI NEUTRALNI ELEMENT v množici  $\mathbb{S}$ , če za  $\forall a \in \mathbb{S}$  velja

$$l \circ a = a$$

Element  $d \in \mathbb{S}$  je DESNI NEUTRALNI ELEMENT v množici  $\mathbb{S}$ , če za  $\forall a \in \mathbb{S}$  velja

$$a \circ d = a$$

Če je  $e \in \mathbb{S}$  hkrati levi in desni neutralni element v množici  $\mathbb{S}$ , mu preprosto rečemo NEUTRALNI ELEMENT.

Oznaka:  $(\mathbb{S}, \circ)$  ... neprazna množica  $\mathbb{S}$  z DNO.

**Trditev 1.8.**

Če  $(\mathbb{S}, \circ)$  premore levi in desni neutralni element, potem sta enaka.

Dokaz:

Naj bo  $l \in \mathbb{S}$  levi neutralni element in  $d \in \mathbb{S}$  desni neutralni element v množici  $\mathbb{S}$ , potem:

$$l = l \circ d = d$$

Torej sklepamo, da je  $l = d$ , kar smo želeli pokazati.

**Zgled 1.9.**

a)  $S = \mathbb{R}^{2 \times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a, b, c, d \in \mathbb{R} \right\}$   
 $\circ$  je običajno množenje matrik.

Sledi, je DNO.

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  je neutralni element, saj za  $\forall A \in S$  velja  $I \cdot A = A \cdot I = A$ .

b)  $S = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \right\}; a, b \in \mathbb{R}$

o je običajno množenje matrik.

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ax & ay \\ 0 & 0 \end{bmatrix}$$

Sledi, je DNO. Levi neutralni element:

$$\begin{bmatrix} ax & ay \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$$

$\Downarrow$

$a = 1, b =$  poljuben

$\Downarrow$

$\forall b \in \mathbb{R}$  je  $\begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix}$  levi neutralni element v  $S$

Desni neutralni element:

$$\begin{bmatrix} ax & ay \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$

$\Downarrow$

$$ax = a \Rightarrow x = 1$$

$$ay = b \Rightarrow y = \frac{b}{a} \text{ ni OK! Ker je odvisno od } a, b.$$

$\Downarrow$

desni neutralni element ne obstaja!

### Definicija 1.10.

Naj  $(S, \circ)$  premore neutralni element  $e \in S$ , ter naj bo  $a \in S$  poljuben.

Potem  $l \in S$  je LEVI OBRAT (ali INVERZ) ELEMENTA  $a \in S$  če velja

$$l \circ a = e$$

Element  $d \in S$  je DESNI OBRAT ELEMENTA  $a \in S$  če velja

$$a \circ d = e$$

OBRAT ELEMENTA  $a \in S$  je tak element iz  $S$  ki je hkrati levi in desni obrat od  $a$ .

Element  $a \in S$  je obrnljiv (v množici  $S$ ) če premore obrat v množici  $S$ .

### Trditev 1.11.

Naj veljajo oznake iz definicije 1.10.

Neutralni element  $e$  je obrat samega sebe.

Dokaz:

$$e \circ e = e$$

### Trditev 1.12.

Naj bo  $S \neq \emptyset$  z DNO  $\circ$ , ki je asociativna in naj bo  $e \in S$  neutralni element.

Če ima element  $a \in S$  levi in desni obrat v  $S$ , potem sta enaka.

Dokaz: Naj veljajo predpostavke iz trditve 1.12. in  $a \in S$ .

$$\exists \text{levi obrat za } a \text{ v } S \Rightarrow \exists l \in S : l \circ a = e$$

$$\exists \text{desni obrat za } a \text{ v } S \Rightarrow \exists d \in S : a \circ d = e$$

Potem je

$$(l \circ a) \circ d = e \circ d = d$$

$$l \circ (a \circ d) = l \circ e = l$$

ker je  $\circ$  asociativna operacija.

Torej, je  $l = d$ .

### Definicija 1.13.

Če je  $S \neq \emptyset$  z DNO  $\circ$ , ki je asociativna, potem rečemo, da je  $(S, \circ)$  POLGRUPA.

Polgrupa z neutralnim elementom je MONOID.

Monoid v katerem je vsak element obrnljiv je GRUPA.

$(S, \circ)$	$\circ$ asociativna	$\exists$ neutralen element	$\forall a \in S$ je obrnljiv
POLGRUPA	✓	×	×
MONOID	✓	✓	×
GRUPA	✓	✓	✓

### Definicija 1.14.

Če izbrano DNO na  $S \neq \emptyset$  označimo s  $+$ , potem govorimo o SEŠTEVAJOČEM (ali ADITIVNEM) ZAPISU.

Element  $a + b$  je VSOTA elementov  $a, b \in S$ , neutralni element označimo z  $0 \in S$  (in mu rečemo ničla), obratu elementa  $a \in S$  rečemo NASPROTNI ELEMENT in ga označimo z  $-a$ .

Če izbrano DNO na  $S \neq \emptyset$  označimo z  $\cdot$ , potem govorimo o MNOŽEČEM (ali MULTIPLIKATIVNEM) ZAPISU.

$$a \cdot b = ab$$

Element  $ab$  je zmnožek (ali PRODUKT) elementa  $a, b \in S$ , neutralni element označimo z  $1 \in S$  (in mu rečemo enka), obrat elementa  $a \in S$  rečemo INVERZ, označimo z  $a^{-1}$ .

**Definicija 1.15.**

Naj bo  $\Omega \neq \emptyset$ .

$Map(\Omega) = \{f : \Omega \rightarrow \Omega\} \leftarrow$  množica vseh preslikav iz  $\Omega$  v  $\Omega$ .

Množico  $Map(\Omega)$  opremimo z (običajno) operacijo levega sestavljanja preslikav:

$$\begin{aligned} \forall f, g : \Omega \rightarrow \Omega \text{ je } f \circ g : \Omega \rightarrow \Omega \\ \text{in } \forall x \in \Omega \text{ velja } (f \circ g)(x) = f(g(x)) \end{aligned}$$

Operacija  $\circ$  iz definicije 1.15 je DNO na  $Map(\Omega)$ .

**Trditev 1.16.**

$(Map(\Omega), \circ)$  je monoid.

Dokaz:

$I) \circ$  je asociativna. (moramo dokazati, oz. dokazano spodaj)

$$\forall f, g, h \in Map(\Omega) : (f \circ g) \circ h = f \circ (g \circ h)$$

Opazimo:

$$\begin{aligned} ((f \circ g) \circ h)(x) &= f(g(h(x))) \\ (f \circ (g \circ h))(x) &= f(g(h(x))) \end{aligned}$$

$II) \exists$  neutralnega elementa v  $Map(\Omega)$  za  $\circ$

$$\forall x \in \Omega \text{ naj bo } id : x \rightarrow x \text{ (identična preslikava)}$$

Pogazati moramo:  $\forall f \in Map(\Omega) : f \circ id = id \circ f = f$

$$\begin{aligned} \forall x \in \Omega \text{ velja: } (f \circ id)(x) &= f(id(x)) = f(x) \\ (id \circ f)(x) &= id(f(x)) = f(x) \end{aligned}$$

**Definicija 1.15.** (nadaljevanje)

Podobno definiramo:

$$Inj(\Omega) = \{f : \Omega \rightarrow \Omega; f \text{ je injektivna} \}$$

$$Sur(\Omega) = \{f : \Omega \rightarrow \Omega; f \text{ je surjektivna} \}$$

$$Bij(\Omega) = \{f : \Omega \rightarrow \Omega; f \text{ je bijektivna} \}$$

in jih opremimo z operacijo sestavljanja preslikav z istim predpisom.

**Trditev 1.17.**

$(Inj(\Omega), \circ)$  in  $(Sur(\Omega), \circ)$  sta monoida,  $(Bij(\Omega), \circ)$  je grupa.

Dokaz: D.N. (za domačo nalogo)