Algebra II - Zapiski predavanj

Amar Ustavdić

Vsebina

1 Osnovne algebrske strukture

1.1 Algebrska struktura

1.1.1 Definicija

Naj bo S poljubna neprazna množica.
Vsaki preslikavi $\varphi : S \times S \to S$ rečemo DVOMESTNA NOTRANJA OPERACIJA (ali DNO) na množici S.

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

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

1.1.2 Zgled

a) $S = \mathbb{N}$
$\circ$ je običajno seštevanje naravnih števil.
$\Rightarrow$ je DNO, saj $\forall a, b \in \mathbb{N}$ je $a \circ b \in \mathbb{N}$.

b) $S = \mathbb{N}$
$\circ$ je običajno odštevanje naravnih števil.
$\Rightarrow$ ni DNO, npr. za $1 \circ 2 = 1 - 2 = -1 \notin \mathbb{N}$.

1.1.3 Definicija

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

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

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

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

1.1.4 Zgled

a) $S = \mathbb{Z}$
$\circ$ je običajno seštevanje celih števil.
$\Rightarrow$ je DNO.
$\Rightarrow \circ$ je komutativna, in je asociativna.

b) $S = \mathbb{Z}$
$\circ$ je običajno odštevanje celih števil.
$\Rightarrow$ je DNO.

$$\begin{aligned} a &= 1, b = 0 \\ a \circ b &= 1 - 0 = 1 \\ b \circ a &= 0 - 1 = -1 \end{aligned}$$

$\Rightarrow$ ni komutativna.

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

$\Rightarrow$ ni asociativna.

c) $S = \mathbb{R}^{n \times n}$ (kvadratne matrike z realnimi koeficienti)
$\circ$ je običajno množenje matrik.
$\Rightarrow$ je DNO, ker je rezultat zmnožka spet kvadratna matrika velikosti $n \times n$ z realnimi koeficienti.

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

$\Rightarrow$ je asociativno.

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

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

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

$\Rightarrow$ ni komutativno.

1.1.5 Trditev

Če je DNO $\circ$ na $S \neq \emptyset$ asociativna, potem je produkt (kompozitum) elementov

$$a_1, a_2, \ldots, a_n \in S \quad (n \in \mathbb{N})$$

natančno določen z vrstnim redom teh elementov. Tak produkt označimo z

$$a_1 \circ a_2 \circ \cdots \circ a_n$$

Dokaz: izpustimo!

1.1.6 Trditev

Če je $\circ$ asociativna in komutativna DNO na $S \neq \emptyset$, potem je naš produkt elementov

$$a_1, a_2, \ldots, a_n \in S \quad (n \in \mathbb{N})$$

enolično določen ne glede na vrstni red naših elementov.

Dokaz: izpustimo!

1.1.7 Definicija

Naj bo $S \neq \emptyset$ z DNO $\circ$.

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

$$l \circ a = a$$

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

$$a \circ d = a$$

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

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

1.1.8 Trditev

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

Dokaz: Naj bo $l \in S$ levi neutralni element in $d \in S$ desni neutralni element v množici S, potem je

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

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

1.1.9 Zgled

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.

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

$\circ$ je običajno množenje matrik.

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

$\Rightarrow$ je DNO.

LEVI NEUTRALNI ELEMENT

$$\begin{bmatrix} ax & ay \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$$
$$\Downarrow$$
$$a = 1, b = \text{ poljuben}$$
$$\Downarrow$$
$$\forall b \in \mathbb{R} \text{ je } \begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix} \text{ levi neutralni element v } S.$$
$$\Downarrow$$
Levih neutralnih elementov je neskončno mnogo.

DESNI NEUTRALNI ELEMENT

$$\begin{bmatrix} ax & ay \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$
$$\Downarrow$$
$$ax = a \Rightarrow x = 1$$
$$ay = b \Rightarrow y = \frac{b}{a}$$
$$\Downarrow$$
Ni OK! Ker je odvisno od a, b.
$$\Downarrow$$
Desni neutralni element ne obstaja!

1.1.10 Definicija

Naj bo $(S, \circ)$ 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 levi in desni obrat elementa a.

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

1.1.11 Trditev

Naj veljajo oznake iz definicije 1.1.10. Neutralni element e je obrat samega sebe.

Dokaz:

$$e \circ e = e$$

1.1.12 Trditev

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 1.1.12 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 $l = d$.

1.1.13 Definicija

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	✓	✓	✓

1.1.14 Definicija

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 $S \in \emptyset$ 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), obratu elementa $a \in S$ rečemo INVERZ, označimo z a^{-1}.

1.1.15 Definicija

Naj bo $\Omega \neq \emptyset$. $Map(\Omega) = \{f : \Omega \to \Omega\} \leftarrow$ množica vseh preslikav iz Ω v Ω.
Množico $Map(\Omega)$ opremimo z (običajno) operacijo levega sestavljanja preslikav:

$$\forall f, g : \Omega \to \Omega \text{ je } f \circ g : \Omega \to \Omega$$

$$\text{in } \forall x \in \Omega \text{ velja } (f \circ g)(x) = f(g(x))$$

Operacija $\circ$ iz definicije 1.1.15 je DNO na $Map(\Omega)$.

1.1.16 Trditev

$(Map(\Omega), \circ)$ 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:

$$((f \circ g) \circ h)(x) = f(g(h(x)))$$
$$(f \circ (g \circ h))(x) = f(g(h(x)))$$

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

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

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

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

1.1.15 Definicija (nadaljevanje)

Podobno definiramo:

$$Inj(\Omega) = \{f : \Omega \to \Omega; f \text{ je injektivna}\}$$
$$Sur(\Omega) = \{f : \Omega \to \Omega; f \text{ je surjektivna}\}$$
$$Bij(\Omega) = \{f : \Omega \to \Omega; f \text{ je bijektivna}\}$$

in jih opremimo z operacijo sestavljanja preslikav z istim predpisom.

1.1.17 Trditev

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

Dokaz: D.N. (za domačo nalogo)

1.1.18 Trditev

2 Vektorski prostori

Vektorski prostor, polje $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p$, p praštevilo, $\mathbb{F}, \mathbb{F}_2, \mathbb{F}_3$.

2.1 Definicija

Naj bo $V \neq \emptyset$ z DNO $+ : V \times V \to V$. Naj bo $\mathbb{F}$ polje in $\cdot : \mathbb{F} \times V \to V$.
Algebrska struktura $(V, \mathbb{F}, +, \cdot)$ je VEKTORSKI PROSTOR, če velja:

(VP1) $\forall u, v, w \in V : (u + v) + w = u + (v + w)$
$+$ je asociativna na množici V.

(VP2) $\forall 0 \in V : \forall v \in V : v + 0 = v = 0 + v$
obstaja neutralni element za $+$.

(VP3) $(\exists - v \in V) : v + (-v) = 0 = (-v) + v$
vsak element iz množice V ima nasprotni element.

(VP4) $\forall u, v \in V : u + v = v + u$
$+$ je komutativna operacija na V.

(VP5) $\forall \alpha, \beta \in \mathbb{F}, \forall v \in V : (\alpha\beta)v = \alpha(\beta v)$

(VP6) $\forall \alpha \in \mathbb{F}, \forall u, v \in V : \alpha(v + u) = \alpha v + \alpha u$

(VP7) $\forall \alpha, \beta \in \mathbb{F}, \forall v \in V : (\alpha + \beta)v = \alpha v + \beta v$

(VP8) $\forall v \in V : 1_{\mathbb{F}} \cdot v = v$

Rečemo, da je V vektorski prostor nad poljem $\mathbb{F}$ za operaciji $+$ in $\cdot$.

Vsakemu elementu iz V rečemo VEKTOR in vsakemu elementu iz polja $\mathbb{F}$ rečemo SKALAR.

$+ : V \times V \to V$	(seštevanje vektorjev)
$\cdot : \mathbb{F} \times V \to V$	(množenje skalarja z vektorjem)
$+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$	(seštevanje skalarjev)
$\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$	(množenje skalarjev)

2.2 Zgled

a)

$V = \{0\}$	$0 + 0 = 0$
$\mathbb{F}$ poljubno polje	$\forall \alpha \in \mathbb{F} : \alpha \cdot 0 = \alpha(0 + 0) = \alpha \cdot + \alpha \cdot 0$

$$(\{0\}, \mathbb{F}, +, \cdot) \text{ je vektorski prostor.}$$

V je v.p. nad poljem $\mathbb{F}$ za tako definirani operaciji $+$, $\cdot$.
Rečemo mu TRIVIALNI VEKTORSKI PROSTOR.

b)

$\mathbb{F}$ polje, $n \in \mathbb{N}$
$\mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F} = \{(a_1, a_2, \ldots, a_n); a_1, a_2, \ldots, a_n \in \mathbb{F}\}$

Trditev 1.18.
Naj bo $(A, \cdot)$ polgrupa z neutralnim elementom in naj bo

$$a_1, a_2, \ldots, a_n \in A \ (n \in \mathbb{N}) \text{ obrnljivi.}$$

Potem velja: produkt $a_1, a_2, \ldots, a_n$ je obrnljiv in njegov obrat je

$$(a_1, a_2, \ldots, a_n)^{-1} = a_n^{-1}, \ldots, a_2^{-1}, a_1^{-1}$$

Dokaz: Indukcija po n:
$n = 2$; Naj bosta $a_1, a_2 \in A$ obrnljiva

$$\begin{aligned}
&(a_1 a_2) \cdot (a_1 a_2)^{-1} = a_1 \cdot a_2 \cdot a_2^{-1} \cdot a_1^{-1} = a_1 \cdot 1 \cdot a_1^{-1} = a_1 a_1^{-1} = 1 \\
&(a_1 a_2)^{-1} \cdot (a_1 a_2) = \ldots \text{ podobno}
\end{aligned}$$

$n = n + 1$; D.N. (za domačo nalogo)

Definicija 1.19.
Naj bo $(A, \cdot)$ polgrupa z neutralnim elementom.
Za $\forall a \in A$ in $\forall n \in \mathbb{N}$ definirajmo POTENCO a^n kot

$$\begin{aligned}
a^1 &= a \\
a^2 &= a \cdot a \\
&\vdots \\
a^{n+1} &= a^n \cdot a = a \cdot a \cdot a \ldots a
\end{aligned}$$

Dodatno definirajmo, $a^0 = 1$.
Če je element $a \in A$ obrnljiv definiramo

$$\forall n \in \mathbb{N} \quad a^{-n} = a^{(-1)n} = (a^{-1})^n$$

Izrek 1.20. (Adicijski izrek)
Naj bo $(A, \cdot)$ polgrupa z neutralnim elementom in naj bosta $m, n \in \mathbb{N}_0$.
Potem $\forall a \in A$ velja $a^{m+n} = a^m \cdot a^n$
Če je $a \in A$ obrnljiv, velja adicijski izrek $\forall m, n \in \mathbb{Z}$.

Definicija 1.21.
Naj bo $(A, \cdot)$ polgrupa z neutralnim elementom.
Element $a \in A$ ima KONČEN RED, če obstaja $n \in \mathbb{N}$, da je $a^n = 1$.
V tem primeru najmanjšem številu $r \in \mathbb{N}$ za katerega je $a^r = 1$, rečemo RED ELEMENTA a.

opomba 1: $|a|$ (red elementa a)
opomba 2: v primeru $(A, +)$ $a^n \rightarrow na$ in $1 \rightarrow 0$

Zgled 1.22.

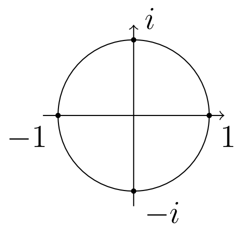
a) $A = \mathbb{Z}\backslash\{0\}$
$\cdot$ je običajno množenje celih števil $\implies (\mathbb{Z}\backslash\{0\}, \cdot)$

$1 \in \mathbb{Z}\backslash\{0\} : 1^1 = 1, 1^2 = 1, 1^3 = 1, \ldots$ element 1 ima končen red, red elementa 1 je 1
$2 \in \mathbb{Z}\backslash\{0\} : 2^1 = 2, 2^2 = 2 \cdot 2 = 4, 2^3 = 2 \cdot 2 \cdot 2 = 8, \ldots$ nima končnega reda

Torej, števila večja od 1 nimajo končnega reda.

$$-1 \in \mathbb{Z}\backslash\{0\} : (-1)^1 = -1, (-1)^2 = (-1) \cdot (-1) = 1 \text{ red elementa -1 je 2}$$

b) $A = S^1 = \{z \in \mathbb{C}; |z| = 1\}$
$\cdot$ običajno množenje kompleksnih števil.



$$0 + 1i = i \in S^1 : i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1 \text{ red elementa } i \text{ je } 4$$

$$\begin{aligned} -i \in S^1 : (-i)^1 &= -i, (-i)^2 = (-i) \cdot (-i) = -1 \\ (-i)^3 &= (-i)^1 \cdot (-i)^2 = -i \cdot (-1) = i \\ (-i)^4 &= (-i)^2 \cdot (-i)^2 = (-1) \cdot (-1) = 1 \text{ red elementa } -i \text{ je } 4 \end{aligned}$$

c) $A = \mathbb{Z}$