Skripta za algebro2

Filip Koprivec

15. oktober 2015

"If I find in myself desires which nothing in this world can satisfy, the only logical explanation is that I was made for another world."

— C. S. Lewis

Kazalo

1 Osnovne algebrske strukture **3**

1.1 Binarne operacije 3

1.2 Polgrupe in monoidi 5

1.3 Grupe 8

1.4 Kolobarji 9

1 Osnovne algebrske strukture

1.1 Binarne operacije

Definicija 1: Binarna Operacija *(tudi dvočlena operacija)* $\circ$ *na množici* $\mathcal{S}$ *je preslikava iz* $\mathcal{S} \times \mathcal{S}$ *v* $\mathcal{S}$.
Torej $\circ : \mathcal{S} \times \mathcal{S} \rightarrow \mathcal{S}$

Primer:
Osnovna zgleda binranih operacij na $\mathbb{Z}$ sta:
1. Seštevanje: $(n, m) \mapsto n + m$
2. Množenje: $(n, m) \mapsto n \times m$

Skalarni produkt v $\mathbb{R}^2$ **ni** binarna operacija.
Vektorski produkt v $\mathbb{R}^3$ **je** binarna operacija.

Definicija 2: *Operacija* $\circ$ *je* ***asociativna****, če ustreza enačbi*

$$\forall x, y, z \in \mathcal{S}.\ (x \circ y) \circ z = x \circ (y \circ z) \tag{1}$$

Enakost 1 imenujemo **Zakon o asociativnosti**
Operacije, ki jih bomo obravnavali bodo praviloma asociativne.

Definicija 3: *Elementa* $x, y \in \mathcal{S}$ ***komutirata****, če velja*

$$\forall x, y \in \mathcal{S}. x \circ y = y \circ x \tag{2}$$

Enakost 2 imenujemo ***Zakon o komutativnosti***

Opomba: Kadar je iz konteksta razvidno, o kateri operaciji govorimo, pogosto namesto "$\circ$ je komutativna rečemo tudi $\mathcal{S}$ je komutativna"
Primer:
1. Operacija $+$ na $\mathbb{Z}$ je tako asociatitivna in komutativna
2. Operacija * na $\mathbb{Z}$ je tako asociatitivna in komutativna
3. Operacija - na $\mathbb{Z}$ **ni** niti asociativna niti komutativna
Opomba: Na opracijo odštevanja gledamo kot na izpeljano operacijo in ne kot na samostojna operacijo, saj jo vpeljemo preko seštevanja in pojma nasprotnega elementa.
4. Naj bo $\mathcal{X}$ poljubna neprazna množica. Z $F(\mathcal{X})$ označimo množico vseh preslikav iz $\mathcal{X}$ v $\mathcal{X}$. Naj bosta $f, g \in \mathcal{X}$, potem je $(f, g) \mapsto f \circ g$ (kompozitum funkcij) binarna operacija na $F(\mathcal{X})$.
Opomba: Operacija je asociativna, in kadar $|\mathcal{X}| \geq 2$ ni komutativna

Definicija 4: *Naj bo* $\circ$ *binarna operacija na na* $\mathcal{S}$ *in* $e \in \mathcal{S}$. e *se imenuje* ***nevtralni element****, če velja*

$$\forall x \in \mathcal{S}. e \circ x = x \circ e = x \tag{3}$$

Primer:
1. 0 je nevtralni element za seštevanje na $\mathbb{Z}$.
2. 1 je nevtralni element za množenje na $\mathbb{Z}$.
3. id_x (identična preslikava) je nevtralni element za $F(\mathcal{X})$

Opomba: Nevtralni element nima zagotovljenega obstoja (recimo + na $\mathbb{N}$ ali $*$ na sodih celih številih).
Trditev 1: Če nevtralni element obstaja je en sam

Dokaz. Naj bosta $f, e \in \mathcal{S}$ nevtralna elementa.

$$e = e \circ f \quad \text{// Ker je f nevtralni element}$$

$$e \circ f = f \quad \text{// Ker je e nevtralni element}$$

$$e = f$$

□

Definicija 5: *Element e' je* ***levi nevtralni element****, če velja:*

$$\forall x \in \mathcal{S}. e' \circ x = x \tag{4}$$

Definicija 6: *Element e'' je* ***desni nevtralni element****, če velja:*

$$\forall x \in \mathcal{S}. x \circ e'' = x \tag{5}$$

Opomba: Levih in desnih nevtralnih elementov je lahko več
Primer:
1. $\circ : (x, y) \mapsto y$.
Vsak element je levi nevtralni element
2. 0 je desni nevtralni element za odštevanje v $\mathbb{Z}$

Trditev 2: Naj bo za operacijo $\circ$ e' levi nevtralni element, e'' pa desni nevtralni element. Tedaj velja $e' = e'' = e$(Sta si levi in desni nevtralni element enaka in je(sta) nevtralni element)

Dokaz.

$$e' = e' \circ e'' = e''$$

□

Definicija 7: *Naj bo $\circ$ operacija na $\mathcal{S}$ in naj bo $\mathcal{T} \subseteq \mathcal{S}$. Rečemo, da je $\circ$* ***notranja operacija na $\mathcal{T}$*** *ali da je množica $\mathcal{T}$* ***zaprta za $\circ$ na $\mathcal{T}$*** *, če velja*

$$\forall t, t' \in \mathcal{T}. t \circ t' \in \mathcal{T} \tag{6}$$

Primer:
Množica $\mathbb{N}$ je zaprta za operaciji $+$ in $*$, ni pa zaprta za operacijo $-$.

Definicija 8: *Preslikavi iz $\mathcal{K} \times \mathcal{S}$ v $\mathcal{S}$ kjer $\mathcal{K}! = \mathcal{S}$ rečemo **Zunanja binarna operacija***

Primer:
1. Množenje vektorja s skalarjem
$(\lambda, \vec{x}) \mapsto \lambda\vec{x}$, kjer je $(K = \mathbb{R}, S = \mathbb{R}^n)$
$\lambda(x_1, x_2, \dots, x_n) = (\lambda x_1, \lambda x_2, \dots, \lambda x_n)$

1.2 Polgrupe in monoidi

Definicija 9: ***Algebrska struktura*** *je množica, opremljena z eno ali več operacijami (notranjimi ali zunanjimi), ki im ajo določene lastnosti*

Definicija 10: ***Polgrupa*** *je par množice $\mathcal{S}$ skupaj z **asociativno binarno operacijo**. Pišemo: $(\mathcal{S}, \circ)$*

Opomba: Kadar je jasno o kateri operaciji govorimo, pogosto govorimo kar o polgrupi $\mathcal{S}$
Primer:
1. $(\mathbb{N}, +), \underbrace{(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{N}, *), \dots}_{Niso\ samo\ polgrupe\ ampak\ kar\ grupe}$

Naj bo $(\mathcal{S}, \circ)$ polgrupa, po zakonu 1 o asociativnosti velja:

$$\forall x, y, z \in \mathcal{S}.\ (x \circ y) \circ z = x \circ (y \circ z)$$

zato lahko okepaje spuščamo in vse to pišemo kot $x \circ y \circ z$. Kaj pa če imamo več kot tri elemente. Ali velja tudi:
$(x_1 \circ x_2) \circ (x_3 \circ x_4) = ((x_1 \circ x_2) \circ x_3) \circ x_4 = x_1 \circ (x_2(\circ x_3 \circ x_4)) = \dots$
Trditev 3: Naj bo $(\mathcal{S}, \circ)$ polgrupa, $n \in \mathbb{N}$ in naj bo $x_1, x_2, \dots, x_n \in \mathcal{S}$. Tedaj je za vsak n enakost izpolnjena na glede na postavitev oklepajev (izraz ima smisel, tudi kadar ne pišemo oklepajev).
$x_1 \circ x_2 \circ \dots \circ x_n = (\dots(x_1 \circ x_2) \circ \dots \circ x_n) = x_1 \circ (x_2(\circ \dots \circ x_n) \dots) = \dots$

Dokaz. Zgolj skica dokaza
Definirajmo: $x := x_1 \circ (x_2(\circ \dots \circ x_n) \dots)$ in
$y :=$ naj bo kombinacija elementov $x_1 \dots x_n$, z drugače postavljenimi oklepaji
Indukcija na n:
$n \leq 3$: Očitno
Ker $n \leq 2$ velja $y = \underbrace{(u)}_{x_1, \dots, x_k} \circ \underbrace{(v)}_{x_{k+1}, \dots, x_n}$ Iz $k < n$ sledi:
$y = (x_1 \circ w) \circ v \underbrace{=}_{Asociativnost(1)} x_1 \circ (w \circ v)$
Po I.P. ($w \circ v$ ima $n - 1$ elementov): $x = x_1 \circ (x_2 \circ \dots \circ x_{n-1})$ □

Zato lahko oklepaje izpuščamo in pišemo kar: $x_1 \circ x_2 \circ \cdots \circ x_4$

Definicija 11: ***Potenca elementa*** x**.** *Naj bo* $n \in \mathbb{N} - \{0\}$ *in* $x \in \mathcal{S}$

$$x^n := \underbrace{x \circ x \circ \cdots \circ x}_{nelementov} \tag{7}$$

Opomba: Brez asociativnosti ni definirano niti x^3
Opomba:
Očitno velja:
$\forall n, m \in \mathbb{N}. x^n \circ x^m = x^{n+m}$ in
$\forall n, m \in \mathbb{N}. (x^n)^m = x^{nm}$

Definicija 12: ***Polgrupa*** *z* ***nevtralnim elementom*** *se imenuje* ***monoid****.*

Primer:
1. $(\mathbb{N}, +)$ **ni** monoid, $(\mathbb{N} \cup \{0\}, +)$ pa je.
2. $(\mathbb{N}, *)$ je monoid
3. $(F(\mathcal{X}), \circ)$ je monoid, nevtralni element je $id_{\mathcal{X}}$

Definicija 13: *Naj bo* $(\mathcal{S}, \circ)$ *monoid z nevtralnim elementom* e*. Element* y *je* ***levi inverz*** *elementa* x*, če velja:* $y \circ x = e$*.*

Definicija 14: *Naj bo* $(\mathcal{S}, \circ)$ *monoid z nevtralnim elementom* e*. Element* y *je* ***desni inverz*** *elementa* x*, če velja:* $x \circ y = e$*.*

Opomba: Levi in desni inverz nimata zagotovljenega obstoja, če pa obstajata ni nujno, da sta enolično določena.
Primer:
1. $f \in F(\mathcal{X})$ ima levi inverz $\iff$ f je injektivna
Če f ni surjektivna ima lahko več levih inverzov, ki so izven $\mathcal{Z}_f$ lahko poljubno definirani.
2. $f \in F(\mathcal{X})$ ima desni inverz $\iff$ f je surjektivna
3. $f \in F(\mathcal{X})$ ima levi in desni inverz $\iff$ f je bijektivna

Definicija 15: *Element* y *iz monida* $\mathcal{S}$ *je inverz elementa* x *Če velja:*

$$x \circ y = y \circ x = e \tag{8}$$

Elementu, ki ima inverz rečemo da je ***obrnljiv*** *in njegov inverz označimo z* x^{-1}*(To ni čisto korektno, saj bomo šele malo naprej pokazali, da ima vsak element en sam inverz). In tako dobimo*

$$x \circ x^{-1} = x^{-1} \circ x = e \tag{9}$$

Opomba: Če je operacija $\circ$ komutativna potem levi inverz, desni inverz in inverz za posamezen element sovpadajo

Trditev 4: Naj bo $(\mathcal{S}, \circ)$ monoid, Če je y levi inverz elementa x in je z njegov desni inverz, potem $z = y = x^{-1}$

Dokaz. $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z$ □

Posledica: Obrnljiv element monoida ima natanko en inverz.
Posledica: Če je x obrnljiv element monoida $\mathcal{S}$ potem iz $y \circ x = e$ sledi $x \circ y = e$.
Trditev 5: Če sta x in y obrnljiva, potem je obrnljiv tudi element $(x \circ y)$ in je njegov inverz $y^{-1} \circ x^1$

Dokaz. To je desni inverz:
$(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e$
in tudi levi inverz:
$(y^{-1} \circ x^{-1}) \circ (x \circ y) = y^{-1} \circ (x^{-1} \circ x) \circ y = y^{-1} \circ e \circ y = y{-}1 \circ y = e$ □

Opomba: Seveda velja za n elementov

$$(x_1 \circ x_2 \circ \cdots \circ x_n)^{-1} = x_n^{-1} \circ \cdots \circ x_2^{-1} \circ x_1^{-1} \tag{10}$$

Primer:
1. $(\mathbb{N} \cup \{0\}, +)$: edini obrnljiv element je 0.
2. $(\mathbb{N}, *)$: edini obrnljiv element je 1
3. $(\mathbb{Z}, *)$: edina obrnljiva elementa sta 1 in -1
4. $(\mathbb{Q}, *)$: Obrnljivi so vsi element razen 0
5. $(F(\mathcal{X}), \circ)$: obrnljive so vse bijektivne preslikave

Opomba: Poseben primer zadnje formule kadar je x obrnljiv je tudi:$(x^n)^{-1} = (x^{-1})^n$ za $n \in \mathbb{N}$

Definicija 16:

$$n \in \mathbb{N}.x^{-n} := (x^n)^{-1} = (x^{-1})^n \tag{11}$$

Definicija 17:

$$x^0 := e \tag{12}$$

Tako kadar je x **obrnljiv** veljata enačbi

$$\forall n, m \in \mathbb{Z}.x^n \circ x^m = x^{n+m} \tag{13}$$

$$\forall n, m \in \mathbb{Z}.(x^n)^m = x^{nm} \tag{14}$$

Trditev 6: Če je x obrnljiv element monida $\mathcal{S}$ potem velja **pravilo krajšanja**:

$$x \circ y = x \circ z \implies y = z \tag{15}$$

In tudi
$$y \circ x = z \circ x \implies y = z \tag{16}$$

Dokaz.
$$x \circ y = x \circ z \implies x^{-1} \circ x \circ y = x^{-1} \circ x \circ z \implies y = z$$

Druga enačba podobno □

Opomba: Iz enačbe $x \circ y = z \circ x$ v splošnem **ne** sledi $y = z$

1.3 Grupe

Dogovor: V grupi bomo namesto $\circ$ uporabljali kar operacijo 'krat', torej se bo operacija imanovala kar množenje. Prav tako bomo izpuščali operator, ko bo le mogoče in pisali kar xy.
Tako xy imenujemo 'produkt' x in y nevtrali element pa označimo z 1 in mu rečemo kar enota.

Definicija 18: ***Monoid*** *v katerem je* ***vsak element obrnljiv****, se imenuje* ***grupa****. Grupa, v kateri je vsaka operacija komutativna se umenuje* ***komutativna grupa*** *ali* ***Abelova grupa****.*

Ki je ekvivalenta bolj čisti definiciji:

Definicija 19: *Množica $\mathbb{G}$ skupaj z binarno operacijo $* : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$, $(x, y) \mapsto xy$ je* ***grupa*** *če zanjo velja:*

G_1:
$$\forall x, y, z \in \mathbb{G}.\ (xy)z = x(yz)$$

G_2:
$$\exists 1 \in \mathbb{G}.\ \forall x \in \mathbb{G}.\ 1x = x1 = x$$

G_3:
$$\forall x \in \mathbb{G}.\ \exists x^{-1} \in \mathbb{G}.\ xx^{-1} = x^{-1}x = 1$$

Če velja tudi:
$$\forall x, y \in \mathbb{G}.\ xy = yx$$

Potem grupo $\mathbb{G}$ imanujemo ***Abelova*** *grupa.*

Grupe delim na komutativne in nekomutativne(glede na lastnosti operacije) ter na končne in neskončne(glede na število elementov).
Primer:
1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,$(\mathbb{R}, +)$,$(\mathbb{C}, +)$
2. $(\mathbb{N} \cup \{0\}, +)$ **ni** grupa
3. $(\mathbb{R}, *)$: **ni** grupa, ker 0 ni obrnljiv

Opomba: Vsak monoid 'skriva' grupo.

Definicija 20: *S $\mathcal{S}^*$ označujemo množico vseh obrnljivih elementov monoida $\mathcal{S}$.*

Trditev 7: Če je $\mathcal{S}$ monoid je $\mathcal{S}$ grupa.

Dokaz. $x, y \in \mathcal{S}^* \implies x \circ y \in \mathcal{S}^*$ // Obrnljiv je tudi njun produkt, torej je množica je zaprta za $*$
Ker je $*$ asociativen na $\mathcal{S}$ je asociativen tudi na $\mathcal{S}^*$
$e \in \mathcal{S}^*$ saj je enota inverz sami sebi
$x \in \mathcal{S}^* \implies x^{-1} \in \mathcal{S}^*$ // Inverz inverza je kar element sam □

Primer:
1. $(\mathbb{N} \cup \{0\}, +)$: $(\mathbb{N} \cup \{0\}, +)^* = 0$
2. $(\mathbb{Z}, +)$: $(\mathbb{Z}, +)^* = -1, 1$
3. $(\mathbb{Q}, *)$: $(\mathbb{Q}, *)^* = \mathbb{Q} - 0$

Opomba: Grupam z enim elementom pravimo **trivialne** grupe.

4. $(F(\mathcal{X}), \circ)$: $(F(\mathcal{X}), \circ)^* = \{f : \mathcal{X} \to \mathcal{X} | f \text{ je bijekcija}\}$

Definicija 21: *Množico $Sim(\mathcal{X})$ imenujemo **simetrična grupa** (množice $\mathcal{X}$).*

$$Sim(\mathcal{X}) := \{f : \mathcal{X} \to \mathcal{X} | f \text{ je bijekcija}\} \tag{17}$$

*Njene emelente(bijektiven preslikave iz $\mathcal{X}$ v $\mathcal{X}$ pa imenujemo **permutacaije** (množice $\mathcal{X}$).*

Opomba: Če je množica končna jo praviloma označimo z $\{1, 2, \dots, n\}$, njej pripadajočo grupo permutacij pa z

$$\mathcal{S}_n := Sim(\{1, 2, \dots, n\}) \tag{18}$$

Včasih bomo operacije na grupah vendarle označevali s + ('seštevanje'). Taki grupi bomo rekli **aditivna grupa**. Nevtralni element bomo označevali z 0 in inverzni elment pa bom oimenovali 'nasprotni element' in ga označevali z $-x$. Namesto $x + (-y)$ bom tako pisali $x - y$ (razlika x in y). S tem smo v aditivno grupo vpeljeli odštevanje. Prav tako bom namesto x^n pisali nx.
Primer takih grup so Abelove grupe. $(x + y = y + x)$

1.4 Kolobarji

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ so aditivne grupe, v katerih je naravno definirano tudi množenje, za katerega so monoidi.

Definicija 22: *Množica $\mathcal{K}$,, skupaj z binarnima operacijama seštevanja $+ : (x, y) \mapsto x + y$ in množenja $* : (x, y) \mapsto xy$ se imenuje **kolobar** če velja*

K_1: *$(K, +)$ je **Abelova grupa***

K_2: *$(K, *)$ je **monoid***

K_3: Izpolnjena sta oba distributivnostna zakona

$$\forall x, y, z \in \mathcal{K}.\ z(x + y) = zx + zy \tag{19}$$

$$\forall x, y, z \in \mathcal{K}.\ (x + y)z = xz + yz \tag{20}$$

Opomba: *Oba zakona potrebujemo zaradi ne nujne komutativnosti množenja v monoidu*