

# Algebra 2

Luka Horjak ([luka.horjak@student.fmf.uni-lj.si](mailto:luka.horjak@student.fmf.uni-lj.si))

29. oktober 2021

# Kazalo

<b>Uvod</b>	<b>3</b>
<b>1 Osnovne algebrske strukture</b>	<b>4</b>
1.1 Linearne operacije . . . . .	4
1.2 Polgrupe in monoidi . . . . .	5
1.3 Grupe . . . . .	6
1.4 Kolobarji in polja . . . . .	7
1.5 Vektorski prostori in algebre . . . . .	8
1.6 Podstrukture . . . . .	9
1.7 Generatorji . . . . .	11
<b>Stvarno kazalo</b>	<b>12</b>

## Uvod

V tem dokumentu so zbrani moji zapiski s predavanj predmeta Algebra 2 v letu 2021/22. Predavatelj v tem letu je bil prof. dr. Matej Brešar.

Zapiski niso popolni. Manjka večina zgledov, ki pomagajo pri razumevanju definicij in izrekov. Poleg tega nisem dokazoval čisto vsakega izreka, pogosto sem kakšnega označil kot očitnega ali pa le nakazal pomembnejše korake v dokazu.

Zelo verjetno se mi je pri pregledu zapiskov izmuznila kakšna napaka – popravki so vselej dobrodošli.

# 1 Osnovne algebrske strukture

## 1.1 Linearne operacije

**Definicija 1.1.1.** Binarna operacija  $*$  na neprazni množici  $S$  je preslikava  $*$ :  $S \times S \rightarrow S$ . Po dogovoru namesto  $*(x, y)$  pišemo  $x * y$ .

**Definicija 1.1.2.** Naj bo  $*$  binarna operacija na  $S$ . Element  $e \in S$  je *nevtralni element* ali *enota*, če za vsak  $x \in S$  velja

$$x * e = e * x = x.$$

**Definicija 1.1.3.** Naj bo  $*$  binarna operacija na  $S$ . Element  $e \in S$  je *levi nevtralni element*, če za vsak  $x \in S$  velja

$$e * x = x.$$

Podobno je  $e$  *desni nevtralni element*, če za vsak  $x \in S$  velja

$$x * e = x.$$

**Trditev 1.1.4.** Veljajo naslednje trditve:

- i) Če je  $e'$  levi in  $e''$  desni nevtralni element, je  $e' = e'' = e$ , kjer je  $e$  nevtralni element.
- ii) Če nevtralni element obstaja, je enolično določen.
- iii) Levih/desnih nevtralnih elementov je lahko več.

*Dokaz.* Za prvo točko preprosto opazimo, da je

$$e' = e' * e'' = e''.$$

Sledi, da je  $e'$  levi in desni nevtralni element, torej je  $e' = e$ .

Druga točka je direktna posledica prve. Če sta  $e$  in  $f$  nevtralna elementa, je namreč  $e$  levi,  $f$  pa desni nevtralni element, zato je  $e = f$ .

Za dokaz tretje trditve si oglejmo operaciji  $*_1, *_2: \mathbb{N} \rightarrow \mathbb{N}$ , ki delujeta s predpisi  $x *_1 y = x$  in  $x *_2 y = y$  za vse naravne  $x$  in  $y$ . Vidimo, da so vsa naravna števila desni nevtralni element prve in levi nevtralni element druge operacije.  $\square$

**Definicija 1.1.5.** Operacija  $*$  na  $S$  je:

- i) *asociativna*, če za vse  $a, b, c \in S$  velja  $a * (b * c) = (a * b) * c$ ,
- ii) *komutativna*, če za vse  $a, b \in S$  velja  $a * b = b * a$ .

**Definicija 1.1.6.** Naj bo  $T \subseteq S$  in  $*$  operacija na  $S$ . Množica  $T$  je *zaprta* za  $*$ , če za vse  $t_1, t_2 \in T$  velja  $t_1 * t_2 \in T$ . Pravimo, da je  $*$  *notranja*<sup>1</sup> binarna operacija za  $T$ .

<sup>1</sup> Zunanja binarna operacija je preslikava  $*$ :  $K \times S \rightarrow S$ .

## 1.2 Polgrupe in monoidi

**Definicija 1.2.1.** *Algebrske strukture* so množice, opremljene z eno ali več binarnimi operacijami, ki izpolnjujejo določene aksiome.

**Definicija 1.2.2.** Množica  $S$  z operacijo  $*$  je *polgrupa*, če je  $*$  asociativna. Polgrupam z nevtralnim elementom pravimo *monoid*.

**Opomba 1.2.2.1.** Če je  $S$  polgrupa, oklepajev ni potrebno postavljati.

**Opomba 1.2.2.2.** V polgrupah z  $x^n$  označujemo  $\underbrace{x * \dots * x}_n$ .

**Definicija 1.2.3.** Naj bo  $(S, *)$  monoid z enoto  $e$ .

- i)  $y \in S$  je *levi inverz*  $x \in S$ , če je  $y * x = e$ .
- ii)  $z \in S$  je *desni inverz*  $x \in S$ , če je  $x * z = e$ .
- iii)  $w \in S$  je *inverz*  $x \in S$ , če je  $x * w = w * x = e$ .

Pravimo, da je  $x$  *obrnljiv*, če ima inverz.

**Trditev 1.2.4.** Naj bo  $S$  monoid. Če obstajata taka  $l, d \in S$ , da za nek  $x \in S$  velja  $lx = xd = e$ , velja  $l = d$ .

*Dokaz.* The proof is obvious and need not be mentioned. □

**Posledica 1.2.4.1.** Obrnljiv element ima samo en inverz. Če je  $x$  obrnljiv, je  $xy = e \iff yx = e$ .

**Opomba 1.2.4.2.** Inverz elementa  $x$  označimo z  $x^{-1}$ . Očitno je  $(x^{-1})^{-1} = x$ . Označimo še  $x^{-n} = (x^{-1})^n = (x^n)^{-1}$  in  $x^0 = e$ .

**Trditev 1.2.5.** Če sta  $x, y \in S$  obrnljiva, je obrnljiv tudi  $xy$  z inverzom  $y^{-1}x^{-1}$ .

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 1.2.6.** Naj bo  $x \in S$  obrnljiv. Potem za vse  $y, z \in S$  velja

$$xy = xz \implies y = z \quad \text{in} \quad yx = zx \implies y = z.$$

*Dokaz.* The proof is obvious and need not be mentioned. □

8. oktober 2021

### 1.3 Grupe

**Definicija 1.3.1.** Monoidu, v katerem so vsi elementi obrnljivi, pravimo *grupa*.

**Definicija 1.3.2.** Grupi, v kateri je operacija komutativna, pravimo *Abelova*.

**Definicija 1.3.3.** Grupa  $G$  je *končna*, če obstaja tak  $n \in \mathbb{N}$ , da je  $|G| = n$ . Številu  $n$  pravimo *red* grupe  $G$ .

**Trditev 1.3.4.** Naj bo  $S$  monoid. Potem je  $\{x \mid x \in S \wedge x \text{ je obrnljiv}\}$  grupa.

**Definicija 1.3.5.** Grupam reda 1 pravimo *trivialne grupe*.

**Definicija 1.3.6.** *Simetrična grupa* množice  $X$  je množica

$$\text{Sim}(X) = \{f \mid f: X \rightarrow X \wedge f \text{ je bijektivna}\}$$

z operacijo kompozitum. Če je  $|X| = n$ , označimo  $\text{Sim}(X) = S_n$ .

**Opomba 1.3.6.1.** V nadaljevanju namesto  $e$  enoto označimo z 1. Za operacije pišemo  $\cdot$ , razen v Abelovih grupah, kjer jo označimo s  $+$ .

## 1.4 Kolobarji in polja

**Definicija 1.4.1.** Množica  $K$  z binarnima operacijama seštevanja in množenja je *kolobar*, če velja:

- i) za seštevanje je  $K$  Abelova grupa,
- ii) za množenje je  $K$  monoid in
- iii) veljata leva in desna distributivnost.

**Trditev 1.4.2.** V poljubnem kolobarju  $K$  velja:

- i)  $\forall x \in K: 0x = x0 = 0$ ,
- ii)  $\forall x, y \in K: (-x)y = x(-y) = -(xy)$ ,
- iii)  $\forall x, y, z \in K: (x - y)z = xz - yz$ ,
- iv)  $\forall x, y \in K: (-x)(-y) = xy$  in
- v)  $\forall x \in K: (-1)x = x(-1) = -x$ .

*Dokaz.* The proof is obvious and need not be mentioned. □

**Definicija 1.4.3.** Kolobarju s komutativnim množenjem pravimo *komutativen kolobar*.

**Definicija 1.4.4.** Element  $x$  kolobarja  $K$  je *delitelj nič*, če je  $x \neq 0$  in obstaja tak  $y \neq 0$  iz  $K$ , da je  $xy = 0$  ali  $yx = 0$ .

**Definicija 1.4.5.** Neničelnemu kolobarju, v katerem je vsak neničelni element obrnljiv, pravimo *obseg*. Komutativnemu obsegu pravimo *polje*.

**Trditev 1.4.6.** Obrnljiv element kolobarja ni delitelj nič.

*Dokaz.* The proof is obvious and need not be mentioned. □

**Posledica 1.4.6.1.** Obseg je kolobar brez deliteljev nič.

## 1.5 Vektorski prostori in algebre

**Definicija 1.5.1.** Naj bo  $\mathbb{F}$  polje. Množica  $V$  s seštevanjem in množenjem s skalarjem je *vektorski prostor* nad  $\mathbb{F}$ , če velja:

- i)  $V$  je Abelova grupa za seštevanje,
- ii)  $\forall \lambda \in \mathbb{F}, u, v \in V: \lambda(u + v) = \lambda u + \lambda v$ ,
- iii)  $\forall \lambda, \mu \in \mathbb{F}, v \in V: (\lambda + \mu)v = \lambda v + \mu v$ ,
- iv)  $\forall \lambda, \mu \in \mathbb{F}, v \in V: \lambda(\mu v) = (\lambda \mu)v$  in
- v)  $\forall v \in V: 1v = v$ .

**Definicija 1.5.2.** Naj bo  $\mathbb{F}$  polje. Množica  $A$  s seštevanjem in množenjem ter množenjem s skalari iz  $\mathbb{F}$  imenujemo *algebra* nad  $\mathbb{F}$ , če velja:

- i)  $A$  je vektorski prostor nad  $\mathbb{F}$  za seštevanje in množenje s skalarji,
- ii)  $A$  je za seštevanje in množenje kolobar in
- iii)  $\forall \lambda \in \mathbb{F}, x, y \in A: \lambda(xy) = (\lambda x)y = x(\lambda y)$ .



## 1.6 Podstrukture

**Definicija 1.6.1.** Podmnožica  $H$  grupe  $G$  je *podgrupa* grupe  $G$ , če je grupa isto operacijo.<sup>2</sup> Pišemo  $H \leq G$ .

**Opomba 1.6.1.1.** Za vsako podgrupo  $H$  je  $1 \in H$ .

**Trditev 1.6.2.** Za neprazno podmnožico  $H$  grupe  $G$  so naslednje izjave ekvivalentne:

- i)  $H \leq G$
- ii)  $\forall x, y \in H: xy^{-1} \in H$
- iii)  $\forall x, y \in H: xy \in H \wedge x^{-1} \in H$

*Dokaz.* The proof is obvious and need not be mentioned. □

**Definicija 1.6.3.** *Center* grupe  $G$  je množica

$$Z(G) = \{c \in G \mid \forall x \in G: cx = xc\}.$$

**Opomba 1.6.3.1.** Velja  $Z(G) \leq G$ .

**Definicija 1.6.4.** Naj bo  $H \leq G$  podgrupa.  $aHa^{-1}$  za  $a \in G$  je *konjugirana podgrupa*<sup>3</sup> grupe  $G$ .

**Definicija 1.6.5.** Podmnožica  $L$  kolobarja  $K$  je *podkolobar*, če je kolobar za isti operaciji in vsebuje enoto 1 kolobarja  $K$ .

**Trditev 1.6.6.** Podmnožica  $L$  kolobarja  $K$  je podkolobar natanko tedaj, ko  $1 \in L$  in velja  $\forall x, y \in L: xy \in L \wedge x - y \in L$ .

*Dokaz.* The proof is obvious and need not be mentioned. □

**Definicija 1.6.7.** *Center* kolobarja  $K$  je množica

$$Z(K) = \{c \in K \mid \forall x \in K: cx = xc\}.$$

**Opomba 1.6.7.1.** Center kolobarja je podkolobar.

**Definicija 1.6.8.** Podmnožica  $U$  vektorskega prostora  $V$  je *podprostor* prostora  $V$ , če je za isti operaciji tudi sama vektorski prostor.

**Trditev 1.6.9.** Za podmnožico  $U$  vektorskega prostora  $V$  so naslednje izjave ekvivalentne:

- i)  $U$  je podprostor  $V$
- ii)  $\forall u, v \in U, \lambda \in \mathbb{F}: u + v \in U \wedge \lambda u \in U$
- iii)  $\forall u, v \in U, \lambda, \mu \in \mathbb{F}: \lambda u + \mu v \in U$

*Dokaz.* The proof is obvious and need not be mentioned. □

<sup>2</sup> S tem je seveda mišljena skrčitev operacije na  $H \times H$ .

<sup>3</sup> Elementa  $x, y \in G$  sta si *konjugirana*, če je  $y = axa^{-1}$  za nek  $a \in G$ .

**Definicija 1.6.10.** Podmnožica  $B$  algebre  $A$  je *podalgebra*, če je algebra za iste operacije in vsebuje enoto  $A$ .

**Trditev 1.6.11.**  $B$  je podalgebra  $A$  natanko tedaj, ko je  $B$  podkolobar in podprostor.

**Definicija 1.6.12.** Podmnožica  $\mathbb{F}$  polja  $\mathbb{E}$  je *podpolje*, če je  $\mathbb{F}$  polje za isti operaciji. Polju  $\mathbb{E}$  pravimo *razširitev* polja  $\mathbb{F}$ .

**Trditev 1.6.13.** Podmnožica  $\mathbb{F}$  polja  $\mathbb{E}$  je podpolje natanko tedaj, ko velja  $1 \in \mathbb{F}$ ,

$$\forall x, y \in \mathbb{F}: x - y \in \mathbb{F} \wedge xy \in \mathbb{F}$$

in  $\forall x \in \mathbb{F}: x \neq 0 \implies x^{-1} \in \mathbb{F}$ .

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 1.6.14.** Presek podstruktur neke strukture je znova podstruktura.

## 1.7 Generatorji

**Definicija 1.7.1.** Naj bo  $G$  grupa in  $X$  neka njena podmnožica. Z  $\langle X \rangle$  označimo najmanjšo podgrupo  $G$ , ki vsebuje  $X$  in jo imenujemo podgrupa, *generirana z  $X$* , elementom  $X$  pa pravimo *generatorji*.

**Opomba 1.7.1.1.** Podobno definiramo generatorje ostalih algebrskih struktur.<sup>4</sup>

**Trditev 1.7.2.** Velja

$$\langle X \rangle = \left\{ \prod_{i=1}^n y_i \mid \forall i: y_i \in X \vee y_i^{-1} \in X \right\}.$$

*Dokaz.* The proof is obvious and need not be mentioned. □

**Definicija 1.7.3.** Grupa  $G$  je *končno generirana*, če obstaja končna množica  $X$ , za katero je  $\langle X \rangle = G$ .

**Opomba 1.7.3.1.** Grupam, generiranim z enim elementom, pravimo *ciklične grupe*.

**Trditev 1.7.4.** Podkolobar, generiran z  $X$ , je množica<sup>5</sup>

$$\overline{X} = \left\{ \sum_{i=1}^n \left( n_i \prod_{j=1}^{m_i} x_{i,j} \right) \mid n, m_i \in \mathbb{N}_0, n_i \in \mathbb{Z}, x_{i,j} \in X \right\}.$$

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 1.7.5.** Podpolje, generirano z  $X$ , je množica

$$\{ uv^{-1} \mid u, v \in \overline{X} \}.$$

*Dokaz.* Dovolj je preveriti zaprtost za seštevanje, kar pa lahko zapišemo kot

$$ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1}.$$

□

**Trditev 1.7.6.** Podprostor, generiran z  $X$ , je  $\text{Lin } X$ .

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 1.7.7.** Podalgebra, generirana z  $X$ , je množica

$$\overline{X} = \left\{ \sum_{i=1}^n \left( \lambda_i \prod_{j=1}^{m_i} x_{i,j} \right) \mid n, m_i \in \mathbb{N}_0, \lambda_i \in \mathbb{F}, x_{i,j} \in X \right\}.$$

<sup>4</sup> Notacijo  $\langle X \rangle$  uporabljamo le pri grupah.

<sup>5</sup> Oznaka  $\overline{X}$  ni standardna.

# Stvarno kazalo

## A

- Algebrska struktura, [5](#)
  - Algebra, [8](#)
  - Grupa, [6](#)
    - Abelova, [6](#)
    - Center, [9](#)
    - Končna, [6](#)
    - Končno generirana, [11](#)
    - Konjugirana podgrupa, [9](#)
    - Red, [6](#)
    - Simetrična, [6](#)
    - Trivialna, [6](#)
- Kolobar, [7](#)
  - Center, [9](#)
  - Delitelj nič, [7](#)
  - Komutativen, [7](#)
- Obseg, [7](#)
- Podstruktura, [9](#)
- Polgrupa, monoid, [5](#)
- Polje, [7](#)
  - Razširitev, [10](#)
- Vektorski prostor, [8](#)

## B

- Binarna operacija, [4](#)
  - Asociativna, [4](#)
  - Inverz, [5](#)
  - Komutativna, [4](#)
  - Nevtralni element, [4](#)
  - Notranja, zunanja, [4](#)
  - Zaprta množica, [4](#)

## G

- Grupa
  - Generatorji, [11](#)