Algebra 2

Luka Horjak (lukahorjak@student.uni-lj.si)

12. november 2021

Kazalo

Uvod 3

1 Osnovne algebrske strukture 4
1.1 Binarne 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
1.8 Direktni produkti in vsote 12

2 Primeri grup in kolobarjev 13
2.1 Cela števila 13
2.2 Modularna aritmetika 15

Stvarno kazalo 16

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 Binarne operacije

1. oktober 2021

Definicija 1.1.1. *Binarna operacija* $*$ na neprazni množici S je preslikava $*\colon S \times S \to S$. 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 $*_1, *_2 \colon \mathbb{N} \to \mathbb{N}$, 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. □

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*[1] binarna operacija za T.

[1] *Zunanja* binarna operacija je preslikava $*\colon K \times S \to S$.

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 $\underbrace{x * \cdots * x}_{n}$.

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 $l = d$. 8. oktober 2021

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. □

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

$$\mathrm{Sim}(X) = \{f \mid f \colon X \to X \wedge f \text{ je bijektivna}\}$$

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

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

1.4 Kolobarji in polja

15. oktober 2021

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) $\forall x \in K \colon 0x = x0 = 0$,

ii) $\forall x, y \in K \colon (-x)y = x(-y) = -(xy)$,

iii) $\forall x, y, z \in K \colon (x - y)z = xz - yz$,

iv) $\forall x, y \in K \colon (-x)(-y) = xy$ in

v) $\forall x \in K \colon (-1)x = x(-1) = -x$.

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 niča*, 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 niča.

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

Posledica 1.4.6.1. Obseg je kolobar brez deliteljev niča.

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) $\forall \lambda \in \mathbb{F}, u, v \in V\colon \lambda(u+v) = \lambda u + \lambda v$,

iii) $\forall \lambda, \mu \in \mathbb{F}, v \in V\colon (\lambda + \mu)v = \lambda v + \mu v$,

iv) $\forall \lambda, \mu \in \mathbb{F}, v \in V\colon \lambda(\mu v) = (\lambda\mu)v$ in

v) $\forall v \in V\colon 1v = v$.

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) $\forall \lambda \in \mathbb{F}, x, y \in A\colon \lambda(xy) = (\lambda x)y = x(\lambda y)$.

1.6 Podstrukture

22. oktober 2021

Definicija 1.6.1. Podmnožica H grupe G je *podgrupa* grupe G, če je grupa isto operacijo.[2] 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) $\forall x, y \in H \colon xy^{-1} \in H$

iii) $\forall x, y \in H \colon xy \in H \land x^{-1} \in H$

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

Definicija 1.6.3. *Center* grupe G je množica

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

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*[3] 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 $\forall x, y \in L \colon xy \in L \land x - y \in L$.

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

Definicija 1.6.7. *Center* kolobarja K je množica

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

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) $\forall u, v \in U, \lambda \in \mathbb{F} \colon u + v \in U \land \lambda u \in U$

iii) $\forall u, v \in U, \lambda, \mu \in \mathbb{F} \colon \lambda u + \mu v \in U$

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

[2] S tem je seveda mišljena skrčitev operacije na $H \times H$.

[3] 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 $1 \in \mathbb{F}$,

$$\forall x, y \in \mathbb{F}\colon x - y \in \mathbb{F} \land xy \in \mathbb{F}$$

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

Dokaz. The proof is obvious and need not be mentioned. $\square$

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.[4]

Trditev 1.7.2. Velja

$$\langle X\rangle = \left\{\prod_{i=1}^{n} y_i \;\middle|\; \forall i\colon y_i \in X \vee y_i^{-1} \in X\right\}.$$

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[5]

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

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

Trditev 1.7.5. Podpolje, generirano z X, je množica

$$\left\{uv^{-1} \;\middle|\; u, v \in \overline{X}\right\}.$$

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 $\operatorname{Lin} X$.

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

Trditev 1.7.7. Podalgebra, generirana z X, je množica

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

[4] Notacijo $\langle X\rangle$ uporabljamo le pri grupah.
[5] Oznaka $\overline{X}$ ni standardna.

1.8 Direktni produkti in vsote

5. november 2021

Definicija 1.8.1. Naj bodo $G_1, \ldots, G_m$ grupe. Grupi

$$\prod_{i=1}^{m} G_i = G_1 \times \cdots \times G_m$$

z operacijami po komponentah pravimo *direktni produkt* grup $G_1, \ldots, G_m$.

Opomba 1.8.1.1. Pri Abelovih grupah namesto o direktnem produktu govorimo o direktni vsoti

$$\bigoplus_{i=1}^{m} G_i.$$

Definicija 1.8.2. Naj bodo $K_1, \ldots, K_m$ kolobarji. Kolobarju

$$\prod_{i=1}^{m} K_i = K_1 \times \cdots \times K_m$$

z operacijami po komponentah pravimo *direktni produkt*[6] kolobarjev $K_1, \ldots, K_m$.

Definicija 1.8.3. Naj bodo $V_1, \ldots, V_m$ vektorski prostori nad $\mathbb{F}$. Vektorskem prostoru

$$\bigoplus_{i=1}^{m} V_i$$

z operacijami po komponentah pravimo *direktna vsota* vektorskih prostorov $V_1, \ldots, V_m$.

Definicija 1.8.4. Naj bodo $A_1, \ldots, A_m$ algebre nad $\mathbb{F}$. Algebram

$$\prod_{i=1}^{m} A_i$$

z operacijami po komponentah pravimo *direktni produkt* algeber $A_1, \ldots, A_m$.

[6] Direktnemu produktu kolobarjev pravimo tudi direktna vsota.

2 Primeri grup in kolobarjev

2.1 Cela števila

Izrek 2.1.1 (Osnovni izrek o deljenju)**.** Naj bo $m \in \mathbb{Z}$ in $n \in \mathbb{N}$. Potem obstajata taki enolični števili q in r, za kateri je

$$m = qn + r \quad \text{in} \quad 0 \leq r < n.$$

Dokaz. Naj bo

$$S = \{k \in \mathbb{Z} \mid kn \leq m\}.$$

S je navzgor omejena, zato ima največji element q, ki ustreza zgornjim pogojem. □

Posledica 2.1.1.1. Podmnožica H aditivne grupe $\mathbb{Z}$ je podgrupa natanko tedaj, ko je H oblike $n\mathbb{Z}$ za $n \in \mathbb{N}_0$.

Dokaz. $n\mathbb{Z}$ je očitno grupa za vsak n, opazimo pa, da najmanjši naravni element H deli vse ostale. □

Definicija 2.1.2. $d \in \mathbb{N}$ je *največji skupni delitelj* celih števil m in n, če $d \mid n$, $d \mid m$ in vsak skupni delitelj m in n deli tudi d. Označimo $d = \gcd(m, n)$.

Trditev 2.1.3. Naj bo G aditivna grupa in $H, K \leq G$. Potem je tudi

$$H + K = \{h + k \mid h \in H \land k \in K\}$$

podgrupa G.

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

Posledica 2.1.3.1. Za vse pare celih števil m in n, ki nista obe 0, obstaja enoličen največji skupni delitelj, ki je oblike

$$d = mx + ny$$

za neka $x, y \in \mathbb{Z}$.

Dokaz. Grupa $n\mathbb{Z} + m\mathbb{Z}$ je grupa oblike $d\mathbb{Z}$. □

Definicija 2.1.4. Če je $\gcd(m, n) = 1$ pravimo, da sta si m in n *tuji*.

Lema 2.1.5 (Evklid)**.** Naj bo $p \in \mathbb{P}$ in $m, n \in \mathbb{Z}$. Potem velja

$$p \mid m \cdot n \implies p \mid n \lor p \mid m.$$

Dokaz. Če $p \nmid m$, je $\gcd(p, m) = 1$, zato obstajata taka x in y, da je

$$px + my = 1.$$

Sledi, da je

$$p \cdot \left(nx + \frac{mn}{p}\right) = n.$$ □

12. november 2021

Izrek 2.1.6 (Osnovni aritmetike)**.** Vsako naravno število lahko zapišemo kot produkt praštevil na enoličen način do vrstnega reda natančno.

Dokaz. Obstoj faktorizacije dokažemo z indukcijo. Če ima n dve različni faktorizaciji, pa lahko pokrajšamo skupne faktorje in pridemo do protislovja. □

Izrek 2.1.7 (Evklid)**.** Praštevil je neskončno.

Dokaz. V nasprotnem primeru števila

$$\prod_{p \in \mathbb{P}} p + 1$$

ne moremo faktorizirati. □

2.2 Modularna aritmetika

Definicija 2.2.1. Pravimo, da sta celi števili a in b *kongruentni po modulu* n, če velja $n \mid a - b$. Pišemo $a \equiv b \pmod{n}$.

Trditev 2.2.2. Kongruentnost je ekvivalenčna.

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

Definicija 2.2.3. Z

$$\mathbb{Z}_n = \{[x] \mid x \in \mathbb{Z}\}$$

označimo množico ekvivalenčnih razredov relacije kongruentnosti po modulu n.

Trditev 2.2.4. Če je $a \equiv b \pmod{n}$ in $c \equiv d \pmod{n}$, je tudi $a + c \equiv b + d \pmod{n}$ in $ac \equiv bd \pmod{n}$.

Dokaz. Velja

$$n \mid (a - b) + (c - d) \quad \text{in} \quad n \mid c \cdot (a - b) + b \cdot (c - d).$$

□

Definicija 2.2.5. Na $\mathbb{Z}_n$ vpeljemo operaciji[7]

$$+ \colon ([x], [y]) \mapsto [x + y] \quad \text{in} \quad \cdot \colon ([x], [y]) \mapsto [xy].$$

Opomba 2.2.5.1. S tema operacijama je $\mathbb{Z}_n$ komutativen kolobar.

Definicija 2.2.6. Komutativnemu kolobarju brez deliteljev niča pravimo *cel kolobar*.

Lema 2.2.7. Končen cel kolobar je polje.

Dokaz. Preslikava $x \mapsto ax$ za $a \neq 0$ je injektivna, zato je surjektivna. □

Posledica 2.2.7.1. Za praštevila p je $\mathbb{Z}_p$ polje.

[7] Po prejšnji trditvi sta operaciji dobro definirani.

Stvarno kazalo

A
Algebrska struktura, 5
- Algebra, 8
  - Direktni produkt, 12
- Grupa, 6
  - Abelova, 6
  - Center, 9
  - Direktni produkt, 12
  - Končna, 6
  - Končno generirana, 11
  - Konjugirana podgrupa, 9
  - Red, 6
  - Simetrična, 6
  - Trivialna, 6
- Kolobar, 7
  - Cel, 15
  - Center, 9
  - Delitelj niča, 7
  - Direktni produkt, 12
  - Komutativen, 7
- Obseg, 7
- Podstruktura, 9
- Polgrupa, monoid, 5
- Polje, 7
  - Razširitev, 10
- Vektorski prostor, 8
  - Direktna vsota, 12

B
Binarna operacija, 4
- Asociativna, 4
- Inverz, 5
- Komutativna, 4
- Nevtralni element, 4
- Notranja, zunanja, 4
- Zaprta množica, 4

C
Cela števila
- Največji skupni delitelj, 13
- Tujost, 13

G
Grupa
- Generatorji, 11

I
Izrek
- Evklidova lema, 13
- Osnovni aritmetike, 14
- Osnovni izrek o deljenju, 13

K
Kongruence, 15