Poglavje V

Algebraične strukture

V tem poglavju bomo spoznali osnovne algebraične strukture na dani množici. Te so podane z eno ali dvema binarnima operacijama. Binarna operacija paru elementov iz množice priredi nek element iz iste množice. Primeri binarnih operacij so seštevanje, množenje, odštevanje... Za binarne operacije na množicah lahko veljajo različne lastnosti. Glede na to ločimo več (abstraktnih) algebraičnih struktur. Zakaj vpeljemo te strukture? Izreki in trditve, ki veljajo za določeno abstraktno algebraično strukturo, potem veljajo za vse konkretne zglede te strukture in nam jih ni potrebno obravnavati za vsak zgled posebej.

Algebraičnih struktur, ki jih bomo predstavili v tem poglavju, ne bomo podrobno študirali. Spoznali jih bomo le zato, ker nastopajo v definiciji *vektorskega prostora*, ki je osnovna algebraična struktura v linearni algebri.

1 Polgrupa, monoid in grupa

Imamo neko (neprazno) množico M. Množico vseh (urejenih) parov (a, b), $a, b \in M$, označimo z $M \times M$. Podobno za dve neprazni množici M_1 in M_2 označimo z $M_1 \times M_2$ množico vseh urejenih parov (a, b), kjer je prvi element $a \in M_1$ in drugi element $b \in M_2$.

Binarna operacija na množici M je preslikava $\circ : M \times M \to M$. Binarna operacija tako urejenemu paru elementov iz M priredi nek element iz M.

Zgled 1.1 **1.)** Na množici realnih števil poznamo več binarnih operacij: $+$, $-$, $\cdot$.

2.) Na množici pozitivnih realnih števil so definirane naslednje binarne operacije: $+$, $-$, $\cdot$, $/$.

3.) Na množici $\mathbb{R}^n$ imamo binarno operacijo $+$.

4.) Na $\mathbb{R}^3$ je vektorski produkt $\times$ binarna operacija.

5.) Skalarni produkt na $\mathbb{R}^n$, $n \geq 2$, pa ni binarna operacija, saj paru vektorjev priredi skalar.

6.) Na množici naravnih števil $\mathbb{N}$ sta binarni operaciji $+$ in $\cdot$. Operaciji odštevanje in deljenje pa nista binarni operaciji na $\mathbb{N}$, saj se lahko zgodi, da rezultat ni naravno število. Npr. $1 - 2$, ali $2/3$. □

Lastnosti binarnih operacij: $\circ : M \times M \to M$

1.) $\circ$ je *asociativna*, če velja $(a \circ b) \circ c = a \circ (b \circ c)$ za poljubne a, b, $c \in M$. Rečemo tudi, da za $\circ$ velja *asociativnost*.

2.) Element $e \in M$ je *enota*, če velja $a \circ e = a$ in $e \circ a = a$ za vse $a \in M$.

3.) Če je $e \in M$ enota, potem je b *inverz* elementa a, če velja $a \circ b = e$ in $b \circ a = e$. Inverz označimo z a^{-1} ali z $-a$ kadar je operacija seštevanje $+$.

4.) $\circ$ je *komutativna*, če velja $a \circ b = b \circ a$ za vse a, $b \in M$. Rečemo tudi, da za $\circ$ velja *komutativnost*.

Definicija 1.2 Naj bo $\circ : M \times M \to M$ binarna operacija na M. Potem rečemo, da je $(M, \circ)$ *polgrupa*, če je operacija $\circ$ asociativna.

Če je $(M, \circ)$ polgrupa in v njej obstaja enota e, potem rečemo, da je $(M, \circ)$ *monoid*. Opazimo, da je $e \circ e = e$ in zato je $e^{-1} = e$.

Če je $(M, \circ)$ monoid in ima vsak element iz M inverz, potem rečemo, da je $(M, \circ)$ *grupa*.

Če je v polgrupi, monoidu ali grupi $(M, \circ)$ operacija $\circ$ komutativna, potem rečemo, da je $(M, \circ)$ *komutativna polgrupa*, *komutativni monoid* ali *komutativna grupa*. Komutativno grupo imenujemo tudi *Abelova grupa*. ◊

Opomba 1.3 Največkrat bo že iz konteksta jasno, katero binarno operacijo $\circ$ mislimo. Tako bomo poslej pogosto pisali kar M namesto $(M, \circ)$. Rekli bomo, da je M polgrupa, monoid ali grupa. Kadar je operacija na M seštevanje in jo označimo s $+$, potem za inverz elementa $a \in M$ uporabimo običajno oznako $-a$ (in ne a^{-1}). ◊

Zgled 1.4 **1**.) $(\mathbb{R}, +)$ je Abelova grupa. Enota je 0 in inverz $-a$.

2.) $(\mathbb{R}, \cdot)$ je komutativen monoid. Enota je 1.

3.) $(\mathbb{R}, -)$ ni niti polgrupa, saj binarna operacija odštevanje ni asociativna. Na primer: $-4 = (1-2)-3 \neq 1-(2-3) = 2$.

4.) $\mathbb{R}^+ = \{\alpha \in \mathbb{R}\ ;\ \alpha > 0\}$ je Abelova grupa za množenje. Enota je 1 in inverz α^{-1}.

5.) $(\mathbb{R}^n, +)$ je Abelova grupa. Enota je vektor $\mathbf{0}$ in inverz vektorja $\mathbf{v} \in \mathbb{R}^n$ je vektor $-\mathbf{v}$.

6.) $(\mathbb{R}^{m\times n}, +)$ je Abelova grupa. Enota je matrika 0 in inverz matrike $A \in \mathbb{R}^{m\times n}$ je matrika $-A$.

7.) $(\mathbb{R}^{n\times n}, \cdot)$, $(n \geq 2)$, je monoid, ki ni komutativen. Enota je I.

8.) $(\mathbb{R}^3, \times)$ ni niti polgrupa, saj vektorski produkt ni asociativen.

9.) Naj bo $M = \{f : \mathbb{R} \to \mathbb{R}\}$ množica vseh funkcij in operacija $\circ$ kompozitum funkcij. Potem je M monoid, enota je funkcija $f(x) = x$ za $x \in \mathbb{R}$. □

Definicija 1.5 Naj bo $(M, \circ)$ polgrupa in $N \subset M$ neprazna podmnožica. Če je $a \circ b \in N$ za poljubna $a, b \in N$, potem rečemo, da je $\circ$ *notranja operacija* za N, oziroma, da je N *zaprta* podmnožica za operacijo $\circ$. Če je N zaprta za $\circ$, potem je tudi $(N, \circ)$ polgrupa, saj je $(M, \circ)$ polgrupa. Rečemo, da je N *podpolgrupa* v M.

Podobno definiramo tudi pojma podmonoid in podgrupa:

Če je $(M, \circ)$ monoid z enoto e in $N \subset M$ neprazna množica, za katero je $\circ$ notranja operacija in $e \in N$, potem rečemo, da je N *podmonoid* v M.

Če je $(M, \circ)$ grupa (e enota v M) in $N \subset M$ neprazna množica, za katero je $\circ$ notranja operacija, $e \in N$ in za vsak $a \in N$ je tudi a^{-1} v N, potem rečemo, da je N *podgrupa*. ◊

Trditev 1.6 *Naj bo M grupa. Potem je $\emptyset \neq N \subseteq M$ podgrupa natanko tedaj, ko je $a \circ b^{-1} \in N$, za poljubna $a, b \in N$.*

Dokaz Naj bo $N \subseteq M$ podgrupa in $a, b \in N$. Potem je tudi $b^{-1} \in N$ in zato tudi $a \circ b^{-1} \in N$.

Obratno, denimo, da je $a \circ b^{-1} \in N$ za poljubna $a, b \in N$. Če vzamemo $a = b \in N$, dobimo $a \circ a^{-1} = e \in N$. Če vzamemo sedaj $a = e$ in izberemo nek $b \in N$, je tudi $b^{-1} \in N$ in zato je $a \circ (b^{-1})^{-1} = a \circ b \in N$. Tako smo preverili, da je N res podgrupa v M. ■

Zgled 1.7 **1.)** $\mathbb{Z} \subseteq \mathbb{R}$ za seštevanje je podgrupa. Velja namreč $m - n \in \mathbb{Z}$ za poljubni celi števili m in n.

2.) $(\mathbb{R}\backslash\{0\}, \cdot)$ je Abelova grupa. $\mathbb{Z}\backslash\{0\} \subseteq \mathbb{R}\backslash\{0\}$ pa je samo podmonoid. Produkt $m \cdot n$ poljubnih celih števil je spet celo število in $1 \in \mathbb{Z}$. Ker je $2^{-1} \notin \mathbb{Z}$, $\mathbb{Z}$ ni podgrupa.

3.) Naj bo T_n podmnožica zgornje-trikotnih matrik v $\mathbb{R}^{n\times n}$ in naj bo binarna operacija seštevanje matrik. Potem je T_n podgrupa v $\mathbb{R}^{n\times n}$.

4.) Označimo $Gl_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \ ; \ \det A \neq 0\}$. Množica $Gl_n(\mathbb{R})$ je grupa za binarno operacijo množenja matrik: Vemo, da je množenje matrik asociativno, enota je I in A^{-1} je inverz. Posledica 5.7 nam pove, da je produkt dveh obrnljivih matrik spet obrnljiva matrika. Zato je $Gl_n(\mathbb{R})$ zaprta za množenje. Ker velja $detA^{-1} = (\det A)^{-1}$ in $\det I = 1$, sledi I, $A^{-1} \in Gl_n(\mathbb{R})$. Torej je $Gl_n(\mathbb{R})$ grupa, ki pa ni Abelova grupa.

Označimo $Sl_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \ ; \ \det A = 1\}$. $Sl_n(\mathbb{R})$ je podgrupa v $Gl_n(\mathbb{R})$: Če je $\det A = \det B = 1$, je potem tudi

$$\det (AB^{-1}) = (\det A) \left(\det (B^{-1})\right) = \det A \cdot (\det B)^{-1} = 1.$$

Zato je $AB^{-1} \in Sl_n(\mathbb{R})$.

5.) Označimo z D_n množico vseh obrnljivih diagonalnih matrik v $\mathbb{R}^{n\times n}$. Potem je D_n podgrupa v $Gl_n(\mathbb{R})$.

6.) $M = \{f : \mathbb{R} \to \mathbb{R}\}$ množica vseh realnih funkcij in N podmnožica vseh zveznih funkcij $f : \mathbb{R} \to \mathbb{R}$. Potem je N podmonoid v M. □

2 Kolobar in obseg

Naj bo M neprazna množica. Denimo, da imamo na M dve binarni operaciji, ki ju označimo s $+ : M \times M \to M$ in $\cdot : M \times M \to M$. Operacijo $+$ imenujemo *seštevanje* in operacijo $\cdot$ *množenje*. Rečemo, da sta operaciji $+$ in $\cdot$ *distributivni*, če velja

$$\begin{aligned} (a+b)\cdot c &= (a\cdot c)+(b\cdot c) \quad \text{in} \\ a\cdot(b+c) &= (a\cdot b)+(a\cdot c) \quad \text{za} \end{aligned}$$

poljubne a, b, $c \in M$.

Zgled 2.1 **1.)** Množica realnih števil $\mathbb{R}$ ima operaciji $+$ in $\cdot$, ki sta distributivni.

2.) Množica $\mathbb{R}^{n\times n}$ ima dve operaciji $+$ in $\cdot$, ki sta distributivni.

3.) Množica $\mathbb{R}^3$ ima dve operaciji $+$ in $\times$, ki sta distributivni. □

Definicija 2.2 Rečemo, da je množica M *kolobar*, če za binarni operaciji $+$ in $\cdot$ na M velja:

1.) $(M,+)$ je Abelova grupa,

2.) $(M,\cdot)$ je polgrupa,

3.) operaciji $+$ in $\cdot$ sta distributivni.

Če je še $(M,\cdot)$ monoid, rečemo, da je K *kolobar z enoto*. Če pa je $(M,\cdot)$ komutativna polgrupa, pa rečemo, da je M *komutativen kolobar*.

Množica M je *obseg*, če za binarni operaciji $+$ in $\cdot$ velja:

1.) $(M,+)$ je Abelova grupa (z enoto 0),

2.) $(M\backslash\{0\},\cdot)$ je grupa,

3.) operaciji $+$ in $\cdot$ sta distributivni.

Če je še $(M,\cdot)$ komutativen monoid, potem rečemo, da je M *komutativen obseg* (za komutativen obseg se včasih uporablja tudi izraz *polje*). ◊

Zgled 2.3 **1.)** $(\mathbb{R},+,\cdot)$ je komutativen obseg.

2.) $(\mathbb{R}^{n\times n},+,\cdot)$ je kolobar z enoto.

3.) $\mathbb{R}[x]=\{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\ ;\ a_n,a_{n-1},\ldots,a_1,a_0\in\mathbb{R}, n\in\mathbb{N}\}$ je množica vseh polinomov s koeficienti v $\mathbb{R}$. $\mathbb{R}[x]$ je komutativen kolobar z enoto.

4.) $(\mathbb{Z},+,\cdot)$ je komutativen kolobar z enoto (ki ni obseg).

5.) $(\mathbb{Q},+,\cdot)$ je komutativen obseg.

6.) $\mathbb{C}=\{a+b\mathrm{i}\ ;\ a,b\in\mathbb{R},\ \mathrm{i}^2=-1\}$ je množica vseh kompleksnih števil. Operaciji na $\mathbb{C}$ sta definirani s predpisoma:

$$\begin{aligned}(a+b\mathrm{i})+(c+d\mathrm{i}) &= (a+c)+(b+d)\mathrm{i}\\ (a+b\mathrm{i})\cdot(c+d\mathrm{i}) &= (ac-bd)+(ad+bc)\mathrm{i}\ .\end{aligned}$$

za poljubne a, b, c, $d \in \mathbb{R}$. Množica je komutativen obseg. Enota za seštevanje je 0 in inverz števila $a+b\mathrm{i}$ za seštevanje je $-a-b\mathrm{i}$. Enota za množenje je 1 in inverz neničelnega kompleksnega števila je $\frac{1}{a^2+b^2}(a-b\mathrm{i})$. Preveri za vajo, da so izpolnjene vse zahteve in da je $\mathbb{C}$ res komutativen obseg.

7.) Naj bo $\mathbb{H} = \left\{ \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \; ; \alpha, \beta \in \mathbb{C} \right\}$, ter $+$ in $\cdot$ operaciji seštevanja in množenja matrik (ki sta definirani enako kot za matrike, katerih elementi so realna števila). Preveri za vajo, da je $\mathbb{H}$ obseg, ki ni komutativen. $\mathbb{H}$ imenujemo *obseg kvaternionov*. □

Definicija 2.4 Naj bo M kolobar. Neprazna množica $N \subseteq M$ je *podkolobar*, če je N podgrupa za seštevanje in podpolgrupa za množenje.

Naj bo M obseg in $N \subseteq M$ neprazna podmnožica. Potem rečemo, da je N *podobseg*, če je N podgrupa za seštevanje in $N \backslash \{0\}$ podgrupa za množenje. ◊

Zgled 2.5 **1**.) $\mathbb{Z} \subseteq \mathbb{R}$ je podkolobar, ki ni podobseg.

2.) $T_n \subseteq \mathbb{R}^{n \times n}$ je podkolobar.

3.) $\mathbb{R} \subseteq \mathbb{C}$ je podobseg.

4.) Naj bo $2\mathbb{Z}$ množica vseh sodih celih števil. Potem je $2\mathbb{Z}$ podkolobar v kolobarju $\mathbb{Z}$. Opazimo še, da kolobar $2\mathbb{Z}$ nima enote za množenje. □

3 Kolobar ostankov celih števil

Naj bo $n \in \mathbb{N}$, $n \geq 2$. Potem v množici

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

vpeljemo dve binarni operaciji. **Seštevanje** je definirano takole:

$$i \dot{+} j = \begin{cases} i+j & , \text{če je } i+j \leq n-1, \\ i+j-n & , \text{če je } i+j \geq n. \end{cases}$$

Povedano drugače, vsota $i \dot{+} j$ je enaka ostanku pri deljenju $i+j$ z n.

Zgled 3.1 Za $n = 3$ je seštevanje v $\mathbb{Z}_3$ podano z naslednjo tabelo:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

. □

Preverimo, da je $(\mathbb{Z}_n, +)$ Abelova grupa. Naj bodo i, j, $k \in \mathbb{Z}_n$. Potem je

$$\begin{aligned}(i+j)+k &= \begin{cases} i+j+k & \text{, če je } i+j+k \leq n-1 \\ i+j+k-n & \text{, če je } n \leq i+j+k \leq 2n-1 \\ i+j+k-2n & \text{, če je } 2n \leq i+j+k \end{cases} \\ &= i+(j+k) \ .\end{aligned}$$

Seštevanje je torej asociativno. Enota za seštevanje je 0, inverz števila i ($\neq 0$) pa je $n - i$. Seštevanje je komutativno.

Množenje v $\mathbb{Z}_n$ definiramo takole:

$$i \cdot j = \text{ostanek pri deljenju produkt } ij \text{ z } n.$$

Zgled 3.2 Tabeli za množenje v $\mathbb{Z}_3$ in $\mathbb{Z}_4$ sta naslednji:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

in

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

. □

Preverimo, da je $\mathbb{Z}_n$ komutativen kolobar z enoto. V kolobarju $\mathbb{Z}$ velja

$$\begin{aligned}(ij)k &= (r_1 + s_1 n)k = r_2 + s_2 n \quad \text{in} \\ i(jk) &= i(r_3 - s_3 n) = r_4 + s_4 n \ .\end{aligned}$$

Pri tem je $ij = r_1 + s_1 n$ in je r_1 ostanek pri deljenju ij z n. Podobno dobimo tudi r_2, r_3 in r_4. Torej je $r_2 - r_4 = (s_4 - s_2)n$ enako 0 ali pa deljivo z n. Ker $0 \leq r_2 \leq n-1$ in $0 \leq r_4 \leq n-1$, mora biti $r_2 = r_4$. Zato v $\mathbb{Z}_n$ velja asociativnost $(ij)k = i(jk)$. Enota za množenje je 1. Distributivnost seštevanja in množenja preverimo podobno, kot smo preverili asociativnost množenja. Množenje je komutativno.

Ali je $\mathbb{Z}_n$ obseg? $\mathbb{Z}_n$ je obseg natanko takrat, ko je $\mathbb{Z}_n \backslash \{0\}$ Abelova grupa za množenje.

Zgled 3.3 Poiščimo tabeli za množenje v $\mathbb{Z}_n\backslash\{0\}$ za $n = 4$ in $n = 5$.

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

in

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

.

Vidimo, da v $\mathbb{Z}_4\backslash\{0\}$ množenje ni notranja operacija, saj je $2 \cdot 2 = 0$. Torej $\mathbb{Z}_4$ ni obseg.

Iz tabele za množenje v $\mathbb{Z}_5\backslash\{0\}$ vidimo, da je množenje notranja operacija in da imamo v vsaki vrstici element 1. Zato ima vsak element inverz za množenje. Ker smo asociativnost, obstoj enote, distributivnost in komutativnost že preverili, je $\mathbb{Z}_5\backslash\{0\}$ Abelova grupa in $\mathbb{Z}_5$ komutativen obseg. □

Izrek 3.4 *Kolobar $\mathbb{Z}_n$ je obseg natanko takrat, ko je n praštevilo.*

Dokaz Če n ni praštevilo, potem je $n = q \cdot r$ za dve naravni števili q in r iz množice $\{2, 3, \ldots, n-1\}$. Zato je $q \cdot r = 0$ v $\mathbb{Z}_n$. Množenje v $\mathbb{Z}_n\backslash\{0\}$ ni notranja operacija in $\mathbb{Z}_n$ ni obseg.

Obratno, naj bo n praštevilo. Izberimo $i \in \{2, 3, \ldots, n-1\}$. Ker je n praštevilo, sta števili i in n tuji. Zato obstajata taki naravni števili p in q, da je $p \cdot n + q \cdot i = 1$. Pri tem lahko izberemo $1 \leq q \leq n-1$. Če to ne velja, q delimo z n in imamo $q = sn + q'$, kjer je $1 \leq q' \leq n-1$. Potem je

$$(p+s)n + q' \cdot i = 1 \quad \text{in} \quad 1 \leq q' \leq n-1 \ .$$

Privzemimo, da je $pn + qi = 1$ in $1 \leq q \leq n-1$. Potem v $\mathbb{Z}_n$ velja $q \cdot i = 1$ in q je inverz za i. Ker je bil i poljuben neničeln element, je $\mathbb{Z}_n$ obseg. ■

4 Homomorfizem in izomorfizem

Definicija 4.1 Naj bosta $(M_1, \circ_1)$ in $(M_2, \circ_2)$ dve polgrupi. Preslikavo $\varphi : M_1 \to M_2$ imenujemo *homomorfizem polgrup* , če je $\varphi(a \circ_1 b) = \varphi(a) \circ_2 \varphi(b)$ za vse $a, b \in M_1$.

Če sta $(M_1, \circ_1)$ in $(M_2, \circ_2)$ monoida (oziroma grupi), potem preslikavo z lastnostjo

$$\varphi(a \circ_1 b) = \varphi(a) \circ_2 \varphi(b)$$

za vse $a, b \in M_1$, imenujemo *homomorfizem monoidov* (oziroma *homomorfizem grup*). ♢

Zgled 4.2 **1.)** Naj bo $M_1 = M_2 = \mathbb{N}$ in operacija seštevanje. Potem pokažimo, da je preslikava $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = 2n$ homomorfizem polgrup. Velja namreč

$$\varphi(n+m) = 2(n+m) = 2n + 2m = \varphi(n) + \varphi(m) \ .$$

2.) Naj bo $M_1 = \mathbb{R}$ Abelova grupa za seštevanje $+$ in $M_2 = \mathbb{R}$ Abelova grupa za množenje. Dana je preslikava $\varphi(x) = \mathrm{e}^x$. Pokažimo, da je φ homomorfizem grup:

$$\varphi(x+y) = \mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y = \varphi(x) \cdot \varphi(y) \ .$$

3.) Naj bosta $R \in \mathbb{R}^{m\times m}$ in $S \in \mathbb{R}^{n\times n}$ dve matriki. Preslikava $\varphi : \mathbb{R}^{m\times n} \to$ $\to \mathbb{R}^{m\times n}$ naj bo definirana s predpisom $\varphi(A) = RAS$. φ je homomorfizem Abelove grupe $\mathbb{R}^{m\times n}$ nase:

$$\varphi(A+B) = R(A+B)S = RAS + RBS = \varphi(A) + \varphi(B) \ . \qquad \square$$

Definicija 4.3 Naj bo $M_1 \to M_2$ homomorfizem (polgrup, monoidov ali grup). Potem rečemo, da je φ *izomorfizem* (polgrup, monoidov ali grup), če je φ bijektivna preslikava. $\Diamond$

Zgled 4.4 **1.)** Preslikava $\varphi : \mathbb{R} \to \mathbb{R}^+$, $\varphi(x) = \mathrm{e}^x$, je izomorfizem $(\mathbb{R}, +)$ na $(\mathbb{R}^+, \cdot)$. Pri tem je $\mathbb{R}^+$ množica vseh pozitivnih realnih števil. Da je $\varphi(x)$ homomorfizem, vemo iz zgleda **2.)** malo prej. Bijektivnost funkcije $f(x) = \mathrm{e}^x$ kot preslikave iz $\mathbb{R}$ v $\mathbb{R}^+$ smo dokazali pri predavanjih iz Matematike.

2.) Če sta $R \in \mathbb{R}^{m\times m}$ in $S \in \mathbb{R}^{n\times n}$ obrnljivi matriki, potem je preslikava $\varphi(A) = RAS$, $\varphi : \mathbb{R}^{m\times n} \to \mathbb{R}^{m\times n}$ izomorfizem. Da je φ homomorfizem, smo že pokazali. Ker sta R in S obrnljivi, iz $RAS = RBS$ dobimo $A = B$. Injektivnost sledi. Če je $A \in \mathbb{R}^{m\times n}$, potem je $\varphi(R^{-1}AS^{-1}) = A$ in zato je φ surjektivna. $\square$

Trditev 4.5 *Naj bosta M_1 in M_2 grupi in $1_A \in M_1$ in $1_B \in M_2$ njuni enoti. Če je $\varphi : M_1 \to M_2$ homomorfizem, potem je $\varphi(1_A) = 1_B$ in $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

Dokaz Ker je $\varphi : M_1 \to M_2$ homomorfizem grup, velja

$$\varphi(a) = \varphi(1_A \circ_1 a) = \varphi(1_A) \circ_2 \varphi(a)$$

za vsak $a \in M_1$. Ker je M_2 grupa, ima $\varphi(a)$ inverz za operacijo $\circ_2$. Zato je

$$1_B = \varphi(a) \circ_2 \varphi(a)^{-1}$$

in tudi

$$1_B = [\varphi(1_A) \circ_2 \varphi(a)] \circ_2 \varphi(a)^{-1} = \varphi(1_A) \ .$$

Za vsak $a \in M_1$ velja

$$\varphi(1_A) = \varphi(a \circ_1 a^{-1}) = \varphi(a) \circ_2 \varphi(a^{-1}).$$

Ker je $\varphi(1_A) = 1_B$, sledi enakost $\varphi(a^{-1}) = \varphi(a)^{-1}$. ■

Definicija 4.6 Naj bosta $(K_1, +_1, \cdot_1)$ in $(K_2, +_2, \cdot_2)$ dva kolobarja. Preslikava $\varphi : K_1 \to K_2$ je *homomorfizem kolobarjev*, če velja

$$\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b) \quad \text{za vse } a, b \in K_1 \tag{V.1}$$

$$\text{in} \quad \varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b) \quad \text{za vse } a, b \in K_1. \tag{V.2}$$

Če sta K_1 in K_2 obsega, preslikavo $\varphi : K_1 \to K_2$ z lastnostima (V.1) in (V.2) imenujemo *homomorfizem obsegov*.

Bijektivni homomorfizem (kolobarjev, obsegov) imenujemo *izomorfizem* (kolobarjev, obsegov). ◊

Zgled 4.7 **1.)** Naj bo $S \in \mathbb{R}^{n\times n}$ obrnljiva matrika. Potem je preslikava $\varphi : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$, $\varphi(a) = SAS^{-1}$, homomorfizem kolobarja $\mathbb{R}^{n\times n}$ nase. φ je celo izomorfizem:

- $\varphi(A + B) = S(A + B)S^{-1} = SAS^{-1} + SBS^{-1} = \varphi(A) + \varphi(B)$
- $\varphi(AB) = SABS^{-1} = SAS^{-1}SBS^{-1} = \varphi(A) \cdot \varphi(B)$
- φ je injektiven: iz $SAS^{-1} = SBS^{-1}$ sledi $A = B$.
- φ je surjektiven: za $A \in \mathbb{R}^{n\times n}$ je $\varphi(S^{-1}AS) = A$.

2.) Za vajo preveri, da je preslikava

$$\begin{aligned} \varphi : \mathbb{C} &\to \mathbb{R}^{2\times 2} \\ \varphi(a + b\,\mathrm{i}) &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \end{aligned}$$

homomorfizem (kolobarjev).

3.) Naj bo n neko naravno število večje ali enako 2 in $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ preslikava definirana s pravilom "$\varphi(m)$ je ostanek pri deljenju m z n". Preveri za vajo, da je φ homomorfizem kolobarjev. □