

# Skripta za algebro2

Filip Koprivec

2. november 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

<b>1</b>	<b>Osnovne algebrske strukture</b>	<b>3</b>
1.1	Binarne operacije . . . . .	3
1.2	Polgrupe in monoidi . . . . .	5
1.3	Grupe . . . . .	8
1.4	Kolobarji . . . . .	9
1.5	Vektorski prostori . . . . .	13
1.6	Algebre . . . . .	14
1.7	Podgrupe, podkolobarji in druge podstrukture . . . . .	15
1.7.1	Podgrupe . . . . .	15
1.7.2	Podkolobarji . . . . .	17
1.7.3	Podprostori . . . . .	17
1.7.4	Podalgebre . . . . .	18
1.7.5	Podpolje . . . . .	18
1.7.6	Logične operacije nad (pod)strukturami . . . . .	19
1.8	Generatorji . . . . .	19
1.8.1	Generatorji grup . . . . .	19
1.8.2	Generatorji kolobarja . . . . .	20
1.8.3	Generatorji vektorskih prostorov . . . . .	20
1.8.4	Generatorji algeber . . . . .	21

# 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 binarnih 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

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

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

$$\forall x, y \in \mathcal{S}. x \circ y = y \circ x \quad (2)$$

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 asociativna in komutativna

2. Operacija  $*$  na  $\mathbb{Z}$  je tako asociativna 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  $\mathcal{S}$  in  $e \in \mathcal{S}$ .  $e$  se imenuje **neutralni element**, če velja

$$\forall x \in \mathcal{S}. e \circ x = x \circ e = x \quad (3)$$

**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.

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

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

$$e = f$$

□

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

$$\forall x \in \mathcal{S}. e' \circ x = x \quad (4)$$

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

$$\forall x \in \mathcal{S}. x \circ e'' = x \quad (5)$$

**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

$$\forall t, t' \in \mathcal{T}. t \circ t' \in \mathcal{T} \quad (6)$$

**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 imajo 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.  $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{N}, *), \dots$

*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 okepaže 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:

$$y = (x_1 \circ w) \circ v \quad \underbrace{\quad}_{\text{Asociativnost(1)}} \quad = \quad x_1 \circ (w \circ v)$$

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  $x \in \mathcal{S}$*

$$x^n := \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ elementov}} \quad (7)$$

**Opomba:** Brez asociativnosti ni definirano niti  $x^3$

**Opomba:**

Očitno velja:

$$\forall n, m \in \mathbb{N}. x^n \circ x^m = x^{n+m} \text{ in}$$

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

**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:*

$$x \circ y = y \circ x = e \quad (8)$$

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

$$x \circ x^{-1} = x^{-1} \circ x = e \quad (9)$$

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

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

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

**Posledica:** Obrnljiv element monoida ima natanko en inverz.

**Posledica:** Če je  $x$  obrnljiv element monoida  $S$  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:

$$(y^{-1} \circ x^{-1}) \circ (x \circ y) = y^{-1} \circ (x^{-1} \circ x) \circ y = y^{-1} \circ e \circ y = y^{-1} \circ y = e$$
  $\square$

**Opomba:** Seveda velja za  $n$  elementov

$$(x_1 \circ x_2 \circ \dots \circ x_n)^{-1} = x_n^{-1} \circ \dots \circ x_2^{-1} \circ x_1^{-1} \quad (10)$$

**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:**

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

**Definicija 17:**

$$x^0 := e \quad (12)$$

Tako kadar je  $x$  **obrnjljiv** veljata enačbi

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

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

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

$$x \circ y = x \circ z \implies y = z \quad (15)$$

In tudi

$$y \circ x = z \circ x \implies y = z \quad (16)$$

*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  $\square$

**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 imenovala 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 imenuje **komutativna grupa** ali **Abelova grupa**.

Ki je ekvivalenta bolj čisti definiciji:

**Definicija 19:** Množica  $\mathbb{G}$  skupaj z binarno operacijo  $*$ :  $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$ ,  $(x, y) \mapsto xy$  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  $\mathbb{G}$  imenujemo **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:**  $S$   $S^*$  označujemo množico vseh obrnljivih elementov monoida  $S$ .

**Trditev 7:** Če je  $S$  monoid je  $S$  grupa.

*Dokaz.*  $x, y \in S^* \implies x \circ y \in S^*$  // Obrnljiv je tudi njun produkt, torej je množica je zaprta za  $*$

Ker je  $*$  asociativen na  $S$  je asociativen tudi na  $S^*$

$e \in S^*$  saj je enota inverz sami sebi

$x \in S^* \implies x^{-1} \in S^*$  // 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.  $(F(\mathcal{X}), \circ)$ :  $(F(\mathcal{X}), \circ)^* = \{f : \mathcal{X} \rightarrow \mathcal{X} | f \text{ je bijekcija}\}$

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

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

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

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

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

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  $K$  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

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

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

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

**Opomba:** Poznamo tudi kolobarje brez enote (kjer je  $(\mathcal{K}, *)$  zgolj monoid. Recimo

$$2\mathbb{Z} := \{2n | n \in \mathbb{Z}\}$$

**Trditev 8:** V poljubnem kolobarju veljajo naslednje lastnosti:

(a)

$$\forall x \in \mathcal{K}. 0x = x0 = 0$$

*Dokaz.*

$$0x = (0 + 0)x = 0x + 0x$$

$$\Downarrow$$

$$0 = 0x$$

Podobno za  $x0 = 0$

□

(b)

$$\forall x, y \in \mathcal{K}. (-x)y = x(-y) = -(xy)$$

*Dokaz.*

$$0 = 0y = (x + (-y))y = xy + (-x)y$$

$$\Downarrow$$

$$-(xy) = (-x)y$$

□

(c)

$$\forall x, y, z \in \mathcal{K}. x(y - z) = xy - xz \wedge (y - z)x = yx - zx$$

*Dokaz.*

$$x(y - z) = x(y + (-z)) = xy + x(-z)$$

Podobno za drugo stran

□

(d)

$$\forall x, y \in \mathcal{K}. (-x)(-y) = xy$$

*Dokaz.*

$$(-x)(-y) = -(x(-y)) = -(-xy) = xy$$

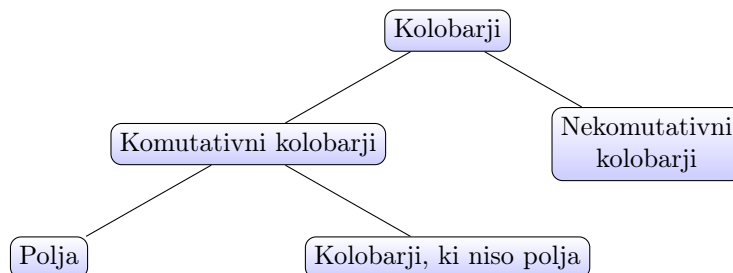
□

(e)

$$\forall x \in \mathcal{K}. (-1)x = x(-1) = -x$$

Sledi iz (b) če vzamemo  $y = -1$

Kolobar  $\mathcal{K}$  je **komutativen**, če za množenje velja zakon komutativnosti (2).



**Primer:**

1.  $\mathbb{Z}$  (tipičen primer kolobarja)
2.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  (to niso tipični primeri kolobarjev, saj so kar polja)
3. **Trivialni ali ničelni kolobar:**

$$\{0\}$$

**Trditev 9:**

$$\text{Kolobar } \mathcal{K} \text{ je ničelen} \iff 1 = 0$$

*Dokaz.*

$\implies$  : Očitno

$$\impliedby : \forall x \in \mathcal{K}. x = 1x = 0x = 0$$

□

4. Matrični kolobarji  $(M_n(\mathbb{R}), M_n(\mathbb{C}))$  z običajnim seštevanjem in množenjem,

$$0 = \underbrace{\begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 0 \end{bmatrix}}_n; \quad 1 = \underbrace{\begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 0 \end{bmatrix}}_n$$

Ta kolobar je nekomutativen za  $n \geq 2$

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}; B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \implies AB = B, BA = 0$$

$A$  in  $B$  ne komutirata, prav tako pa smo videlo da je lahko produkt dveh neničelnih elementov 0.

**Definicija 23:** Element  $x \neq 0$  kolobarja  $\mathcal{K}$ , je **levi deljitelj ničla**, če obstaja tak  $y \neq 0, y \in \mathcal{K}$ , da velja:  $xy = 0$ .

**Definicija 24:** Element  $x \neq 0$  kolobarja  $\mathcal{K}$ , je **desni deljitelj ničā**, če obstaja tak  $y \neq 0, \in \mathcal{K}$ , da velja:  $yx = 0$ .

**Definicija 25:** Element  $x$  je **delitelj ničā**, če je **hkrati levi in desni delitelj ničā**.

**Opomba:**

$$\mathcal{K} \text{ ima leve deljitelje ničā} \iff \mathcal{K} \text{ ima desne deljitelje ničā} \quad (21)$$

*Dokaz.*

$\implies$  : Obstajata taka  $y \neq 0, x \neq 0$ , imamo dve možnosti

1.  $xy = 0 \implies$  Dokaz je končan
2.  $xy \neq 0$ :  $x(yx) = 0$  in je  $yx$  desni deljitelj ničā

$\impliedby$  : Podobno

□

V Kolobarju brez deliteljev ničā velja:

$$\forall x, y \in \mathcal{K}. xy = 0 \implies x = 0 \vee y = 0 \quad (22)$$

V takih kolobarjih velja pravilo krajšanja:

$$xy = xz \wedge x \neq 0 \implies y = z$$

$$yx = zx \wedge x \neq 0 \implies y = z$$

$$xy = xz \iff x(y - z) = 0$$

$$yx = zx \iff (y - z)x = 0$$

Kolobar je monoid za množenje zato lahko govorimo o obrnljivih elementih.

**Primer:**

1. V  $\mathbb{Z}$  sta obrnljiva  $1, -1$ .
2. V  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  so obrnljivi vsi elementi razen  $0$

**Definicija 26:** Kolobar, v katerem  $1 \neq 0$  in v katerem so **vsī neničelni elementi obrnljivi** se imenuje **obseg**.

**Definicija 27:** Komutativni obseg se imenuje **polje**

**Primer:**

1.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ , so polja
2. Nekomutativne obsege bomo dodali kasneje

**Trditev 10:** Obrnljiv element kolobarja ni levi(alī desni) delitelj ničā. Obsegi so zato kolobarji brez deliteljev ničā.

*Dokaz.*  $x$  je obrnljiv:  $xy = 0$

$$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0 \text{ Torej } x \text{ ni delitelj ničā.}$$

□

## 1.5 Vektorski prostori

**Definicija 28:** Naj bo  $\mathcal{F}$  polje. Množica  $\mathcal{V}$  skupaj z (notranjo) binarno operacijo seštevanje  $+: \mathcal{V} \times \mathcal{V} \rightarrow \mathcal{V}$  in zunanjo binarno operacijo  $\mathcal{F} \times \mathcal{V} \rightarrow \mathcal{V}$  imenovano **množenje s skalarji** in označeno z  $(\lambda, v) \mapsto \lambda v$  se imenuje **vektorski prostor nad poljem  $\mathcal{F}$** , če zanj velja:

$V_1$ : Za seštevanje je  $\mathcal{V}$  Abelova grupa

$V_2$ : Velja distributivnost v vektorskem faktorju

$$\forall \lambda \in \mathcal{F}. \forall u, v \in \mathcal{V}. \lambda(u + v) = \lambda u + \lambda v \quad (23)$$

$V_3$ : Velja distributivnost v skalarnem faktorju

$$\forall \lambda, \mu \in \mathcal{F}. \forall v \in \mathcal{V}. (\lambda + \mu)v = \lambda v + \mu v \quad (24)$$

$V_4$ : Velja zakon homogenosti

$$\forall \lambda, \mu \in \mathcal{F}. \forall v \in \mathcal{V}. (\lambda\mu)v = \lambda(\mu v) \quad (25)$$

$V_5$ : Enota

$$\forall v \in \mathcal{V}. 1v = v \quad (26)$$

Za vsak vektorski prostor očitno veljajo naslednje trditve

•

$$\forall \lambda \in \mathcal{F}. \lambda 0 = 0$$

•

$$\forall u, v \in \mathcal{V}. 0u = 0$$

•

$$\forall \lambda, \mu \in \mathcal{F}. \lambda\mu = 0 \implies \lambda = 0 \vee \mu = 0$$

•

$$\forall \lambda, \mu \in \mathcal{F}. (-\lambda)\mu = \lambda(-\mu) = -(\lambda\mu)$$

**Opomba:** Elementom polja  $\mathcal{F}$  pravimo **skalarji**, elementom  $\mathcal{V}$  pa vektorji

- $\mathcal{F} = \mathbb{R}$ : Realni vektorski prostor
- $\mathcal{F} = \mathbb{C}$ : Kompleksni vektorski prostor

**Primer:**

1. Splošni prostor  $\mathcal{F}^n$ , kjer vpeljemo operaciji:

**Seštetavnje**

$$(u_1, u_2, \dots, u_n) + (v_1, v_2, \dots, v_n) \mapsto (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n) \quad (27)$$

**Množenje s skalarjem**

$$\lambda(u_1, u_2, \dots, u_n) \mapsto (\lambda u_1, \lambda u_2, \dots, \lambda u_n) \quad (28)$$

2. Trivialni vektorski prostor:  $\{0\}$
3. Vektorski prostor polinomov stopnje največ  $n$ , kjer seštevanje in množenje definiramo na običajen način
4.  $\mathbb{C}$  je vektorski prostor nad  $\mathbb{R}$  (za  $+$  je Abelova grupa, množenje pa definiramo po komponentah, tako je nad  $\mathbb{C}$  to 2-dimenzionalen, nad  $\mathbb{R}$  pa 1-dimenzionalen)

## 1.6 Algebre

Mnogi pomembni primeri kolobarjev so hkrati tudi vektorski prostori, dejansko so algebre

**Definicija 29:** Naj bo  $\mathcal{F}$  polje (komutativen obseg). Množica  $\mathcal{A}$  skupaj z (notranjima) binarnima operacijama  $+$  (seštevanje) in  $*$  (množenje) ter zunanjo binarno operacijo  $\mathcal{F} \times \mathcal{A} \rightarrow \mathcal{A}$  (množenje s skalarji) je **Algebra na poljem  $\mathcal{F}$  ali  $\mathcal{F}$ -algebra**, če velja:

$V_1$ : Za seštevanje in množenje s skalarji je  $\mathcal{A}$  vektorski prostor

$V_2$ : Za množenje je  $\mathcal{A}$  monoid

$V_3$ : Veljata neke vrste levi in desni distributivnostni zakon

$$\forall x, y, z \in \mathcal{A}. \forall \lambda, \mu \in \mathcal{F}. (\lambda x + \mu y)z = \lambda(xz) + \mu(yz)$$

$$\forall x, y, z \in \mathcal{A}. \forall \lambda, \mu \in \mathcal{F}. z(\lambda x + \mu y) = \lambda(zx) + \mu(zy)$$

**Opomba:** Za  $\lambda = \mu = 1$  je to navadna distributivnost. Torje je Algebra kolobar, ki je hkrati vektorski prostor, v katerem velja še:

$$\lambda(xz) = (\lambda x)z = x(\lambda z)$$

### Primer:

1. Vektorski prostor  $\mathcal{F}^n$  postane algebra, če definiramo množenje, najlažje kar po komponentah:

$$(x_1, x_2, \dots, x_n)(y_1, y_2, \dots, y_n) \mapsto (x_1 y_1, x_2 y_2, \dots, x_n y_n) \quad (29)$$

2. Kolobar  $M_n(\mathbb{R})$  postane algebra, če definiramo množenje s skalarji

$$\lambda(a_{ij}) = (\lambda a_{ij}) \quad (30)$$

3. Vektorski prostor polinomov postane algebra, če vpeljemo množenje polinomov na standardni način

**Opomba:** 'Teorija kolobarjev' in 'teorija kolobarjev in algeber' se razlikujeta zgolj v povdarku.

## 1.7 Podgrupe, podkolobarji in druge podstrukture

$(\mathbb{R}, +)$  in  $(\mathbb{C}, +)$  sta različni strukturi, a očitno povezani Abelovi grupi. Operacija je seštevanje in  $\mathbb{R} \subseteq \mathbb{C}$ . Rečemo:  $(\mathbb{R}, +)$  je podgrupa  $(\mathbb{C}, +)$ .

Podobno rečemo  $(\mathbb{R}, +, *)$  je podkolobar  $(\mathbb{C}, +, *)$

In ker sta to tudi polji rečemo kar kar  $(\mathbb{R}, +, *)$  je podpolje  $(\mathbb{C}, +, *)$

### 1.7.1 Podgrupe

**Definicija 30:** *Neprazna podmnožica  $\mathcal{H}$  grupe  $\mathcal{G}$  je **podgrupa** grupe  $\mathcal{G}$ , če je za isto operacijo (zožitev na  $\mathcal{H} \times \mathcal{H}$ ) tudi sama grupa.*

**Primer:**

1. Vsaka grupa  $\mathcal{G}$  ima vsaj dve podgrupi:  $\mathcal{G}$  in  $\{1\}$

**Opomba:**  $\{1\}$  se imenuje **trivialna podgrupa**

**Opomba:** Vsaka od  $\mathcal{G}$  različna podgrupa se imenuje **prava podgrupa**

**Trditev 11:** Za naprazno podmnožico  $\mathcal{H}$  grupe  $\mathcal{G}$  so naslednje trditve ekvivalentne:

(i)

$\mathcal{H}$  je podgrupa  $\mathcal{G}$

(ii)

$\forall x, y \in \mathcal{H}. xy^{-1} \in \mathcal{H}$

(iii)

$\forall x, y \in \mathcal{H}. xy \in \mathcal{H} \wedge x^{-1} \in \mathcal{H}$

*Dokaz.*

(i)  $\implies$  (ii) : Očitno iz definicije da je  $\mathcal{H}$  grupa

(ii)  $\implies$  (iii) :

$x \in \mathcal{H} \implies 1 = xx^{-1} \in \mathcal{H} \implies x^{-1} = 1x^{-1} \in \mathcal{H}$  // Zaprta za inverz

$x, y \in \mathcal{H} \implies xy = x(y^{-1})^{-1} \in \mathcal{H}$  Zaprta za poljubna dva

(iii)  $\implies$  (i):

Očitno zaprta za množenje, asociativna, ker velja na večji množici ( $\mathcal{G}$ )

$$1 = xx^{-1} \in \mathcal{H}$$

$$x \in \mathcal{H} \implies x^{-1} \in \mathcal{H}$$

□

Govorimo 'grupa  $\mathcal{H}$ ' ali 'podgrupa  $\mathcal{H}$ ' označimo:

$$\mathcal{H} \leq \mathcal{G}$$

**Primer:**

1.  $\mathbb{R} - \{0\}$  je podgrupa  $(\mathbb{C} - \{0\})$
2.  $\{x \in \mathbb{R} | x < 0\}$  je podgrupa  $(\mathbb{C} - \{0\})$
3.  $\{1, -1, i, -i\}$  je podgrupa  $(\mathbb{C} - \{0\})$
4.  $\{z \in \mathbb{C} | |z| = 1\}$  je podgrupa  $(\mathbb{C} - \{0\})$
5.  $\{x \in \mathbb{R} | |x| > 1\}$  **ni** podgrupa  $(\mathbb{C} - \{0\})$
6.  $\{z \in \mathbb{C} - \{0\} | |z| \leq 1\}$  **ni** podgrupa  $(\mathbb{C} - \{0\})$

**Opomba:**

V aditivni grupi velja

(ii) :  $\forall x, y \in \mathcal{H}. x - y \in \mathcal{H}$  in

(iii):  $\forall x, y \in \mathcal{H}. x + y \in \mathcal{H} \wedge -x \in \mathcal{H}$

**Primer:**

Pogdgrupe  $(\mathbb{Z}, +)$

1. Trivialna primera podgrup sta  $\mathbb{Z}$  in  $\{0\}$
2.  $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$
3.  $k\mathbb{Z} = \{kn | n \in \mathbb{Z}\} // k \in \mathbb{Z}$

**Definicija 31:** Elementa  $a, b$  iz grupe  $\mathcal{G}$  sta si **konjugirana**, če velja:

$$\exists c \in \mathcal{G}. b = cac^{-1} \quad (31)$$

**Opomba:** Relacija 'elementa sta si konjugirana' je ekvivalenčna

**Definicija 32:** Če je  $c \in \mathcal{H} \leq \mathcal{G}$  je

$$c\mathcal{H}c^{-1} := \{chc^{-1} | h \in \mathcal{H}\} \quad (32)$$

**konjugirana podgrupa** podgrupe  $\mathcal{H}$ .

**Trditev 12:**

$$\begin{aligned} chc^{-1}ch'c^{-1} &= c \underbrace{hh'}_{\in \mathcal{H}} c^{-1} \in \mathcal{H} \\ (chc^{-1})^{-1} &= (c^{-1})^{-1}h^{-1}c^{-1} = c \underbrace{h^{-1}}_{\in \mathcal{H}} c^{-1} \in \mathcal{H} \end{aligned}$$

**Opomba:** Pojem konjugiranih podgrup ima smisel v nekomutativnih grupah



### 1.7.2 Podkolobarji

**Definicija 33:** Podmonžica  $\mathcal{L}$  kolobarja  $\mathcal{K}$  je **podkolobar** kolobarja  $\mathcal{K}$ , če vsebuje enoto (1) kolobarja  $\mathcal{K}$  in če je kolobar za isti operaciji.

**Primer:**

$$1. \mathcal{L} = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \mid x \in \mathbb{R} \right\}$$

Sicer je kolobar za isti operaciji, a ne podeduje enote (ima svojo) torej **ni** podkolobar

**Trditev 13:** Podmnožica  $\mathcal{L}$  kolobarja  $\mathcal{K}$  je podkolobar natanko tedaj, ko velja

$$1 \in \mathcal{L} \wedge \forall x, y \in \mathcal{L}. x - y \in \mathcal{L} \quad (33)$$

*Dokaz.*

$\Rightarrow$  : Sledi iz definicije

$\Leftarrow$  : Iz predpostavke sledi, da je  $\mathcal{L}$  podgrupa za +.

Prav tako je  $(\mathcal{L}, *)$  monoid

Izpolnjevanje distributivnih zakonov pa sledi iz tega da so izpolnjeni tudi na  $\mathcal{K}$

**Opomba:** Uporabili smo tridtev (11) in (ii) pogoj zamenjali z (iii)  $\square$

**Primer:**

1. Kolobar  $\mathbb{Z}$  je podkolobar  $\mathbb{Q}$ .
2. Kolobar  $\mathbb{Q}$  je podkolobar  $\mathbb{R}$ .

### 1.7.3 Podprostori

**Definicija 34:** Podmnožica  $\mathcal{U}$  vektorskega prostora  $\mathcal{V}$  je **podprostor**  $\mathcal{V}$ , če je za isti operaciji tudi sama vektorski prostor.

**Trditev 14:** Za neprazno podmnožico  $\mathcal{U}$  vektorskega prostora  $\mathcal{V}$  so naslednje trditve ekvivalentne

(i)

$\mathcal{U}$  je podprostor  $\mathcal{V}$

(ii)

$$\forall x, y \in \mathcal{U}. \forall \lambda, \mu \in \mathcal{F}. \lambda x + \mu y \in \mathcal{U}$$

(iii)

$$\forall x, y \in \mathcal{U}. x + y \in \mathcal{U} \wedge \forall x \in \mathcal{U}. \forall \lambda \in \mathcal{F}. \lambda x \in \mathcal{U}$$

*Dokaz.* Očitno  $\square$

**Primer:**

Edini podprostori vektorskega prostora  $\mathbb{R}^3$  so:

- $\{0\}, \mathbb{R}^3$
- premice skozi izhodišče
- ravnine skozi izhodišče

**1.7.4 Podalgebre**

**Definicija 35:** Podmnožica  $\mathcal{B}$  algebre  $\mathcal{A}$  je **podalgebra**  $\mathcal{A}$ , če je za iste operacije tudi sama algebra in vsebuje enoto (1) iz algebre  $\mathcal{A}$ .

**Trditev 15:** Neprazna podmnožica  $\mathcal{B}$  algebre  $\mathcal{A}$  je **podalgebra** algebre  $\mathcal{A}$  natanko tedaj ko zanjo velja:

$$1 \in \mathcal{B} \wedge \forall x, y \in \mathcal{B}. \forall \lambda \in \mathcal{F}. \underbrace{x + y, \lambda x, xy}_{\text{podprostor}} \in \mathcal{B} \quad (34)$$

Torej je zaprta za seštevanje, množenje in množenje s skalarji

*Dokaz.* Enako kot za podkolobarje □

**Primer:**

$$1. \ A = \mathcal{M}_2(\mathbb{R}) \ B = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} \mid a_{ij} \in \mathbb{R} \right\}$$

**1.7.5 Podpolje**

**Definicija 36:** Podmočica  $\mathcal{F}$  polja  $\mathcal{E}$  je **podpolje** polja  $\mathcal{E}$ , če je za isti operaciji tudi sama polje

**Opomba:** Podpolje nujno vsebuje isto enoto 1 kot polje  $\mathcal{E}$ , naj bo  $e \in \mathcal{F}$  enota.  $e^2 = e \implies e(\underbrace{1}_{\text{enota } \mathcal{E}} - e) = 0$  Ker v poljih ni deliteljev nič, velja  $e = 1$ .

**Trditev 16:** Podmnožica  $\mathcal{F} \neq \{0\}$  polja  $\mathcal{E}$  je podpolje natanko tedaj ko velja

$$\forall x, y \in \mathcal{F}. xy, x - y \in \mathcal{F} \wedge 0 \neq x \in \mathcal{F}. x^{-1} \in \mathcal{F} \quad (35)$$

*Dokaz.* Podobno kot prej □

Praši muhata!!!!

**Definicija 37:** Polje  $\mathcal{E}$  je **razširitev** polja  $\mathcal{F}$  če je  $\mathcal{F}$  podpolje  $\mathcal{E}$ .

**Primer:**

1.  $\mathbb{R}$  je podpolje  $\mathbb{C}$
2.  $\mathbb{C}$  je razširitev  $\mathbb{R}$ , ki je razširitev  $\mathbb{Q}$

### 1.7.6 Logične operacije nad (pod)strukturami

Če so  $\mathcal{H}_i$  podgrupe grupe  $\mathcal{G}$  je tudi njihov presek  $\cap \mathcal{H}_i$  podgrupa.

**Opomba:** Družina  $\mathcal{H}_i$  je **lahko končna ali neskončna** torej poljubna

**Presek** algebrskih struktur (podgrup, podkolobarjev, podprostorov, podalgeber, podpolji) **ohrani lastnosti** te algebrske strukture.

**Unija** algebrskih struktur praviloma **ne ohrani** lastnosti te algebrske strukture.

**Primer:**

1.  $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$  in  $3\mathbb{Z} = \{3n | n \in \mathbb{Z}\}$  sta podgrupi  $\mathbb{Z}$ , njuna unija pa ni podgrupa (saj ni grupa), ker  $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

## 1.8 Generatorji

$\mathbb{R}^3$  je generiran z vektorji:  $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ . Edini podprostor, ki te vektorje vsebuje je namreč  $\mathbb{R}^3$  sam. Seveda je generiran tudi z drugimi vektorji:  $(1, 1, 0), (0, 1, 0), (0, 0, 1)$ .

Vekotrja  $(1, 0, 0), (0, 1, 0)$  pa generirata ravnino:  $z = 0$ .

### 1.8.1 Generatorji grup

Naj bo  $\mathcal{X}$  neprazna podmnožica grupe  $\mathcal{G}$ , Vzemimo množico vseh elementov oblike  $x_1 x_2 \dots x_n$ , kjer velja  $x, x^{-1} \in \mathcal{X}$  in jo označimo z  $\langle \mathcal{X} \rangle$ .

Če je  $\mathcal{X} = \{y_1, y_2, \dots, y_n\}$  pišemo tudi  $\mathcal{X} = \langle y_1, y_2, \dots, y_n \rangle$ .

Tako  $\langle x, y \rangle$  sestoji iz elementov kot so:  $1, x, y, x^2, x^3, x^{-1}, x^{-2}, x^{-1}y, y^{-1}, x^5 y^{-1} x^3 y^{-3} x y^2, \dots$

**Opazimo**, da je  $\langle \mathcal{X} \rangle$  podgrupa

$$u, v \in \langle \mathcal{X} \rangle \implies uv \in \langle \mathcal{X} \rangle \wedge u^{-1} \in \langle \mathcal{X} \rangle$$

$(x_1, \dots, x_n)^{-1} = x_1^{-1} \dots x_n^{-1}$ , ki vsebuje množico  $\mathcal{X}$ .

Velja pa tudi obratno: vsaka podgrupa grupe  $\mathcal{G}$ , ki vsebuje  $\mathcal{X}$  vsebuje tudi to podgrupo  $\langle \mathcal{X} \rangle$ .

Torej je  $\langle \mathcal{X} \rangle$  najmanjša podgrupa, ki vsebuje  $\mathcal{X}$ . Pravimo ji **podgrupa, generirana z  $\mathcal{X}$** .

Če velja  $\langle \mathcal{X} \rangle = \mathcal{G}$ , rečemo, da je  $\mathcal{G}$  generirana z množico  $\mathcal{X}$ , elemente iz  $\mathcal{X}$  pa imenujemo **generatorji** grupe  $\mathcal{G}$ , množici  $\mathcal{X}$  pa **množica generatorjev**.

**Primer:**

1.  $\mathbb{Q}^+$  je grupa za množenje. Velja:  $\langle \mathbb{N} \rangle = \mathbb{Q}^+$ , ker  $\langle 2, 3 \rangle = \{2^i 3^j | i, j \in \mathbb{Z}\}$

**Opomba:** V aditivni grupi  $\langle \mathcal{X} \rangle$  za komponiranje elementov uporabljamo drugo operacijo, vse ostalo ostane isto.

**Primer:**

1. Grupa  $(\mathbb{Z}, +)$  je generirana z  $\langle 1 \rangle$  in prav tako z  $\langle -1 \rangle$ . Velja  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ .

**Opomba:** Grupe generirane z enim samim elementom imenujemo **ciklične**. ( $\langle 2 \rangle = \langle 4, 6 \rangle = 2\mathbb{Z}$ )

Cilj je poiskati najmanjše množice generatorjev (očitno  $\langle \mathcal{G} \rangle = \mathcal{G}$ ).

**Definicija 38:** Grupa je **končno generirana** če je generirana s kako končno množico.

### 1.8.2 Generatorji kolobarja

Naj bo  $\mathcal{K}$  kolobar,  $\emptyset \neq \mathcal{X} \subseteq \mathcal{K}$ .

Označimo z  $\overline{\mathcal{X}}$  podgrupo za seštevanje  $\mathcal{K}$ , ki vsebuje vse produkte elementov iz  $\mathcal{X} \cup \{1\}$ .

Opazimo:  $\overline{\mathcal{X}}$  je podkolobar, ki vsebuje  $\mathcal{X}$  in je vsebovan v vsakem podkolobarju, ki  $\mathcal{X}$  vsebuje. Zato mu rečemo **podkolobar generiran z množico  $\mathcal{X}$** .

**Primer:**

1.  $\mathcal{K} = \mathbb{C}$

- $\overline{\{1\}} = \mathbb{Z}$
- $\overline{\{i\}} = \{n + mi \mid n, m \in \mathbb{Z}\} = \mathbb{Z}[i]$  (Kolobar **Gaussovih celih števil**)

**Opomba:** Pojme, kot so **generator kolobarja**, **končno generiran kolobar**, ... definiramo enako kot za grupo.

### 1.8.3 Generatorji vektorskih prostorov

**Definicija 39:** Naj bo  $\mathcal{V}$  vektorski prostor nad  $\mathcal{F}$ . Vsakemu vektorju  $v$  oblike

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n; \lambda_i \in \mathcal{F} \wedge v_i \in \mathcal{V} \quad (36)$$

pravimo **linearna kombinacija** vektorjev  $v_1, v_2, \dots, v_n$ .

**Definicija 40:** Naj bo  $\emptyset \neq \mathcal{X} \subseteq \mathcal{V}$ . Podprostor generiran z  $\mathcal{X}$ , torej podprostor, ki  $\mathcal{X}$  vsebuje in je vsebovan v vsakem podprostoru, ki vsebuje  $\mathcal{X}$  je množica  $\mathcal{L}(\mathcal{X})$ , vseh linearnih kombinacij vektorjev iz  $\mathcal{X}$ ,  $\mathcal{L}(\mathcal{X})$  imenujemo **linearna lupina množice  $\mathcal{X}$** .

**Definicija 41:** Naj bo  $\mathcal{X}$  množica generatorjev za  $\mathcal{V}$  tedaj  $\mathcal{X}$  imenujemo **ogrodje**  $\mathcal{V}$ , velja še  $\mathcal{L}(\mathcal{X}) = \mathcal{V}$ .

**Opomba:** Posebnost vektorskega prostora je v tem, da imamo pojem **linearne neodvisnosti**, preko katerega vpeljemo pojem **baze** vektorskega prostora.

#### 1.8.4 Generatorji algeber

**Definicija 42:** Naj bo  $\mathcal{A}$  algebra na  $\mathcal{F}$ , naj bo  $\emptyset \neq \mathcal{X} \subseteq \mathcal{A}$ . **Podalgebra generirana z  $\mathcal{X}$**  je množica, ki sestoji iz elementov  $x$  oblike

$$x = \lambda_1 x_{11} x_{12} \dots x_{1n_1} + \dots + \lambda_r x_{r1} x_{rn_r}; \lambda_i \in \mathcal{F} \wedge x_i \in \mathcal{X} \cup \{1\} \quad (37)$$

**Primer:**

1.  $\mathcal{A} = \mathcal{M}_2(\mathbb{R})$

- Podalgebra generirana z:

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

je algebra diagonalnih matrik:

$$\begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}; \lambda, \mu \in \mathbb{R}$$

- Podalgebra generirana z:

$$e_{11} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, e_{22} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

pa je celotna algebra  $\mathcal{M}_2(\mathbb{R})$ . (torej je generirana samo z dvema elementoma!)

Ker velja:

$e_{12}e_{21} = e_{11}$  in  $e_{21}e_{12} = e_{22}$ , vidimo, da  $e_{12}, e_{21}$  generirata algebro  $\mathcal{M}_2(\mathbb{R})$ .  $\{e_{12}, e_{21}, e_{11}, e_{22}\}$  je baza algebre  $\mathcal{M}_2(\mathbb{R})$

**Opomba:**

Za primerjavo: podkolobar  $\mathcal{M}_2(\mathbb{R})$  generiran z  $e_{12}$  in  $e_{21}$  pa je

$$\mathcal{M}_2(\mathbb{Z}) = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}; u_{ij} \in \mathbb{Z}$$