

Skripta za algebro 2

Filip Koprivec

17. 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

1	Osnovne algebrske strukture	3
1.1	Binarne operacije	3
1.2	Polgrupe in monoidi	5
1.3	Grupe	8
1.4	Kolobarji	10
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
1.8.5	Generatorji podpolji	22
1.9	Direktni produkti in vsote	22
1.9.1	Direktni produkti grup	22
1.9.2	Direktni produkti kolobarjev	23
1.9.3	Direktna vsota vektorskih prostorov	23
1.9.4	Direktni produkt algebr	24
2	Primeri grup in kolobarjev	24
2.1	Cela števila	24
2.2	Grupa in kolobar ostankov	28

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

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

Če za poljubna dva elementa iz \mathcal{S} velja

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

pravimo, da je operacija \circ komutativna. Enakost 3 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 operacijo 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 **nevtralni element**, če velja

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

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:

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

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

$$\forall x \in \mathcal{S}. x \circ e'' = x \quad (6)$$

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

$$\forall t, t' \in \mathcal{T}. t \circ t' \in \mathcal{T} \quad (7)$$

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

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 oklepaje 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:

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

Po I.P. ($w \circ v$ ima $n - 1$ elementov): $x = x_1 \circ (x_2 \circ \dots \circ x_n)$ □

Zato lahko oklepaje izpuščamo in pišemo kar: $x_1 \circ x_2 \circ \dots \circ x_n$

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

$$x^n := \underbrace{x \circ x \circ \dots \circ x}_{n \text{ elementov}} \quad (8)$$

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 monoida \mathcal{S} je inverz elementa x Če velja:*

$$x \circ y = y \circ x = e \quad (9)$$

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

$$x \circ x^{-1} = x^{-1} \circ x = e \quad (10)$$

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

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:

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

Opomba: Seveda velja za n elementov

$$(x_1 \circ x_2 \circ \dots \circ x_n)^{-1} = x_n^{-1} \circ \dots \circ x_2^{-1} \circ x_1^{-1} \quad (11)$$

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:

$$n \in \mathbb{N}. x^{-n} := (x^n)^{-1} = (x^{-1})^n \quad (12)$$

Definicija 17:

$$x^0 := e \quad (13)$$

Tako kadar je x **obrnljiv** veljata enačbi

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

$$\forall n, m \in \mathbb{Z}. (x^n)^m = x^{nm} \quad (15)$$

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

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

In tudi

$$y \circ x = z \circ x \implies y = z \quad (17)$$

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 imenovala kar množenje. Prav tako bomo izpuščali operator, ko bo le mogoče in pisali kar xy .

Tako xy imenujemo 'produkt' x in y , nevtralni 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 vsaka dva elementa komutirata, 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: \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. $(F(\mathcal{X}), \circ)$: $(F(\mathcal{X}), \circ)^* = \{f : \mathcal{X} \rightarrow \mathcal{X} | f \text{ je bijekcija}\}$

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

$$\text{Sim}(\mathcal{X}) := \{f : \mathcal{X} \rightarrow \mathcal{X} | f \text{ je bijekcija}\} \quad (18)$$

Njene elemente (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

$$\mathcal{S}_n := \text{Sim}(\{1, 2, \dots, n\}) \quad (19)$$

Včasih bomo operacije na grupah vendarle označevali s + ('seštevanje'). Taki grupi bomo rekli **aditivna grupa**. Nevtralni element bomo označevali z 0, inverzni element pa bomo imenovali '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 vpeljali odštevanje. Prav tako bom namesto x^n pisali nx .

Primer takih grup so Ablove 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

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

$$\forall x, y, z \in \mathcal{K}. (x + y)z = xz + yz \quad (21)$$

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.

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

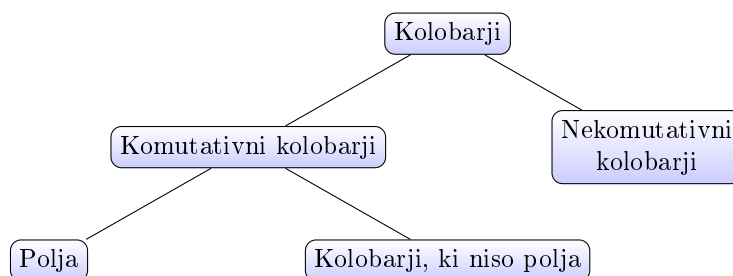
□

(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 (3).



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,

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

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 delitelj ničā**, 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 delitelj ničā**, če obstaja tak $y \neq 0, y \in \mathcal{K}$, da velja: $yx = 0$.

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

Opomba:

$$\mathcal{K} \text{ ima leve delitelje ničā} \iff \mathcal{K} \text{ ima delitelje ničā} \quad (22)$$

Dokaz.

\implies : Obstajata taka $y \neq 0, x \neq 0$, da je $xy = 0$. Imamo dve možnosti

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

\impliedby : Očitno. □

V Kolobarju brez deliteljev ničā velja:

$$\forall x, y \in \mathcal{K}. xy = 0 \implies x = 0 \vee y = 0 \quad (23)$$

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(al desni) delitelj ničā. Obsegi so zato kolobarji brez deliteljev ničā.

Dokaz. x je obrnljiv: $xy = 0$

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

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

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

V_3 : Velja distributivnost v skalarnem faktorju

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

V_4 : Velja zakon homogenosti

$$\forall \lambda, \mu \in \mathcal{F}. \forall v \in \mathcal{V}. (\lambda\mu)v = \lambda(\mu v) \quad (26)$$

V_5 : Enota

$$\forall v \in \mathcal{V}. 1v = v \quad (27)$$

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:

Seštevanje

$$(u_1, u_2, \dots, u_n) + (v_1, v_2, \dots, v_n) \mapsto (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n) \quad (28)$$

Množenje s skalarjem

$$\lambda(u_1, u_2, \dots, u_n) \mapsto (\lambda u_1, \lambda u_2, \dots, \lambda u_n) \quad (29)$$

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{R} to 2-dimenzionalen, nad \mathbb{C} 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. Torej 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:

$$(x_1, x_2, \dots, x_n)(y_1, y_2, \dots, y_n) \mapsto (x_1y_1, x_2y_2, \dots, x_ny_n) \quad (30)$$

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

$$\lambda(a_{ij}) = (\lambda a_{ij}) \quad (31)$$

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 poudarku.

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 neprazno 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) :

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

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

(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:

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

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

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

$$\exists c \in \mathcal{G}. b = cac^{-1} \quad (32)$$

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

Trditev 12: Če je $c \in \mathcal{H} \leq \mathcal{G}$, je

$$c\mathcal{H}c^{-1} := \{chc^{-1} | h \in \mathcal{H}\} \quad (33)$$

konjugirana podgrupa podgrupe \mathcal{H} .

Dokaz.

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

□

Opomba: Pojem konjugiranih podgrup ima smisel v nekomutativnih grupah

1.7.2 Podkolobarji

Definicija 32: Podmnožica \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

$$1 \in \mathcal{L} \wedge \forall x, y \in \mathcal{L}. x - y \in \mathcal{L} \quad (34)$$

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 trditev (11) in (ii) pogoj zamenjali z (iii) □

Primer:

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

1.7.3 Podprostori

Definicija 33: 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

□

Primer:

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

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

1.7.4 Podalgebre

Definicija 34: 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:

$$1 \in \mathcal{B} \wedge \forall x, y \in \mathcal{B}. \forall \lambda \in \mathcal{F}. \underbrace{x + y, \lambda x, xy}_{\text{podprostor}} \in \mathcal{B} \quad (35)$$

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 35: Podmnožica \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

$$\forall x, y \in \mathcal{F}. xy, x - y \in \mathcal{F} \wedge 0 \neq x \in \mathcal{F}. x^{-1} \in \mathcal{F} \quad (36)$$

Dokaz. Podobno kot prej

□

Trditev 17: $\mathcal{F} = \{0\} \iff 1 = 0$

Dokaz.

\implies

$\forall x \in \mathcal{F}. 0x = x$ torej je 0 nevtralni element

\impliedby

$\forall x \in \mathcal{F}. x = 1x = 0x = 0$ vsi elementi so ničelni

□

Definicija 36: 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: $(1, 1, 0), (0, 1, 0), (0, 0, 1)$.

Vektorja $(1, 0, 0), (0, 1, 0)$ 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: $\langle \mathbb{N} \rangle = \mathbb{Q}^+$
2. $\langle 2, 3 \rangle = \{2^i 3^j \mid i, j \in \mathbb{Z}\}$

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 tudi 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 37: 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 38: Naj bo \mathcal{V} vektorski prostor nad \mathcal{F} . Vsakemu vektorju v oblike

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n; \lambda_i \in \mathcal{F} \wedge v_i \in \mathcal{V} \quad (37)$$

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

Definicija 39: 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 40: 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 41: 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

$$x = \lambda_1 x_{11} x_{12} \dots x_{1n_1} + \dots + \lambda_r x_{r1} x_{rn_r}; \lambda_i \in \mathcal{F} \wedge x_i \in \mathcal{X} \cup \{1\} \quad (38)$$

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

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

1.8.5 Generatorji podpolji

Definicija 42: Naj bo $\mathcal{X} \neq \emptyset$ podmnožica polja \mathcal{F} . **Podpolje generirano z \mathcal{X}** je množica

$$\{uv^{-1} | u, v \in \mathcal{X} \wedge v \neq 0\} \quad (39)$$

Opomba: Podkolobar $\overline{\mathcal{X}}$ generiran z \mathcal{X} ni nujno polje.

Očitno vsako podpolje, ki \mathcal{X} vsebuje, vsebuje tudi podpolje generirano z \mathcal{X} , toda zakaj ta množica je podpolje?

Pomembno je dokazati, da je podgrupa za seštevaje (zaprtost za množenje, inverz, in 1 so očitne) **Trditev 18:**

$$uv^{-1} - wz^{-1} = \underbrace{(uz - vw)}_{\in \overline{\mathcal{X}}} \underbrace{(vz)^{-1}}_{\in \overline{\mathcal{X}}}$$

Primer:

$\mathcal{F} = \mathbb{C}$

1. $\mathcal{X} = \{1\}$ Podpolje generirano z \mathcal{X} je \mathbb{Q} , medtem, ko $\overline{\mathcal{X}} = \mathbb{Z}$ Vsako podpolje \mathbb{C} vsebuje 1 in zato vsako podpolje vsebuje tudi \mathbb{Q}
2. $\mathcal{X} = i$: $\overline{\mathcal{X}} = \mathbb{Z}[i]$ (Gaussova cela števila), podpolje generirano z \mathcal{X} je

$$\mathbb{Q}[i] := \{p + qi | p, q \in \mathbb{Q}\} \quad (40)$$

Opomba: Med drugim smo pokazali, da najmanjša podgrupa (podkolobar ...), ki vsebuje dano množico res obstaja. Zadevo pa lahko dokažemo tudi hitreje, tako da vzamemo presek vseh podstruktur, ki to strukturo vsebujejo.

1.9 Direktni produkti in vsote

Iz danih struktur lahko konstruiramo nove na različne načine.

1.9.1 Direktni produkti grup

Definicija 43: Naj bodo $\mathcal{G}_1, \dots, \mathcal{G}_n$ grupe. Grupi

$$\mathcal{G} := \mathcal{G}_1 \times \dots \times \mathcal{G}_n$$

ki jo dobimo kot kartezični produkt teh grup, pravimo (**zunanji**) **direktni produkt**.

Opomba: Da je ta struktura res grupa, operacijo definiramo po komponentah. Brez težav se prepričamo, da je to res grupa.

$$(x_1, x_2, \dots, x_n) * (y_1, y_2, \dots, y_n) := (x_1 y_1, x_2 y_2, \dots, x_n y_n)$$

Očitno:

$$1 = (1, 1, \dots, 1)$$

$$(x_1, x_2, \dots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \dots, x_n^{-1})$$

Opomba: Če so vse grupe v produktu aditivne, potem namesto $\mathcal{G} := \mathcal{G}_1 \times \dots \times \mathcal{G}_n$ pišemo $\mathcal{G} := \mathcal{G}_1 \oplus \dots \oplus \mathcal{G}_n$ in govorimo o **(zunanji) direktni vsoti grup**.

1.9.2 Direktni produkti kolobarjev

Definicija 44: Naj bodo $\mathcal{K}_1, \dots, \mathcal{K}_n$ kolobarji. Kolobarju

$$\mathcal{K} := \mathcal{K}_1 \times \dots \times \mathcal{K}_n$$

ki ga dobimo kot kartezični produkt teh kolobarjev pravimo **(zunanji) direktni produkt**.

Opomba: Da je ta struktura res kolobar operacijo definiramo po komponentah. Brez težav se prepričamo da je to res kolobar.

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) := (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

$$(x_1, x_2, \dots, x_n) * (y_1, y_2, \dots, y_n) := (x_1 y_1, x_2 y_2, \dots, x_n y_n)$$

Opomba: Temu rečemo tudi **direktna (zunanja) vsota kolobarjev**.

1.9.3 Direktna vsota vektorskih prostorov

Definicija 45: Naj bodo $\mathcal{V}_1, \dots, \mathcal{V}_n$ vektorski prostori nad \mathcal{F} . Vektorskemu prostoru

$$\mathcal{V} := \mathcal{V}_1 \times \dots \times \mathcal{V}_n$$

ki ga dobimo kot kartezični produkt teh vektorskih prostorov pravimo **direktna vsota** prostorov $\mathcal{V}_1, \dots, \mathcal{V}_n$ in ga označujemo kot $\mathcal{V}_1 \oplus \dots \oplus \mathcal{V}_n$.

Opomba: Da je ta struktura res vektorski prostor, operacijo definiramo po komponentah. Brez težav se prepričamo, da je to res vektorski prostor.

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) := (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

$$\lambda(x_1, x_2, \dots, x_n) := (\lambda x_1, \lambda x_2, \dots, \lambda x_n)$$

Opomba: \mathcal{F}^n je direktna vsota n -kopij enorazsežnega prostora \mathcal{F}

1.9.4 Direktni produkt algebr

Definicija 46: Naj bodo $\mathcal{A}_1, \dots, \mathcal{A}_n$ algebre nad \mathcal{F} . Algebri

$$\mathcal{A} := \mathcal{A}_1 \times \dots \times \mathcal{A}_n$$

ki jo dobimo kot kartezični produkt teh algebr, pravimo **direktni produkt**.

Opomba: Da je ta struktura res algebra, operacijo definiramo po komponentah. Brez težav se prepričamo, da je to res algebra.

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) := (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

$$(x_1, x_2, \dots, x_n) * (y_1, y_2, \dots, y_n) := (x_1 y_1, x_2 y_2, \dots, x_n y_n)$$

$$\lambda(x_1, x_2, \dots, x_n) := (\lambda x_1, \lambda x_2, \dots, \lambda x_n)$$

Opomba: Lahko govorimo tudi o direktnem produktu (direktni vsoti) neskončne družine struktur

Primer:

1. \mathbb{R} glejmo kot algebro nad \mathbb{R} . Direktni produkt števno kopij z operacijami po komponentah je algebra $\mathbb{R} \times \mathbb{R} \times \dots$.

Operacije po komponentah točno sovpadajo z operacijami po komponentah za zaporedja. To je torej algebra realnih zaporedij.

2. Naj bodo $\mathcal{F}_1, \dots, \mathcal{F}_n$ polja nad ne nujno istimi kolobarji. Definiramo operacije po komponentah in opazimo, da za $n \geq 2$ ima direktni produkt (polj ali kolobarjev) delitelje nič.

$$(x_1, 0, \dots, 0) * (0, x_2, x_3, \dots, x_n) = 0$$

2 Primeri grup in kolobarjev

2.1 Cela števila

Ker so \mathbb{N} zgolj polgrupa za $+$, imamo v algebri raje \mathbb{Z} .

Definicija 47: Množica \mathcal{A} zadostuje **načelu dobre urejenosti**, če vsaka neprazna podmnožica množice \mathcal{A} , vsebuje najmanjši element.

Opomba: Je ekvivalentno:

Če v množici \mathcal{A} , ki ustreza načelu dobre urejenosti, množica $\mathcal{B} \subseteq \mathcal{A}$ nima najmanjšega elementa, potem velja $\mathcal{B} = \emptyset$

Trditev 19: \mathbb{N} ustreza načelu dobre urejenosti.

Dokaz.

\mathbb{Z} indukcijo na n : $n = 1$: $1 \notin \mathbb{N}$

$n \implies n + 1$: $1 \notin \mathbb{N}, 2 \notin \mathbb{N}, \dots, n \notin \mathbb{N}$



$n + 1 \notin \mathbb{N} \quad \square$

Ker nima najmanjšega elementa

Po indukciji isto velja tudi za $\mathbb{N} \cup \{0\}$, $\mathbb{N} \cup \{0, -1\}$, $\mathbb{N} \cup \{0, -1, -2\} \dots$

Torej: Vsaka neprazna navzdol omejena podmnožica \mathbb{Z} vsebuje najmanjše število.

Analogno: Vsaka neprazna navzgor omejena podmnožica \mathbb{Z} vsebuje največje število.

Izrek 1: Osnovni izrek o deljenju

Za poljubna $m, n \in \mathbb{Z}$ obstajata taki števili $p, q \in \mathbb{Z}$, da velja:

$$m = qn + r \wedge 0 \leq r < n$$

Dokaz. Vpeljimo

$$\mathcal{S}_{(n,m)} := \{k \in \mathbb{Z} | kn \leq m\}$$

Če $\mathcal{S} = \emptyset \checkmark \mathcal{S}$ je navzgor omejena, ker lahko najdemo tako število k , tako da je $kn > m$ in to velja tudi za vsako od k večje število, zato \mathcal{S} vsebuje največje število q . Tako velja

$$qn \leq m \quad // \text{ saj } q \in \mathcal{S}$$

$$(q+1)n > m \quad // \text{ saj } (q+1) \notin \mathcal{S}$$

$$r := m - qn \leq 0$$

$$qn + n > m \quad // \text{ torej } n > r$$

□

Opomba: r imenujemo **ostanek** pri deljenju m z n .

$(\mathbb{Z}, +)$ Primeri podgrup

Primer:

1. Trivialni primeri: $\{0\}$, \mathbb{Z}

2. $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\} \quad // \quad n \in \mathbb{Z}$ je podgrupa za seštevanje

Opomba: Ker $n\mathbb{Z} = (-n)\mathbb{Z}$, praviloma izberemo $n \in \mathbb{N}$

Izrek 2:

Podmnožica \mathcal{H} množice \mathbb{Z} je podgrupa za seštevanje natanko tedaj, ko obstaja tak $n \geq 0$, da je $\mathcal{H} = n\mathbb{Z}$.

Dokaz.

\implies

\mathcal{H} je podgrupa \mathbb{Z}

$$\mathcal{H} = \{0\} \implies n = 0$$

$\mathcal{H} \neq \{0\}$, $k \in \mathcal{H} \iff -k \in \mathcal{H} \implies \mathcal{H} \cap \mathbb{N} \neq \emptyset$ Po načelu dobre urejenosti obstaja najmanjše število v \mathcal{H} , recimo mu n .

$$n \in \mathcal{H} \implies n\mathbb{Z} \subseteq \mathcal{H} \quad // \text{ ker je podgrupa}$$

$$\text{Vzemimo sedaj: } m \in \mathcal{H} \implies \underbrace{r}_{\in \mathcal{H}} = \underbrace{m}_{\in \mathcal{H}} - \underbrace{qn}_{\in \mathcal{H}}$$

In dobimo $r = 0$, ker iz $1 \leq r \leq n - 1$ sledi, da \mathcal{H} vsebuje od n manjše število, kar je protislovje.

Torej $m = qn \in \mathcal{H}$

\Longleftarrow

$n\mathbb{Z}$ je podgrupa $\implies (nk - nl) = n(k - l) \in n\mathbb{Z}$

□

Definicija 48: Naj bosta $m, k \in \mathbb{Z}$. Rečemo, da k **deli** m (pišemo tudi $k|m$), če obstaja tak $q \in \mathbb{Z}$, da velja $m = qk$.

Opomba: Rečemo tudi m **je deljiv** s k ali k je **delitelj** m . Prav tako uporabljamo $k \nmid m$, da povemo, da k **ne deli** m .

Definicija 49: Naj bosta $m, n \in \mathbb{Z}$, naravno število d je **največji skupni delitelj** m in n , če velja:

1. $d|m \wedge d|n$

2. $\forall d' \in \mathbb{N}. d'|m \wedge d'|n \implies d'|d$ // Vsak drugi skupni delitelj deli največji skupni delitelj

Opomba: Če sta \mathcal{H} in \mathcal{K} podgrupi aditivne grupe \mathcal{G} , je podgrupa tudi

$$\mathcal{H} + \mathcal{K} := \{h + k | h \in \mathcal{H}, k \in \mathcal{K}\}$$

Očitno $\mathcal{H}, \mathcal{K} \subseteq \mathcal{H} + \mathcal{K}$, to je tudi najmanjša podgrupa, ki vsebuje obe podgrupi.

Dokaz.

$$(h + k) - (h' + k') = (h - h') + (k - k') \in \mathcal{H} + \mathcal{K}$$

□

Izrek 3:

Za vsak par celih števil m, n , od katerih vsaj eno ni enako 0, obstaja največji skupni delitelj d , ki ga označimo z $\gcd(m, n)$, in je oblike $d = mx + ny$ za neka $x, y \in \mathbb{Z}$.

Dokaz. $m\mathbb{Z}$ in $n\mathbb{Z}$ sta podgrupi \mathbb{Z} , zato je tudi njuna vsota podgrupa. Po opombi zgoraj obstaja tak $d \in \mathbb{N}$, da velja $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ in ker eno izmed m, n ni 0 velja $d \neq 0$. Torej velja

$d = mx + ny$ za neka $x, y \in \mathbb{Z}$ Torej velja:

$d\mathbb{Z} \supseteq n\mathbb{Z} \implies m \in m\mathbb{Z} \subseteq d\mathbb{Z} \implies d|m$ in podobno za n . Dokazali smo, da je d skupni delitelj števil m in n . Potrebno je še dokazati, da je največji.

Naj velja $c|m$ in $c|n$, potem $m = cz$ in $n = cw$.

Vemo da $d = mx + ny = c(zx + wy) \implies c|d$

□

Opomba: Dokaz za to se pojavi že v Evklidovi knjigi Elementi, približno 300 let pr. Kr.

Definicija 50: Števili $m, n \in \mathbb{Z}$, ne obe enaki 0, sta si **tuji**, če je njun največji skupni delitelj enak 1.

Posledica: Celi števili m, n sta si tuji natanko tedaj, ko obstajata taki celi števili x, y , ki zadostita enačbi:

$$1 = mx + ny$$

Dokaz.

\Rightarrow

Sledi iz izreka o obstoju največjega skupnega delitelja (3)

\Leftarrow

$c|m \wedge c|n \Rightarrow c|1$ Torej je njun največji skupni delitelj 1 in sta si tuji. \square

Opomba: Splošneje lahko definiramo največji skupni delitelj števil $n_1, n_2, \dots, n_k \in \mathbb{Z}$ na enak način ter njegovo eksistenco dokažemo na enak način ($d = n_1x_1 + n_2x_2 + \dots + n_kx_k$). To seveda ne pomeni, da so si števila paroma tuja (2, 3, 6 so si tuja, ne pa tudi paroma tuja).

Definicija 51: Naravno število p je **praštevilo**, če sta 1 in p edini praštevili, ki ga delita in velja $p \neq 1$.

Lema 1. Naj bo p praštevilo in $mn \in \mathbb{Z}$, tedaj velja:

$$p|mn \Rightarrow p|m \vee p|n$$

Dokaz. Predpostavimo, da $p \nmid m$.

$$\gcd(p, m) = 1 \Rightarrow 1 = px + my \Rightarrow n = pxn + \underbrace{mn}_{pz}y = p(xn + zy)$$

Podobno za drugo možnost. \square

Opomba: Tudi ta dokaz je bil poznan že Evklidu.

Izrek 4: Osnovni izrek aritmetike

Vsako naravno število $n \geq 2$ lahko napišemo kot produkt praštevil. Ta zapis je do vrstnega reda faktorjev natančno enoličen.

Dokaz. Indukcija na n :

$$n = 2 \checkmark$$

$$n - 1 \Rightarrow n$$

Če je n praštevilo je dokaz zaključen. Če ni, ima vsaj dva delitelja ki nista 1 ali p (lahko sta enaka).

$$n = kl; \quad l, k < n$$

Po indukcijski predpostavki sta l in k produkta praštevil, torej je tudi p produkt praštevil.

In še edinost zapisa:

$$n = p_1 * p_2 * \dots * p_r = q_1 * q_2 * \dots * q_s, \text{ produkt samih praštevil}$$

$p_1|q_1 * q_2 * \dots * q_s$ torej po lemi (1) deli natančno enega izmed faktorjev q_i . Brez škode za splošnost: $p_1|q_1 \Rightarrow p_1 = q_1$ Krajšamo s p_1 in nadaljujemo

ker sta praštevili

dokler ne pridemo do $1 = 1$.

Če pa imamo $s > r \Rightarrow q_{r+1} \dots q_s = 1$, kar pa je protislovje. \square

Izrek 5:

Množica praštevil je neskončna.

Dokaz. Predpostavimo, da jih je končno, torej da so p_1, p_2, \dots, p_n vsa praštevila. Teda $p_1 * p_2 * \dots * p_n + 1$ ni praštevilo in je zato gotovo deljivo z nekim praštevilom p_i .

$$p_1 * p_2 * \dots * p_n + 1 = k * p_i \implies p_i(k - p_1 * p_2 * \dots * p_{i-1} * p_{i+1} * \dots * p_n) = 1, \text{ protislovje.} \quad \square$$

2.2 Grupa in kolobar ostankov

Definicija 52: Celi števili a in b sta **kongruenti modulo n** , če

$$n \mid (a - b)$$

Primer:

1. $13 \equiv 1 \pmod{12}$, $21 \equiv -3 \pmod{12}$
2. $a \equiv b \pmod{1}$

Lema 2.

$$a \equiv a' \pmod{n} \wedge b \equiv b' \pmod{n} \implies a + b \equiv a' + b' \pmod{n} \wedge ab \equiv a'b' \pmod{n}$$

Dokaz.

$$(a + b) - (a' + b') = \underbrace{(a - a') + (b - b')}_{\text{sta si kongruentna}}$$

$$(ab) - (a'b') = \underbrace{b(a - a') + a(b - b')}_{\text{sta si kongruentna}}$$

\square

Trditev 20: Relacija $a \equiv b \pmod{n}$ je ekvivalenčna:

Dokaz.

Refleksivna: \checkmark

Simetrična: \checkmark

Tranzitivna:

$$a \equiv b \pmod{n} \text{ in } b \equiv c \pmod{n} \implies c - a = \underbrace{(c - b) + (b - a)}_{\text{sta si kongruentna}} \quad \square$$

Ker je relacija ekvivalenčna, lahko vpeljemo ekvivalenčne razrede. Z $[a]$ označimo ekvivalenčni razred, ki mu pripada a .

Definicija 53: Ekvivalenčni razredi kongruentni z n so:

$$\underbrace{[0]}, \quad \underbrace{[1]}, \quad \dots, [n-1]$$

števila deljiva z n ostane pri deljenju z n je 1

in jih označimo z \mathbb{Z}_n .

Potrebno je preveriti še dobro definiranost operacij.

Trditev 21: Če v množici \mathbb{Z}_n vpeljemo seštevanje:

$$[a] + [b] := [a + b] \quad (41)$$

Postane \mathbb{Z}_n Abelova grupa.

Dokaz. Dobra definiranost seštevanja:

$$\underbrace{[a] = [a']}_{a \equiv a' \pmod{n}} \wedge \underbrace{[b] = [b']}_{b \equiv b' \pmod{n}} \implies [a + b] = [a' + b']$$

Drugi del izjave pa je ekvivalenten: $a + b \equiv a' + b' \pmod{n}$, kar sledi iz leme (2).

Preverimo še asociativnost:

$$([a] + [b]) + [c] = [a + b] + [c] \quad \underbrace{=}_{\text{po definiciji}} \underbrace{[(a + b) + c] = [a + (b + c)] = \dots = [a] + ([b] + [c])}_{\text{asociativnost celih števil}}$$

Nevtralni element:

$$0 = [0]$$

Nasprotni element:

$$-[a] = [-a]$$

Komutativnost:

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

□