

Skripta za algebro 2

Filip Koprivec

14. marec 2016

*“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	4
1.1	Binarne operacije	4
1.2	Polgrupe in monoidi	6
1.3	Grupe	9
1.4	Kolobarji	11
1.5	Vektorski prostori	14
1.6	Algebre	15
1.7	Podgrupe, podkolobarji in druge podstrukture	16
1.7.1	Podgrupe	16
1.7.2	Podkolobarji	18
1.7.3	Podprostori	18
1.7.4	Podalgebre	19
1.7.5	Podpolje	19
1.7.6	Logične operacije nad (pod)strukturami	20
1.8	Generatorji	20
1.8.1	Generatorji grup	20
1.8.2	Generatorji kolobarja	21
1.8.3	Generatorji vektorskih prostorov	21
1.8.4	Generatorji algeber	22
1.8.5	Generatorji podpolj	23
1.9	Direktni produkti in vsote	23
1.9.1	Direktni produkti grup	23
1.9.2	Direktni produkti kolobarjev	24
1.9.3	Direktna vsota vektorskih prostorov	24
1.9.4	Direktni produkt algebr	25
2	Primeri grup in kolobarjev	25
2.1	Cela števila	25
2.2	Grupa in kolobar ostankov	29
2.3	Obseg kvaternionov	31
2.4	Kolobar matrik	32
2.5	Kolobar funkcij	33
2.6	Kolobar polinomov ene spremenljivke	34
2.7	Kolobar polinomov več spremenljivk	37
2.8	Simetrična grupa	38
2.9	Diedrska grupa	38
2.10	Linearne grupe	40
3	Homomorfizmi in kvocientne strukture	42
3.1	Izomorfizmi grup, ciklične grupe	42
3.2	Izomorfnost vektorskih prostorov	44
3.3	Pojem homomorfizma	45
3.4	Primeri homomorfizmov	49
3.4.1	Primeri homomorfizmov grup	49
3.4.2	Primeri homomorfizmov kolobarjev in algeber	50
3.5	Cayleyev izrek in drugi izreki o vložitvah	51
3.5.1	Cayleyev izrek	51
3.5.2	Vložitev kolobarja v kolobar endomorfizmov	52

3.5.3	Vložitev algebre v algebro endomorfizmov vektorskega prostora	53
3.6	Vložitev celega kolobarja v polje	53
3.7	Karakteristika kolobarja in vložitev prapolja v polje	54
4	Kvocientne strukture	55
4.1	Odseki	55
4.2	Podgrupe edinke in kvocientne grupe	57
4.2.1	Definicija edinke in kvocientne grupe	57
4.2.2	Produkti podgrup	58
4.2.3	Podgrupe (edinke) kvocientne grupe	59
4.3	Ideali in kvocientni kolobarji	61
4.3.1	Definicija ideala in kvocientnega kolobarja	61
4.3.2	Izpustimo zaradi kolokvija	62
4.3.3	Izpustimo zaradi kolokvija	62
4.3.4	Izpustimo zaradi kolokvija	62
4.3.5	Kvocientni prostori in kvocientne algebre	62
4.4	Izrek o izomorfizmih	62

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.

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

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

$$e = f$$

□

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 $\mathcal{K} \neq \mathcal{S}$ 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:

$$y = (x_1 \circ w) \circ v = \underbrace{(x_1 \circ w)}_{= x_1 \circ (w \circ v)} \circ v$$

Asociativnost(1)

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 (\mathcal{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 \mathcal{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

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

Opomba: Poseben primer, kadar je x obrnljiv je tudi: $(x^n)^{-1} = (x^{-1})^n$ za $n \in \mathbb{N}$

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

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 delimo 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^* 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 $\text{Sim}(\mathcal{X})$ 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 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 \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.

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

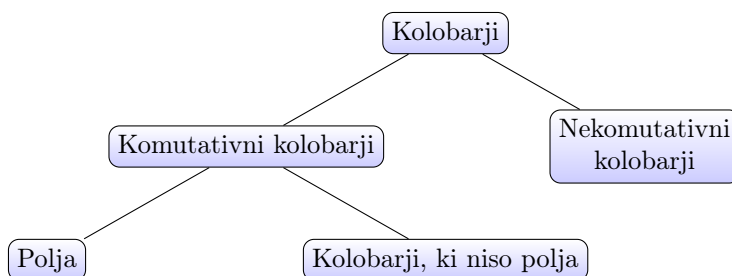
□

(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:

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

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

•

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

•

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

•

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

•

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

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:

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

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) :

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

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

(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. $k\mathbb{Z} = \{kn | n \in \mathbb{Z}\}$ // $k \in \mathbb{Z}$

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 Podprostorji

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

\longleftarrow

$\forall x \in \mathcal{F}. x = 1x = 0x = 0$ 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, podpolj) **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 podpolj

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

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

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 seštevanje (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

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

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 navzdol omejena 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 $\mathcal{S} = \emptyset \vee \mathcal{S}$ 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

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

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

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

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

□

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 .

$n \in \mathcal{H} \implies n\mathbb{Z} \subseteq \mathcal{H}$ // 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:

$d\mathbb{Z} \supseteq m\mathbb{Z} \implies m \in m\mathbb{Z} \subseteq d\mathbb{Z} \implies d|m$ 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 naravni števili, 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 zapišemo 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 .

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

$$\underbrace{[0]}_{\text{števila deljiva z } n}, \underbrace{[1]}_{\text{ostanek pri deljenji z } n \text{ je } 1}, \dots, [n-1]$$

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:

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

Nevtralni element:

$$0 = [0]$$

Nasprotni element:

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

Komutativnost:

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

□

Trditev 22: Aditivna grupa \mathbb{Z}_n postane **komutativen kolobar** \mathbb{Z}_n , če vpeljemo množenje s predpisom:

$$[a] * [b] := [a * b] \quad (42)$$

Dokaz.

Dobra definiranost sledi iz leme (2), asociativnost in distributivnost pokažemo kot pri seštevanju (se sklicujemo na te lastnosti v celih številih).

Enota: [1]

□

Opomba: Da oznake poenostavimo, namesto $[a]$, $0 \leq a \leq n - 1$ pišemo kar a , in tako $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$, pri čemer moramo obdržati v mislih, da to niso 'prava' cela števila.

Vsoto $a + b$ izračunamo tako, da pogledamo ostanek pri deljenju običajne vsote, podobno s produktom.

Primer:

1. V \mathbb{Z}_{12} : $3 + 4 = 7$ in $3 + 11 = 2 + 1 * 12 = 2$ ter $3 * 7 = 9$ in $3 * 8 = 0$.

\mathbb{Z}_n ima torej lahko delitelje nič. Očitno je to res vedno, kadar je n sestavljeno število. Če pa je n praštevilo, pa to ni res, še več, \mathbb{Z}_p je polje.

Definicija 54: Komutativen kolobar brez deliteljev nič se imenuje **cel kolobar**.

Primer:

$\underbrace{\mathbb{Z}}_{\text{cel kolobar, ki ni polje}}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Trditev 23: Končen cel kolobar je polje.

Dokaz. Naj bo \mathcal{K} končen cel kolobar. $0 \neq a \in \mathcal{K} \implies a$ je obrnljiv, naj bo $f: \mathcal{K} \rightarrow \mathcal{K}, f(x) = ax$. Potrebno je pokazati, da $1 \in \mathcal{Z}_f$. Dokazali bomo kar surjektivnost f , kar je v končnem polju ekvivalentno njeni injektivnosti.

$$ax = ax \implies x = y \text{ torej } a(x - y) = 0 \wedge a \neq 0 \implies x = y$$

cel kolobar

Komutativnost(eksistenca levega inverza \implies eksistenca desnega inverza \implies eksistenca inverza) □

Opomba: Izkaže se, da končnih nekomutativnih obsegov ni (dokaz je netrivialen).

Posledica: Za vsako praštevilo p je \mathbb{Z}_p polje.

Dokaz. Zadošča pokazati, da \mathbb{Z}_p nima deliteljev nič.

$a, b \in \mathbb{Z}_p, ab = 0$. Torej je v običajnem produktu ab večkratnik p , zato po lemi(1) p deli vsaj eno, ker pa $a, b \in \{0, 1, \dots, p-1\}$ velja $a = 0 \vee b = 0$ □

2.3 Obseg kvaternionov

Pojavi se naravno vprašanje, kako nadaljevati zaporedje:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset ?$$

Definicija 55:

Vzemimo 4-razsežen vektorski prostor nad \mathbb{R} , označimo ga s \mathbb{H} , njegovo bazo pa z $\{1, i, j, k\}$, tako dobimo značilni element

$$h := \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k, \lambda_i \in \mathbb{R} \quad (43)$$

Seštevanje in množenje s skalarji uvedemo enako kot pri normalnem 4 razsežnem vektorskem prostoru. Elemente \mathbb{H} imenujemo kvaternioni.

Opomba: \mathbb{H} izhaja iz priimka irskega matematika, fizika in astronoma Sira Williama Rowana Hamiltona, ki jih je vpeljal leta 1843.

Definicija 56: Množenje vpeljemo po kosih in sicer: 1 je enota za množenje, za druge pa velja:

$$i^2 = j^2 = k^2 = ijk = -1 \quad (44)$$

Iz teh sledi:

$$ij = -ji = k, jk = -kj = i, ki = -ik = j$$

Ko poznamo množenje baznih elementov, lahko množimo tudi vse ostale.

Trditev 24: S tako definiranim množenjem postane prostor \mathbb{H} ne samo kolobar, ampak tudi algebra nad \mathbb{R} .

Opomba: Preverimo po definiciji.

Definicija 57:

$$\bar{h} := \lambda_0 - \lambda_1 i - \lambda_2 j - \lambda_3 k \quad (45)$$

Trditev 25: Vsak neničelen kvaternion je obrnljiv in zanj velja

$$h^{-1} = \frac{\bar{h}}{h\bar{h}} \quad (46)$$

Dokaz. Izračunamo:

$$h\bar{h} = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2$$

$h \neq 0 \implies h\bar{h} \in \mathbb{R} - \{0\}$, zato je vsak neničelen kvaternion obrnljiv in velja

$$h^{-1} = \frac{\bar{h}}{h\bar{h}}$$

□

Opomba: \mathbb{H} je tako nekomutativen obseg.

Lahko pa uporabljamo tudi drugačen zapis: $\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k$ pišemo

$$(\lambda_0, \vec{u}), \vec{u} = \lambda_1 i + \lambda_2 j + \lambda_3 k$$

Množenje se tako glasi:

$$(\lambda_0, \vec{u}) * (\mu_0, \vec{v}) = (\lambda_0 \mu_0 - \vec{u} \cdot \vec{v}, \lambda_0 \vec{v} + \mu_0 \vec{u} + \vec{u} \times \vec{v}) \quad (47)$$

Opomba: Množica $\{\pm 1, \pm i, \pm j, \pm k\}$ je antikomutativna grupa za množenje z osmimi elementi, ki ji rečemo tudi **kvaternionjska grupa**.

2.4 Kolobar matrik

$\mathcal{M}_n(\mathbb{R})$ in $\mathcal{M}_n(\mathbb{C})$ sta kolobarja (celo algebri).

Trditev 26: Za vsak kolobar \mathcal{K} , je množica $\mathcal{M}_n(\mathcal{K})$ kolobar nad \mathcal{K} za običajno seštevanje in množenje matrik.

Dokaz. Preverimo po definiciji. \mathcal{K} je lahko celo nekomutativen. Enota in ničeln element sta enaka kot pri $\mathcal{M}_n(\mathbb{R})$. □

$\mathcal{M}_n(\mathcal{K})$ je nekomutativen za $n \geq 2$ (za $n = 1$ je kolobar matrik kar \mathcal{K})

Definicija 58: Element e kolobarja \mathcal{K} je **idempotent**, če zanj velja:

$$e^2 = e \quad (48)$$

Definicija 59: Element a kolobarja \mathcal{K} je **nilpotent**, če zanj velja:

$$\exists n \in \mathbb{N}. a^n = 0 \quad (49)$$

Primer:

1. Vsaka diagonalna matrika, z 0 in 1 na diagonalni, je idempotent.
2. Vsaka strogo zgoraj (ali spodaj) trikotna matrika je nilpotentna.

Trditev 27: Naj bo \mathcal{K} kolobar brez deliteljev nič in naj bo $e \in \mathcal{K}$ idempotent. Velja: $e = 1 \vee e = 0$.

$$\text{Dokaz. } e^2 = e \implies e(1 - e) = 0 \quad \underbrace{\implies}_{\text{ker nima deliteljev nič}} \quad e = 1 \vee e = 0 \quad \square$$

Trditev 28: e je idempotent $\iff 1 - e$ je idempotent

Dokaz. Račun. \square

Če je \mathcal{K} algebra na poljem \mathcal{F} , tudi kolobar $\mathcal{M}_n(\mathcal{K})$ potem postane algebra, če definiramo:

$$\lambda(a_{ij}) := (\lambda a_{ij})$$

Poseben primer: $\mathcal{M}_n(\mathcal{F})$ je algebra na \mathcal{F} , $\dim(\mathcal{M}_n(\mathcal{K})) = n^2$

2.5 Kolobar funkcij

Naj bo \mathcal{X} množica in naj bo $\mathcal{K} = \{f : \mathcal{X} \rightarrow \mathbb{R}\}$

\mathcal{K} postane kolobar, če definiramo običajno seštevanje in množenje funkcij:

$$(f + g)(x) := f(x) + g(x)$$

$$(f * g)(x) := f(x) * g(x)$$

Skupaj z enoto: $e(x) = 1$ in nasprotnim elementom: $(-f)(x) = -f(x)$

Primer:

1. Če je $\mathcal{X} = [a, b]$ ali \mathbb{R} , ipd., lahko govorimo o kolobarju $\mathcal{C}(x) = \{f : \mathcal{X} \rightarrow \mathbb{R} \mid f \text{ zvezna}\}$. Res je kolobar, saj so vsote in produkti zveznih funkcij spet zvezne funkcije. Ne samo to, je tudi algebra.

Poznamo več primerov kolobarjev funkcij:

- odvedljive funkcije
- omejene funkcije
- integrabilne funkcije
- polinomi (ta kolobar nima deliteljev nič).
- ...

Če v te kolobarje vpeljemo še množenje s skalarji:

$$(\lambda f)(x) = \lambda f(x) \quad (50)$$

postanejo vsi ti kolobarji tudi algebre.

Na podoben način vpeljemo tudi kolobar (algebro) zaporedij $\mathcal{X} = \mathbb{N} \rightarrow \mathcal{A}$, kjer so vse operacije definirane po komponentah (seštevanje, množenje, množenje s skalarjem). Ter različne podalgebre (konvergentna zaporedja, omejena zaporedja, ...).

Primer:

1. V algebri zveznih funkcij $(\mathcal{C}(\mathbb{R}))$ je podalgebra generirana z $id(x) = x$ ravno algebra polinomov.

2.6 Kolobar polinomov ene spremenljivke

Vajeni smo, da je polinom funkcija, v algebri pa polinom obravnavamo kot formalen izraz.

Definicija 60: Polinom p nad kolobarjem \mathcal{K} je izraz oblike:

$$p(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n, \quad a_n \neq 0 \quad (51)$$

Kjer so $a_i \in \mathcal{K}$ t.i. koeficienti tega polinoma.

- a_0 imenujemo **prosti (ali konstantni) člen**
- a_n (zadnji neničlen člen) imenujemo **vodilni člen (koeficient)**
- X imenujemo **spremenljivka**, a dejansko igra le formalno vlogo kot simbol

Alternativno lahko polinom definiramo tudi kot

Definicija 61: Polinom p nad kolobarjem \mathcal{K} je zaporedje elementov iz \mathcal{K} , ki je od nekega mesta naprej ničelno

$$p(n) : \mathbb{N} \rightarrow \mathcal{K}, \quad \exists n \in \mathbb{N}. \forall m \in \mathbb{N}. m > n \implies p(m) = 0 \quad (52)$$

Torej:

$$p = (a_0, a_1, \dots, a_n, 0, 0, \dots)$$

Vendar pa ta definicija ni udobna za množenje.

Da si prihranimo čas pri zapisu, spuščamo ničelne koeficiente:

$$0 + 3X + 0x^2 - 5X = 3X - 5X^3$$

Udoben pa se nam zdi tudi zapis

$$p(X) = \sum_{k \geq 0} a_k X^k$$

Kjer se zavedamo, da od nekje naprej so vsi a_k enaki 0.

Definicija 62: Seštevanje polinomov

$$\sum_{k \geq 0} a_k X^k + \sum_{k \geq 0} b_k X^k := \sum_{k \geq 0} (a_k + b_k) X^k \quad (53)$$

Definicija 63: Množenje polinomov

$$\left(\sum_{k \geq 0} a_k X^k \right) * \left(\sum_{k \geq 0} b_k X^k \right) := \sum_{k \geq 0} c_k X^k \quad (54)$$

Kjer velja $c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_n b_0$

Opomba: V ozadju smo uporabili $(a_i X^i) * (b_j X^j) = (a_i b_j) X^{i+j}$ in distributivnostni zakon.

Definicija 64: Stopnja polinoma

$$st(p(X)) = \min\{n \in \mathbb{N} \mid \forall m \in \mathbb{N}. m > n \implies a_m = 0\} \quad (55)$$

Torej indeks zadnjega neničelnega koeficienta.

Opomba: Polinom 0 nima definirane stopnje, a jo običajno definiramo kot -1 ali $-\infty$.

Množico polinomov, skupaj s tema dvema operacijama, bomo od sedaj naprej označevali s $K[x]$. $K[x]$ je kolobar. Preveriti to je rutinsko.

Definicija 65: Konstanten polinom je polinom stopnje 0 ali pa polinom 0.

Hitro opazimo nekatere lastnosti:

- Če \mathcal{K} nima deliteljev nič, jih prav tako nima tudi $\mathcal{K}[X]$ in velja:

$$st(f(X)g(X)) = st(f(X)) + st(g(X))$$

- \mathcal{K} je komutativen $\iff \mathcal{K}[X]$ je komutativen.

Definicija 66:

- **Linearni polinom** := polinom stopnje 1
- **Kvadratni polinom** := polinom stopnje 2
- **Kubični polinom** := polinom stopnje 3

Definicija 67: Vrednost polinoma $p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ v elementu $x \in \mathcal{K}$ je

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathcal{K} \quad (56)$$

Tako vsak polinom $F(X)$ porodi **polinomska funkcija**

$$x \mapsto f(x)$$

Opomba: Polinomska funkcija je seveda natanko določena s polinomom. Navrno pa se nam porodi vprašanje, ali je tudi polinom natančno določen s polinomska funkcijo.

Primer:

$$p(X) = X + X^2 \in \mathbb{Z}_2[X]$$

porodi funkcijo $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, za katero velja:

$$0 \mapsto 0$$

$$1 \mapsto 1^2 + 1^2 = 0$$

Enako funkcijo pa nam porodi tudi polinom 0. Očitno polinomska funkcija ne določa polinoma.

Opomba: V $\mathbb{R}[X]$, $\mathbb{C}[X]$ pa je razlika med polinomom in polinomska funkcijo zgolj formalna.

Če je $\mathcal{K} \subseteq \mathcal{L}$ (\mathcal{K} je podkolobar \mathcal{L}) in velja $f(x) \in \mathcal{K}[X]$, lahko izračunamo $f(x)$ tudi za $x \in \mathcal{L}$.

Definicija 68: Ničla polinoma

$x \in \mathcal{K}$ je **ničla (koren)** polinoma $f(X)$, če velja $f(x) = 0$.

Opomba: Polinom nima nujno ničel, recimo $X^2 + 1 \in \mathbb{R}[X]$ nima ničel v \mathbb{R} , jih pa ima v \mathbb{C} .

Če je \mathcal{K} algebra nad \mathcal{F} , tudi $\mathcal{K}[X]$ postane algebra nad \mathcal{F} . če definiramo množenje s skalarjem.

Definicija 69:

$$(\lambda f)(X) := \lambda a_0 + \lambda a_1X + \lambda a_2X^2 + \cdots + \lambda a_nX^n \quad (57)$$

Opomba: Če si še enkrat pogledamo definicijo množenja polinomov (54) in pozabimo na pogoj, da so od nekje naprej vsi členi enaki 0, potem govorimo o **kolobarju formalnih potenčnih vrst**, ki ga označimo s

$$\mathcal{K}[[X]]^k$$

2.7 Kolobar polinomov več spremenljivk

Preprost primer polinoma več spremenljivk:

$$f(X, Y) = 2X^4Y^2 - 3XY^8 + 7X + 3$$

Zgornji primer je sestavljen iz 4-ih členov, ki jih imenujemo **monomi**, s stopnjami: 6, 9, 1, 0

Stopnja polinoma pa je največja stopnja monomov, torej $st(f(X, Y)) = 9$

Definicija 70: Kolobar polinomov dveh spremenljivk je

$$(\mathcal{K}[X])[Y]$$

in ga označimo kot $\mathcal{K}[X, Y]$.

Elementi $\mathcal{K}[X, Y]$ so torej :

$$\sum_{l \geq 0} \left(\sum_{k \geq 0} a_k X^k \right) Y^l$$

Po dogovoru oklepaje izpuščamo in pišemo kar

$$\sum_{l \geq 0} \sum_{k \geq 0} a_{kl} X^k Y^l, \quad a_{kl} \in \mathcal{K}$$

Opomba: Ker je kolobar komutativen, je vseeno v kakšnem vrstnem redu definiramo polinom $((\mathcal{K}[X])[Y])$ je vsebinsko enak $(\mathcal{K}[Y])[X]$.

Opomba: Induktivno definiramo tudi polinom n spremenljivk

$$\mathcal{K}[X_1, X_2, \dots, X_n] := (\mathcal{K}[X_1, X_2, \dots, X_{n-1}])[X_n]$$

Polinomi z več spremenljivkami se študirajo v algebrski geometriji.

Primer:

1.

$$X_1^2 + X_2^2 + X_3^2 - 1$$

Ničle tega polinoma so sfere.

2.

$$X_1^n + X_2^n - X_3^n$$

za $n \geq 3$ v \mathbb{N}^3 nima ničel (gre za zadnji Fermatov izrek, ki je bil dokazan leta 1995)

2.8 Simetrična grupa

Definicija 71: Simetrična grupa \mathcal{S}_n , za $n \in \mathbb{N}$, je grupa permutacij množice $\{1, 2, \dots, n\}$. Element te grupe zapišemo kot

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

Opomba: Očitno

$$|\mathcal{S}_n| = n!$$

Definicija 72: *Transpozicija* zamenja dva elementa in jo zapišemo kot (i, j) , kjer sta i in j elementa, ki se med seboj zamenjata.

Izrek 6:

Vsako permutacijo se da zapisati kot produkt transpozicij.

Dokaz. Algebra 1. □

Trditev 29: Če je permutacija enaka produktu sodega (lihega) števila transpozicij, je tudi drug način zapisa te permutacije sod (lih).

$$\text{sgn}(\sigma\rho) = \text{sgn}(\sigma)\text{sgn}(\rho)$$

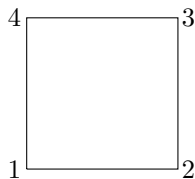
Sode permutacije tvorijo podgrupo. To podgrupo imenujemo **alternirajoča podgrupa** in jo označimo z A_n .

Definicija 73: Permutacijo oblike: $i_{j_1} \mapsto i_{j_2}, i_{j_2} \mapsto i_{j_3}, \dots, i_{j_{k-1}} \mapsto i_{j_k}$ imenujemo k -cikel in ga označimo z $(i_{j_1}, i_{j_2}, \dots, i_{j_k})$ (Zamenja zgolj vrstni red nekaterih elementov, ostale pa pusti pri miru)

Definicija 74: 2-cikel imenujemo transpozicija.

Opomba: Ni težko opaziti, da lahko vsako permutacijo zapišemo kot produkt disjunktnih ciklov.

2.9 Diedrska grupa



Definicija 75: *Simetrija kvadrata je ustrezna permutacija oglišč.*

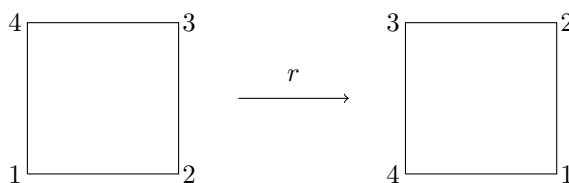
Opomba: To si lahko predstavljamo kot da vzamemo kvadrat iz ravnine, ga v prostoru vrtimo okoli simetrijskih osi, ter ga položimo nazaj, tako da so oglišča na mestih, kjer so bila že prej (mesta oglišč se ne ujemajo nujno z mesti oglišč preden smo lik dvignili).

Opomba: Očitno je produkt (kompozitum) simetrij enak produktu ustreznih permutacij in je spet simetrija kvadrata (to je tako, kot da bi zaporedoma izvajali te operacije).

Opomba: Opazimo, da je inverz simetrije prav tako simetrija, ki vrne kvadrat nazaj v prejšnjo lego

Primer:

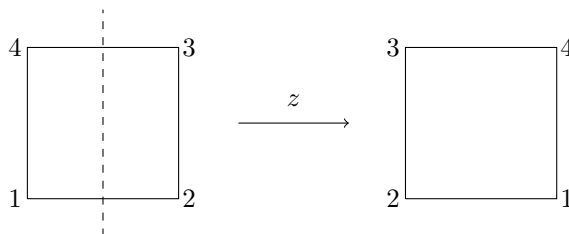
1. Naj bo r rotacija kvadrata za $\frac{\pi}{2}$ v pozitivni smeri (v nasprotni smeri urinega kazalca), ustreza ji cikel $(1, 2, 3, 4)$.



Slika 1: Rotacija za $\frac{\pi}{2}$

Vidimo: $r^2 =$ vrtenje za π , $r^3 =$ vrtenje za $\frac{3}{2}\pi$, $r^4 =$ vrtenje za $0 = id$

2. Naj bo z 'obračanje na glavo', tej simetriji ustreza permutacija: $z = (12)(34)$



Slika 2: Obračanje na glavo (zrcaljenje prek simetrijske osi)

Opomba: Očitno simetrijska grupa ni komutativna ($zr \neq rz$).

Definicija 76: *Diedrska grupa reda $2n$ je simetrijska grupa pravilnega n -kotnika.*

$$\mathcal{D}_{2n} := \{1, r, r^2, \dots, r^{n-1}, z, zr, zr^2, \dots, zr^{n-1}\} \quad (58)$$

Pomembne enakosti: $r^n = 1, z^2 = 1, rz = zr^{-1}, (rz)^2 = 1, |D_{2n}| = 2n$

Vsak element D_{2n} lahko zapišemo kot $a = z^j r^i$; $i \in \{0, 1\}, 0 \leq j < n$

Primer:

1. D_8 je grupa simetrij kvadrata
2. D_4 je grupa simetrij pravokotnika, ki ni kvadrat
3. $D_2 = \{1, r\}$

Opomba: Opazimo, da je splošna diedrska grupa generirana z rotacijo in zrcaljenjem (r, z)

Opomba: Diedrsko grupo reda $2n \geq 3$ si lahko predstavljamo kot podgrupo simetrične grupe \mathcal{S}_n

Opomba: V splošnem lahko za diedrsko grupo proglasimo katerokoli grupo, ki ustreza osnovnim enakostim te grupe: $(r^n = 1, z^2 = 1, rz = zr^{-1})$

V \mathbb{R}^2 je tako diedrska grupa tudi grupa D_{2n} , kjer

$$r = \begin{bmatrix} \cos \frac{2\pi}{n} & \sin \frac{2\pi}{n} \\ -\sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{bmatrix}, z = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Tu si pravilni n -kotnik predstavljamo v ravnini, in ga prav tako tudi zrcalimo/rotiramo. Če pa je n sod, potem je v tej grupi tudi rotacija prek vertikalne osi, ki jo zapišemo kot $z_v = -z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Ker pa si želimo, da bi imele naše matrike determinanto 1 (To pomeni, da ne spreminjajo volumna objekta, ki ga preslikamo) lahko to grupo razširimo na podgrupo $\mathcal{SL}_3(\mathbb{R})$ kot:

$$r' = \begin{bmatrix} \cos \frac{2\pi}{n} & \sin \frac{2\pi}{n} & 0 \\ -\sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} & 0 \\ 0 & 0 & 1 \end{bmatrix}, z' = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Podobno lahko kot Diedrsko grupo vidimo podgrupo $D_{2n} \subseteq \mathcal{GL}_2(\mathbb{Z}_n)$, kjer:

$$r = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, z = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Na ta način dobimo generirano ogrodje torusa, če pa $n \rightarrow \infty$, pa dobimo kar $\mathcal{GL}(\mathbb{Z})$.

2.10 Linearne grupe

Naj bo $n \in \mathbb{N}$ in \mathcal{F} polje. Tedaj je $(\mathcal{M}_n(\mathcal{F}), *)$ monoid (ni pa grupa, saj niso vsi elementi obrnljivi).

Definicija 77: Naj bo $n \in \mathbb{N}$ in \mathcal{F} polje. **Splošna linearna grupa** je

$$\mathcal{GL}_n := \mathcal{M}_n(\mathcal{F})^* = \{A \in \mathcal{M}_n(\mathcal{F}) \mid A \text{ je obrnljiva}\} \quad (59)$$

$$\mathcal{GL}_n := M_n(\mathcal{F})^* = \{\mathcal{A} \in M_n(\mathcal{F}) \mid \det(\mathcal{A}) \neq 0\}$$

Opomba: Če bi imeli matrike zgolj nad kolobarjem, bi potrebovali vsaj komutativnost, da bi bila determinanta sploh smiselna ($ad - bc = da - bc$).

Definicija 78:

Naj bo $n \in \mathbb{N}$ in \mathcal{F} polje. *Specialna linearna grupa* je

$$\mathcal{SL}_n := \{\mathcal{A} \in M_n(\mathcal{F}) \mid \det(\mathcal{A}) = 1\} \quad (60)$$

Definicija 79:

Naj bo $n \in \mathbb{N}$ in \mathcal{F} polje. *Ortogonalna (linearna) grupa* je

$$\mathcal{O}_n := \{\mathcal{A} \in M_n(\mathcal{F}) \mid \mathcal{A}\mathcal{A}^t = \mathcal{A}^t\mathcal{A} = \mathcal{I}\} \quad (61)$$

Kjer \mathcal{A}^* označuje transponirano konjugirano matriko

Definicija 80:

Naj bo $n \in \mathbb{N}$. *Unitarna (linearna) grupa* je

$$\mathcal{U}_n := \{\mathcal{A} \in M_n(\mathbb{C}) \mid \mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \mathcal{I}\} \quad (62)$$

Definicija 81: Naj bo $n \in \mathbb{N}$. *Specialna ortogonalna (linearna) grupa* je

$$\mathcal{SO}_n := \{\mathcal{A} \in \mathcal{O}_n(\mathbb{C}) \mid \det(\mathcal{A}) = 1\} \quad (63)$$

Definicija 82: Naj bo $n \in \mathbb{N}$. *Specialna unitarna (linearna) grupa* je

$$\mathcal{SU}_n := \{\mathcal{A} \in \mathcal{U}_n(\mathbb{C}) \mid \det(\mathcal{A}) = 1\} \quad (64)$$

Definicija 83: Naj bo $n \in \mathbb{N}$ in \mathcal{F} polje. *Simplektična (linearna) grupa* je

$$\mathcal{Sp}_n(\mathcal{F}) := \{\mathcal{A} \in M_{2n}(\mathcal{F}) \mid \mathcal{A}\mathcal{J}\mathcal{A}^t = \mathcal{A}^t\mathcal{J}\mathcal{A} = \mathcal{I}\} \quad (65)$$

Kjer je

$$\mathcal{J} = \begin{bmatrix} 0 & \mathcal{I}_n \\ -\mathcal{I}_n & 0 \end{bmatrix}$$

3 Homomorfizmi in kvocientne strukture

3.1 Izomorfizmi grup, ciklične grupe

Definicija 84: Naj bosta $(\mathcal{G}_1, *)$ in $(\mathcal{G}_2, *)$ grupi. Grupi \mathcal{G}_1 in \mathcal{G}_2 sta **izomorfni**, če obstaja taka bijektivna preslikava $\varphi : \mathcal{G}_1 \rightarrow \mathcal{G}_2$ da velja:

$$\forall g_1, g_2 \in \mathcal{G}_1. \varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2) \quad (66)$$

Pišemo:

$$\mathcal{G}_1 \cong \mathcal{G}_2$$

Opomba: Če je katera izmed grup (ali pa obe) aditivna, primerno spremenimo operacijo.

Opomba: Če imamo končni grupi, ki sta si izomorfni, potem sta njuni grupni tabeli 'enaki'.

$\varphi : \mathcal{G}_1 \rightarrow \mathcal{G}_2$, izomorfizem, potem $\mathcal{G}_2 = \{\varphi(g_1), \varphi(g_2), \dots, \varphi(g_n)\}, g_i \in \mathcal{G}_1$.

Torej se g_i in $\varphi(g_i)$ v tablah pojavita na istem mestu.

Primer:

Grupna tabela za $(\mathbb{Z}_4, +)$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathcal{U}_4 = \{1, i, -1, -i\}$ s tabelo

*	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Tabeli se nam zdita sumljivo podobni $0 \sim 1, 1 \sim i, 2 \sim -1, 3 \sim -i$, saj nastopajo na istih mestih.

Če si pogledamo splošno grupo $(\mathbb{Z}_n, +)$ in $\mathcal{U}_n := \{z \in \mathbb{C} \mid z^n = 1\} = \underbrace{\{1, a, a^2, \dots, a^{n-1}\}}_{a = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})}$

Vidimo:

$$a_i * a_j = \begin{cases} a_{i+j} & ; i+j < n \\ a_{i+j-n} & ; i+j \geq n \end{cases}$$

V čemer prepoznamo seštevanje v \mathbb{Z}_n

Trditev 30:

$$\mathcal{U}_n \cong \mathbb{Z}_n$$

Dokaz.

$$\varphi : \mathcal{U}_n \rightarrow \mathbb{Z}_n$$

$$\varphi : z_i \mapsto i$$

φ je bijekcija in $\varphi(z_i * z_j) = \varphi(z_i) + \varphi(z_j)$, torej sta si grupi izomorfni. □

Trditev 31: Če je $\varphi : \mathcal{G} \rightarrow \mathcal{G}_1$ izomorfizem je tudi $\varphi^{-1} : \mathcal{G}_1 \rightarrow \mathcal{G}$ izomorfizem.

Dokaz. Ker je φ injektivna je dovolj pokazati: $\varphi(\varphi^{-1}(uv)) = uv = \varphi(\varphi^{-1}(u))\varphi(\varphi^{-1}(v)) = \underbrace{\varphi(\varphi^{-1}(u))\varphi^{-1}(v))}_{\text{Ker je } \varphi \text{ homomorfizem}} \quad \square$

Ker je φ homomorfizem

Primer:

1. $\mathcal{G} \cong \mathcal{G}$ Izomorfizem je kar identiteta
2. $(\mathbb{R}, +) \cong (\mathbb{R}_+, *)$, kjer $\varphi : x \mapsto e^x$
3. $(\mathbb{Z}, +) \cong (n\mathbb{Z}, +)$, kjer $\varphi : x \mapsto nx$, to velja za $n \geq 1$

Definicija 85: Grupi, ki je generirana z enim samim elementom pravimo **ciklična grupa**.

Če je \mathcal{G} generirana z a pišemo: $\mathcal{G} = \langle a \rangle$

Primer:

1. $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ za množenje
2. $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$ za seštevanje
3. $\langle 1 \rangle = \langle -1 \rangle = (\mathbb{Z}, +)$
4. $\langle 1 \rangle = (\mathbb{Z}_n, +)$, podgrupa $(\mathbb{Z}, +)$
5. $\langle i \rangle = \langle -i \rangle = \{1, i, -1, -i\} = \mathcal{U}_4$

Izrek 7:

Naj bo \mathcal{G} ciklična grupa:

- (a) Če je \mathcal{G} neskončna, je izomorfna $(\mathbb{Z}, +)$
- (b) Če je \mathcal{G} končna, je izomorfna $(\mathbb{Z}_n, +)$ za nek $n \in \mathbb{N}$

Dokaz. Naj bo a generator grupe \mathcal{G}

1. $\forall n \in \mathbb{Z}. \forall m \in \mathbb{Z}. m \neq n \implies a^n \neq a^m$

Torej je grupa neskončna, dokazujemo: $\mathcal{G} \cong (\mathbb{Z}, +)$

Vzemimo: $\varphi : \mathbb{Z} \rightarrow \mathcal{G}, n \mapsto a^n$, ki je zaradi predpostavke injektivna in surjektivna, ker generira a^n generira grupo. Prav tako pa velja:

$$\varphi(n+m) = \underbrace{a^{n+m} = a^n * a^m}_{(14)} = \varphi(n) * \varphi(m) \text{ in je torej izomorfizem.}$$

2. $\exists m \in \mathbb{Z}. \exists n \neq m \in \mathbb{Z}. a^n = a^m$

Torej $a^{n-m} = 1 \iff \exists s \in \mathbb{N}. a^s = 1$.

Če $n = 1$, potem $\mathcal{G} = \{1\}$ in je izomorfna $(\mathbb{Z}_1, +)$

Naj bo n sedaj najmanjše tako naravno število ($a^n = 1, a^k \neq 1, 0 < k < n$)

Očitno so si elementi $1, a, a^2, \dots, a^{n-1}$ različni, saj smo tako izbrali n , torej je $|\mathcal{G}| \geq n$.

Za drugo smer pa vzemimo $x = a^m \in \mathcal{G}, m = qn + r, 0 \leq r \leq n-1$.

Torej $x = a^m = a^{qn+r} = (a^n)^q * a^r = a^r \implies |\mathcal{G}| \leq n$

Iz zgornjih ugotovitev velja: $|\mathcal{G}| = n, z_i = a^i$ in $\varphi(z_i) = i$, kar pa je izomorfizem. \square

Posledica: Če je \mathcal{G} poljubna grupa, tako vsak element generira ciklično podgrupo ($\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$).

Definicija 86: Naj bo a element grupe \mathcal{G} . Če obstaja tak $s \in \mathbb{N}$, da velja $a^s = 1$ (1 je enota grupe), rečemo, da ima a **končen red**, najmanjšemu naravnemu številu s to lastnostjo pravimo **red elementa** a . Če pa takega elementa ni, potem pravimo, da ima a **neskončen red**.

Trditev 32: $\text{red}(a) = |\langle a \rangle|$

Dokaz. $\text{red}(a) = n \iff a^n = 1 \wedge a^k \neq 1, 1 \leq k < n$
 $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\} \implies |\langle a \rangle| = n$ □

Opomba: Če je \mathcal{G} grupa za seštevanje, je red elementa tak najmanjši $n \in \mathbb{N}$, da $na = 0$.

Primer:

1. V vsaki grupi ima enota red 1.
2. V $(\mathbb{Z}, +)$ imajo vsi elementi razen 0 neskončen red.
3. \mathbb{Z}_4 , 1 in 3 imata red 4, 2 ima red 2.
4. \mathcal{D}_4 (Simetrije pravokotnika, ki ni kvadrat) Vsi razen enote imajo red 2

Opomba: Očitno izomorfizmi ohranjajo red elementov.

Opomba: \mathbb{Z}_4 in \mathcal{D}_4 nista izomorfni. Je pa res, da velja:

$$\mathcal{D}_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

3.2 Izomorfnost vektorskih prostorov

Definicija 87: Naj bosta \mathcal{V} in \mathcal{V}' vektorska prostora nad istim poljem \mathcal{F} . Vektorski prostor \mathcal{V} je izomorfen \mathcal{V}' , če obstaja bijektivna linearna preslikava $\varphi : \mathcal{V} \rightarrow \mathcal{V}'$. To preslikavo imenujemo izomorfizem vektorskih prostorov.

Izrek 8:

Končno razsežna vektorska prostora sta si izomorfna natanko tedaj, ko imata isto dimenzijo.

Dokaz. \implies

Naj ima \mathcal{V} dimenzijo n in bazo: $\{b_1, b_2, \dots, b_n\}$.

Naj bo $\lambda_1 \varphi(b_1) + \dots + \lambda_n \varphi(b_n) = 0$ za neke $\lambda_i \in \mathcal{F}$

Ker je φ linearna in injektivna velja:

$$\text{Ker}(A) = \{0\} \text{ in ker velja: } \varphi(\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_n b_n) = 0$$

iz tega sledi: $\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_n b_n$ v jedru.

Torej velja $\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_n b_n = 0$

Ker so si bazni vektorji neodvisni, so vsi skalarji ničelni: $\lambda_i = 0$.

Tako smo dobili linearno neodvisne vektorje, pokazati moramo še, da so tudi

ogrodje.

Ker φ je surjektivna velja: $v' \in \mathcal{V}' = \varphi(\mathcal{V})$ za poljuben v' .

$v' = \lambda_1 \varphi(b_1) + \dots + \lambda_n \varphi(b_n)$, vidimo da ima \mathcal{V}' linearno ogrodje z močjo n ($\varphi(b_1), \dots, \varphi(b_n)$).

Tako smo dobili linearno ogrodje neodvisnih vektorjev, ki je torej baza z močjo n . Dimenzija \mathcal{V}' je torej n , enaka dimenziji \mathcal{V} .

\Leftarrow

Vzemimo $\{b_1, b_2, \dots, b_n\}$ za bazo \mathcal{V} in $\{b'_1, b'_2, \dots, b'_n\}$ za bazo \mathcal{V}' .

Definirajmo:

$$\varphi(\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_n b_n) = \lambda_1 b'_1 + \lambda_2 b'_2 + \dots + \lambda_n b'_n$$

Potrebno je zgolj še preveriti, da je to bijektivna linearna preslikava. □

3.3 Pojem homomorfizma

Definicija 88: Naj bosta \mathcal{G} in \mathcal{G}_1 grupi, $\varphi : \mathcal{G} \rightarrow \mathcal{G}_1$ je homomorfizem grup, če velja:

$$\varphi(xy) = \varphi(x)\varphi(y), \quad \forall x, y \in \mathcal{G} \quad (67)$$

Opomba: Če je grupa aditivna, predznak smiselno spremenimo.

Definicija 89: Naj bosta \mathcal{K} in \mathcal{K}_1 kolobarja, $\varphi : \mathcal{K} \rightarrow \mathcal{K}_1$ je homomorfizem kolobarjev, če velja:

$$\varphi(x + y) = \varphi(x) + \varphi(y) \wedge \varphi(xy) = \varphi(x)\varphi(y), \quad \forall x, y \in \mathcal{G} \quad (68)$$

Ker pa smo pri kolobarju zahtevali tudi enoto, potrebujemo še dodaten pogoj:

$$\varphi(1) = 1$$

Definicija 90: Naj bosta \mathcal{V} in \mathcal{V}_1 vektorska prostora nad istim obsegom \mathcal{F} , $\varphi : \mathcal{V} \rightarrow \mathcal{V}_1$ je homomorfizem vektorskih prostorov, če velja:

$$\varphi(x + y) = \varphi(x) + \varphi(y) \wedge \varphi(\lambda x) = \lambda \varphi(x), \quad \forall x, y \in \mathcal{G}, \forall \lambda \in \mathcal{F} \quad (69)$$

Definicija 91: Naj bosta \mathcal{A} in \mathcal{A}_1 algebri nad istim obsegom \mathcal{F} , $\varphi : \mathcal{A} \rightarrow \mathcal{A}_1$ je homomorfizem algebr, če velja:

$$\begin{aligned} \varphi(1) &= 1 \wedge \varphi(x + y) = \varphi(x) + \varphi(y) \wedge \varphi(\lambda x) = \lambda \varphi(x) \wedge \\ &\varphi(x)\varphi(y) = \varphi(xy), \quad \forall x, y \in \mathcal{G}, \forall \lambda \in \mathcal{F} \end{aligned} \quad (70)$$

Primer:

$\varphi : \mathbb{R} \rightarrow \mathcal{M}_2(\mathbb{R}), \varphi(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ ni homomorfizem, čeprav ustreza pogojem glede operacij, saj enote ne slika v enoto.

Opomba: Kadar je iz konteksta razvidno, za homomorfizem katerih struktur gre, to izpuščamo (homomorfizem grup \mapsto homomorfizem, ...).

Definicija 92: Trivialni homomorfizem je $\varphi : \mathcal{A} \rightarrow \mathcal{A}_1, x \mapsto 1$

Definicija 93: *Epimorfizem* je surjektivni homomorfizem.

Definicija 94: *Monomorfizem* (vložitev) je injektivni homomorfizem.

Definicija 95: *Izomorfizem* je bijektivni homomorfizem.

Definicija 96: *Endomorfizem* je homomorfizem strukture same vase.

Definicija 97: *Automorfizem* je bijektivni endomorfizem (izomorfizem strukture same vase).

Opomba: Homomorfizmom v vektorskih prostorih pravimo tudi linearne preslikave.

Opomba: Izraz vložitev uporabljamo predvsem takrat, ko želimo poudariti, da lahko vsak element identificiramo z njegovo sliko.

Primer:

1. Vložitev \mathbb{R} v $\mathbb{C} : x \mapsto x + 0i$
2. Vložitev \mathcal{K} v $\mathcal{K}[X] : a \mapsto a + 0X + 0X^2 + \dots$ Tako vsak element identificiramo s konstantnim polinomom.

Opomba: Ker je polje tudi kolobar (z nekaj dodatnimi lastnostmi), je homomorfizem kolobarja tudi homomorfizem polja.

Trditev 33: Kompozitum homomorfizmov je homomorfizem.

Dokaz. Dokaz zgolj za grupe, za ostale strukture pokažemo podobno.

Naj bosta: $\varphi : \mathcal{G} \rightarrow \mathcal{G}_1$ in $\psi : \mathcal{G}_1 \rightarrow \mathcal{G}_2$ homomorfizma grup, tedaj velja:

$$(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = (\psi \circ \varphi)(x)(\psi \circ \varphi)(y) \quad \square$$

Trditev 34: Inverz izomorfizma je izomorfizem.

Dokaz. Za grupe smo že dokazali (31), za ostale strukture pa to poteka na isti način. \square

Definicija 98: Pravimo, da sta si strukturi \mathcal{A} in \mathcal{A}_1 izomorfni, če obstaja izomorfizem iz \mathcal{A} v \mathcal{A}_1 . Tedaj pišemo

$$\mathcal{A} \cong \mathcal{A}_1$$

Trditev 35: Relacija $\mathcal{A} \cong \mathcal{A}_1$ je ekvivalenčna.

Dokaz.

- 1) $\mathcal{A} \cong \mathcal{A}$ Očitno, saj je id izomorfizem
- 2) $\mathcal{A} \cong \mathcal{A}_1 \implies \mathcal{A}_1 \cong \mathcal{A}$ Inverz izomorfizma je tudi sam izomorfizem, torej je izomorfizem v drugo smer kar inverz prvega.
- 3) $\mathcal{A} \cong \mathcal{A}_1 \wedge \mathcal{A}_1 \cong \mathcal{A}_2 \implies \mathcal{A} \cong \mathcal{A}_2$ Ker je kompozitum bijektivnih preslikav bijektivna preslikava, kompozitum homomorfizmov pa homomorfizem, je naš izomorfizem kar kompozitum izomorfizmov.

□

Posledica: Množica vseh avtomorfizmov v \mathcal{A} je grupa za komponiranje.

Dokaz. Tip strukture \mathcal{A} je nepomemben. Potrebno je samo preveriti aksiome za grupo:

Zaprto: Kompozitum avtomorfizmov je avtomorfizem

Asociativnost: Kompozitum je v splošnem asociativen

Enota: Id za komponiranje je tudi avtomorfizem

Inverz: Inverz avtomorfizma je tudi avtomorfizem.

□

Primer:

$\mathcal{GL}_n(\mathcal{F})$ = grupa vseh obrnljivih matrik = grupa vseh linearnih preslikav iz $\mathcal{F}^n \rightarrow \mathcal{F}^n$ = grupa avtomorfizmov vektorskega prostora \mathcal{F}^n .

Trditev 36: Če je $\varphi : \mathcal{G} \rightarrow \mathcal{G}_1$ homomorfizem grup, za poljuben $x \in \mathcal{A}$ velja $\varphi(1_{\mathcal{G}}) = 1_{\mathcal{G}_1}$ in $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Dokaz. $\varphi(1) = \varphi(1 * 1) = \varphi(1)\varphi(1) \implies \varphi(1) = 1$

$1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) \implies \varphi(x^{-1}) = \varphi(x)^{-1}$

□

Trditev 37: Za poljuben homomorfizem grup $\varphi : \mathcal{G} \rightarrow \mathcal{G}_1$ in poljuben $n \in \mathbb{Z}$ velja

$$\varphi(x^n) = \varphi(x)^n$$

Dokaz. Sledi iz prejšnje trditve in iz poznavanja enakosti (12).

□

Definicija 99: Zalogi vrednosti homomorfizma $\varphi : \mathcal{A} \rightarrow \mathcal{A}_1$ pravimo **slika** φ in jo označimo z $Im(\varphi)$

$$Im(\varphi) := \{\varphi(x) \mid x \in \mathcal{A}\} \subseteq \mathcal{A}_1 \quad (71)$$

Trditev 38: Slika homomorfizma poljubne strukture je tudi sama podstruktura te strukture.

Dokaz. Dokažemo zgolj za grupe, za ostale podstrukture se pokaže na podoben način.

$$\begin{aligned} \varphi(x)\varphi(y) &= \varphi(xy) \in Im(\varphi) \\ \varphi(x)^{-1} &= \varphi(x^{-1}) \in Im(\varphi) \end{aligned}$$

□

Opomba: Vsak homomorfizem je epimorfizem (na svojo zalogo vrednosti).

Definicija 100: Naj bo $\varphi : \mathcal{A} \rightarrow \mathcal{A}_1$ homomorfizem poljubnih struktur. **Jedro** φ je množica vseh elementov, ki se slikajo v nevtralni element, označimo jo z $Ker(\varphi)$.

$$Ker(\varphi) := \{x \in \mathcal{A} \mid \varphi(x) = 1\} \quad (72)$$

Opomba: Spomnimo se, da za vektorske prostore, kolobarje in algebre velja $1 = 0$, torej govorimo o nevtralnem elementu za seštevanje.

Definicija 101: Jedro homomorfizma φ je **trivialno**, če je v jedru zgolj en element (1 oziroma 0, če gre za aditivne strukture).

Trditev 39: Homomorfizem $\varphi : \mathcal{A} \rightarrow \mathcal{A}_1$ je injektiven natanko tedaj, ko je njegovo jedro trivialno.

Dokaz. Dokažemo zgolj za grupe, za ostale strukture so dokazi podobni.

$$\implies$$

Naj velja: φ je injektivna, $x \in Ker(\varphi)$

$$\varphi(x) = 1 = \varphi(1) \text{ od tod zaradi injektivnosti } \varphi \text{ sledi: } x = 1$$

$$\impliedby$$

Naj velja $Ker(\varphi) = \{1\}$ in $\varphi(x) = \varphi(y)$

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = 1, \text{ torej: } xy^{-1} \in Ker(\varphi) = \{1\}, \text{ in dobimo } x = y$$

□

Opomba: Na jedro/sliko preslikave lahko gledamo kot na mero za injektivnost/surjektivnost. Čim manjše kot je jedro, tem 'bližje' injektivnosti je φ in podobno, večja kot je slika, 'bolj' je φ surjektivna.

Primer:

1. 'Najlepši' homomorfizem je tak, ki ima trivialno jedro, slika pa je celotna kodomena
2. 'Najgrši' homomorfizem je tak, ki ima jedro enako domeni, slika pa je zgolj

$\{1\}$ (trivialni homomorfizem).

Opomba: Zaradi naše definicije (89), ki za homomorfizem zahteva $\varphi(1) = 1$, lahko trivialni homomorfizem slika zgolj v ničelni kolobar $(\{0\})$.

3.4 Primeri homomorfizmov

Najbolj splošen primer

$$a^x a^y = a^{x+y}, a > 0$$

3.4.1 Primeri homomorfizmov grup

1. Naj bo \mathcal{G} Abelova grupa
 $\varphi(x) = x^{-1}$ je avtomorfizem
 $\varphi(xy) = (xy)^{-1} = (yx)^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$ Splošneje, za vsak $m \in \mathbb{Z}$ je $\varphi(x) = x^m$ endomorfizem grupe \mathcal{G} .
2. Naj bo $\varphi : \mathbb{C} - \{0\} \rightarrow \mathbb{R}^+, \varphi(w) = |w|$, očitno je φ epimorfizem ($|zw| = |z||w|$)
 $\text{Ker}(\varphi) = \mathcal{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$
3. $\varphi : (\mathbb{R}, +) \rightarrow (\mathcal{S}^1, *)$, $\varphi(x) = \cos(x) + i\sin(x)$, $\text{Ker}(\varphi) = \{2k\pi \mid k \in \mathbb{Z}\}$
4. $\text{sgn} : \mathcal{S}_n \rightarrow (\{-1, 1\}, *)$, $\text{sgn}(\sigma\rho) = \text{sgn}(\sigma)\text{sgn}(\rho)$, $\text{Ker}(\text{sgn}) = \mathcal{A}_n$
5. $\det : \text{Gl}(n, \mathcal{F}) \rightarrow \mathcal{F}^*$ je epimorfizem $\text{Ker}(\det) = \text{Sl}(n, \mathcal{F})$

Definicija 102: Naj bo \mathcal{G} poljubna grupa, za poljuben $a \in \mathcal{G}$ je $\varphi_a : \mathcal{G} \rightarrow \mathcal{G}$, $\varphi_a(x) = axa^{-1}$ avtomorfizem \mathcal{G} , vsak tak avtomorfizem imenujemo **notranji avtomorfizem**

Dokaz da je to res avtomorfizem je trivialen:

$$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$$

$$\text{Ker}(\varphi_a) = \{x \in \mathcal{G} \mid axa^{-1} = 1\} = \{1\}$$

$$\text{Im}(\varphi_a) = \mathcal{G}, \text{ saj } x = \varphi_a(a^{-1}xa)$$

Opomba: Če se spomnimo poglavja o grupah, sta si x, y **konjugirana**, če obstaja tak a , da $y = axa^{-1}$ (31), tako sta si x in $\varphi_a(x)$ konjugirana. Za poljubno podgrupo $\mathcal{H} \subseteq \mathcal{G}$ tako velja $\mathcal{H} \cong a\mathcal{H}a^{-1}$

Opomba: Edini notranji avtomorfizem katerekoli Abelove grupe je id .

Definicija 103: $\text{Aut}(\mathcal{G})$ je množica vseh avtomorfizmov grupe \mathcal{G}

Opomba: Preveriti da je to grupa je trivialno

$$\Phi : \mathcal{G} \rightarrow \text{Aut}(\mathcal{G}), \Phi(a) = \varphi_a$$

Preverimo dobro definiranost:

$$\varphi_a \circ \varphi_b(x) = abxb^{-1}a^{-1} = \varphi_{ab}(x) \text{ in } \Phi(ab) = \varphi_a \circ \varphi_b$$

Φ je torej homomorfizem grup, njegova slika pa je množica vseh notranjih avtomorfizmov grupe \mathcal{G} .

Definicija 104: $\text{Inn}(\mathcal{G})$ je grupa vseh notranjih avtomorfizmov grupe \mathcal{G}

Opomba: Očitno $\text{Im}(\Phi) = \text{Inn}(\mathcal{G})$

3.4.2 Primeri homomorfizmov kolobarjev in algeber

Definicija 105: Naj bo \mathcal{K} poljubnen kolobar, za poljuben obrnljiv $a \in \mathcal{K}$ je $\varphi_a : \mathcal{K} \rightarrow \mathcal{K}, \varphi_a(x) = axa^{-1}$ avtomorfizem \mathcal{K} , vsak tak avtomorfizem imenujemo **notranji avtomorfizem** kolobarja \mathcal{K} .

Opomba: Tako kot pri grupah ima tudi tu notranji avtomorfizem smisel zgolj za nekomutativne kolobarje

Definicija 106: Naj bo \mathcal{V} vektorski prostor nad \mathcal{F} in naj velja $\dim(V) = n$. Algebro vseh endomorfizmov \mathcal{V} nad \mathcal{F} označimo z :

$$\text{End}_{\mathcal{F}}(\mathcal{V}) = \{f : \mathcal{V} \rightarrow \mathcal{V} | f \text{ je linearna (je endomorfizem)}\} \quad (73)$$

Opomba: Rutinsko preverimo da je to res algebra (množenje je komponiranje funkcij).

1. $\varphi : \mathbb{Z}_2 \rightarrow \mathbb{Z}, \varphi(x) = x$ ni homomorfizem. Veljajo sicer skoraj vse lastnosti, a pade pri $0 = \varphi(1+1) \neq \varphi(1) + \varphi(1) = 2$
2. V nasprotni smeri pa zadeva deluje $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_2$

$$\varphi(x) = \begin{cases} 0 & ; n \text{ sod} \\ 1 & ; n \text{ lih} \end{cases}, \text{ očitno } \varphi(n+m) = \varphi(n) + \varphi(m), \text{ Ker}(\varphi) = 2\mathbb{Z}$$
3. \mathcal{K} vložimo v $\mathcal{K}[X]$ ($a \mapsto a + 0X + 0X^2 \dots$)
 $\varphi : \mathcal{K}[X] \rightarrow \mathcal{K}, \varphi(a_0 + a_1X + \dots) = a_0$, očitno $\varphi(f+g) = \varphi(f) + \varphi(g)$ in $\varphi(f * g) = \varphi(f) * \varphi(g)$
 $\text{Ker}(\varphi) = \{a_1X + a_2X^2 + \dots + a_nX^n\}$, velja tudi $\varphi(f(X)) = f(0)$.

Opomba: Če je \mathcal{K} komutativen, je za poljuben $x \varphi : \mathcal{K}[X] \rightarrow \mathcal{K}, \varphi(f(X)) = f(x)$ homomorfizem.

4. Naj bo $f \in C[0, 1]$. Za poljuben $x \in [0, 1]$ je $\varphi_x : C[0, 1] \rightarrow \mathbb{R}, f \mapsto f(x)$ homomorfizem. $\text{Ker}(\varphi_x) = \{f \in C[0, 1] | f(x) = 0\}$
5. $\varphi : \text{End}_{\mathcal{F}}(\mathcal{V}) \rightarrow M_n(\mathcal{F}), \varphi(f) = [f]$, kjer je $[f]$ matrika, ki pripada f glede na vnaprej izbrano bazo. φ je izomorfizem elgeber. Torej velja $\text{End}_{\mathcal{F}}(\mathcal{V}) \cong M_n(\mathcal{F})$.
6. Primeri posebnih izomorfizmov
 - (a) $\mathcal{K}_1 = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in \mathbb{R} \right\}$, kaj hitro lahko preverimo da je to kolobar, da pa velja $\mathcal{K}_1 \cong \mathbb{R}$ vzemimo $\varphi(x) = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} = xI$, ki ustreza vsem zahtevam.
 - (b) $\mathcal{K}_2 = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$, podobno kot prej brez težav preverimo, da je kolobar, velja pa tudi $\mathcal{K}_2 \cong \mathbb{R} \times \mathbb{R}$ (enak direktnemu produktu \mathbb{R} s samim seboj), kar preverimo z $\varphi((x, y)) = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$.

- (c) $\mathcal{K}_3 = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$ Velja $\mathcal{K}_3 \cong \mathbb{C}$ z izomorfizmom $\varphi(x+yi) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$
- (d) $\mathcal{K}_4 = \left\{ \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \mid w, z \in \mathbb{C} \right\}$ Na pogled se nam zdi podoben \mathbb{H} , saj je prav tako kot v kvaternionih vsak neničelen element obrnljiv in je kot \mathbb{H} 4-razsežna algebra nad \mathbb{R} , res je, saj imamo izomorfizem:
- $$\varphi(x + yi + uj + vk) = \begin{bmatrix} x + yi & u + vi \\ -u + vi & x + yi \end{bmatrix}$$

3.5 Cayleyev izrek in drugi izreki o vložitvah

Definicija 107: Naj bo \mathcal{X} množica, $\text{Sim}(\mathcal{X})$ je simetrična grupa množice \mathcal{X} , torej je grupa bijektivnih preslikav iz \mathcal{G} v \mathcal{G} .

3.5.1 Cayleyev izrek

Izrek 9: Cayleyev izrek

Vsako grupo \mathcal{G} lahko vložimo v kako simetrično grupo.

Dokaz. Naj bo $a \in \mathcal{G}$ definirajmo $l_a : \mathcal{G} \rightarrow \mathcal{G}, l_a(x) = ax$. Preveriti moramo, da velja $l_a \in \text{Sim}(\mathcal{G})$.

Injektivnost: $l_a(x) = l_a(y) \implies ax = ay \implies x = y$

Surjektivnost: $x \in \mathcal{G} \implies x = l_a(a^{-1}x) = aa^{-1}x = x$

Definirajmo $\varphi : \mathcal{G} \rightarrow \text{Sim}(\mathcal{G}), \varphi(a) = l_a$ in preverimo, da je l homomorfizem.

$l_{ab}(x) = (ab)x = a(bx) = l_a(l_b(x)) = l_a * l_b(x) \implies l_{ab} = l_a * l_b$

Preverimo še, da ima φ trivialno jedro: $a \in \text{Ker}(\varphi) \implies l_a = \text{id}_{\mathcal{G}} \implies \forall x \in \mathcal{G}. ax = x \implies a = 1$

Torej je φ vložitev. \square

Opomba: Iz dokaza opazimo, da lahko \mathcal{G} vložimo v $\text{Sim}(\mathcal{G})$, kjer \mathcal{G} gledamo zgolj kot množico.

Zanima nas, ali lahko grupo \mathcal{G} vložimo v $\text{Sim}(\mathcal{X})$ za kako bolj posrečeno množico. (Če je grupa že sama simetrična grupa velja $\text{Sim}(\mathcal{G}) \cong S_n$).

Posledica: Vsako končno grupo lahko vložimo v S_n za nek $n \in \mathbb{N}$.

Našli smo injektivni homomorfizem iz \mathcal{G} v $\text{Sim}(\mathcal{X})$ (Kjer je bil naš \mathcal{X} kar \mathcal{G}). Nasploh se izkažejo kot pomembni homomorfizmi (ne nujno injektivni) iz grup v permutacije. Zato pogosteje obravnavamo ekvivalenten pojem:

Definicija 108: Grupa \mathcal{G} deluje na množici \mathcal{X} če obstaja preslikava $\varphi : \mathcal{G} \times \mathcal{X} \rightarrow \mathcal{X}, \varphi(a, x) = ax$, za katero velja $\varphi(ab, x) = \varphi(a, bx)$ in $\varphi(1, x) = x$ za $a, b \in \mathcal{G}, x \in \mathcal{X}$.

Trditev 40: Vsakemu delovanju \mathcal{G} na \mathcal{X} lahko priredimo homomorfizem iz \mathcal{G} na $\text{Sim} \mathcal{X}$ in obratno.

Dokaz. \implies

Imejmo delovanje \mathcal{G} na \mathcal{X} . Priredimo mu homomorfizem $\varphi : \mathcal{G} \rightarrow \text{Sim}(\mathcal{X})$, kjer je $\varphi(a)$ premutacija definirana kot: $\varphi(a)(x) = ax$. Bralec bo lahko za domoačo nalogo dokazal, da je $\varphi(a)$ res premutacija in homomorfizem.

\longleftarrow

Homomorfizmu $\varphi(a) : \mathcal{G} \rightarrow \text{Sim}(\mathcal{X})$ priredimo delovanje $(a, x) \mapsto \varphi(a)(x)$ \square

Primer:

\mathcal{G} deluje na \mathcal{G} z običajnim množenjem. To delovanje smo srečali že v dokazu Cayleyevaga izreka(9).

3.5.2 Vložitev kolobarja v kolobar endomorfizmov

Naj bo \mathcal{M} aditivna (in zato Abelova) grupa. Množica vseh endomorfizmov($\text{End}(\mathcal{M})$) postane kolbar, če vpeljemo vsoto in produkt kot običajno seštevanje in komponiranje.

Izrek 10:

Vsak kolobar \mathcal{K} lahko vložimo v kolobar endomorfizmov neke aditivne grupe.

Dokaz. \mathcal{K} bomo vložili v $\text{End}(\mathcal{K})$, kjer bomo na drugi \mathcal{K} gledali le še kot na aditivno grupo.

Definiramo $\varphi : \mathcal{K} \rightarrow \text{End}(\mathcal{K})$, $\varphi(a) = l_a$, kjer je $l_a : \mathcal{K} \rightarrow \mathcal{K}$ in $l_a(x) = ax$. Zaradi distributivnosti je tako $l_a(x + y) = l_a(x) + l_a(y)$. φ je prav tako homomorfizem(prevedemo na l_a). Injektivnost je trivialna. \square

Podobno vlogo kot jih imajo pri grupah delovanja, imajo pri kolobarjih moduli.

Definicija 109: Aditivna grupa \mathcal{M} je **modul nad kolobarjem** \mathcal{K} , če obstaja operacija $*$: $\mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$, $(a, m) \mapsto am$ za katero velja.

$$(a) \quad (a + b) * m = am + bm$$

$$(b) \quad a * (m + n) = am + an$$

$$(c) \quad (ab) * m = a(bm)$$

$$(d) \quad 1 * m = m$$

Za $a, b \in \mathcal{K}$ in $m, n \in \mathcal{M}$.

Opomba: Opazimo, da je modul nad poljem \mathcal{F} kar vektorski prostor nad istim poljem.

Trditev 41: Vsak modul \mathcal{M} porodi homomorfizem iz \mathcal{K} v $\text{End}(\mathcal{M})$ podan s preslikavo $\varphi(a)(m) = am$ in obratno, vsak homomorfizem $\varphi : \mathcal{K} \rightarrow \text{End}(\mathcal{M})$ porodi modul $a * m = \varphi(a)(m)$

Dokaz. Enako kot prej. \square

3.5.3 Vložitev algebre v algebro endomorfizmov vektorskega prostora

Naj bo \mathcal{V} vektorski prostor nad poljem \mathcal{F} in naj bo $\text{End}_{\mathcal{F}}(\mathcal{V})$ množica vseh linearnih preslikav iz \mathcal{V} v \mathcal{V} . Ta množica je algebra če definiramo običajne operacije.

Trditev 42: Vsako algebro \mathcal{A} lahko vložimo v algebro endomorfizmov nekega vektorskega prostora.

Dokaz. Postopamo podobno kot prej. □

Če je \mathcal{A} končno razsežna je tudi $\text{End}_{\mathcal{F}}(\mathcal{A})$ končno razsežna in zato velja $\text{End}_{\mathcal{F}}(\mathcal{A}) \cong \mathcal{M}_n(\mathcal{F})$.

Posledica: Vsako končno razsežno algebro lahko vložimo v matrično algebro $\mathcal{M}_n(\mathcal{F})$.

Primer:

\mathcal{A} naj bo končno razsežna algebra nad \mathbb{R} , zanima nas, ali lahko velja $ab - ba = 1$ kar je glede na posledico enakovredno problemu:

Ali za $A, B \in \mathcal{M}_n(\mathbb{R})$ lahko velja $AB - BA = I$?

Očitno to ne velja, saj: $\text{sl}(AB - BA) = 0 \neq 1 = \text{sl}(I)$.

3.6 Vložitev celega kolobarja v polje

Zanima nas, ali lahko poljuben kolobar \mathcal{K} vložimo v polje (npr. ali lahko \mathbb{Z} vložimo v \mathbb{C}).

Takoj opazimo da mora imeti kolobar nekaj značilnosti:

1. \mathcal{K} mora biti komutativen (da ima to lastnost tudi polje).
2. \mathcal{K} ne sme imeti deliteljev ničla (da je tudi polje brez deliteljev ničla)

Zahtevati moramo torej, da je \mathcal{K} cel.

Lema 3. S predpisom $(a, b) \sim (a', b') \iff ab' = a'b$ je definirana ekvivalenčna relacija na kartezičnem produktu kolobarja in kolobarja brez ničle ($\mathcal{K} \times \mathcal{K} - \{0\}$).

Dokaz. Brez težav preverimo, da ustreza zahtevam za ekvivalenčno relacijo. □

Tako dobimo $\frac{a}{b} := [(a, b)]$ kot predstavnika ekvivalenčnega razreda (a, b) , in pišemo $\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b$.

Lema 4. Za poljubne $a, a', c, c' \in \mathcal{K}$ in $b, b', d, d' \in \mathcal{K} - \{0\}$ velja

$$\frac{a}{b} = \frac{a'}{b'} \wedge \frac{c}{d} = \frac{c'}{d'} \implies \frac{ab + bc}{bd} = \frac{a'd' + b'c'}{b'd'} \wedge \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

Dokaz. Preprosto premečemo številke □

Izrek 11:

Če v množico vseh ekvivalenčnih razredov

$$\mathcal{F} := \left\{ \frac{a}{b} \mid a \in \mathcal{K}, b \in \mathcal{K} - \{0\} \right\}$$

vpelejmo seštevanje in množenje s predpisoma: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ in $\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$, potem \mathcal{F} postane polje.

Dokaz. Preprosto preverimo dobro lastnosti za polje, dobro definirano nam daje že prejšnja lema. \square

S predpisom $\varphi : \mathcal{K} \rightarrow \mathcal{F}, \varphi(a) = \frac{a}{1}$ je definirano vložitev iz \mathcal{K} v \mathcal{F} .

Dokaz. Prejšnja lema nam da dobro definirano, ostale lastnosti pa preverimo s preprostim računom. \square

Dogovor: Namesto $\frac{a}{1}$ pišemo kar a in v tem smislu \mathcal{K} obravnavamo kot podmnožico \mathcal{F} , $\mathcal{K} \subseteq \mathcal{F}$.

Opomba: Polje \mathcal{F} je generirano s (podmnožico) \mathcal{K} , torej med \mathcal{K} in \mathcal{F} ni drugega polja (če obstaja polje $\mathcal{F}', \mathcal{K} \subseteq \mathcal{F}' \subseteq \mathcal{F}$, to polje zagotovo vsebuje vse inverze elementov iz \mathcal{K} in zato tudi vse elemente \mathcal{F}).

Definicija 110: Polju

$$\mathcal{F} := \left\{ \frac{a}{b} \mid a \in \mathcal{K}, b \in \mathcal{K} - \{0\} \right\} \quad (74)$$

Pravimo **polje ulomkov** celega kolobarja \mathcal{K}

Primer:

1. $\mathcal{K} = \mathbb{Z} \implies \mathcal{F} = \mathbb{Q}$
2. Če je \mathcal{K} že sam polje, velja $\mathcal{F} = \mathcal{K}$

Definicija 111: Naj bo \mathcal{F} polje in $\mathcal{K} = \mathcal{F}[X]$ polju ulomkov \mathcal{K} pravimo **polje racionalnih funkcij**, katerega elementi so $\frac{f(x)}{g(x)}$

Opomba: Na podoben način definiramo polje racionalnih funkcij za polinom več spremenljivk.

3.7 Karakteristika kolobarja in vložitev prapolja v polje

Definicija 112: Naj bo \mathcal{K} kolobar, Če obstaja tako naravno število n , da velja $n * 1 = 0$ (spomnimo se $n * 1 = 1 + 1 + \dots + 1$), potem najmanjšemu izmed njih pravimo **karakteristika kolobarja**, če pa takih števil ni, potem pravimo, da ima kolobar **karakteristiko 0**

Opomba: Karakteristiko kolobarja označimo z $\text{kar}(\mathcal{K})$.

Primer:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ imajo karakteristiko 0.

2. $\text{kar}(\mathbb{Z}_n) = n$
3. $\text{kar}(M_k(\mathbb{Z}_n)) = \text{kar}(\mathbb{Z}_n[X]) = n$
4. $\text{kar}(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$
5. $\text{kar}(k) = n \iff \forall x \in \mathcal{K}. nx = 0$

Lema 5. Karakteristika kolobarja brez deliteljev nič je bodisi 0 bodisi praštevilo.

Dokaz. Danimo da je $\text{kar}(\mathbb{K}) = n$. če velja $n = r * s \implies n * 1 = r * s * 1 = (r * 1) * (s * 1) \implies r * 1 = 0 \vee s * 1 = 0$, ker je po definiciji karakteristika najmanjše tako število, je $n = s \vee n = r \implies n$ je praštevilo. \square

Izrek 12:

Naj bo \mathcal{F} polje

1. Če velja $\text{kar}(\mathcal{F}) = 0$ lahko \mathcal{F} vložimo v \mathbb{Q}
2. Če velja $\text{kar}(\mathcal{F}) = p$ lahko \mathcal{F} vložimo v \mathbb{Z}_p

Dokaz. $\text{kar}(\mathcal{F}) = 0$, $\varphi : \mathbb{Q} \rightarrow \mathcal{F}, \frac{n}{m} \mapsto n * m^{-1}$ Brez težav preverimo, da je φ dobro definirana in homomorfizem, $\text{Ker}(\varphi) = \{0\}$, torej je res vložitev.

$\text{kar}(\mathcal{F}) = p$, $\varphi : \mathbb{Z}_p \rightarrow \mathcal{F}, k \mapsto k * 1 = (1 + 1 + \dots + 1)$

$\varphi(k) = 0 \iff k = 0$, saj $k < p = \text{kar}(\mathcal{F})$ torej je φ injektivna.

Preverimo še $\varphi(k * l) = \varphi(k) * \varphi(l)$, $\varphi(k)\varphi(l) = k * l = q * p + r, r < p = r$ Enako pa velja tudi v \mathbb{Z}_p , zato $\varphi(kl) = \varphi(r) = r$. \square

Polje \mathbb{Q} imenujemo **prapolje s karaktersitiko 0**, polje \mathbb{Z}_p pa **prapolje s karakteristiko p**.

Vidimo, da vsako polje s karakteristiko 0 'vsebuje' \mathbb{Q} (natančneje, vsebuje izomorfno kopijo \mathbb{Q}), vsako polje s karakteristiko p pa vsebuje \mathbb{Z}_p .

4 Kvocientne strukture

4.1 Odseki

Definicija 113: Naj bo \mathcal{H} podgrupa grupe \mathcal{G} in naj bo $a \in \mathcal{G}$. **Odsek** grupe \mathcal{G} po podgrupi \mathcal{H} je:

$$a\mathcal{H} := \{ah \mid h \in \mathcal{H}\} \quad (75)$$

Opomba: Če je \mathcal{G} aditivna grupa odsek pišemo kot $a + \mathcal{H} := \{a + h \mid h \in \mathcal{H}\}$

Opomba: Natančneje, $a\mathcal{H}$ je **levi odsek**, desni odsek definiramo na podoben način $\mathcal{H}a := \{ha \mid h \in \mathcal{H}\}$ in se obnaša podobno. Pri Algebri 2 bomo obravnavali zgolj leve odseke.

Če je $a \in \mathcal{H}$ velja $a\mathcal{H} = \mathcal{H}$, velja tudi obratno, če $a\mathcal{H} = a$ potem $a \in \mathcal{H}$ ($a\mathcal{H} = \mathcal{H} \iff a \in \mathcal{H}$).

Če $a \in \mathcal{G} - \mathcal{H}$, potem $a\mathcal{H}$ ni niti podgrupa (saj ne vsebuje niti enote).

Primer:1. $\mathcal{G} = \mathbb{Z}, \mathcal{H} = n\mathbb{Z}$

Odseki so: $0 + n\mathbb{Z} = n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$, elementi posameznih odsekov pa so števila, ki dajo pri deljenju z n enak ostanek. Tako je vseh odsekov n . S podobnim opisom smo se že srečali, le da smo $a + n\mathbb{Z}$ označili z $[a]$.

2. $\mathcal{G} = \mathbb{R}^2, \mathcal{H} = \text{abscisna os.}$

Vsi možni odseki so premice, vzporedne abscisni osi.

3. $\mathcal{G} = \mathbb{C}^* = \mathbb{C} - \{0\}, \mathcal{H} = \mathcal{S}^1$

Tukaj so odseki koncentrične krožnice.

4. $\mathcal{G} = \mathcal{S}_n, \mathcal{H} = \mathcal{A}_n$

$$\delta(\in \mathcal{S}_n)\mathcal{H} = \begin{cases} \mathcal{H} & ; \\ \text{vse lihe permutacije} & ; \delta \notin \mathcal{H} \end{cases}$$

Tu imamo le dva odseka lihe in sode permutacije.

Lema 6. Za poljubna $a, b \in \mathcal{G}$ velja:

$$a\mathcal{H} = b\mathcal{H} \iff a^{-1}b \in \mathcal{H}$$

Dokaz. \implies

$$a\mathcal{H} = b\mathcal{H}$$

$$b = b * 1 \in b\mathcal{H} = a\mathcal{H}, b = a * h_0 \text{ za nek } h_0 \in \mathcal{H}$$

$$a^{-1} * b = h_0 \in \mathcal{H}$$

 \Longleftarrow

$$a^{-1} * b = h_0 \in \mathcal{H}$$

$$b = a * h_0 \implies b * h = a * \underbrace{(h_0 * h)}_{\in \mathcal{H}} \in a\mathcal{H} \text{ Enako pokažemo tudi za vsebovanje v}$$

drugo smer. □

Hitro nas to spomni na karakterizacijo podgrupe: (30)

$$\mathcal{H} \text{ je podgrupa} \iff a^{-1}b \in \mathcal{H} \forall a, b \in \mathcal{H}$$

Pomembna razlika je v tem, da zdaj ta dva poljubna elementa nista element podgrupe ampak kar cele (nad)grupe \mathcal{G} .

Opomba: Za desne odseke se pogoj glasi: $\mathcal{H}a = \mathcal{H}b \iff ab^{-1} \in \mathcal{H}$ **Opomba:** Očitno za Abelove (komutativne) grupe vrstni red a in b ni pomemben**Opomba:** Za aditivne grupe se lema glasi:

$$a + \mathcal{H} = b + \mathcal{H} \iff b - a \in \mathcal{H}$$

Ideja, odseki se nam zdijo kot neke vrste ekvivalenčni razredi, poskusimo to tudi bolj algebraično utemeljiti.

Lema 7. Za poljubna $a, b \in \mathcal{G}$ sta odseka $a\mathcal{H}$ in $b\mathcal{H}$ bodisi enaka, bodisi sta si disjunktna.

Dokaz. Predpostavimo $a\mathcal{H} \cap b\mathcal{H} \neq \emptyset$ in naj velja $a * h_1 = b * h_2$ za neka $h_1, h_2 \in \mathcal{H}$, oboje z desne pomnožimo z h_2^{-1}

$$\underbrace{h_1 * h_2}_{\in \mathcal{H}} = a^{-1} * b$$

Vidimo, da $a \in \mathcal{H}$ leži v kakem odseku (namreč $a\mathcal{H}$). Različna odseka pa sta si disjunktna. \mathcal{G} je tako disjunktna unija svojih odsekov. Tako smo dobili particijo množice \mathcal{G} , torej je v ozadju neka ekvivalenčna relacija.

Iz leme prej(6) razberemo, da je ta ekvivalenčna relacija definirana kot :

$$a \sim b \iff a^{-1}b \in \mathcal{H}$$

□

4.2 Podgrupe edinke in kvocientne grupe

Spomnimo se $\mathcal{G} = \mathbb{Z}, \mathcal{H} = n\mathbb{Z}$, potem množica vseh odsekov

$$\{[a] = a + n\mathbb{Z}\}$$

postane grupa, če definiramo

$$[a] + [b] = [a + b] \text{ // Običajno seštevanje v } \mathbb{Z}$$

To bi seveda radi posplošili. tako lahko v novih oznakah napišemo

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

4.2.1 Definicija edinke in kvocientne grupe

Označimo podgrupo (namesto s \mathcal{H}) z \mathcal{N} . Na množico vseh odsekov

$$\mathcal{G}/\mathcal{N} := \{a\mathcal{N} \mid a \in \mathcal{G}\} \quad (76)$$

bi radi vpeljali operacijo, da dobimo grupo. Po izkušnji od prej se nam sam od sebe ponuja predpis:

$$a\mathcal{N} * b\mathcal{N} := (ab)\mathcal{N}$$

Vendar pa se pojavi problem dobre definiranosti.

Lema 8. Naj bo \mathcal{N} podgrupa grupe \mathcal{G} . Naslednja pogoja sta si ekvivalentna:

1. Za poljubne $a, b, a', b' \in \mathcal{G}$ velja $a\mathcal{N} = a'\mathcal{N} \wedge b\mathcal{N} = b'\mathcal{N} \implies (ab)\mathcal{N} = (a'b')\mathcal{N}$
2. $\forall a \in \mathcal{G} \text{ in } \forall n \in \mathcal{N} \implies ana^{-1} \in \mathcal{N}$

Dokaz. \implies Očitno iz premetavanja definicij

\Longleftarrow

Iz leme(6) lahko prvi pogoj zapišemo kot:

$$a^{-1}a' \in \mathcal{N} \wedge b^{-1}b' \in \mathcal{N} \implies b^{-1}a^{-1}a'b' \in \mathcal{N}$$

Definiramo si $n_1 = a^{-1}a', n_2 = b^{-1}b'$. Tako dobimo:

$$b^{-1}a^{-1}a'b' = b^{-1}n_1b' = \underbrace{b^{-1}n_1b}_{\in \mathcal{N}} \underbrace{b^{-1}b'}_{n_2 \in \mathcal{N}} \in \mathcal{N}$$

□

Definicija 114: Če podgrupa \mathcal{N} za poljuben $a \in \mathcal{G}$ zadošča pogoju

$$\forall a \in \mathcal{G} \wedge \forall n \in \mathcal{N} \implies ana^{-1} \in \mathcal{N}$$

jo imenujemo **podgrupa edinka** in to označimo z:

$$\mathcal{N} \triangleleft \mathcal{G}$$

Izrek 13:

Naj bo $\mathcal{N} \triangleleft \mathcal{G}$. Če v množico vseh odsekov \mathcal{G}/\mathcal{N} vpeljemo operacijo s predpisom $a\mathcal{N} * b\mathcal{N} := (ab)\mathcal{N}$, potem postane \mathcal{G}/\mathcal{N} grupe. Preslikava $\Pi(a) = a\mathcal{N}$ je epimorfizem grupe in $\text{Ker}(\Pi) = \mathcal{N}$

Dokaz. Po prejšnji lemi je ta operacija dobro definirana. Enota je očitno $\mathcal{N} = 1\mathcal{N}$, prav tako je inverz $(a\mathcal{N})^{-1} = a^{-1}\mathcal{N}$

Asociativnost preverimo s preprostim računom $(a\mathcal{N} * b\mathcal{N}) * c\mathcal{N} = ((ab)c)\mathcal{N} = (a(bc))\mathcal{N} = a\mathcal{N} * (b\mathcal{N} * c\mathcal{N})$

Prav tako je očitna surjektivnost in homomorfnost $((ab)\mathcal{N} = a\mathcal{N} * b\mathcal{N})$

$$a \in \text{Ker}(\Pi) \iff \Pi(a) = \mathcal{N} \iff a \in \mathcal{N}$$

□

Trditev 43: Podmnožica \mathcal{N} grupe \mathcal{G} je podgrupa edinka natanko tedaj, ko je \mathcal{N} jedro kakega homomorfizma iz \mathcal{G} v neko grupo.

Dokaz.

$$\implies : \mathcal{N} \text{ je edinka} \implies \mathcal{N} = \text{Ker}(\Pi)$$

\longleftarrow

$$\mathcal{N} := \text{Ker}(\varphi), \varphi: \mathcal{G} \rightarrow \mathcal{G}'$$

$$\text{Naj velja } n, m \in \mathcal{N}: \varphi(nm^{-1}) = \varphi(n)\varphi(m)^{-1} = 1 * 1^{-1} = 1 \implies nm^{-1} \in \mathcal{N}$$

$$\text{Preverimo, da za } a \in \mathcal{G} \text{ velja } ana^{-1} \in \mathcal{N}: \varphi(ana^{-1}) = \varphi(a) \underbrace{\varphi(n)}_{=1} \varphi(a)^{-1} = 1,$$

Torej je \mathcal{N} grupa edinka.

□

4.2.2 Produkti podgrup

Definicija 115:

Naj bosta $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$, njun produkt je

$$\mathcal{HK} := \{hk \mid h \in \mathcal{H}, k \in \mathcal{K}\} \quad (77)$$

Opomba:

Produkt podgrup v splošnem ni nujno podgrupa

Definicija 116:

Naj bosta $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$, njuna vsota je

$$\mathcal{H} + \mathcal{K} := \{h + k \mid h \in \mathcal{H}, k \in \mathcal{K}\} \quad (78)$$

Lema 9. Naj bo \mathcal{G} grupa:

1. Če sta $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$ in velja $\mathcal{HK} = \mathcal{KH}$ potem je ta množica podgrupa
2. Če je $\mathcal{H} \leq \mathcal{G}$ in $\mathcal{N} \triangleleft \mathcal{G}$ potem velja $\mathcal{NH} = \mathcal{NH} \leq \mathcal{G}$
3. Če velja $\mathcal{H}, \mathcal{K} \triangleleft \mathcal{G}$, potem $\mathcal{HK} = \mathcal{KH} \triangleleft \mathcal{G}$

Dokaz.

1. $\mathcal{HK} = \mathcal{KH}$. Pokazati moramo: $\forall k_1, k_2 \in \mathcal{K} \wedge \forall h_1, h_2 \in \mathcal{H}. (h_1 k_2)(h_2 k_2)^{-1} \in \mathcal{HK}$ (definicija podgrupe).
 $(h_1 k_2)(h_2 k_2)^{-1} = h_1 \underbrace{k_1 k_2^{-1}}_{k_3 \in \mathcal{K}} h_2^{-1} = h_1 \underbrace{k_3 h_1^{-1}}_{h_3 k_4 // (\mathcal{HK} = \mathcal{KH})} = \underbrace{(h_1 h_3)}_{\in \mathcal{H}} \underbrace{k_4}_{\in \mathcal{K}}$
2. Iz tega da je \mathcal{N} edinka vemo da velja $h\mathcal{N} = \mathcal{N}h \forall h \in \mathcal{H}$ torej seveda $\mathcal{HK} = \mathcal{KH}$.
3. Vemo da $\mathcal{MN} = \mathcal{NM} \leq \mathcal{G}$ torej $a(mn)a^{-1} = \underbrace{ama^{-1}}_{\in \mathcal{M}} \underbrace{ana^{-1}}_{\in \mathcal{N}} \in \mathcal{MN}$

□

Če je \mathcal{G} aditivna grupa in sta $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$ (in zato tudi grupi edinki) ne govorimo o produktu, pač pa o vsoti.

Opomba:

To je pogrupa \mathcal{G} .

Opomba:

1. Če velja $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$, potem velja tudi $\mathcal{H} \cap \mathcal{K} \leq \mathcal{G}$
2. Če velja $\mathcal{N}, \mathcal{M} \triangleleft \mathcal{G}$, je tudi $\mathcal{N} \cap \mathcal{M} \triangleleft \mathcal{G}$ (Seveda velja $\mathcal{N} \cap \mathcal{M} \subseteq \mathcal{N} \subseteq \mathcal{NM}$)

Za $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_r \leq \mathcal{G}$ definiramo produkt kot

$$\mathcal{H}_1 \dots \mathcal{H}_r = \{h_1, \dots, h_r \mid h_i \in \mathcal{H}_i\}$$

4.2.3 Podgrupe (edinke) kvocientne grupe

Pojavi se naravno vprašanje, kdaj so podgrupe edinke \mathcal{G}/\mathcal{N}

Prej pa se spomnimo definicij slike in praslike

$$f : \mathcal{X} \rightarrow \mathcal{Y} \quad \mathcal{X}_0 \subseteq \mathcal{X}, \mathcal{Y}_0 \subseteq \mathcal{Y}$$

$$f(\mathcal{X}_0) = \{f(x_0) \mid x_0 \in \mathcal{X}_0\}$$

$$f^{-1}(\mathcal{Y}_0) = \{x \in \mathcal{X} \mid f(x) \in \mathcal{Y}_0\}$$

Lema 10. Naj bo $\varphi : \mathcal{G} \rightarrow \mathcal{G}'$ homomorfizem grup.

1. Če je $\mathcal{H}' \leq \mathcal{G}'$ potem je tudi $\varphi^{-1}(\mathcal{H}') \leq \mathcal{G}$

2. Če je $\mathcal{N}' \triangleleft \mathcal{G}'$ potem je tudi $\varphi^{-1}(\mathcal{N}') \triangleleft \mathcal{G}$
3. Če je $\mathcal{H} \leq \mathcal{G}$ potem je tudi $\varphi(\mathcal{H}) \leq \mathcal{G}$
4. Če je $\mathcal{N} \triangleleft \mathcal{G}$ in je φ epimorfizem, je $\varphi(\mathcal{N}) \triangleleft \mathcal{G}'$

Dokaz.

1. $h_1, h_2 \in \varphi^{-1}(\mathcal{H}')$ Torej: $\varphi(h_1 h_2^{-1}) = \varphi(h_1) \varphi(h_2)^{-1} \in \mathcal{H}'$ Saj je \mathcal{H}' podgrupa.
2. Iz prve točke velja da je praslika edinke podgrupa. Pokažimo še $ana^{-1} \in \varphi^{-1}(\mathcal{N}')$ kar je enakovredno $\varphi(ana^{-1}) \in \mathcal{N}'$. $\varphi(ana^{-1}) = \varphi(a) \varphi(n) \varphi(a)^{-1} \in \mathcal{N}$ Saj je le ta edinka.
3. DOBI IZ VAJ.

□

Trditev 44: Če je $\mathcal{N} \leq \mathcal{H} \leq \mathcal{G}$ potem je $\mathcal{N} \triangleleft \mathcal{H}$, zato lahko tvorimo \mathcal{H}/\mathcal{N} in trdimo: $\mathcal{H}/\mathcal{N} \leq \mathcal{G}/\mathcal{N}$.

Dokaz. Dokažemo neposredno, ali pa uporabimo tretjo točko prejšnje leme za $\varphi = \Pi : \mathcal{G} \rightarrow \mathcal{G}/\mathcal{N}$ (Kanonični epimorfizem). □

Trditev 45: Če je $\mathcal{N} \leq \mathcal{M} \triangleleft \mathcal{G}$ potem velja $\mathcal{M}/\mathcal{N} \triangleleft \mathcal{G}/\mathcal{N}$

Dokaz. Dokažemo neposredno, ali pa uporabimo četrto točko prejšnje leme. □

Izrek 14:

Naj bo $\mathcal{N} \triangleleft \mathcal{G}$

1. Vsaka podgrupa \mathcal{G}/\mathcal{N} je oblike \mathcal{H}/\mathcal{N} za neko podgrupo $\mathcal{H} : \mathcal{N} \leq \mathcal{H} \leq \mathcal{G}$
2. Vsaka podgrupa edinka \mathcal{G}/\mathcal{N} je oblike \mathcal{M}/\mathcal{N} za neko edinko $\mathcal{M} : \mathcal{N} \leq \mathcal{M} \triangleleft \mathcal{G}$

Dokaz.

Naj bo $\mathcal{H}' \leq \mathcal{G}/\mathcal{N}$, Definirajmo $\mathcal{H} := \Pi^{-1}(\mathcal{H}')$, kjer je $\Pi : \mathcal{G} \rightarrow \mathcal{G}/\mathcal{N}$. Po prvi točki prejšnje leme je $\mathcal{H} \leq \mathcal{G}$, seveda pa vsebuje tudi \mathcal{N} . (za nek $n \in \mathcal{N}$, $\Pi(n) = n\mathcal{N} = \mathcal{N} \in \mathcal{H}'$, ker je \mathcal{N} enota grupe \mathcal{H}').

Ker je Π surjektivna velja $\Pi(\Pi^{-1}(\mathcal{H}')) = \mathcal{H}'$

Dokažemo na enak način, le da velja $\mathcal{N} := \Pi^{-1}(\mathcal{N}')$, Za vsebovanost pa namesto prve točke uporabimo drugo. □

Primer:

Kaj so podgrupe \mathbb{Z}_n ? Hitro opazimo, da za poljuben $k \in \mathbb{Z}$ velja $k\mathbb{Z}n = \{ka \mid a \in \mathbb{Z}_n\}$ je podgrupa \mathbb{Z}_n .

Recimo: $2\mathbb{Z}_4 = \{0, 2\}$ in $1\mathbb{Z}_4 = 3\mathbb{Z}_4 = \mathbb{Z}_4$

Prav tako vidimo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, podgrupe \mathbb{Z}_n so torej oblike $\mathcal{H}/n\mathbb{Z}$, kjer je $n\mathbb{Z} \leq \mathcal{H} \leq \mathbb{Z}$, kjer je \mathcal{H} oblike $k\mathbb{Z}$, $k \geq 0$.

Kdaj pa velja $n\mathbb{Z} \subseteq k\mathbb{Z}$, natanko tedaj, kadar $n|k$.

Edine podgrupe \mathbb{Z}_n so torej oblike :

$$k\mathbb{Z}/n\mathbb{Z}, n|k$$

4.3 Ideali in kvocientni kolobarji

4.3.1 Definicija ideala in kvocientnega kolobarja

Naj bo $\mathcal{I} \subseteq \mathcal{K}$ in naj bo \mathcal{I} podgrupa za seštevanje, kjer je \mathcal{K} kolobar. Množica

$$\mathcal{K}/\mathcal{I} := \{a + \mathcal{I} \mid a \in \mathcal{K}\}$$

postane aditivna grupa, če definiramo:

$$(a + \mathcal{I}) + (b + \mathcal{I}) = (a + b) + \mathcal{I}$$

Seveda nas normalno zanima, kaj moramo zahtevati, da bomo \mathcal{K}/\mathcal{I} lahko opremili z množenjem. Torej nas zanima, kdaj bo spodnja operacija dobro definirana:

$$(a + \mathcal{I}) * (b + \mathcal{I}) = (a * b) + \mathcal{I}$$

Lema 11. *Naj bo \mathcal{I} podgrupa za seštevanje kolobarja \mathcal{K} . Naslednja pogoja sta si ekvivalentna:*

- $\forall a, a', b, b' \in \mathcal{K}. (a + \mathcal{I} = a' + \mathcal{I} \wedge b + \mathcal{I} = b' + \mathcal{I}) \implies ab + \mathcal{I} = a'b' + \mathcal{I}$
- $\forall a \in \mathcal{K}, u \in \mathcal{I}. au \in \mathcal{I} \wedge ua \in \mathcal{I}$

Dokaz.

\implies Bralec bo brez težav to preveril sam

\longleftarrow

$$u := a' - a \in \mathcal{I}, v := b' - b \in \mathcal{I}$$

$$a'b' - ab = (a + u)(b + v) - ab = \underbrace{ub}_{\text{Po predpostavki } \in \mathcal{I}} + \underbrace{av + uv}_{\in \mathcal{I}} \in \mathcal{I}$$

□

Definicija 117: *Podgrupa za seštevanje \mathcal{I} kolobarja \mathcal{K} se imenuje ideal(kolobarja \mathcal{K}), če zadošča pogoju kateremukoli izmed pogojev iz prejšnje leme (pogoja sta si ekvivalentna). Označimo: $\mathcal{I} \triangleleft \mathcal{K}$*

Primer:

Ideali kolobarja \mathbb{Z} so $n\mathbb{Z}, n \geq 0$ (To so (edine) podgrupe za $+$, in hkrati ustrezajo zahtevam)

Izrek 15:

Naj bo $\mathcal{I} \triangleleft \mathcal{K}$. Če v množico cseh odsekov \mathcal{K}/\mathcal{I} vpeljemo seštevanje in množenje s predpisoma od prej, potem postane \mathcal{K}/\mathcal{I} kolobar.

Preslikava $\pi : \mathcal{K} \rightarrow \mathcal{K}/\mathcal{I}, \Pi(a) = a + \mathcal{I}$ je opimorfizem in njeno jedro je \mathcal{I} .

Dokaz. Zaradi leme je množenje dobro definirano, seštevanje prav tako.

Enote ostanje iste $(0, 1)$, distributivnost sledi iz originalne distributivnosti, homomorfizem in jedro preslikave pa iz preprostega premetavanja definicij. □

4.3.2 Izpustimo zaradi kolokvija**4.3.3 Izpustimo zaradi kolokvija****4.3.4 Izpustimo zaradi kolokvija****4.3.5 Kvocientni prostori in kvocientne algebre****Izrek 16:**

Naj bo \mathcal{U} podprotor vektorsksega protora \mathcal{V} na obsegu \mathcal{F} . Če v množico vseh odsekov

$$\mathcal{V}/\mathcal{U} := \{v + \mathcal{U} \mid v \in \mathcal{V}\}$$

vpeljemo seštevanje in množenje s skalarji na enak način kot pri grupah in kolobarjih glede na odseke, postane \mathcal{U}/\mathcal{V} vektorski prostor. Preslikava $\Pi : \mathcal{V} \rightarrow \mathcal{V}/\mathcal{U}, v \mapsto v + \mathcal{U}$ je homomorfizem in $\text{Ker}(\Pi) = \mathcal{U}$. \mathcal{U}/\mathcal{V} imenujemo kvocientni vektorski prostor, Π pa kvocientni epimorfizem.

Dokaz. Od prej vemo, da je $(\mathcal{V}/\mathcal{U}, +)$ aditivna grupa. Preverimo še dobro definirano ostalih stvari.

$$v + \mathcal{U} = v' + \mathcal{U} \implies \lambda(v + \mathcal{U}) = \lambda(v' + \mathcal{U})$$

ali ekvivalentno $v - v' \in \mathcal{U} \implies \lambda v - \lambda v' \in \mathcal{U}$, to je res, saj $\lambda v - \lambda v' = \lambda(v - v') \in \mathcal{U}$. \square

Opomba: Ideal algebre definiramo anako kot ideal kolobarja. Ideal algebre je avtomatsko tudi vektorski podprostor, saj velja $\lambda u = (\lambda * 1)u$, kar pa je v idealu.

Izrek 17:

Naj bo \mathcal{I} ideal algebre \mathcal{A} , če v množico vseh odsekov

$$\mathcal{A}/\mathcal{I} := \{a + \mathcal{I} \mid a \in \mathcal{A}\}$$

vpelejmo operacija na enak način kot pri vektorskih prostorih in kolobarju, postane \mathcal{A} algebra. Preslikava $\Pi : \mathcal{A} \rightarrow \mathcal{A}/\mathcal{I}, a \mapsto a + \mathcal{I}$ je homomorfizem in $\text{Ker}(\Pi) = \mathcal{I}$. \mathcal{A}/\mathcal{I} imenujemo kvocientna algebra, Π pa kvocientni epimorfizem.

4.4 Izrek o izomorfizmih

Ob prejšnjih definicijah se naravno vprašamo, kakšen je pomen homomorfizmov, ki niso bijektivni ali injektivni.

Izrek 18: Izrek o izomorfizmih

Naj bo $\varphi : \mathcal{A} \rightarrow \mathcal{A}'$ homomorfizem poljubne algebraične strukture (grup, kolobarjev, vektorskih prostorov, ali algebr), potem velja:

$$\mathcal{A}/\text{Ker}(\varphi) \cong \text{Im}(\varphi) \quad (79)$$

Dokazali bomo samo za grupe, za ostale strukture postopamo podobno.

Dokaz. Naj bosta $\mathcal{A}, \mathcal{A}'$ grupi. $\text{Ker}(\varphi)$ je edinka in zato ima kvocientna struktura smisel, $\text{Im}(\varphi)$ pa je grupa (kar podgrupa \mathcal{A}').

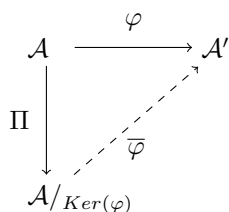
$$a\text{Ker}(\varphi) = a'\text{Ker}(\varphi) \iff a^{-1}a' \in \text{Ker}(\varphi) \iff \varphi(a^{-1}a') = 1 \iff \varphi(a)^{-1}\varphi(a') = 1 \iff \varphi(a) = \varphi(a')$$

Definirajmo novo preslikavo $\bar{\varphi} : \mathcal{A}/\text{Ker}(\varphi) \rightarrow \text{Im}\varphi, \bar{\varphi}(a\text{Ker}(\varphi)) := \varphi(a)$

Očitno je $\bar{\varphi}$ dobro definirana, injektivna ($\varphi(a) = \varphi(a') \implies a\text{Ker}(\varphi) = a'\text{Ker}(\varphi)$) in je surjektivna (slika na sliko φ).

Pokazati je treba še to, da je $\bar{\varphi}$ homomorfizem.

$$\bar{\varphi}(a\text{Ker}(\varphi)*b\text{Ker}(\varphi)) = \bar{\varphi}((ab)*\text{Ker}(\varphi)) = \varphi(ab) = \varphi(a)*\varphi(b) = \bar{\varphi}(a\text{Ker}(\varphi))*\bar{\varphi}(b\text{Ker}(\varphi)) \quad \square$$



Slika 3: Komutativni diagram, $\varphi = \bar{\varphi} \circ \Pi$

Opomba: Izrek nam da inducirano preslikavo $\bar{\varphi}$