Skripta za algebro 2

Filip Koprivec

16. junij 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

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

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

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

$$x, y \in \mathcal{S}.x \circ y = y \circ x \tag{2}$$

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

$$\forall x, y \in \mathcal{S}.x \circ y = y \circ x \tag{3}$$

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 na $\mathcal{S}$ in $e \in \mathcal{S}$. e se imenuje **nevtralni element**, če velja

$$\forall x \in \mathcal{S}. e \circ x = x \circ e = x \tag{4}$$

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.

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

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

$$e = f$$

□

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

$$\forall x \in \mathcal{S}. e' \circ x = x \tag{5}$$

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

$$\forall x \in \mathcal{S}. x \circ e'' = x \tag{6}$$

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

$$\forall t, t' \in \mathcal{T}. t \circ t' \in \mathcal{T} \tag{7}$$

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 $(K = \mathbb{R}, S = \mathbb{R}^n)$
$\lambda(x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$

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. $(\mathbb{N}, +)$, $\underbrace{(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), \ldots}_{Niso\ samo\ polgrupe\ ampak\ kar\ grupe}$

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:
$(x_1 \circ x_2) \circ (x_3 \circ x_4) = ((x_1 \circ x_2) \circ x_3) \circ x_4 = x_1 \circ (x_2(\circ x_3 \circ x_4)) = \ldots$
Trditev 3: Naj bo $(\mathcal{S}, \circ)$ polgrupa, $n \in \mathbb{N}$ in naj bo $x_1, x_2, \ldots, x_n \in \mathcal{S}$. Tedaj je za vsak n enakost izpolnjena na glede na postavitev oklepajev (izraz ima smisel, tudi kadar ne pišemo oklepajev).
$x_1 \circ x_2 \circ \cdots \circ x_n = (\ldots(x_1 \circ x_2) \circ \cdots \circ x_n) = x_1 \circ (x_2(\circ \cdots \circ x_n)\ldots) = \ldots$

Dokaz. Zgolj skica dokaza
Definirajmo: $x := x_1 \circ (x_2(\circ \cdots \circ x_n)\ldots)$ in
$y :=$ naj bo kombinacija elementov $x_1 \ldots x_n$, z drugače postavljenimi oklepaji

Indukcija na n:
$n \leq 3$: Očitno
Ker $n \leq 2$ velja $y = \underbrace{(u)}_{x_1,\ldots,x_k} \circ \underbrace{(v)}_{x_{k+1},\ldots,x_n}$ Iz $k < n$ sledi:
$y = (x_1 \circ w) \circ v \underbrace{=}_{Asociativnost(1)} x_1 \circ (w \circ v)$
Po I.P. ($w \circ v$ ima $n-1$ elementov): $x = x_1 \circ (x_2 \circ \cdots \circ x_n)$ □

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

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

$$x^n := \underbrace{x \circ x \circ \cdots \circ x}_{n\text{elementov}} \tag{8}$$

Opomba: Brez asociativnosti ni definirano niti x^3
Opomba:
Očitno velja:
$\forall n, m \in \mathbb{N}. x^n \circ x^m = x^{n+m}$ 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:

$$x \circ y = y \circ x = e \tag{9}$$

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

$$x \circ x^{-1} = x^{-1} \circ x = e \tag{10}$$

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

Opomba: Seveda velja za n elementov

$$(x_1 \circ x_2 \circ \cdots \circ x_n)^{-1} = x_n^{-1} \circ \cdots \circ x_2^{-1} \circ x_1^{-1} \tag{11}$$

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:

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

Definicija 17:

$$x^0 := e \tag{13}$$

Tako kadar je x **obrnljiv** veljata enačbi

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

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

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

$$x \circ y = x \circ z \implies y = z \tag{16}$$

In tudi

$$y \circ x = z \circ x \implies y = z \tag{17}$$

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 $* : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$, $(x, y) \mapsto xy$ 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 $\mathcal{S}^*$ označujemo množico vseh obrnljivih elementov monoida $\mathcal{S}$.

Trditev 7: Če je $\mathcal{S}$ monoid je $\mathcal{S}^*$ grupa.

Dokaz. $x, y \in \mathcal{S}^* \implies x \circ y \in \mathcal{S}^*$ // Obrnljiv je tudi njun produkt, torej je množica je zaprta za $*$
Ker je $*$ asociativen na $\mathcal{S}$ je asociativen tudi na $\mathcal{S}^*$
$e \in \mathcal{S}^*$ saj je enota inverz sami sebi
$x \in \mathcal{S}^* \implies x^{-1} \in \mathcal{S}^*$ // Inverz inverza je kar element sam □

Primer:
1. $(\mathbb{N} \cup \{0\}, +)$: $(\mathbb{N} \cup \{0\}, +)^* = 0$
2. $(\mathbb{Z}, +)$: $(\mathbb{Z}, +)^* = -1, 1$
3. $(\mathbb{Q}, *)$: $(\mathbb{Q}, *)^* = \mathbb{Q} - \{0\}$
Opomba: Grupam z enim elementom pravimo **trivialne** grupe.
4. $(F(\mathcal{X}), \circ)$: $(F(\mathcal{X}), \circ)^* = \{f : \mathcal{X} \to \mathcal{X} | f \text{ je bijekcija}\}$

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

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

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 $\{1, 2, \ldots, n\}$, njej pripadajočo grupo permutacij pa z

$$\mathcal{S}_n := Sim(\{1, 2, \ldots, n\}) \tag{19}$$

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

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

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

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.

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

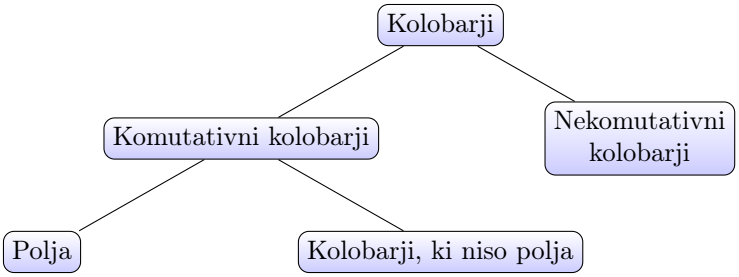
□

(e)

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

Sledi iz (b) če vzamemo $y = -1$

Kolobar K je **komutativen**, če za množenje velja zakon komutativnosti (3).



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

$$\{0\}$$

Trditev 9:

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

Dokaz.
$\Longrightarrow$: Očitno
$\Longleftarrow$: $\forall x \in \mathcal{K}.\ x = 1x = 0x = 0$ □

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

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

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

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

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

Opomba:

$$\mathcal{K} \text{ ima leve deljitelje niča} \iff \mathcal{K} \text{ ima deljitelje niča} \tag{22}$$

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 niča .

$\impliedby$: Očitno. □

V **Kolobarju brez deliteljev niča** velja:

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

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 **vsi 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(ali desni) delitelj niča.
Obsegi so zato kolobarji brez deliteljev niča.

Dokaz. x je obrnljiv: $xy = 0$
$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0$ Torej x ni delitelj niča. □

1.5 Vektorski prostori

Definicija 28: Naj bo $\mathcal{F}$ polje. Množica $\mathcal{V}$ skupaj z (notranjo) binarno operacijo seštevanje $+ : \mathcal{V}\times\mathcal{V} \to \mathcal{V}$ in zunanjo binarno operacijo $\mathcal{F}\times\mathcal{V} \to \mathcal{V}$ 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

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

V_3: Velja distributivnost v skalarnem faktorju

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

V_4: Velja zakon homogenosti

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

V_5: Enota

$$\forall v \in \mathcal{V}.\ 1v = v \tag{27}$$

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

$$(u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) \mapsto (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n) \tag{28}$$

Množenje s skalarjem

$$\lambda(u_1, u_2, \ldots, u_n) \mapsto (\lambda u_1, \lambda u_2, \ldots, \lambda u_n) \tag{29}$$

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 $\mathcal{F} \times \mathcal{A} \to \mathcal{A}$ (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:

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) \mapsto (x_1y_1, , x_2y_2, \ldots, x_ny_n) \tag{30}$$

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

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

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

(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:

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

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

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

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

konjugirana podgrupa podgrupe $\mathcal{H}$.

Dokaz.

$$chc^{-1}ch'c^{-1} = c\underbrace{hh'}_{\in\mathcal{H}}c^{-1} \in \mathcal{H}$$

$$(chc^{-1})^{-1} = (c^{-1})^{-1}h^{-1}c^{-1} = c\underbrace{h^{-1}}_{\in\mathcal{H}}c^{-1} \in \mathcal{H}$$

□

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

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

Dokaz.
$\implies$: Sledi iz definicije
$\impliedby$ Iz predpostavke sledi, da je $\mathcal{L}$ podgrupa za $+$.
Prav tako je $(\mathcal{L}, *)$ monoid
Izpolnjevanje distributivnih zakonov pa sledi iz tega da so izpolnjeni tudi na $\mathcal{K}$
Opomba: Uporabili smo trditev (11) in (ii) pogoj zamenjali z (iii) □

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

1.7.3 Podprostori

Definicija 33: Podmnožica $\mathcal{U}$ vektorskega prostora $\mathcal{V}$ je **podprostor** $\mathcal{V}$, če je za isti operaciji tudi sama vektorski prostor.

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

(i)

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

(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:

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

Torej je zaprta za seštevanje, množenje in množenje s skalarji

Dokaz. Enako kot za podkolobarje □

Primer:
1. $A = \mathcal{M}_2(\mathbb{R})$, $B = \{\begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} | a_{ij} \in \mathbb{R}\}$

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. $e^2 = e \implies e(\underbrace{1}_{enota\ \mathcal{E}} - e) = 0$ Ker v poljih ni deliteljev niča, velja $e = 1$.

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

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

Dokaz. Podobno kot prej

□

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

Dokaz.
$\Longrightarrow$
$\forall x \in \mathcal{F}.\ 0x = x$ 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 $< \mathcal{X} >$.
Če je $\mathcal{X} = \{y_1, y_2, \dots, y_n\}$ pišemo tudi $\mathcal{X} =< y_1, y_2, \dots, y_n >$.
Tako $< x, y >$ sestoji iz elementov kot so: $1, x, y, x^2, x^3, x^{-1}, x^{-2}, x^{-1}y, y^{-1}, x^5y^{-1}x^3y^{-3}xy^2, \dots$
Opazimo, da je $< \mathcal{X} >$ podgrupa

$$u, v \in < x > \implies uv \in < \mathcal{X} > \wedge u^{-1} \in < x >$$

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

Velja pa tudi obratno: vsaka podgrupa grupe $\mathcal{G}$, ki vsebuje $\mathcal{X}$ vsebuje tudi to podgrupo($< \mathcal{X} >$).
Torej je $< \mathcal{X} >$ najmanjša podgrupa, ki vsebuje $\mathcal{X}$. Pravimo ji **podgrupa, generirana z** $\mathcal{X}$.
Če velja $< \mathcal{X} >= \mathcal{G}$, 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: $< \mathbb{N} >= \mathbb{Q}^+$
2. $< 2, 3 >= \{2^i 3^j | i, j \in \mathbb{Z}\}$

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

Primer:
1. Grupa $(\mathbb{Z}, +)$ je generirana z $< 1 >$ in prav tako tudi z $< -1 >$. Velja $\mathbb{Z} =< 1 >=< -1 >$.

Opomba: Grupe generirane z enim samim elementom imenujemo **ciklične**.($< 2 >=< 4, 6 >= 2\mathbb{Z}$)
Cilj je poiskati najmanjše množice generatorjev(očitno $< \mathcal{G} >= \mathcal{G}$).

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

- $\overline{\{1\}} = \mathbb{Z}$
- $\overline{\{i\}} = \{n + mi | n, m \in \mathbb{Z}\} = \mathbb{Z}[i]$ (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

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

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

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

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

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

$$\{uv^{-1} | u, v \in \overline{\mathcal{X}} \wedge v \neq 0\} \tag{39}$$

Opomba: Podkolobar $\overline{\mathcal{X}}$ generiran z $\mathcal{X}$ ni nujno polje.
Očitno vsako podpolje, ki $\mathcal{X}$ vsebuje, vsebuje tudi podpolje generirano z $\mathcal{X}$, toda zakaj ta množica je podpolje?.
Pomembno je dokazati, da je podgrupa za seštevaje (zaprtost za množenje, inverz, in 1 so očitne) **Trditev 18:**

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

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

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

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 $\mathcal{G}_1, \ldots, \mathcal{G}_n$ grupe. Grupi

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

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.

$$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) := (x_1y_1, x_2y_2, \ldots, x_ny_n)$$

Očitno:

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

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

1.9.2 Direktni produkti kolobarjev

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

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

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.

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

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

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

1.9.3 Direktna vsota vektorskih prostorov

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

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

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

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

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

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

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

1.9.4 Direktni produkt algebr

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

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

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.

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

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

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

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 $\mathbb{R} \times \mathbb{R} \times \ldots$.
Operacije po komponentah točno sovpadajo z operacijami po komponentah za zaporedja. To je torej algebra realnih zaporedij.
2. Naj bodo $\mathcal{F}_1, \ldots, \mathcal{F}_n$ polja nad ne nujno istimi kolobarji. Definiramo operacije po komponentah in opazimo, da za $n \geq 2$ ima direktni produkt(polj ali kolobarjev) delitelje niča.

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

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.
Z indukcijo na n: $n = 1$: $1 \notin \mathbb{N}$
$n \implies n+1$: $1 \notin \mathbb{N}, 2 \notin \mathbb{N}, \ldots, n \notin \mathbb{N} \underbrace{\implies}_{\text{Ker nima najmanjšega elementa}} n+1 \notin \mathbb{N}$ □

Po indukciji isto velja tudi za $\mathbb{N} \cup \{0\}$, $\mathbb{N} \cup \{0, -1\}$, $\mathbb{N} \cup \{0, -1, -2\}$ ...
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 $\mathcal{S} = \emptyset$ ✓ $\mathcal{S}$ 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. $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$ // $n \in \mathbb{Z}$ 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
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.
$\Longrightarrow$
Sledi iz izreka o obstoju največjega skupnega delitelja (3)
$\Longleftarrow$
$c|m \wedge c|n \implies c|1$ Torej je njun največji skupni delitelj 1 in sta si tuji. □

Opomba: Splošneje lahko definiramo največji skupni delitelj števil $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ na enak način ter njegovo eksistenco dokažemo na enak način ($d = n_1x_1 + n_2x_2 + \ldots n_kx_k$). 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:*

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

Dokaz. Predpostavimo, da $p \nmid m$.
$gcd(p, m) = 1 \implies 1 = px + my \implies n = pxn + \underbrace{mn}_{pz} y = p(xn + zy)$
Podobno za drugo možnost. □

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:
$n = 2$ ✓
$n - 1 \implies n$
Če je n praštevilo je dokaz zaključen. Če ni, ima vsaj dva delitelja ki nista 1 ali p (lahko sta enaka).
$n = kl;\ l, k < n$
Po indukcijski predpostavki sta l in k produkta praštevil, torej je tudi p produkt praštevil.
In še edinost zapisa:

$n = p_1 * p_2 * \cdots * p_r = q_1 * q_2 * \cdots * q_s$, produkt samih praštevil
$p_1 | q_1 * q_2 * \cdots * q_s$ torej po lemi (1) deli natančno enega izmed faktorjev q_i. Brez škode za splošnost: $p_1 | q_1 \underbrace{\implies}_{\text{ker sta praštevili}} p_1 = q_1$ Krajšamo s p_1 in nadaljujemo dokler ne pridemo do $1 = 1$.
Če pa imamo $s > r \implies q_{r+1} \dots q_s = 1$, kar pa je protislovje. □

Izrek 5:
Množica praštevil je neskončna.

Dokaz. Predpostavimo, da jih je končno, torej da so $p_1, p_2, \dots, p_n$ vsa praštevila. Tedaj $p_1 * p_2 * \cdots * p_n + 1$ ni praštevilo in je zato gotovo deljivo z nekim praštevilom p_i.
$p_1 * p_2 * \cdots * p_n + 1 = k * p_i \implies p_i(k - p_1 * p_2 * \cdots * p_{i-1} * p_{i+1} * \cdots * p_n) = 1$, protislovje. □

2.2 Grupa in kolobar ostankov

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

$$n | (a - b)$$

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

Lema 2.

$a \equiv a' \ (mod\ n) \wedge b \equiv b' \ (mod\ n) \implies a + b \equiv a' + b' \ (mod\ n) \wedge ab \equiv a'b' \ (mod\ n)$

Dokaz.

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

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

□

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

Dokaz.
Refleksivna: ✓
Simetrična: ✓
Tranzitivna:
$a \equiv b \pmod{n}$ in $b \equiv c \pmod{n} \implies c - a = \underbrace{(c - b) + (b - a)}_{\text{sta si kongruentna}}$ □

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

Definicija 53: Ekvivalenčni razredi kongurgento z n so:

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

in jih označimo z $\mathbb{Z}_n$.

Potrebno je preveriti še dobro definiranost operacij.

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

$$[a] + [b] := [a + b] \tag{41}$$

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:

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

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:

$$[a] * [b] := [a * b] \tag{42}$$

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 $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, 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 niča. 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 niča 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 $f : \mathcal{K} \to \mathcal{K}, f(x) = ax$. Potrebno je pokazati, da $1 \in \mathcal{Z}_f$
Dokazali bomo kar surjektivnost f, kar je v končnem polju ekvivalentno njeni injektivnosti.
$ax = ax \underbrace{\implies}_{\text{cel kolobar}} x = y$ torej $a(x-y) = 0 \wedge a \neq 0 \implies x = y$
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 niča.
$a, b \in \mathbb{Z}_p, ab = 0$. Torej je v običajnem produktu ab večkratnik p, zato po lemi(1) p deli vsaj eno, ker pa $a, b \in \{0, 1, \ldots, p-1\}$ 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

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

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:

$$i^2 = j^2 = k^2 = ijk = -1 \tag{44}$$

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:

$$\overline{h} := \lambda_0 - \lambda_1 i - \lambda_2 j - \lambda_3 k \tag{45}$$

Trditev 25: Vsak neničelen kvaternion je obrnljiv in zanj velja

$$h^{-1} = \frac{\overline{h}}{h\overline{h}} \tag{46}$$

Dokaz. Izračunamo:
$h\overline{h} = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2$
$h \neq 0 \implies h\overline{h} \in \mathbb{R} - \{0\}$, zato je vsak neničelen kvaternion obrnljiv in velja

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

□

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:

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

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

$$e^2 = e \tag{48}$$

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

$$\exists n \in \mathbb{N}.\ a^n = 0 \tag{49}$$

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

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

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

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

Dokaz. Račun. □

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 $\mathcal{K} = \{f : \mathcal{X} \to \mathbb{R}\}$

$\mathcal{K}$ 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 $\mathcal{C}(x) = \{f : \mathcal{X} \to \mathcal{R} | \ f \text{ zvezna}\}$. 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 niča).
- ...

Če v te kolobarje vpeljemo še množenje s skalarji:

$$(\lambda f)(x) = \lambda f(x) \tag{50}$$

postanejo vsi ti kolobarji tudi algebre.

Na podoben način vpeljemo tudi kolobar (algebro) zaporedij $\mathcal{X} = \mathbb{N} \to \mathcal{A}$, 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:

$$p(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, \ a_n \neq 0 \tag{51}$$

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

- a_0 imenujemo **prosti (ali konstantni) člen**

- a_n (zadnji neničelen 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

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

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

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

Definicija 63: Množenje polinomov

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

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

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

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 niča, 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

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

Tako vsak polinom $F(X)$ porodi **polinomsko funkcijo**

$$x \mapsto f(x)$$

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

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

porodi funkcijo $\mathbb{Z}_2 \to \mathbb{Z}_2$, 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 polinomsko 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:

$$(\lambda f)(X) := \lambda a_0 + \lambda a_1 X + \lambda a_2 X^2 + \cdots + \lambda a_n X^n \tag{57}$$

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 sestavljenih 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 :

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

Po dogovoru oklepaje izpuščamo in pišemo kar

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

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 algebraični 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

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

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).

$$sgn(\sigma\rho) = sgn(\sigma)sgn(\rho)$$

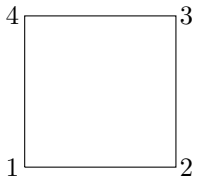
Sode permutacije tvorijo podgrupo. To podgrupo imenujemo **alternirajoča podgrupa** in jo označimo z A_n.

Definicija 73: Permutacijo oblike: $i_{j_1} \mapsto i_{j_2}, i_{j_2} \mapsto i_{j_3}, \ldots, i_{j_{k-1}} \mapsto i_{j_k}$ imenujemo $k-$cikel in ga označimo z $(i_{j_1}, i_{j_2}, \ldots, i_{j_k})$ (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



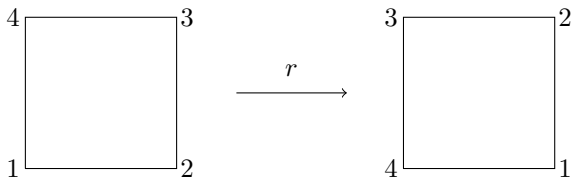
Definicija 75: Simetrija kvadrata je ustrezna permutacija oglišč.

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.

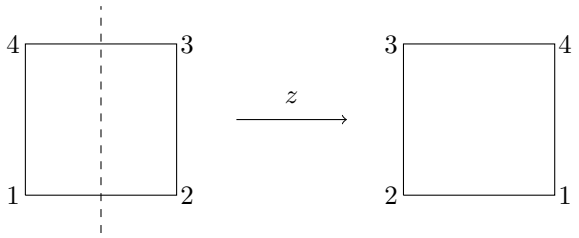
Primer:
1. Naj bo r rotacija kvadrata za $\frac{\pi}{2}$ v pozitivni smeri (v nasprotni smeri urinega kazalca). Ustreza ji cikel $(1, 2, 3, 4)$.



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.

$$\mathcal{D}_{2n} := \{1, r, r^2, \ldots, r^{n-1}, z, zr, zr^2, \ldots, zr^{n-1}\} \tag{58}$$

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

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

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, ki ga prav tako tudi zrcalimo/rotiramo, predstavljamo v ravnini. Če je n sod, 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 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. Ko $n \to \infty$, dobimo $\mathcal{GL}(\mathbb{Z})$.

2.10 Linearne grupe

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

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

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

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

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

Definicija 78:
Naj bo $n \in \mathbb{N}$ in $\mathcal{F}$ polje. **Specialna linearna grupa** je

$$\mathcal{SL}_n(\mathcal{F}) := \{\mathcal{A} \in \mathcal{M}_n(\mathcal{F}) |\ det(\mathcal{A}) = 1\} \tag{60}$$

Definicija 79:
Naj bo $n \in \mathbb{N}$ in $\mathcal{F}$ polje. **Ortogonalna (linearna) grupa** je

$$\mathcal{O}_n(\mathcal{F}) := \{\mathcal{A} \in \mathcal{M}_n(\mathcal{F}) |\ \mathcal{A}\mathcal{A}^t = \mathcal{A}^t\mathcal{A} = \mathcal{I}\} \tag{61}$$

Definicija 80:
Naj bo $n \in \mathbb{N}$. **Unitarna (linearna) grupa** je

$$\mathcal{U}_n(\mathbb{C}) := \{\mathcal{A} \in \mathcal{M}_n(\mathbb{C}) |\ \mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \mathcal{I}\} \tag{62}$$

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

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

$$\mathcal{SO}_n(\mathcal{F}) := \{\mathcal{A} \in \mathcal{O}_n(\mathbb{C}) |\ det(\mathcal{A}) = 1\} \tag{63}$$

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

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

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

$$\mathcal{S}p_n(\mathcal{F}) := \{\mathcal{A} \in \mathcal{M}_{2n}(\mathcal{F}) |\ \mathcal{A}\mathcal{J}\mathcal{A}^t = \mathcal{A}^t\mathcal{J}\mathcal{A} = \mathcal{I}\} \tag{65}$$

Kjer je

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

3 Homomorfizmi

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 si **izomorfni**, če obstaja taka bijektivna preslikava $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$, da velja:

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

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'.
Bodi $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ izomorfizem, tedaj $\mathcal{G}_2 = \{\varphi(g_1), \varphi(g_2), \ldots, \varphi(g_n)\}, g_i \in \mathcal{G}_1$.
Torej se g_i in $\varphi(g_i)$ v tablah pojavita na istem mestu.

Primer:

Tabeli se nam zdita sumljivo podobni $0 \sim 1, 1 \sim i, 2 \sim -1, 3 \sim -i$, saj omenjeni elementi v tabelah nastopajo na istih mestih.
V splošnem si sedaj poglejmo grupi $(\mathbb{Z}_n, +)$ in $\mathcal{U}_n := \{z \in \mathbb{C} |\ z^n = 1\} = \underbrace{\{1, a, a^2, \ldots, a^{n-1}\}}_{a=cos(\frac{2\pi}{n})+isin(\frac{2\pi}{n})}$ Vidimo:

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

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

V tem zapisu prepoznamo seštevanje v $\mathbb{Z}_n$

Trditev 30:

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

Dokaz.

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

$$\varphi : z_i \mapsto i$$

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

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

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

Primer:
1. $\mathcal{G} \cong \mathcal{G}$; izomorfizem je identiteta
2. $(\mathbb{R}, +) \cong (\mathbb{R}_+, *)$, kjer $\varphi : x \mapsto e^x$
3. $(\mathbb{Z}, +) \cong (n\mathbb{Z}, +)$, kjer $\varphi : x \mapsto nx$, kar 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 $\mathcal{G} =< a >$
Primer:
1. $< a >= \{a^n |\ n \in \mathbb{Z}\}$ za množenje
2. $< a >= \{na |\ n \in \mathbb{Z}\}$ za seštevanje
3. $< 1 >=< -1 >= (\mathbb{Z}, +)$
4. $< 1 >= (\mathbb{Z}_n, +)$
5. $< i >=< -i >= \{1, i, -1, -i\} = \mathcal{U}_4$

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: $\varphi : \mathbb{Z} \to \mathcal{G}, n \mapsto a^n$, ki je po predpostavki injektivna, očitno pa je tudi surjektivna, saj a^n generira grupo. Prav tako velja:
$\varphi(n+m) = \underbrace{a^{n+m} = a^n * a^m}_{(14)} = \varphi(n) * \varphi(m)$ 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 naravno število z lastnostjo $a^n = 1, a^k \neq 1, 0 < k < n$
Očitno so si elementi $1, a, a^2, \ldots a^{n-1}$ 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. □

Posledica: Naj bo $\mathcal{G}$ poljubna grupa, tedaj vsak element generira ciklično podgrupo ($< a >= \{a^n |\ n \in \mathbb{Z}\}$).

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: $red(a) = | < a > |$

Dokaz. $red(a) = n \iff a^n = 1 \wedge a^k \neq 1, 1 \leq k < n$
$< a >= \{1, a, a^2, \ldots, a^{n-1}\} \iff | < a > | = n$ □

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 $\varphi : \mathcal{V} \to \mathcal{V}'$. 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: $\{b_1, b_2, \ldots, b_n\}$.
Naj bo $\lambda_1\varphi(b_1) + \cdots + \lambda_n\varphi(b_n) = 0$ za neke $\lambda_i \in \mathcal{F}$
Ker je φ linearna in injektivna velja:
$Ker(A) = \{0\}$ in ker velja: $\varphi(\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n) = 0$
iz tega sledi: $\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n$ v jedru.
Torej velja $\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n = 0$

Ker so bazni vektorji linearno neodvisni, so vsi skalarji ničelni: $\lambda_i = 0$.
Tako smo dobili linearno neodvisne vektorje. Pokazati moramo še, da so tudi ogrodje.
Ker je φ surjektivna, velja: $v' \in \mathcal{V}' = \varphi(v)$ za poljuben v'.
$v' = \lambda_1\varphi(b_1) + \cdots + \lambda_n\varphi(b_n)$, vidimo da ima $\mathcal{V}'$ linearno ogrodje z močjo n $(\varphi(b_1), \ldots, \varphi(b_n))$.
Dobili smo ogrodje linearno neodvisnih vektorjev, ki je torej baza z močjo n.
Dimenzija $\mathcal{V}'$ je torej n, kar je enako dimenziji $\mathcal{V}$.
$\impliedby$
Vzemimo $\{b_1, b_2, \ldots, b_n\}$ za bazo $\mathcal{V}$ in $\{b'_1, b'_2, \ldots, b'_n\}$ za bazo $\mathcal{V}'$.
Definirajmo:
$\varphi(\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n) = \lambda_1 b'_1 + \lambda_2 b'_2 + \cdots + \lambda_n b'_n$
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. $\varphi : \mathcal{G} \to \mathcal{G}_1$ je homomorfizem grup, če velja:

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

Opomba: Če je grupa aditivna, operacijo smiselno spremenimo.

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

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

Ker smo pri definiciji kolobarja zahtevali tudi enoto, potrebujemo dodaten pogoj:

$$\varphi(1) = 1$$

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

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

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

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

Primer:
$\varphi : \mathbb{R} \to \mathcal{M}_2(\mathbb{R}), \varphi(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ **ni** homomorfizem, čeprav ustreza pogojem glede operacij, saj enote ne slika v enoto.
Opomba: Kadar je iz konteksta razvidno, za homomorfizem katerih struktur gre, govorimo le o homomorfizmu (izpuščamo grup, kolobarjev, itd.).

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

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: Avtomorfizem je bijektivni endomorfizem (izomorfizem strukture same vase).

Opomba: Homomorfizmom vektorskih prostorov 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 $\mathcal{K}[X] : a \mapsto a+0X+0X^2+\ldots$ 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: $\varphi : \mathcal{G} \to \mathcal{G}_1$ in $\psi : \mathcal{G}_1 \to \mathcal{G}_2$ homomorfizma grup, tedaj velja:
$(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)$ □

Trditev 34: Inverz izomorfizma je izomorfizem.

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

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 preveriti le aksiome za grupo:
Zaprtost: 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 obrnljivih linearnih preslikav iz $\mathcal{F}^n \to \mathcal{F}^n$ = grupa avtomorfizmov vektorskega prostora $\mathcal{F}^n$.

Trditev 36:Če je $\varphi : \mathcal{G} \to \mathcal{G}_1$ 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 $\varphi : \mathcal{G} \to \mathcal{G}_1$ 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 $\varphi : \mathcal{A} \to \mathcal{A}_1$ pravimo **slika** φ in jo označimo z $Im(\varphi)$.

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

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.
$\varphi(x)\varphi(y) = \varphi(xy) \in Im(\varphi)$
$\varphi(x)^{-1} = \varphi(x^{-1}) \in Im(\varphi)$ □

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

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

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

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 $\varphi : \mathcal{A} \to \mathcal{A}_1$ je injektiven natanko tedaj, ko je njegovo jedro trivialno.

Dokaz. Dokažemo zgolj za grupe, za ostale strukture so dokazi podobni.
$\Longrightarrow$
Naj velja: φ je injektivna, $x \in Ker(\varphi)$
$\varphi(x) = 1 = \varphi(1)$ od tod zaradi injektivnosti φ sledi: $x = 1$
$\Longleftarrow$
Naj velja $Ker(\varphi) = \{1\}$ in $\varphi(x) = \varphi(y)$
$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = 1$, torej: $xy^{-1} \in Ker(\varphi) = \{1\}$, 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 $\varphi : \mathbb{C} - \{0\} \to \mathbb{R}^+, \varphi(w) = |w|$, očitno je φ epimorfizem ($|zw| = |z||w|$)
   $Ker(\varphi) = \mathcal{S}^1 = \{z \in \mathbb{C} |\ |z| = 1\}$

3. $\varphi : (\mathbb{R}, +) \to (\mathcal{S}^1, *), \varphi(x) = cos(x) + isin(x)$, $Ker(\varphi) = \{2k\pi |\ k \in \mathbb{Z}\}$

4. $sgn : \mathcal{S}_n \to (\{-1, 1\}, *), sgn(\sigma\rho) = sgn(\sigma)sgn(\rho)$, $Ker(sgn) = \mathcal{A}_n$

5. $det : Gl(n, \mathcal{F}) \to \mathcal{F}^*$ je epimorfizem, $Ker(det) = Sl(n, \mathcal{F})$

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

Dokaz, da je to res avtomorfizem je trivialen:
$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$
$Ker(\varphi_a) = \{x \in \mathcal{G} |\ axa^{-1} = 1\} = \{1\}$
$Im(\varphi_a) = \mathcal{G}$, 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: $Aut(\mathcal{G})$ je množica vseh avtomorfizmov grupe $\mathcal{G}$

Opomba: Preveriti da je to grupa je trivialno
$\Phi : \mathcal{G} \to Aut(\mathcal{G}), \Phi(a) = \varphi_a$
Preverimo dobro definiranost:
$\varphi_a \circ \varphi_b(x) = abxb^{-1}a^{-1} = \varphi_{ab}$ 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:$Inn(\mathcal{G})$ je grupa vseh notranjih avtomorfizmov grupe $\mathcal{G}$

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

3.4.2 Primeri homomorfizmov kolobarjev in algeber

Definicija 105: Naj bo $\mathcal{K}$ poljuben kolobar. Za poljuben obrnljiv $a \in \mathcal{K}$ je $\varphi_a : \mathcal{K} \to \mathcal{K}, \varphi_a(x) = axa^{-1}$ 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 :

$$End_{\mathcal{F}}(\mathcal{V}) = \{f : \mathcal{V} \to \mathcal{V} | f \text{ je linearna (je endomorfizem)}\} \tag{73}$$

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

1. $\varphi : \mathbb{Z}_2 \to \mathbb{Z}, \varphi(x) = x$ **ni** homomorfizem. Veljajo sicer skoraj vse lastnosti, a se zatakne pri $0 = \varphi(1+1) \neq \varphi(1) + \varphi(1) = 2$
2. V nasprotni smeri zadeva deluje; $\varphi : \mathbb{Z} \to \mathbb{Z}_2$
   $\varphi(x) = \begin{cases} 0 & ; n \text{ sod} \\ 1 & ; n \text{ lih} \end{cases}$, očitno $\varphi(n+m) = \varphi(n) + \varphi(m)$, $Ker(\varphi) = 2\mathbb{Z}$

3. $\mathcal{K}$ vložimo v $\mathcal{K}[X]$ $(a \mapsto a + 0X + 0X^2 \dots)$
   $\varphi : \mathcal{K}[X] \to \mathcal{K}, \varphi(a_0 + a_1X + \dots) = a_0$, očitno $\varphi(f+g) = \varphi(f) + \varphi(g)$ in $\varphi(f * g) = \varphi(f) * \varphi(g)$
   $Ker(\varphi) = \{a_1X + a_2X^2 + \dots + a_nX^n\}$, velja tudi $\varphi(f(X)) = f(0)$.
   Opomba: Če je $\mathcal{K}$ komutativen, je za poljuben x $\varphi : \mathcal{K}[X] \to \mathcal{K}, \varphi(f(X)) = f(x)$ homomorfizem.

4. Naj bo $f \in C[0,1]$. Za poljuben $x \in [0,1]$ je $\varphi_x : C[0,1] \to \mathbb{R}, f \mapsto f(x)$ homomorfizem. $Ker(\varphi_x) = \{f \in C[0,1] | f(x) = 0\}$

5. $\varphi : End_{\mathcal{F}}(\mathcal{V}) \to M_n(\mathcal{F}), \varphi(f) = [f]$, kjer je $[f]$ matrika, ki pripada f glede na vnaprej izbrano bazo. φ je izomorfizem algeber. Torej velja $End_{\mathcal{F}}(\mathcal{V}) \cong M_n(\mathcal{F})$.

6. Primeri posebnih izomorfizmov

   (a) $\mathcal{K}_1 = \{\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in \mathbb{R}\}$; kaj hitro lahko preverimo, da je to kolobar. Da velja $\mathcal{K}_1 \cong \mathbb{R}$, vzemimo $\varphi(x) = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} = xI$, ki ustreza vsem zahtevam.

   (b) $\mathcal{K}_2 = \{\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in \mathbb{R}\}$; podobno kot prej brez težav preverimo, da je kolobar. Velja tudi $\mathcal{K}_2 \cong \mathbb{R} \times \mathbb{R}$ (enak direktnemu produktu $\mathbb{R}$ s samim seboj), kar preverimo s $\varphi((x,y)) = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$.

   (c) $\mathcal{K}_3 = \{\begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mid x, y \in \mathbb{R}\}$; velja $\mathcal{K}_3 \cong \mathbb{C}$. Izomorfizem $\varphi(x + yi) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$

   (d) $\mathcal{K}_4 = \{\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid w, z \in \mathbb{C}\}$; na pogled se nam zdi podoben $\mathbb{H}$, saj je prav tako kot v kvaternionih vsak neničelen element obrnljiv in je tako kot $\mathbb{H}$ 4-razsežna algebra nad $\mathbb{R}$. Res, 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. $Sim(\mathcal{X})$ je simetrična grupa množice $\mathcal{X}$, torej 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 $l_a : \mathcal{G} \to \mathcal{G}, l_a(x) = ax$. Preveriti moramo, da velja $l_a \in Sim(\mathcal{G})$.
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 $\varphi : \mathcal{G} \to Sim(\mathcal{G}), \varphi(a) = l_a$ in preverimo, da je φ vložitev.
$l_{ab}(x) = (ab)x = a(bx) = l_a(l_b(x)) = l_a * l_b(x) \implies l_{ab} = l_a * l_b$
Preverimo še, da ima φ trivialno jedro: $a \in Ker(\varphi) \implies l_a = id_{\mathcal{G}} \implies \forall x \in \mathcal{G}.\ ax = x \implies a = 1$
Torej je φ vložitev. □

Opomba: Iz dokaza opazimo, da lahko $\mathcal{G}$ vložimo v $Sim(\mathcal{G})$, kjer $\mathcal{G}$ gledamo zgolj kot množico.
Zanima nas, ali lahko grupo $\mathcal{G}$ vložimo v $Sim(\mathcal{X})$ za kako bolj posrečeno množico $\mathcal{X}$ (npr. če je $\mathcal{G}$ že sama simetrična grupa)
Velja: $\mathcal{G}$ končna $\implies Sim(\mathcal{G})$ končna, torej $Sim(\mathcal{G}) = S_n$.
Posledica: Vsako končno grupo lahko vložimo v S_n za nek $n \in \mathbb{N}$.
Našli smo injektivni homomorfizem iz $\mathcal{G}$ v $Sim(\mathcal{X})$ (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 $\varphi : \mathcal{G} \times \mathcal{X} \to \mathcal{X}, \varphi(a, x) = ax$, 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 $Sim(\mathcal{X})$ in obratno.

Dokaz. $\implies$
Imejmo delovanje $\mathcal{G}$ na $\mathcal{X}$. Priredimo mu homomorfizem $\varphi : \mathcal{G} \to Sim(\mathcal{X})$, kjer je $\varphi(a)$ permutacija definirana kot: $\varphi(a)(x) = ax$. Bralec lahko sam preveri, da je $\varphi(a)$ res permutacija in homomorfizem.
$\impliedby$
Homomorfizmu $\varphi(a) : \mathcal{G} \to Sim(\mathcal{X})$ priredimo delovanje $(a, x) \mapsto \varphi(a)(x)$ □

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 ($End(\mathcal{M})$) postane kolobar, 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 $End(\mathcal{K})$, kjer bomo na drugi $\mathcal{K}$ gledali le še kot na aditivno grupo.
Definiramo $\varphi : \mathcal{K} \to End(\mathcal{K}), \varphi(a) = l_a$, kjer je $l_a : \mathcal{K} \to \mathcal{K}$ 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. □

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 $* : \mathcal{K} \times \mathcal{M} \to \mathcal{M}, (a, m) \mapsto am$ za katero velja.

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

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

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

(d) $1 * m = m$

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 $End(\mathcal{M})$ podan s preslikavo $\varphi(a)(m) = am$ in obratno, vsak homomorfizem $\varphi : \mathcal{K} \to End(\mathcal{M})$ porodi modul $a * m = \varphi(a)(m)$

Dokaz. Enako kot prej. □

3.5.3 Vložitev algebre v algebro endomorfizmov vektorskega prostora

Naj bo $\mathcal{V}$ vektorski prostor nad poljem $\mathcal{F}$ in naj bo $End_{\mathcal{F}}(\mathcal{V})$ množica vseh linearnih preslikav iz $\mathcal{V}$ v $\mathcal{V}$. Ta množica postane algebra, če definiramo operacije na običajen način.
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 $End_{\mathcal{F}}(\mathcal{A})$ končno razsežna in zato velja $End_{\mathcal{F}}(\mathcal{A}) \cong \mathcal{M}_n(\mathcal{F})$.

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: $sl(AB - BA) = 0 \neq 1 = sl(I)$.

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 $\mathcal{K}$ nekaj značilnosti:

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

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. Rutinski račun prepuščamo bralcu. □

Izrek 11:
Če v množico vseh ekvivalenčnih razredov

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

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

Dokaz. Preprosto preverimo lastnosti, katerim mora množica zadoščati, da jo imenujemo polje. Dobro definiranost operacij nam zagotovi prejšnja lema. □

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

Dokaz. Prejšnja lema nam zagotovi dobro definiranost, ostale lastnosti pa preverimo s preprostim računom. □

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

$$\mathcal{F} := \{\frac{a}{b} | a \in \mathcal{K}, b \in \mathcal{K} - \{0\}\} \tag{74}$$

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

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

Opomba: Karakteristiko kolobarja označimo s $kar(\mathcal{K})$.
Primer:
1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ imajo karakteristiko 0.
2. $kar(\mathbb{Z}_n) = n$
3. $kar(M_k(\mathbb{Z}_n)) = kar(\mathbb{Z}_n[X]) = n$
4. $kar(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$
5. $kar(k) = n \iff \forall x \in \mathcal{K}.\ nx = 0$

Lema 5. *Karakteristika kolobarja brez deliteljev niča je bodisi* 0 *bodisi praštevilo.*

Dokaz. Danimo da je $kar(\mathbb{K}) = n$. 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. □

Izrek 12:
Naj bo $\mathcal{F}$ polje

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

Dokaz. $kar(\mathcal{F}) = 0$, $\varphi : \mathbb{Q} \to \mathcal{F}, \frac{n}{m} \mapsto n * m^{-1}$ Brez težav preverimo, da je φ dobro definirana in homomorfizem, $Ker(\varphi) = \{0\}$, torej je res vložitev.
$kar(\mathcal{F}) = p$, $\varphi : \mathbb{Z}_p \to \mathcal{F}, k \mapsto k * 1 = (1 + 1 + \ldots + 1)$
$\varphi(k) = 0 \iff k = 0$, saj $k < p = kar(\mathcal{F})$, 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 velja tudi v $\mathbb{Z}_p$, zato $\varphi(kl) = \varphi(r) = r$.

□

Polje $\mathbb{Q}$ imenujemo **prapolje s karakteristiko** 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:

$$a\mathcal{H} := \{ah|\ h \in \mathcal{H}\} \tag{75}$$

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

Opomba: Natančneje, $a\mathcal{H}$ je **levi odsek**. Desni odsek definiramo na podoben način $\mathcal{H}a := \{ha|\ h \in \mathcal{H}\}$ 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 podrgupa, saj ne vsebuje niti enote.
Primer:
1. $\mathcal{G} = \mathbb{Z}, \mathcal{H} = n\mathbb{Z}$
Odseki so: $0 + n\mathbb{Z} = n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. Elementi posameznih odsekov 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. $\mathcal{G} = \mathbb{R}^2, \mathcal{H} =$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. $\mathcal{G} = \mathcal{S}_n, \mathcal{H} = \mathcal{A}_n$
$\delta(\in \mathcal{S}_n)\mathcal{H} = \begin{cases} \mathcal{H} & ;\ \delta \in \mathcal{H} \\ \text{vse lihe permutacije} & ;\ \delta \notin \mathcal{H} \end{cases}$
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. $\implies$
$a\mathcal{H} = b\mathcal{H}$
$b = b * 1 \in b\mathcal{H} = a\mathcal{H}$, $b = a * h_0$ za nek $h_0 \in \mathcal{H}$
$a^{-1} * b = h_0 \in \mathcal{H}$
$\impliedby$
$a^{-1} * b = h_0 \in \mathcal{H}$
$b = a * h_0 \implies b * h = a * \underbrace{(h_0 * h)}_{\in \mathcal{H}} \in a\mathcal{H}$
Enako pokažemo inkluzijo v drugo smer. □

Hitro nas to spomni na karakterizacijo podgrupe:(30)
$\mathcal{H}$ je podgrupa $\mathcal{G} \iff a^{-1}b \in \mathcal{H}\ \forall a, b \in \mathcal{H}$
Pomembna razlika je v tem, da sta ta dva elementa zdaj elementa 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 zdaj 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 vsak $a \in \mathcal{G}$ 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 zgoraj(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

$$[a] + [b] = [a + b] \text{ (seštevanje v } \mathbb{Z}_n)$$

To bi seveda radi posplošil. 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 vsh odsekov

$$\mathcal{G}/_{\mathcal{N}} := \{a\mathcal{N} |\ a \in \mathcal{G}\} \tag{76}$$

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

Dokaz. $\implies$ Sledi iz definicij in preprostega računa.
$\Longleftarrow$
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 $\mathcal{G}/_{\mathcal{N}}$ grupa. Preslikava $\Pi(a) = a\mathcal{N}$ je epimorfizem grupe in $Ker(\Pi) = \mathcal{N}$

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 očitno, da je ta preslika surjektivna in homomorfizem $((ab)\mathcal{N} = a\mathcal{N} * b\mathcal{N})$
$a \in Ker(\Pi) \iff \Pi(a) = \mathcal{N} \iff a \in \mathcal{N}$

□

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.
$\implies$: $\mathcal{N}$ je edinka $\implies \mathcal{N} = Ker(\Pi)$
$\Longleftarrow$
$\mathcal{N} := Ker(\varphi), \varphi : \mathcal{G} \to \mathcal{G}'$
Naj velja $n, m \in \mathcal{N}$: $\varphi(nm^{-1}) = \varphi(n)\varphi(m)^{-1} = 1 * 1^{-1} = 1 \implies nm^{-1} \in \mathcal{N}$
Preverimo, da za $a \in \mathcal{G}$ 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

$$\mathcal{HK} := \{hk|\ h \in \mathcal{H}, k \in \mathcal{K}\} \tag{77}$$

Opomba:
Produkt podgrup v splošnem ni nujno podgrupa.

Definicija 116:
Naj bosta $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$, njuna vsota je

$$\mathcal{H} + \mathcal{K} := \{h + k|\ h \in \mathcal{H}, k \in \mathcal{K}\} \tag{78}$$

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: $\forall k_1, k_2 \in \mathcal{K} \wedge \forall h_1, h_2 \in \mathcal{H}.\ (h_1k_2)(h_2k_2)^{-1} \in \mathcal{HK}$ (ekvivalenten pogoj za podgrupo).
   $(h_1k_2)(h_2k_2)^{-1} = h_1 \underbrace{k_1k_2^{-1}}_{k_3 \in \mathcal{K}} h_2^{-1} = h_1 \underbrace{k_3h_1^{-1}}_{h_3k_4 // (\mathcal{HK}=\mathcal{KH})} = \underbrace{(h_1h_3)}_{\in \mathcal{H}} \underbrace{k_4}_{\in \mathcal{K}}$
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 podgrupa $\mathcal{G}$.
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 $\mathcal{H}_1, \mathcal{H}_2, \ldots \mathcal{H}_r \leq \mathcal{G}$ definiramo produkt kot

$$\mathcal{H}_1 \ldots \mathcal{H}_r\ = \{h_1, \ldots, h_r | h_i \in \mathcal{H}_i\}$$

4.2.3 Podgrupe (edinke) kvocientne grupe

Pojavi se naravno vprašanje, kaj so podgrupe edinke $\mathcal{G}/_{\mathcal{N}}$
Prej pa se spomnimo definicij slike in praslike:

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

$$f(\mathcal{X}_0) = \{f(x_0) |\ x_0 \in \mathcal{X}_0\}$$
$$f^{-1}(\mathcal{Y}_0) = \{x \in \mathcal{X} | f(x) \in \mathcal{Y}_0\}$$

Lema 10. *Naj bo $\varphi : \mathcal{G} \to \mathcal{G}'$ 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 sledi, 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 $\varphi = \Pi : \mathcal{G} \to \mathcal{G}/_{\mathcal{N}}$ (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 $\Pi : \mathcal{G} \to \mathcal{G}/_{\mathcal{N}}$ 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 dokaz inkluzije, pa namesto prve točke uporabimo drugo. □

Primer:
Kaj so podgrupe $\mathbb{Z}_n$? Hitro opazimo, da za poljuben $k \in \mathbb{Z}$ velja $k\mathbb{Z}n = \{ka |\ a \in \mathbb{Z}_n\}$ 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

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

postane aditivna grupa, če definiramo:

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

Seveda nas zanima, kaj moramo zahtevati, da bomo $\mathcal{K}/_{\mathcal{I}}$ lahko opremili z množenjem. Zanima nas torej, 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.
$\impliedby$
$u := a' - a \in \mathcal{I}, v := b' - b \in \mathcal{I}$
$a'b' - ab = (a + u)(b + v) - ab = \underbrace{ub}_{\text{Po predpostavki } \in \mathcal{I}} + \underbrace{av + uv}_{\in \mathcal{I}} \in \mathcal{I}$

□

Definicija 117: Podgrupa za seštevanje $\mathcal{I}$ kolobarja $\mathcal{K}$ se imenuje ideal (kolobarja $\mathcal{K}$), če zadošča kateremukoli pogoju 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 $+$, ki hkrati ustrezajo zahtevam).
Izrek 15:
Naj bo $\mathcal{I} \triangleleft \mathcal{K}$. Če v množico vseh odsekov $\mathcal{K}/_{\mathcal{I}}$ vpeljemo seštevanje in množenje s predpisoma od prej, potem postane $\mathcal{K}/_{\mathcal{I}}$ kolobar.
Preslikava $\pi : \mathcal{K} \to \mathcal{K}_{\mathcal{I}}, \Pi(a) = a + \mathcal{I}$ je epimorfizem, katere jedro je $\mathcal{I}$.

Dokaz. Zaradi leme je množenje dobro definirano, seštevanje prav tako.
Enoti ostaneta isti $(0, 1)$. Distributivnost sledi iz originalne distributivnosti. Da je zgoraj omenjena preslikava homomorfizem, njeno jedro pa $\mathcal{I}$, sledi iz poznavanja definicij in preprostega računa. □

4.3.2 Operacije z ideali

Naravno se pojavi vprašanje, ob katerih operacijah med ideali je rezultat tudi ideal.
Trditev 46:
Naj velja $\mathcal{I}, \mathcal{J} \triangleleft \mathcal{K}$, potem velja tudi

1. $\mathcal{I} \cap \mathcal{J} \triangleleft \mathcal{K}$
2. $\mathcal{I} + \mathcal{J} := \{u + v |\ u \in \mathcal{I}, v \in \mathcal{J}\} \triangleleft \mathcal{K}$
3. $\mathcal{I}\mathcal{J} := \underbrace{\{u_1v_1 + u_2v_2 + \cdots + u_nv_n |\ u_i \in \mathcal{I}, v_i \in \mathcal{J}, n \in \mathbb{N}\}}_{\text{Aditivna podgrupa generirana z vsemi produkti}} \triangleleft \mathcal{K}$

Primer:
$\mathcal{I} = 4\mathbb{Z}, \mathcal{J} = 6\mathbb{Z}$
$\mathcal{I}\mathcal{J} = 24\mathbb{Z}$
$\mathcal{I} \cap \mathcal{J} = 12\mathbb{Z}$
$\mathcal{I} + \mathcal{J} = 2\mathbb{Z}$

4.3.3 Enostranski ideali in enostavni kolobarji

Definicija 118: Podmnožica $\mathcal{L}$ kolobarja $\mathcal{K}$ je **levi ideal**, če velja:

- $\mathcal{L}$ je podgrupa za seštevanje
- $\mathcal{K}\mathcal{L} \subseteq \mathcal{L}$, torej: $\forall x \in \mathcal{K}, l \in \mathcal{L}.\ xl \in \mathcal{L}$

Definicija 119: Podmnožica $\mathcal{L}$ kolobarja $\mathcal{K}$ je **desni ideal**, če velja:

- $\mathcal{L}$ je podgrupa za seštevanje
- $\mathcal{L}\mathcal{K} \subseteq \mathcal{L}$

Opomba: Opazimo, da je podmnožica kolobarja ideal, če je hkrati desni in levi ideal.

Definicija 120: Ideal je enostranski, če je bodisi levi bodisi desni ideal.

Definicija 121: Ideal je dvostranski ideal, če je hkrati levi in desni ideal.

Definicija 122:V komutativnem kolobarju pojmi levi, desni in obojestranski ideal sovpadajo.

Primer:
$\mathcal{K} = \mathcal{M}_2(\mathcal{F})$, $\mathcal{L} = \{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \in \mathcal{F}\}$
$\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} x_1a + x_2b & 0 \\ x_3a + x_4b & 0 \end{bmatrix} \in \mathcal{K}$
$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} x_1a & x_2a \\ x_1b & x_2b \end{bmatrix} \notin \mathcal{K}$
Vidimo, da je $\mathcal{L}$ levi ideal, ki ni desni. Podobno je $\mathcal{D} = \{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathcal{F}\}$ desni ideal, ki ni levi.

Lema 12. *Če levi ideal $\mathcal{L}$ kolobarja $\mathcal{K}$ vsebuje kak obrnljiv element, velja $\mathcal{L} = \mathcal{K}$*

Dokaz. Naj bo $l \in \mathcal{L}$ obrnljiv. Ker je $\mathcal{L}$ levi ideal velja $1 = \underbrace{l^{-1}}_{\in\mathcal{K}} l \in \mathcal{L}$. Torej za poljuben $x \in \mathcal{K}$ velja $x = x * 1 \in \mathcal{L}$. Dobimo $\mathcal{K} = \mathcal{L}$. □

Opomba: Iz prejšnje leme sledi, da ideali kolobarja (ki mu niso enaki) ne vsebujejo obrnljivih elementov.

Definicija 123: Center kolobarja $\mathcal{K}$ so vsi elementi, ki komutirajo z ostalimi.

$$Z(\mathcal{K}) := \{c \in \mathcal{K} | \forall x \in \mathcal{K}. cx = xc\} \tag{79}$$

Iz prejšnje leme prav tako sledi, da center kolobarja (z enoto) ni ideal, če $\mathcal{K}$ ni komutativen.
Opomba: Spomnimo se, da je center grupe edinka, tako da tu ne moremo potegniti analogije.
Trditev 47: Kolobar $\mathcal{K}$ je obseg natanko tedaj, ko sta $\{0\}$ in $\mathcal{K}$ njegova edina leva ideala.

Dokaz.
$\Longrightarrow$
Naj bo $\mathcal{K}$ obseg, in $\mathcal{L}$ neničelni levi ideal. Ker $\mathcal{L}$ vsebuje obrnljive elemente je po lemi $\mathcal{L} = \mathcal{K}$.
$\Longleftarrow$

Naj bosta $\{0\}$ in $\mathcal{K}$ edina leva ideala kolobarja $\mathcal{K}$. Vzemimo $0 \neq a \in \mathcal{K}$. $Ka := \{xa | x \in \mathcal{K}\}$ je levi ideal in ker $a \neq 0$ je torej enak $\mathcal{K}$. $1 \in \mathcal{K} \implies \exists b \in \mathcal{K} : ba = 1$. To pomeni, da ima a levi inverz. Vzemimo sedaj b in $\mathcal{K}b$, ki je enako kot prej enak celemu kolobarju. Tako ima tudi b levi inverz ($\exists c.cb = 1$). Skupaj dobimo: $ba = 1 = cb$, torej $a = c$ je obrnljiv.

□

Definicija 124: Neničelen kolobar $\mathcal{K}$ je **enostaven**, če sta $\{0\}$ in $\mathcal{K}$ njegova edina ideala.

Primer:
1. Obsegi
2. $\mathcal{M}_2(\mathcal{F})$ (Ta kolobar sicer ima netrivialne enostranske odseke, nima pa netrivialnih dvostranskih odsekov)

Posledica: Komutativen kolobar je enostaven natanko tedaj, ko je polje.

4.3.4 Ideali kvocientnega kolobarja in maksimalni ideali

Lema 13. *Naj bo $\varphi : \mathcal{K} \to \mathcal{K}'$ homomorfizem kolobarjev. Potem veljata naslednji trditvi:*

1. $\mathcal{I}' \triangleleft \mathcal{K}' \implies \varphi^{-1}(\mathcal{I}') \triangleleft \mathcal{K}$
2. *Če je φ epimorfizem in $\mathcal{I} \triangleleft \mathcal{K} \implies \varphi(\mathcal{I}) \triangleleft \mathcal{K}'$*

Dokaz. Lemo dokažemo na enak način kot analogno trditev za grupe. □

Izrek 16:
Naj bo $\mathcal{I} \triangleleft \mathcal{K}$. Potem je vsak ideal $\mathcal{K}/_{\mathcal{I}}$ oblike $\mathcal{J}/_{\mathcal{I}}$, kjer velja $\mathcal{J} \triangleleft \mathcal{K}, \mathcal{I} \subseteq \mathcal{J} \subseteq \mathcal{K}$.

Dokaz. Izrek dokažemo na enak način kot analogno trditev za grupe. □

Opomba: Obratno $\mathcal{J}/_{\mathcal{I}}$ je ideal $\mathcal{K}/_{\mathcal{I}}$, če velja $\mathcal{J} \triangleleft \mathcal{K}$ in $\mathcal{I} \subseteq \mathcal{J}$
Posledica: Ideal $\mathcal{I}$ kolobarja $\mathcal{K}$ je maksimalen natanko tedaj, ko je $\mathcal{K}/_{\mathcal{I}}$ enostaven.

Dokaz.
$\implies$ Naj bo $\mathcal{I}$ maksimalen. Vsak ideal $\mathcal{K}_{\mathcal{I}}$ je po prejšnjem izreku oblike $\mathcal{J}/_{\mathcal{K}}$, kjer je $\mathcal{J} \triangleleft \mathcal{K}$ in $\mathcal{I} \subseteq \mathcal{J} \subseteq \mathcal{K}$. Ker je $\mathcal{I}$ maksimalen, velja $\mathcal{I} = \mathcal{K}$ (in $\mathcal{J}/_{\mathcal{I}} = \{0\}$) ali $\mathcal{J} = \mathcal{K}$ (in $\mathcal{J}/_{\mathcal{I}} = \mathcal{K}/_{\mathcal{I}}$).
$\impliedby$
Naj bo $\mathcal{K}/_{\mathcal{I}}$ enostaven. Če je $\mathcal{J} \triangleleft \mathcal{K}$, velja $\mathcal{I} \not\subseteq \mathcal{J} \not\subseteq \mathcal{K}$ in je $\mathcal{J}_{\mathcal{K}}$ pravi neničelni ideal $\mathcal{K}/_{\mathcal{I}}$. To pa je v protislovju z našo predpostavko, torej je ideal maksimalen.
□

Posledica: Ideal $\mathcal{I}$, komutativnega kolobarja $\mathcal{K}$, je maksimalen natanko tedaj, ko je $\mathcal{K}/_{\mathcal{I}}$ polje.

Dokaz. Uporabimo prejšnjo posledico. □

Primer:
1. $\mathbb{Z}/_{p\mathbb{Z}} = \mathbb{Z}_p$ je polje, če je p praštevilo, zato je $p\mathbb{Z}$ maksimalni ideal.
2. $\mathcal{I} := \{f \in C[a,b] |\ \exists x \in [a,b].f(x) = 0\}$, $C[a,b]/_{\mathcal{I}} \cong \mathbb{R}$ je polje, zato je $\mathcal{I}$ maksimalen.
3. Za poljubno polje $\mathcal{F}$ velja: $\mathcal{F}[X]/_{(X)} \cong \mathcal{F}$ je polje, zato je (X) maksimalen.

Opomba: S pomočjo Zornove leme lahko dokažemo, da vsak kolobar vsebuje kakšen maksimalen ideal.

4.3.5 Kvocientni prostori in kvocientne algebre

Izrek 17:
Naj bo $\mathcal{U}$ podprostor vektorskega prostora $\mathcal{V}$ nad obsegom $\mathcal{F}$. Če v množico vseh odsekov

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

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 $\Pi : \mathcal{V} \to \mathcal{V}_{\mathcal{U}}, v \mapsto v + \mathcal{U}$ je homomorfizem, katere $Ker(\Pi) = \mathcal{U}$. $\mathcal{U}/_{\mathcal{V}}$ imenujemo kvocientni vektorski prostor, preslikavo Π pa kvocientni epimorfizem.

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

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

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

Opomba: Ideal algebre definiramo enako kot ideal kolobarja. Ideal algebre je avtomatsko tudi vektorski podprostor, saj velja $\lambda u = (\lambda * 1)u$, kar pa je v idealu.
Izrek 18:
Naj bo $\mathcal{I}$ ideal algebre $\mathcal{A}$, če v množico vseh odsekov

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

vpeljemo operacije na enak način kot pri vektorskih prostorih in kolobarjih, postane $\mathcal{A}/_{\mathcal{I}}$ algebra. Preslikava $\Pi : \mathcal{A} \to \mathcal{A}/_{\mathcal{I}}, a \mapsto a + \mathcal{A}$ je homomorfizem, katere $Ker(\Pi) = \mathcal{I}$. $\mathcal{A}/_{\mathcal{I}}$ imenujemo kvocientna algebra, Π pa kvocientni epimorfizem.

4.4 Izrek o izomorfizmih

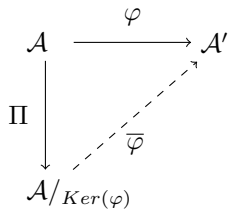
Ob prejšnjih definicijah se naravno pojavi vprašanje, kakšen je pomen homomorfizmov, ki niso bijektivni ali injektivni.

Izrek 19:*Izrek o izomorfizmih*
Naj bo $\varphi : \mathcal{A} \to \mathcal{A}'$ homomorfizem poljubne algebraične strukture (grup, kolobarjev, vektorskih prostorov ali algeber). Potem velja:

$$\mathcal{A}/_{Ker(\varphi)} \cong Im(\varphi) \tag{80}$$

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

Dokaz. Naj bosta $\mathcal{A}, \mathcal{A}'$ grupi. $Ker(\varphi)$ je edinka, zato ima kvocientna struktura smisel, $Im(\varphi)$ pa je grupa (kar podgrupa $\mathcal{A}'$).
$aKer(\varphi) = a'Ker(\varphi) \iff a^{-1}a' \in Ker(\varphi) \iff \varphi(a^{-1}a') = 1 \iff \varphi(a)^{-1}\varphi(a') = 1 \iff \varphi(a) = \varphi(a')$
Definirajmo novo preslikavo $\overline{\varphi} : \mathcal{A}/_{Ker(\varphi)} \to Im\varphi, \overline{\varphi}(aKer(\varphi)) := \varphi(a)$.
Očitno je $\overline{\varphi}$ dobro definirana, injektivna ($\varphi(a) = \varphi(a') \implies aKer(\varphi) = a'Ker(\varphi)$ in surjektivna (slika v sliko preslikave φ).
Pokazati je potrebno še, da je $\overline{\varphi}$ homomorfizem.
$\overline{\varphi}(aKer(\varphi) * bKer(\varphi)) = \overline{\varphi}((ab) * Ker(\varphi)) = \varphi(ab) = \varphi(a) * \varphi(b) = \overline{\varphi}(aKer(\varphi)) * \overline{\varphi}(bKer(\varphi))$ □



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

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

4.5 Zunanji in notranji direktni produkti grup

Spomnimo se definicije zunanjega produkta grup 43. Zunanji produkti nam iz danih grup gradijo nove grupe, medtem ko nam notranji produkti dano grupo (strukturo) razgradijo na "manjše".

Definicija 125: Naj bo $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2 \times \cdots \times \mathcal{G}_n$ zunanji direktni produkt grup $\mathcal{G}_j$.

$$\widetilde{\mathcal{G}_i} = \{(1, \ldots, 1, x_i, 1, \ldots, 1) | x_i \in \mathcal{G}_i\} \tag{81}$$

Poglejmo si primere za direktni produkt dveh grup. $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$
$\widetilde{\mathcal{G}_1} = \{(x, 1) | x \in \mathcal{G}_1\}$
$\widetilde{\mathcal{G}_2} = \{(1, x) | x \in \mathcal{G}_2\}$

Trditev 48:
$\mathcal{G}/_{\widetilde{\mathcal{G}_1}} \cong \mathcal{G}_2$

Dokaz. $(x_1, x_2) \mapsto x_2$ je epimorfizem iz $\mathcal{G}$ v $\mathcal{G}_2$, katerega jedro je $\mathcal{G}_1$. Enako velja, če indeksa grup zamenjamo. □

Opomba: S skoraj povsem enakim dokazom zadevo posplošimo na produkt več grup.
Hitro opazimo naslednje splošne lastnosti grupe $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2 \times \cdots \times \mathcal{G}_n$:

- $\widetilde{\mathcal{G}}_i \triangleleft \mathcal{G}\ \forall i < n$
- $\mathcal{G} = \widetilde{\mathcal{G}}_1\widetilde{\mathcal{G}}_2 \dots \widetilde{\mathcal{G}}_n$
- $\widetilde{\mathcal{G}}_i \cap (\widetilde{\mathcal{G}}_1\widetilde{\mathcal{G}}_2 \dots \widetilde{\mathcal{G}}_{i-1}\widetilde{\mathcal{G}}_{i+1} \dots \widetilde{\mathcal{G}}_n) = \{1, 1, \dots, 1, 1\} = \{1\}$; za vsak i

Definicija 126: Grupa $\mathcal{G}$ je **notranji direktni produkt** svojih edink $\mathcal{N}_1, \mathcal{N}_2, \dots, \mathcal{N}_n$, če velja:

- $\mathcal{G} = \mathcal{N}_1\mathcal{N}_2 \dots \mathcal{N}_n$
- $\mathcal{N}_i \cap (\mathcal{N}_1\mathcal{N}_2 \dots \mathcal{N}_{i-1}\mathcal{N}_{i+1} \dots \mathcal{N}_n) = \{1\}$; za vsak i.

Primer:
1. Če je $\mathcal{G}$ zunanji direktni produkt $\mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_n$, potem je $\mathcal{G}$ notranji direktni produkt $\widetilde{\mathcal{G}}_1, \widetilde{\mathcal{G}}_2, \dots, \widetilde{\mathcal{G}}_n$.
2. $D_4 = \{1, r, z, rz\}$ (komutativna), $\mathcal{N}_1 = \{1, r\}, \mathcal{N}_2 = \{1, z\}$. Potem je D_4 njun notranji produkt. Spomnimo se, da velja tudi $D_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
3. $\mathcal{G} = \mathbb{C}^\times, \mathcal{N}_1 = \mathbb{R}^+ = \{r \in \mathbb{R}^\times | r > 0\}, \mathcal{N}_2 = \mathbb{S}^1$
Poljuben $z \in \mathcal{G} = |z| * \frac{z}{|z|}$, prav tako pa velja: $\mathbb{R}^\times \cap \mathbb{S}^1 = \{1\}$. $\mathbb{C}^\times$ je tako notranji direktni produkt $\mathbb{R}^+$ in $\mathbb{S}^1$. Sledi tudi: $\mathbb{C}^\times/_{\mathbb{R}^+} \cong \mathbb{S}^1$ in $\mathbb{C}^\times/_{\mathbb{S}^1} \cong \mathbb{R}^+$.

Lema 14. *Grupa $\mathcal{G}$ je notranji direktni produkt svojih podgrup edink $\mathcal{N}_1, \mathcal{N}_2, \dots \mathcal{N}_n$ natanko tedaj, ko lahko vsak element iz $\mathcal{G}$ na en sam način zapišemo kot produkt $n_1n_2 \dots n_n$, kjer $n_i \in \mathcal{N}_i$.*

Dokaz.
$\Longrightarrow$
$\mathcal{G} = \mathcal{N}_1, \mathcal{N}_2 \dots \mathcal{N}_n$. Vsak element lahko na vsaj en način zapišemo kot $n_1n_2, \dots n_n$. Dokažimo enoličnost:
$n_1n_2 \dots n_n = r_1r_2 \dots r_n,\ n_i, r_i \in \mathcal{N}_i$. Pomnožimo z leve z r_1^{-1} in z desne z $(n_2n_3 \dots n_n)^{-1}$
$\underbrace{r_1^{-1}n_1}_{\in\mathcal{N}_1} = \underbrace{(r_2r_3 \dots r_n)(n_2n_3 \dots n_n)^{-1}}_{\in\mathcal{N}_2\mathcal{N}_3 \dots \mathcal{N}_n}$ Ker velja $\mathcal{N}_1 \cap (\mathcal{N}_2\mathcal{N}_3 \dots \mathcal{N}_n) = \{1\}$, sledi da $r_1n_1^{-1} = 1$ in torej $r_1 = n_1$. Obe strani enačbe krajšamo in dobimo: $n_2n_3 \dots n_n = r_2r_3 \dots r_n,\ n_i, r_i \in \mathcal{N}_i$. Ponavljamo dokler ne pridemo do rezultata, da so vsi členi enaki.
$\Longleftarrow$
$\mathcal{G} = \mathcal{N}_1, \mathcal{N}_2 \dots \mathcal{N}_n$ sledi iz tega, da obstaja zapis (ne nujno enoličen).
$x \in \mathcal{N}_i \cap (\mathcal{N}_1\mathcal{N}_2 \dots \mathcal{N}_{i-1}\mathcal{N}_{i+1} \dots \mathcal{N}_n)$, $x = 1*1* \dots n_i* \cdots *1*1 = n_1 \dots n_{i-1}n_{i+1} \dots n_n$ iz enoličnosti zapisa sledi $n_j = 1$, torej $\mathcal{N}_i \cap (\mathcal{N}_1\mathcal{N}_2 \dots \mathcal{N}_{i-1}\mathcal{N}_{i+1} \dots \mathcal{N}_n) = \{1\}$ □

Definicija 127: Naj bo $\mathcal{G}$ grupa in $x, y \in \mathcal{G}$. **Komutator** elementov x, y je:

$$[x, y] = xyx^{-1}y^{-1} \tag{82}$$

Opomba: Uporablja se tudi podobna definicija: $[x, y] = x^{-1}y^{-1}xy$.

Lema 15. *Naj bosta $\mathcal{N}, \mathcal{M} \triangleleft \mathcal{G}$. Potem je komutator $[n, m] \in \mathcal{N} \cap \mathcal{M}$ za poljubna $n \in \mathcal{N}, m \in \mathcal{M}$.*

Dokaz.
$[n, m] = \underbrace{nmn^{-1}}_{\in\mathcal{M}} m^{-1} \in \mathcal{M}$ in $[n, m] = n \underbrace{mn^{-1}m^{-1}}_{\in\mathcal{N}} \in \mathcal{N}$ □

Posledica: Če je presek $\mathcal{N} \cap \mathcal{M} = \{1\}$ trivialen, potem je $nm = mn, n \in \mathcal{N}, m \in \mathcal{M}$, torej $\mathcal{N}$ in $\mathcal{M}$ med seboj komutirata.

Izrek 20:
Če je grupa $\mathcal{G}$ notranji direktni produkt svojih podgrup edink $\mathcal{N}_1, \mathcal{N}_2 \ldots \mathcal{N}_n$, potem je $\mathcal{G}$ izomorfna svojemu zunanjemu direktnemu produktu. Oziroma: $\mathcal{N}_1\mathcal{N}_2 \ldots \mathcal{N}_n \cong \mathcal{N}_1 \times \mathcal{N}_2 \times \cdots \times \mathcal{N}_n$.

Dokaz.
Definirajmo $\varphi : \mathcal{N}_1 \times \mathcal{N}_2 \times \cdots \times \mathcal{N}_n \to \mathcal{G}$, $\varphi((n_1, n_2, \ldots, n_n)) = n_1 n_2 \ldots n_n$
Bijektivnost φ dobimo iz prejšnje leme o enoličnosti zapisa. Preveriti moramo še, da je tako definirana preslikava res homomorfizem.
$\varphi((n_1, n_2, \ldots, n_n)(r_1, r_2, \ldots r_n)) = n_1 r_1 n_2 r_2 \ldots n_n r_n$. Ali je to enako $n_1 n_2 \ldots n_n r_1 r_2 \ldots, r_n$?
Iz prejšnje leme se spomnimo, da posamezni elementi iz različnih edink med sabo komutirajo (ker imajo po predpostavki trivialen presek), torej enakost velja.
□

Opomba: Ker sta si notranji in zunanji produkt po prejšnjem izreku izomorfna, tudi notranji produkt označujemo z $\mathcal{N}_1 \times \mathcal{N}_2 \times \cdots \times \mathcal{N}_n$ in pogosto sploh ne ločujemo med notranjim in zunanjim produktom.

Opomba: Če je $\mathcal{G}$ aditivna grupa, namesto o produkt govorimo o vsoti in pišemo $\mathcal{G} = \mathcal{N}_1 \oplus \mathcal{N}_2 \oplus \cdots \oplus \mathcal{N}_n$. Seveda smiselno spremenimo trivialni presek, ki je zdaj $\{0\}$.

Primer:
$\mathcal{N}_1 = \{0, 2, 4\} \cong \mathbb{Z}_3, \mathcal{N}_2 = \{0, 3\} \cong \mathbb{Z}_2$
$\mathbb{Z}_6 = \mathcal{N}_1 \oplus \mathcal{N}_2 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$, vendar pa $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. V $\mathbb{Z}_4$ imamo namreč element reda 4, v $\mathbb{Z}_2$ pa ne (vemo, da bi izomorfizem ohranil red elementa).

4.6 Direktni produkti in direktne vsote v kolobarjih

Kolobar $\mathcal{K}$ je med drugim aditivna grupa, zato lahko pišemo

$$\mathcal{K} = \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus \cdots \oplus \mathcal{I}_n$$

kjer so $\mathcal{I}_j$ poljubne podgrupe za seštevanje. Nas bo bolj zanimal primer, ko so $\mathcal{I}_j$ ideali.
Če je $\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_n$ direktni produkt kolobarjev $\mathcal{K}_1, \ldots, \mathcal{K}_n$, potem je enak direktni vsoti svojih idealov:

$$\mathcal{I}_j = \{(0, \ldots, 0, x, 0, \ldots, 0) | x \in \mathcal{K}_j\}$$

Da je to res ideal, ni težko pokazati.
Radi bi pokazali obratno: če je $\mathcal{K}$ direktna vsota svojih idealov, je $\mathcal{K}$ izomorfen njihovemu direktnemu produktu.
Spomnimo se definicije idempotenta. $e \in \mathcal{K}$ je idempotent, če velja $e^2 = e$. Velja tudi $e^2 = e \iff (1-e)^2 = (1-e)$

Definicija 128: Idempotent e kolobarja $\mathcal{K}$ je **centralni idempotent**, če velja $e \in Z(\mathcal{K})$, torej $ex = xe, \forall x \in \mathcal{K}$.

Definicija 129: Idempotenta e in f sta si **ortogonalna**, če velja $ef = fe = 0$

Opomba: V tem primeru je idempotent tudi $e + f$

Definicija 130: Idempotenti e_k so si paroma ortogonalni, če velja $e_j e_i = e_i e_j = 0, j \neq i$.

Primer:
$\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_n$, $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$(1 na i-tem mestu) so si paroma ortogonalni centralni idempotenti z vsoto 1.
Izrek 21:
Naj bodo $\mathcal{I}_1, \ldots, \mathcal{I}_n$ ideali kolobarja $\mathcal{K}$. Potem velja $\mathcal{K} = \mathcal{I}_1 \oplus \cdots \oplus \mathcal{I}_n$ natanko tedaj, ko obstajajo taki paroma ortogonalni idempotenti $e_1, \ldots, e_n$, da je njihova vsota $e_1 + \cdots + e_n = 1$ in $\mathcal{I}_j = e_j\mathcal{K} := \{e_j x | x \in \mathcal{K}\}$.

Dokaz.
$\Longrightarrow$
$\mathcal{K} = \mathcal{I}_1 \oplus \cdots \oplus \mathcal{I}_n$. Velja $1 = e_1 + e_2 + \cdots + e_n$ za neke $e_j \in \mathcal{I}_j$; velja tudi $i \neq j \implies \mathcal{I}_i\mathcal{I}_j \subseteq \mathcal{I}_i\mathcal{I}_j = \{0\}$ in zato $u_i \in \mathcal{I}_i \implies u_i e_j = 0 \implies u_i = u_i * 1 = u_i e_i$ in podobno $u_i = e_i u_i$. Posebej $e_i^2 = e_i \in \mathcal{I}_i \implies e_i\mathcal{K} \subseteq \mathcal{I}_i$ in $\mathcal{I}_i \subseteq e_i\mathcal{K}$.
Dobimo torej $\mathcal{I}_i = e_i\mathcal{K}$. Iz enakosti prej ($e_i u_i = u_i e_i$) sledi, da so e_i centralni idempotenti.
$\Longleftarrow$
$x \in \mathcal{K} \implies x = 1x = e_1x + e_2x + \ldots e_nx$. Poglejmo si presek $\mathcal{I}_1 \cap (\mathcal{I}_2 \oplus \cdots \oplus \mathcal{I}_n)$. $e_1x = e_2y_2 + \cdots + e_ny_n$ za neke $x, y_i \in \mathcal{K}$. Pomnožimo z leve z e_1. $e_1x = e_1e_2y_2 + \ldots e_1e_ny_n = 0$, torej je presek ničelen.
□

Opomba: Ideali $\mathcal{I}_j = e_j\mathcal{K}$ sicer niso podkolobarji (ker ne vsebujejo enote), so pa sami zase kolobarji s svojo enoto e_j.
Izrek 22:
Če je kolobar $\mathcal{K}$ direktna vsota svojih idealov, potem je izomorfen direktnemu produktu teh idealov:

$$\mathcal{K} = \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus \cdots \oplus \mathcal{I}_n \cong \underbrace{\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n}$$

Operacija ima smisel v luči opombe, da so ti ideali sami zase kolobarji

Dokaz. Dokaz bomo zgolj skicirali. Podobno kot pri enakovrednem izreku za grupe definiramo $\varphi : \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n \to \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus \cdots \oplus \mathcal{I}_n$, $\varphi((u_1, u_2, \ldots, u_n)) = u_1 + u_2 + \cdots + u_n$.
Preverimo, da je φ izomorfizem kolobarjev.

□

Primer:
$(\mathbb{Z}_6, +, *)$ je izomorfen $\mathbb{Z}_3 \times \mathbb{Z}_2$ in enak vsoti idealov $\mathcal{I}_1 = \{0, 2, 4\}, \mathcal{I}_2 = \{0, 3\}; e_1 = 4, e_2 = 3$

5 Končne grupe

5.1 Lagrangeov izrek

Definicija 131: Red grupe $\mathcal{G}$ je število njenih elementov.

$$\operatorname{red} \mathcal{G} := |\mathcal{G}| \tag{83}$$

Lema 16. *Naj bo $\mathcal{H} \leq \mathcal{G}$ in $a \in \mathcal{G}$. Velja: $|a\mathcal{H}| = |\mathcal{H}|$*

Dokaz. $f : \mathcal{H} \to a\mathcal{H}, h \mapsto ah$ je očitno bijektivna preslikava □

Definicija 132: Naj bo $\mathcal{H}$ podgrupa grupe $\mathcal{G}$. **Indeks podgrupe** $\mathcal{H}$ je moč množice vseh odsekov.

$$[\mathcal{G} : \mathcal{H}] := |\{a\mathcal{H} | a \in \mathcal{G}\}| \tag{84}$$

Primer:
$[\mathbb{Z} : n\mathbb{Z}] = n$

Izrek 23:*Lagrangeov izrek*
Če je $\mathcal{H}$ podgrupa končne grupe $\mathcal{G}$, velja:

$$|\mathcal{G}| = [\mathcal{G} : \mathcal{H}]|\mathcal{H}| \tag{85}$$

Dokaz. Spomnimo se, da je $\mathcal{G}$ disjunktna unija svojih odsekov: $\mathcal{G} = a_1\mathcal{H} \cup \cdots \cup a_r\mathcal{H}$, $r = [\mathcal{G} : \mathcal{H}]$
$|\mathcal{G}| = |a_1\mathcal{H}| + |a_2\mathcal{H}| + \cdots + |a_r\mathcal{H}| = r|\mathcal{H}| = [\mathcal{G} : \mathcal{H}]|\mathcal{H}|$ □

Opomba: Očitno sledi: če $\mathcal{N} \triangleleft \mathcal{G}$, potem $|\mathcal{G}/_{\mathcal{N}}| = \frac{|\mathcal{G}|}{|\mathcal{N}|}$ (ob predpostavki, da je $\mathcal{G}$ končna).
Posledica: Red vsake podgrupe končne grupe deli red grupe.
Opomba: Naj bo $\mathcal{G}$ grupa in $a \in \mathcal{G}$, potem veljajo naslednje trditve:

1. Naj bo $n = \operatorname{red} a$, potem velja: $a^m = 1 \iff n|m$
2. Če je p praštevilo in je $a^p = 1, a \neq 1$, potem velja $p = \operatorname{red} a$
3. Naj bo $n = \operatorname{red} a$ in $\varphi : \mathcal{G} \to \mathcal{G}'$ homomorfizem, potem velja $\operatorname{red} \varphi(a) | \operatorname{red} a$
4. $\mathcal{N} \triangleleft \mathcal{G} \implies \operatorname{red}(a\mathcal{N}) | \operatorname{red} a$
5. $a \in \mathcal{G}, \operatorname{red} a = \operatorname{red} < a >$

Dokaz.

1. $m = kn \implies a^m = (a^n)^k = 1^k = 1$ Obratno: $m = qn + r$, $a^m = a^{qn+r} = a^r = 1 \implies r = 0$ (saj mora biti $r \in \mathbb{N} < n$).
2. Sledi iz prejšnje točke (nobeno drugo število ne deli praštevila).
3. $a^n = 1 \implies \varphi(a)^n = \varphi(a^n) = \varphi(1) = 1$. Po prvi točki torej sledi: če obstaja tak $m < n$, da $\varphi(a)^m = 1$, potem $m|n$. Torej $\operatorname{red} \varphi(a) | \operatorname{red} a$.
4. V prejšnjo točko za homomorfizem vstavimo Π.
5. Podgrupa generirana z a vsebuje elemente $1, a, a^2, \ldots, a^{\operatorname{red} a - 1}$, torej ravno $\operatorname{red} a$.

□

Posledica: Red vsakega elementa končne grupe deli red grupe
Posledica: Če je $\mathcal{G}$ končna grupa, za poljuben $a \in \mathcal{G}$ velja $a^{\operatorname{red} G} = 1$

Dokaz. Vzemimo $a \in \mathcal{G}$ in naj bo $n = \operatorname{red} a$, vemo $|\mathcal{G}| = kn$, torej $a^{|\mathcal{G}|} = (a^n)^k = 1^k = 1$ □

Poglejmo si še poseben primer: $\mathcal{G} = \mathbb{Z}_p^\times$, kjer je p praštevilo, kot grupo za množenje. Elementi $\mathcal{G}$ so odseki $x + p\mathbb{Z}, x \notin p\mathbb{Z}$. Opazimo naslednjo posledico.

Izrek 24:*Mali Fermatov izrek*
Naj bo p praštevilo in $a \in \mathbb{N}$. Če $p \not| a$, potem $p|a^{p-1} - 1$.

Opomba: Ekvivalentna formulacija izreka se glasi: Za poljubno naravno število a in praštevilo p velja:

$$a^p \equiv a \pmod{p} \tag{86}$$

Dokaz. $a + p\mathbb{Z} \in \mathbb{Z}_p^\times$ □

Posledica: $(a - p\mathbb{Z})^{p-1} = a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z} \iff a^{p-1} - 1 \in p\mathbb{Z}$
Posledica: Vsaka grupa s praštevilskim redom je ciklična (in zato izomorfna $\mathbb{Z}_p$).

Dokaz. Naj bo $|\mathcal{G}| = p$ praštevilo.
Izberimo si $a \in \mathcal{G} - \{1\}$. Potem velja $\{1\} \subsetneq < a > \leq \mathcal{G}$. Od prej vemo $\operatorname{red} < a > | p \implies \operatorname{red} < a > = p \implies < a > = \mathcal{G}$ □

Opomba: To velja za poljuben $a \neq 1$, torej za vsak $a \neq 1$. $< a >= \mathcal{G}$. Vidimo, da $\mathcal{G}$ ne vsebuje pravih netrivialnih podgrup (edini podgrupi sta $\{1\}$ in $\mathcal{G}$).
Posledica: Grupa $\mathcal{G}$ nima pravih netrivialnih podgrup natanko tedaj, ko je njen red praštevilo.

Dokaz.
$\Longrightarrow$
$\mathcal{G}$ nima pravih netrivialnih podgrup. Vzemimo $a \neq 1$ in poglejmo $< a >$. Ker $\mathcal{G}$ nima trivialnih podgrup, velja $< a >= \mathcal{G}$. Torej je $\mathcal{G}$ ciklična in izomorfna $\mathbb{Z}_n$ ali pa $\mathbb{Z}$. Ker $\mathbb{Z}$ vsebuje podgrupe, je torej $\mathcal{G} \cong \mathbb{Z}_n$ za nek n. Če $d|n$ in $d \notin \{1, n\}$, je $d\mathbb{Z}_n$ prava netrivialna podgrupa $\mathbb{Z}_n$, torej je n praštevilo.
$\Longleftarrow$ Smo dokazali že v opombi. □

Če je torej moč grupe praštevilo, je taka grupa ciklična. Kaj pa se zgodi, če moč grupe ni praštevilo?
$|\mathcal{G}| = 4, \mathcal{G} = \{1, a, b, c\}$
Predpostavimo, da $\mathcal{G}$ ni ciklična. Ker je red grupe 4, imajo lahko elementi a, b, c zgolj red 2 ali 4. Če bi bil red kateregakoli izmed njih 4, bi bila grupa ciklična (generirana s tem elementom). Torej velja $a^2 = b^2 = c^2 = 1$. Torej $ab \neq 1 \neq a \neq b$. Ostane zgolj še $ab = c$ in podobno za ostale pare. Ugotovimo $\mathcal{G} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
Poglejmo si nekaj osnovnih grup velikosti n

1. $\{1\}$
2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_4, \mathbb{Z}_1 \oplus \mathbb{Z}_2$(Med seboj si nista izomorfni, sej se red elemento ne ujema)
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_3 \oplus \mathbb{Z}_2, \mathcal{S}_3$
7. $\mathbb{Z}_7$
8. $\mathbb{Z}_8 \qquad \underbrace{\mathbb{Z}_4 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathcal{D}_2, \mathbb{Q}}_{\text{Niso izomorfne } \mathbb{Z}_8\text{, saj so elementi različnih redov}}$
9. ...

Naravno se pojavi vprašanje, kako bi lahko klasificirali končne enostavne grupe. Izkaže se, da si jih da razdeliti na 18 (neskončnih) družin ($\mathbb{Z}_p, \mathbb{A}_n(n > 5), \dots$) in 26 sporadičnih grup (največja med njimi se imenuje "monster"in ima približno $8 * 10^{53}$ elementov).

5.2 Razredna formula

Spomnimo se definicije, kdaj sta si elementa konjugirana(31) in tega, da je to ekvivalenčna relacija.

Definicija 133: Grupa $\mathcal{G}$ glede na ekvivalenčno relacijo razpade na ekivalenčne razrede $\mathcal{R}_i$, ki jim pravimo **konjugirani razredi** in $\mathcal{R}(a)$ označuje ekvivalenčni razred, ki mu pripada a.

$$\mathcal{R}(a) := \{gag^{-1} | g \in \mathcal{G}\} \tag{87}$$

Ker je $\mathcal{G}$ disjunktna unija svojih ekvivalenčnih razredov lahko zapišemo formulo:

$$|\mathcal{G}| = \sum |\mathcal{R}_i| \tag{88}$$

Definicija 134: Centralizator elementa a grupe $\mathcal{G}$, je grupa vseh elementov, ki z njim komutirajo

$$C(a) := \{x \in \mathcal{G} | ax = xa\} \tag{89}$$

Lema 17. *$C(a)$ je podgrupa $\mathcal{G}$ in velja $|\mathcal{R}(a)| = [\mathcal{G} : C(a)]$*

Dokaz. Vzemimo $x, y \in C(a)$, očitno $xy \in C(a)$, prav tako $ax = xa \implies ax^{-1} = x^{-1}a$ če iz obeh strani pomnožimo z x^{-1}.
Dokažimo še drug del:
$gC(a) = hC(a) \iff h^{-1}g \in C(a) \iff h^{-1}ga = ah^{-1}g \iff gag^{-1} = hah^{-1}$, od tod dobimo da je $gag^{-1} \mapsto gC(a)$ dobro definirana bijekcija iz $\mathcal{R}(a) v \{gC(a) | g \in \mathcal{G}\}$.

□

Prav tako sledi $a \in \mathcal{Z}(\mathcal{G}) \iff \mathcal{R}(a) = \{a\} \iff |\mathcal{R}(a)| = 1$.
Iz 88 sledi dodatek:

$$|\mathcal{G}| = |Z(\mathcal{G})| + \sum \mathcal{R}_j \tag{90}$$

pri čemer so $\mathcal{R}_j$ razredi, ki vsebujejo vsaj dva elementa.
Izrek 25:
Za vsako končno grupo $\mathcal{G}$ je

$$|\mathcal{G}| = |Z(\mathcal{G})| + \sum [\mathcal{G} : C(a_j)] \tag{91}$$

kjer vsota teče po vseh predstavnikih konjugiranih razredov, ki ne sestojijo iz elementov $Z(\mathcal{G}$

5.3 Cauchiyjev izrek

NAravno se pojavi vprašanje, če je $\mathcal{G}$ končna grupa, in če $m | \operatorname{red} \mathcal{G}$, ali potem $\mathcal{G}$ vsebuje element reda m? V splošnem, če $\mathcal{G}$ ni ciklična ne vsebuje elementa z redom, ki je enak moči grupe.
Izrek 26: ***Cauchiyjev izrek***
Naj bo $\mathcal{G}$ končna grupa. Če praštevilo p deli $|\mathcal{G}|$, potem $\mathcal{G}$ vsebuje element reda p.

Dokaz. Naj bo $\mathcal{G}$ grupa moči $n = p * k$, pokazali bomo z indukcijo na n: Če je $n = p$, potem je $\mathcal{G}$ ciklična in ima vsak neničelen element red p Če $n > p$, in izrek velja za vse grupe, ki imajo manj kot n elementov:
Predpostavimo, da $\mathcal{G}$ ni Abelova in torej $Z(\mathcal{G}) \subsetneq \mathcal{G}$. Če $p|Z(\mathcal{G}$, potem po indukcijski predpostavki obstaja tak element. Torej $p \nmid Z(\mathcal{G})$. Iz razredne formule sledi, da $p \nmid [\mathcal{G} : C(a_j)]$ za nek $a_j \in \mathcal{G}$. Spet nam preostaneta dve možnosti če $p||C(a_j)|$ po indukcijsi prespostavki $C(a_j)$ vsebuje element rada p. V nasprotnem primeru $p \nmid [\mathcal{G} : C(a_j)]|C(a_j)| = |\mathcal{G}|$ kar pa je v protislovju.
Če pa je $\mathcal{G}$ abelova, in ker n ni praštevilo, potem $\mathcal{G}$ kot posledica Lagrangevega izreka vsebuje kako pravo netrivialno podgrupo $\{1\} \subsetneq \mathcal{N} \subsetneq \mathcal{G}$ in je $\mathcal{N}$ edinka lahko govorimo o $\mathcal{G}/_{\mathcal{N}}$
Če $p||\mathcal{N}|$, po indukcijski predpostavki imamo tak element, v nasprotnem pa $p \nmid \mathcal{N}$, velja pa $p|\mathcal{G} = |\mathcal{N}||\mathcal{G}/_{\mathcal{N}}|$ torej $p||\mathcal{G}/_{\mathcal{N}}$ in ker $\mathcal{N}$ ni trivialna edinka lahko uporabimo predpostavko in dobimo element reda p. □

Opomba: Izrek lahko ekvivalentno formuliramo: Če p deli $|\mathcal{G}|$ potem $\mathcal{G}$ vsebuje podgrupi s p elementi. Res, če je $\mathcal{H} = p$ $\mathcal{H} \leq \mathcal{G}$ potem je $\mathcal{H}$ ciklična in vsak njen neničelen element ima red p, obratno, če je $a^p = 1 \implies | < a > | = p$.
Nasploh, ali iz $m||\mathcal{G}|$ sledi, da $\mathcal{G}$ vsebuje pogrupo z m elementi. V splošnem to ni res(A_n ne vsebuje podgrupe s 6 elementi). Odgovor pa ni pozitiven zgolj za praštevila, ampak tudi za vse njihove potence: $p^k||\mathcal{G}|$, potem $\mathcal{G}$ vsebuje elemepte reda p^k, to pravi prvi izrek Sylowa.

Definicija 135: Grupa $\mathcal{G}$ se imenuje p-grupa, kjer je p praštevilo, če je red vsakega njenega neničelenega elementa potenca števila p.

Primer:
$\mathbb{Z}_p, \mathbb{Z}_{p^2}, \mathbb{Z}_{p^3}, \ldots$
Direktni produkti p-grup so p-grupe, prav tako so to njihove podgrupe($\mathcal{D}_4, \mathbb{Q}$)
Posledica: Končna grupa $\mathcal{G}$ je p-grupa natanko tedaj, ko je $|\mathcal{G}| = p^l$ za nek $l \in \mathbb{N}$.

Dokaz. Če je $\mathcal{G}$ p-grupa, potem je po Cauchyjevem izreku $|\mathcal{G}| = p^l$, obratno, $|\mathcal{G}| = p^l \implies$ vsi elementi imajo red $p^k, k \leq l$, po posledici Lagrangevega izreka. □

5.4 Končne Abelove grupe

Tipični primeri končnih Abelovih grup so ciklične grupe $\mathbb{Z}_n$ in njihove direktne vsote.
Primer:
$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \mathbb{Z}_{n_r}$
Ali jih imamo še kaj? Ne.
$\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_6 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$
Po dogovoru bodo grupe v tem razdelku aditivne, im bom operacijo pisali kot $+$.

Lema 18. *Demimo, da je $|\mathcal{G}| = mn$ in sta si m in n tuji števili. potem je $\mathcal{G}$ direktna vsota svojih podgrup $\mathcal{H} = \{x \in \mathcal{G} | mx = n\}, \mathcal{K} = \{x \in \mathcal{G} | nx = 0\}$*

Dokaz. Očitno sta $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$
$x^{|\mathcal{G}|} = 1 \forall x \in \mathcal{G} \implies x^{mn} = 0 \forall x \in \mathcal{G}$, torej je $nx \in \mathcal{H}$ in $mx \in \mathcal{K}$, ker sta si tuji, $\exists u, v \in \mathbb{Z}. um + vn = 1$ in $u\underbrace{(mx)}_{\in\mathcal{K}} + v\underbrace{(nx)}_{\in\mathcal{H}} = x \implies \mathcal{G} = \mathcal{H} + \mathcal{K}$, preverimo, še da je presek ničelen $x \in \mathcal{H} \cap \mathcal{K} \implies mx = nx = 0 \implies x = 0$ □

Tako lahko posplošimo: $\mathbb{Z}_m n \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$, kjer sta si m in n tuji števili.

Lema 19. *Naj bo $\mathcal{G}$ grupa in naj velja $|\mathcal{G}| = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, kjer so p_i različna praštevila, potem je*

$$\mathcal{G} = \mathcal{H}_1 \oplus \mathcal{H}_2 \oplus \dots \oplus \mathcal{H}_n$$

kjer so $\mathcal{H}_i$ p_i- grupe in velja $|\mathcal{H}_i| = p_i^{k_i}$

Dokaz. Definirajmo: $\mathcal{H}_1 := \{x \in \mathcal{G} | x p_1^{k_1} = 0\}$ in
$\mathcal{K} = \{x \in \mathcal{G} | p_2^{k_2} \dots p_n^{k_n}\}$
Vemo, da $p_1 \nmid |\mathcal{K}|$, saj bi sicer po Cauchyjevem izreku $\mathcal{K}$ vsebovala element reda p in bi zato veljalo $p_1 | p_2^{k_2} \dots p_n^{k_n}$, kar pa je protislovje. Tako je edina možnost $|\mathcal{G}| = |\mathcal{H}_1||\mathcal{K}| = p_1 * p_2^{k_2} \dots p_n^{k_n}$ □

Lema 20. *Naj go $\mathcal{G}$ $p-$grupa. Potem je $\mathcal{G}$ ciklična natanko tedaj, ko vsebuje eno samo podgrupo reda p.*

Opomba: Vsaka $p-$grupa vsebuje kako podgrupo reda p (Po Cauchyjevem izreku), če pa ni siklična pa vsaj 2.

Dokaz.
$\implies$ Ker je $\mathcal{G}$ ciklična velja $\mathcal{G} \cong \mathbb{Z}_{p^m}$, kot vemo pa so edine pogrupe $\mathcal{G}$ grupe oblike: $p^i \mathbb{Z}_{p^k}$, kjer ima samo $p^{m-1}\mathbb{Z}_{p^m}$ p elementov.
$\impliedby$ Naj ima $\mathcal{G}$ natanko eno podgrupo reda p, imenujmo jo $\mathcal{N}$. Imamo dve možnosti, če $|\mathcal{G}| = p$, potem velja $\mathcal{G} = \mathcal{N}$ in $\mathcal{G}$ je ciklična. drugače pa velja $|\mathcal{G}| > p$ in predpostavimo, da lema velja za vse grupe, ki imajo manj elementov, kot grupe $\mathcal{G}$.
Vpeljimo $\varphi : \mathcal{G} \to \mathcal{G}, \varphi(x) = px$, ki je endomorfizem, katerega jedro sestoji iz elementov z redom p. Zato velja $Ker(\varphi) = \mathcal{N}$. Po izreku o izomorfizmih tako velja: $\mathcal{G}/_{\mathcal{N}} \cong Im(\varphi) \leq \mathcal{G}$ in $|Im(\varphi)| = \frac{|\mathcal{G}|}{|\mathcal{N}|} \leq \mathcal{G}$. Tako lema po predpostavki velja za grupo $Im(\varphi)$.
Kot prodgrupa $Im(\varphi)$ ne more vsebovati več podgrup reda p kot $\mathcal{G}$, zato vsebuje eno samo in je torej ciklična. zato je tudi $\mathcal{G}/_{\mathcal{N}}$ ciklična z generatorjem $a + \mathcal{N}$, iz tega sledi: $\mathcal{G} =< a > +\mathcal{N}$. Tako dobimo $|\mathcal{G}| > p = |\mathcal{N}|$ in zato je $< a >$ netrivialna podgrupa $\mathcal{G}$ in po Cauchyjevem izreku zato vsebuje element reda p. Sledi $\mathcal{N} \subseteq < a >$ in zato $\mathcal{G} =< a >$. □

Spomnimo se vektroskih prostorov. Če je $\mathcal{U}$ vektorski podprostor $\mathcal{V}$, potem obsjata podprostor $\mathcal{W}$, da velja $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$. Za grupe ne velja nič podobnega. Grupa $\mathbb{Z}_4$ in podgrupa $\{0, 2\}$ nimata komplementa da velja $\mathbb{Z}_4 = \{0, 2\} \oplus \mathcal{G}$.

Lema 21. *Naj bo $\mathcal{G}$ $p-$grupa. Če je $\mathcal{C}$ njena ciklična podgrupa, ki ima izmed vseh cikličnih podgrup največji red, potem $\mathcal{G}$ vsebuje tako podgrupo $\mathcal{K}$, da velja: $\mathcal{G} = \mathcal{V} \oplus \mathcal{K}$.*

Dokaz. Če je $\mathcal{G}$ ciklična, potem $\mathcal{G} = \mathcal{C}$ in $\mathcal{K} = \{0\}$, torej smemo privzeti, da $\mathcal{G}$ ni ciklična, $|\mathcal{G}| > p$ in da lema velja za vse grupe z manj elementi kot p.
Ker po lemi vemo, da če $\mathcal{G}$ ni ciklična ima vsaj dve podgrupi reda p, $\mathcal{C}$ pa zgolj eno samo. Naj bo $\mathcal{N}$ podgrupa reda p, ki ni vsebovana v $\mathcal{C}$. Dobimo $\mathcal{C} \cap \mathcal{N} = \{0\}$ saj je presek podgrupa grupe $\mathcal{N}$ in ima zato p^j elementov ($j = 0$). Tako velja $\mathcal{C} + \mathcal{N} = \mathcal{C} \oplus \mathcal{N}$ in $\mathcal{C} + \mathcal{N}/_{\mathcal{N}} \cong \mathcal{C}$ $(c \mapsto c + \mathcal{N})$ in tako dobimo: $(\mathcal{C} + \mathcal{N})/_{\mathcal{N}} \cong \mathcal{C}$.
v $\mathcal{G}/_{\mathcal{N}}$ tako ni cikličnih podgrup z več elemnti kot jih ima $\mathcal{C}$ (saj je red elemeta $x + \mathcal{N} \in \mathcal{G}/_{\mathcal{N}}$ kvečjemu manjši kot red elementa x. Zato ima $(\mathcal{C} + \mathcal{N})/_{\mathcal{N}}$ izmed vseh cikličnih pogrup grupe $\mathcal{G}/_{\mathcal{N}}$ največji red $|\mathcal{G}/_{\mathcal{N}}| < \mathcal{G}$ in tako po naši predpostavki velja $\mathcal{G}/_{\mathcal{N}} = (\mathcal{C} + \mathcal{N})/_{\mathcal{N}} \oplus \mathcal{L}$ za neko podgrupo $\mathcal{L} \leq \mathcal{G}/_{\mathcal{N}}$.
Po znane izreku je tako res: $\mathcal{L} = \mathcal{K}/_{\mathcal{N}}, \mathcal{N} \leq \mathcal{K} \leq \mathcal{G}$, potrebno je še dokazati: $\mathcal{G} = \mathcal{V} \oplus \mathcal{K}$. Vemo: $\mathcal{G}/_{\mathcal{N}} = ((\mathcal{C} + \mathcal{N})/_{\mathcal{N}}) \oplus (\mathcal{K}/_{\mathcal{N}} \implies \mathcal{G} = \mathcal{C} + \mathcal{N} + \mathcal{K}$ in potrebujemo zgolj še $\mathcal{C} \cap \mathcal{K} = \{0\}$.
Vzemimo $x \neq 0$ iz preseka. $x \notin \mathcal{N} \implies x + \mathcal{N}$ je neničelen element $(\mathcal{C} + \mathcal{N})/_{\mathcal{N}} \cap \mathcal{K}/_{\mathcal{N}}$, kar pa je protislovje.

□

Izrek 27: ***Osnovni izrek o končnih Abelovh grupah***
Vsaka končna Abelova grupa je direktna vsota cikličnih podgrup. Te podgrupe lahko izberemo tako, da je red vsake izmed njih potenca praštevil.

Dokaz. Po predzadnji lemi zadošča obravnavati zgolj situacijo, ko je $\mathcal{G}$ $p-$grupa in tako po zadnji lemi dobimo $\mathcal{G} = \mathcal{C} \oplus \mathcal{K}$, $|\mathcal{C}| \geq p$ in $\mathcal{G}$ ciklična, potem $|\mathcal{K}| < |\mathcal{G}|$. Uporabimo zadnjo lemo za $\mathcal{K}$ in po končnem številu korakov dobimo željeno. □

Opomba: Krajše lahko zadevo zapišemo: $\mathcal{G}$ je (notranja) direktna vsota cikličnih p podgrup. Ali ekvivalentno: $\mathcal{G}$ je izomorfna (zunanji) direktni vsoti grup oblike $\mathbb{Z}_{p^i}$, kjer je p praštevilo.
Naravno nas zanima, katere izmed teh grup so si med seboj izomorfne.
Naj bosta $\mathcal{G}$ in $\mathcal{G}'$ končni Abelovi grupi: $\mathcal{G} \cong \mathcal{G}'$, $|\mathcal{G}| = |\mathcal{G}'| \implies \mathcal{G} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_s, \mathcal{G}' = \mathcal{H}'_1 \oplus \ldots \mathcal{H}'_s$, kjer sta $\mathcal{H}_i, \mathcal{H}'_i$ p_i-grupi.
Izomorfizem $\varphi\mathcal{G} \to \mathcal{G}'$ pa slika eno v drugo. Zato je potrebno odgovoriti le za $p-$grupe.
$\mathcal{G}$ je $p-$grupa $\implies \mathcal{G} \cong \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_n}}$, brez škode za splošnost pa lahko privzamemo $k_1 <\geq k_2 \geq \cdots \geq k_n$

Izrek 28:
Naj bo p preštevilo. Če za naravna števila $k_1 \geq k_2 \geq \cdots \geq k_u$ in $l_1 \geq l_2 \geq \cdots \geq l_v$ velja $\mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_u}} \cong \mathbb{Z}_{p^{l_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_v}}$ potem je $k_i = l_i$ in $u = v$.

Dokaz. Seveda se vsoti ujemata in sta enaki moči grup. Naj bo $|\mathcal{G}| > p$ in privzemimo, da izrek velja za grupe z manj elementi kot $\mathcal{G}$. Za nako poljubno podgrupo $\mathcal{K}$ pišimo $p\mathcal{K} := \{px | x \in \mathcal{K}\}$. Tako dobimo $p\mathbb{Z}_{p^m} \cong \mathbb{Z}_{p^{m-1}} (m = 1 : p\mathbb{Z}_p = \{0\}$ in $\mathcal{G} \cong \mathcal{G}' \implies p\mathcal{G} \cong p\mathcal{G}' \implies \mathbb{Z}_{p^{k_1 - 1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_w - 1}} \cong \mathbb{Z}_{p^{l_1 - 1}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_z - 1}}$, kjer je w največji indeks $k_w > 1$ in z največji indeks $k_z > 1$.
Po predpsotavki tako dobimo $w = z$ in $k_i - 1 = l_i - 1$, ker pa $k_1 + \cdots + k_w - w = l_1 + \cdots + l_w - w$ in imata grupi enako moč dobmio $u = v$.

□

Primer:
$|\mathcal{G}|$ je Abelova in $|\mathcal{G}| = 200 = 5^2 * 2^3$, $\mathcal{G} = \mathcal{H} \oplus \mathcal{K}$, $|\mathcal{H}| = 25$ in $|\mathcal{K}| = 8$.
Za $\mathcal{H}$ imamo (do izomorfizma natančno) dve možnosti: $\mathbb{Z}_25$ ali $\mathbb{Z}_5 \oplus \mathbb{Z}_5$, za $\mathcal{K}$ pa $\mathbb{Z}_8$ ali $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ ali $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Torej je $\mathcal{G}$ izomorfna eni izmed grup, ki o dobimo s kombinacijo prve ali druge možnosti.
Opomba: Osnovni izrek za **končno generirane** Abelove grupe: Vsaka taka grupa je izomorfna $\mathbb{Z}^m \oplus \mathcal{K}$, kjer je $\mathcal{K}$ končna Abelova grupa. Tako je vsaka taka grupa direktna vsota cikličnih grup.

6 Deljivost v komutativnih kolobarjih

6.1 Glavni ideal

Definicija 136: Naj bo $\mathcal{K}$ komutativen kolobar in $a \in \mathcal{K}$. Množica

$$(a) := \{ax | x \in \mathcal{K}\} \tag{92}$$

je **ideal generiran z** a.

Definicija 137: Ideal kolobarja je glavni ideal, če je generiran z enim samim elementom.

Opomba: Če $\mathcal{K}$ ni komutativen kolobar je

$$(a) := \{\sum_i x_i a y_i \mid x_i, y_i \in \mathcal{K}\}$$

Primer:
$\mathcal{K} = \{1\}$ in $(0) = \{0\}$
Trditev 49:$\mathcal{K} = (a)$ natanko tedaj, ko je a obrnljiv.

Dokaz.
$\Longrightarrow$ Enačba $ax = 1$ ima rešitev, torej je a obrnljiv
$\Longleftarrow$ Vemo od prej

□

Primer:
$\mathcal{K} = \mathbb{Z}$, vsi ideali so oblike $n\mathbb{Z}, n \geq 0$ in zato so vsi glavni.

Definicija 138: Ideal je **končno generiran**, če je generiran s končno mnogo množico elementov. Oznalimo ga z $(a_1, a_2, \ldots, a_n)$

Opomba: Opazimo, da velja $(a_1, a_2, \ldots, a_n) = (a_1) + (a_2) + \cdots + (a_n)$ in torej $(a_1, a_2, \ldots, a_n) = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_i \in \mathcal{K}\}$
Primer:
1. $(4, 6) \triangleleft \mathbb{Z}$ $(4, 6) = \{4x + 6y \mid x, y \in \mathbb{Z}\} = (2)$, torej lahko generatorja $4, 6$ nadomestimo z enim samim 2.

2. Naj bo $\mathcal{F}$ polje in naj bo $\mathcal{I}$ množica vseh polinomov iz $\mathcal{F}[X]$ s konstantnim členom 0. Velja $\mathcal{I} = (X)$. Kasneje bomo pokazali, da so vsi ideali $\mathcal{F}[X]$ glavni.
3. $\mathbb{Z}[X]$ ($\mathbb{Z}$ ni polje), $(2, X)$ sestoji iz polinomov, ki imajo konstanten člen sod. Ta ideal pa ni glavni, saj če bi veljalo: $(2, X) = (f(X))$, cin $2 \in (f(X))$, sledi, da je $f(X)$ konstanten polinom a_0, ki je sod, kar pa je v protislovju s predpostavko da $X \in (a_0)$
4. $\mathcal{F}[X, Y]$, $\mathcal{I}$ vsebuje vse polinome s konstantim členom 0, torej $\mathcal{I} = (X, Y)$, bralec pa bo za domačo nalogo lahko preveril, da $\mathcal{I}$ ni glavni ideal.

6.2 Deljivost

Definicija 139: Naj bo $\mathcal{K}$ komutativen kolobar. Neničelen element b **deli** element a, če obstaja tak $q \in \mathcal{K}$, da velja $a = bq$. V tem primeru rečemo, da je a deljiv z b.

$$b \mid a \iff \exists q \in \mathcal{K}.\ a = bq \tag{93}$$

Trditev 50:

$$b \mid a \iff (a) \subseteq (b)$$

Dokaz.
$\Longrightarrow$
$b \mid a \implies a = bq \implies (a) \subseteq (b)$
$\Longleftarrow$
$(a) \subseteq (b) \implies a \in (b) \implies a = bq$ □

Opomba: V posebnem primeru dobimo:

$$b \mid a \wedge a \mid b \iff (a) = (b)$$

Definicija 140:V primeru, da $a \mid b$ in $b \mid a$ pravimo, da sta si a in b **asociirana**.

Trditev 51: Naj bo $\mathcal{K}$ cel kolobar (torej komutativen in brez deliteljev niča), potem sta si neničelna elementa a in b asiciiriana natanko tedaj, ko obstaja tak obrnljiv elementa $u \in \mathcal{K}$, da velja $a = ub$.

Dokaz.
$\Longrightarrow$
$a \mid b \wedge b \mid a, a, b \neq 0$
$b = ar, a = bq \implies b = ar = (bq)r = b(qr) \implies b(1 - qr) = 0$, ker pa $b \neq 0$, sta q, r obrnljiva.
$\Longleftarrow$
Zgolj premečemo definicjo.

□

Primer:
1. V $\mathbb{Z}$ sta si števili asociirani natanko tedaj, ko sta si enaki ali ko velja $n = -m$, saj sta 1 in -1 edina obrnljiva elementa.
2. Obrnljivi elementi v $\mathcal{F}[X]$ so neničelni konstanti polinomi, $f(x) in g(x)$ sta si asociirana $\iff f(X) = ug(X)$ za nek $u \in \mathcal{F} \neq 0$

Opomba: Iz definicij sledi, da asociirana elementa delite iste elemente in sta z istimi elementi deljiva. S stališča teorije deljivosti ju zato lahko identificiramo.

Definicija 141: Naj bo $\mathcal{K}$ komutativen kolobar in $a, b \in \mathcal{K}$ neničelna. Neničelni $d \in \mathcal{K}$ je njun **največji skupni delitelj**, če velja:

- $d \mid a \wedge d \mid b$
- $c \mid a \wedge c \mid b \implies c \mid d$

Pišemo $\gcd(a, b) = d$

Opomba: Največji skupni delitelj števil ne obstaja vedno, če pa obstaja, potem je določen do asociiranosti natančno.
Opomba: Po dogovoru v $\mathbb{Z}$ za gcd izberemo naravno število in je tako gcd natančno določen. Podobno v $\mathcal{F}[X]$ za gcd izberemo polinom, ki ima vodilni koeficient 1.

Definicija 142: Elementa a in b sta si **tuja**, če velja $gcd(a, b) = 1$

Trditev 52: Naj bo $\mathcal{K}$ komutativen in $a, b \in \mathcal{K}$ ne oba enaka 0, če je idal (a, b) glavni, potem $\gcd(a, b)$ obstaja in je oblike $d = ax + by$ za neka $x, y \in \mathcal{K}$.

Dokaz. Po predpostavki je $(a, b) = (d)$ za nek $d \neq 0 \in \mathcal{K}$, vemo $a \in (d) \implies d \mid a, b \in d \implies d \mid b$
$d \in (d) = (a, b) \implies d = ax + by$
$c \mid a, c \mid d$, $a = cz, b = cw \implies d = c(zx + wy) \implies c \mid d$ □

Opomba: Četudi ideal (a, b) ni glavni ideal lahko njun gcd še vedno obstaja. V $\mathbb{Z}[X]$ je tako $\gcd(2, X) = 1$.

Definicija 143: Naj bo $\mathcal{K}$ komutativen. Neničelen $p \in \mathcal{K}$, ki ni obrnljiv je **nerazcepen**, če iz $p = ab$ sledi, da je (vsaj) eden izmed elementov a, b obrnljiv.

Primer:
V $\mathbb{Z}$ so nerazcepni elementi $p, -p$, kjer je p praštevilo.
Trditev 53: Naj bo $\mathcal{K}$ cel kolobar in $p \in \mathcal{K}$, tedaj sta za neničelen in neobrnljiv p naslednji trditvi ekvivalentni:

- p je nerazcepen
- Če je $a \in \mathcal{K}$ tak, da $(p) \subseteq (a)$ in $(a) \neq \mathcal{K}$, potem $(p) = (a)$

Dokaz. $(p) \subseteq (a)$ pomeni $p = ab$ za nek b. $(a) \neq \mathcal{K}$ pomeni, da a ni obrnljiv, $(p) = (a)$ pa, da sta si p in a asociirana ($ua = p$ za nek obrnljiv u)
$p = ab = ua \implies b = u$ in sledi, da sta si trditvi ekvivalentni.

□

6.3 Evklidski kolobarji

Če si podrobneje pogledamo, vidimo da sta si $\mathbb{Z}$ in $\mathcal{F}[X]$ zelo podobna, oba sta cela in imata zelo "malo"obrnljivih elementov. Oba zadoščata osnovnemu izreku o deljenju (1).

Izrek 29: ***Osnovni izrek o deljenju polinomov***
Naj bo $\mathcal{F}$ polje in naj bosta $f(X), g(X) \in \mathcal{F}[X]$, Če $g(X) \neq 0$ potem obstajata taka $q(X), r(X) \in \mathcal{F}[X]$, da velja

$$f(X) = q(X)g(X) + r(X), r(X) = \vee st(r(X)) < st(g(X)) \tag{94}$$

Dokaz. $n := st(g(X)), m := st(f(X))$, $m < n \implies q(X) = 0, r(X) = f(X)$, torej naj bo $m \geq n$, izrek pa bomo dokazali z indukcijo na m.
$m = 0 \implies n = 0$ in trivialno dobimo $r(X) = 0$
$f(X) = aX^n + f_1(X), st(f_1(X)) < m$. $g(X) = bX^n + g_1(X)$, $st(g_1(X)) < n$
$h(X) := f(X) - ab^{-1}X^{m-n}g(X) = \underbrace{f_1(X) - ab^{-1}X^{m-n}g_1(X)}_{\text{stopnja } <m}$
Po indukcijski predpostavki velja $h(X) = q_1(X)g(X)+r(X), r = 0 \vee st(r(X)) < n$ $f(X) - ab^{-1}X^{m-n}g(X) = q_1(X)g(X) + r(X) \implies$
$f(X) = \underbrace{(ab^{-1}X^{m-n} + q_1(X))}_{q(X)}g(X) + r(X)$ □

Definicija 144: Cel kolobar $\mathcal{K}$ je **evklidksi kolobar** če obstaja taka preslikava $\sigma : \mathcal{K} - \{0\} \to \mathbb{N} \cup \{0\}$, za katero velja:

- $\forall a, b \in \mathcal{K}, b \neq 0. \exists q, r \in \mathcal{K}.\ a = qb + r, r = 0 \vee \sigma(r) < \sigma(b)$ (izrek o deljenju)
- $\forall a, b \in \mathcal{K} - \{0\}.\ \sigma(a) \leq \sigma(ab)$

Primer:
1. $\mathbb{Z}, \sigma(n) = |n|$
2. $\mathcal{F}[X], \sigma(f(X)) = st(f(X))$
3. $\mathbb{Z}[i]$ je evklidski za $\sigma(n + mi) = n^2 + m^2$
4. $\mathcal{F}$ je evklidski, saj je zaradi deljenja vedno: $r = 0$, tako je lahko σ poljubna funkcija, ki ustreza drugemu pogoju.

Trditev 54: $\sigma(a) = \sigma(ab) \implies b$ je obrnljiv

Dokaz. $a = qab + r, r = 0 \vee \sigma(r) < \sigma(ab)$.
Če $r = 0 \implies a(1 - qb) = 0 \underbrace{\implies}_{a \neq 0} b = q^{-1}$
Če $r \neq 0 \implies r = a(q - qb)$ in zato $\sigma(r) \geq (a)$, kar pa je protislovje. □

Opomba: $\sigma(u) = 0 \implies u$ je obrnljiv. $1 = qu + r \implies r = 0$
Izrek 30:
Vsak ideal evklidskega kolobarja je glavni.

Dokaz. Naj bo $\mathcal{I} \triangleleft \mathcal{K}$, kjer je $\mathcal{K}$ evklidski. Izberimo si $a \in \mathcal{I} - \{0\}$, da zanj velja $\sigma(a) \leq \sigma(x), x \in \mathcal{I}$ (to lahko naredimo, saj za naravna števila velja načelo dobre urejenosti. Pokazali bomo da velja $\mathcal{I} = (a)$, vemo že da $(a) \subseteq \mathcal{I}$. Vemo tudi $x \in \mathcal{I}.x = qa + r$ Če $r = 0 : x = qa \in (a)$, Če pa $\sigma(r) < \sigma(a), r = x - qa \in \mathcal{I}$, kar pa je protislovje. □

Posledica: Naj bo $\mathcal{K}$ evklidksi kolobar in $p \in \mathcal{K}, p \neq 0$, naslednje trditve so si ekvivalentne:

1. p je nerazcepen
2. (p) je maksimalen ideal
3. $\mathcal{K}/_{(p)}$ je polje

Dokaz. (1) $\iff$ (2), v prejšnjem razdelku smo dokazali, da je nerazcepnost ekvivalentena maksimalnosti.
(2) $\iff$ (3) Smo dokazali v poglavju 4. □

Primer:
Za $\mathbb{Z}$ to že poznamo (p je praštevilo $\iff \mathbb{Z}/_{p\mathbb{Z}} = \mathbb{Z}_p$ je polje
Posledica: Naj bo $\mathcal{K}$ evklidski kolobar. Za vsaka $a, b \in \mathcal{K}$, ki nista oba 0 velja, da obstaja njun gcd, ki je oblike $\gcd(a, b) = ax + by;\ x, y \in \mathcal{K}$

Dokaz. Že prej smo dokazali, da je vsak tak kolobar glavni in da temu ustreza. □

Posledica: Naj bo $\mathcal{K}$ evklidski kolobar in $a, b, p \in \mathcal{K}$. Če je p nerazcepen in $p \mid ab$, potem $p \mid a \vee p \mid b$.

Dokaz. Denimo, da $p \nmid a$, potem sta si p in a tuja, zato po prejšnji posledici velja $ax + py = 1$ za nkea $x, y \in \mathcal{K}$
$abx = bpy = y \implies p(cx + by) = b \implies p \mid b$ □

Opomba: Fraza **enoličnost do vrstnega reda asociiranosti** pomeni $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$, ker so p_i, q_i nerazcepni pomeni, da ob pogoju $s = t$ obstaja permutacija $\sigma \in \mathcal{S}_s$, da velja p_i je asociiran $q_{\sigma(i)}$.
Izrek 31:
Naj bo $\mathcal{K}$ evklidski kolobar, vsak neničelni $a \in \mathcal{K}$, ki ni obrnljiv lahko zapišemo kot produkt nerazcepnih elementov. Ta zapis je enoličen do vrstnega reda in asociiranosti faktorjev natančno.

Dokaz. $a \in \mathcal{K}, a \neq 0$, a ni obrnljiv. Predpostavimo, da a ni nerazcepen, torej $a = a_1 a_2$, kjer sta a_1 in a_2 obrnljiva, velja tudi $\sigma(a_1) < \sigma(a), \sigma(a_2) < \sigma(a)$ tako nadaljujemo za navzdol, doker ne pridemo do $a$ja, kjer velja $\sigma(a) = 0$.
Potrebno je dokazati še enoličnost. $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$, kjer so p_i, q_i nerazcepni, po posledici pa $p_1 \mid p_i$ za nek i. q-je permutiramo, in $p_1 \mid q_1$ in $q_1 = p_1 u$, kjer je u obrnljiv. p_1 in q_1 sta si asociirana. Krajšamo s p_1 in dobimo

$p_2 \dots p_s = (uq_2) \dots q_t$, kjer je uq_2 nerazcepen. Postopek ponavljamo dokler ne končamo. □

Opomba: Vse posledice zadnjega izreka veljajo tudi za **glavne kolobarje** (celi kolobarji, v katerih je vsak ideal glaven), venad se je za dokaz potrebno nekoliko bolj potruditi.
Opomba: Vsak evklidski kolobar je glavni, obratno pa v splošnem ne velja.

Definicija 145:Kolobar z enolično faktorizacijo je cel komutativen kolobar, za katerega velja izrek (31).

Definicija 146:Noetherski kolobar je komutativen kolobar, v katerem je vsak ideal končno generiran.

Opomba: Izkaže se:
$\mathcal{K}$ je kolobar z enolično faktorizacijo $\implies$ $\mathcal{K}[X]$ je kolobar z enolično faktorizacjio.
$\mathcal{K}$ je noeterski kolobar $\implies$ $\mathcal{K}[X]$ noeterski kolobar.
Zato sta $\mathbb{Z}[X]$ in $\mathcal{K}[X,Y] = (\mathcal{K}[X])[Y]$ kolobarja z enolično faktorizacijo/noetrska(ob primernih predpostavkah), nista pa niti evklidska niti glavna.

6.4 Nerazcepni polinomi

Spomnimo se prejšnjega poglavja in rezultata, da je vsak ideal $\mathcal{F}[X]$ glavni, torej oblike:

$$(a(X)) = \{a(X)f(X) |\ f(X) \in \mathcal{F}[X]\}$$

Za vsaka $a(X), b(X) \in \mathcal{F}[X]$, ki nista oba 0 obstaja gcd, ki je oblike: $\gcd(a(X) = d(X) = b(X)) = a(X)f(X) + b(X)g(X)$, z zahtevo da ima d vodilni koeficient 1 pa je gcd celo enolično določen.

Lema 22. *Polinom $f(X) \in \mathcal{F}[X]$ ima ničlo v $a \in \mathcal{F}$ natanko tedaj, ko je $f(X)$ deljiv z $(X-a)$ $(f(X) = g(X)(X-a))$.*

Dokaz. $f(X) = q(X)(X-a) + r(X)$, kjer je $r(X)$ konstanten polinom izračunamo f v a. $f(a) = 0 + a_0 = 0 \iff a_0 = 0$ □

Posledica: Če neničelen in nelinearen polinom $f(X) \in \mathcal{F}[X]$ ima ničlno v $\mathcal{F}$, potem ni razcepen.
Opomba: V nasprotno smer ne gre. $(X^2+1)^2 \in \mathbb{R}[X]$ ni nerazcepen, a nima ničle v $\mathbb{R}$
Opomba: Linearni polinomi so nerazcepni (v $\mathbb{C}$ so to tudi edini nerazcepni polinomi (Osnovni izrek algebre)).
Opomba: V $\mathbb{R}[X]$ so nerazcepni linearni polinomi in kvadratni polinomi, katerih diskriminanta je manjša od 0.
Pojavi s vprašanje, kaj so nerazcepni polinomi v $\mathbb{Q}[X]$, izkaže se da je dovolj, da si pogledamo $\mathbb{Z}[X]$, saj lahko poljuben polinom pomnožimo z skupnim imenovalcem in smo v $\mathbb{Z}$

Definicija 147: Polinom $p \in \mathbb{Z}[X]$ je **primitiven**, če je največji skupni delitelj njegovih koeficientov enak 1.

Primer:
$2 - 3X + 6X^5$ je primitiven, $2 - 4X + 6X^5$ pa ni.

Lema 23 (Gaussova lema)**.** *Produkt dveh primitivnih polinomov je primitiven polinom.*

Dokaz. $f(X), g(X)$ sta primitivna, njun produkt $p(X)q(X)$ pa ni. Torej obstaja praštevilo p, da p ki deli vse koeficiente $p(X)g(X)$. p lahko obravnavamo ko polinom v $\mathbb{Z}[X]$, vemo da velja $f(X)g(X) \in (p) = \{pq(X) |\ q(X) \in \mathbb{Z}[X]\}$. Vemo da je $f(X) + \underbrace{p\mathbb{Z}[X]}_{(p)} \in \mathbb{Z}[X]/_{(p)}$ neničelen odsek, saj p ne deli vseh koeficientov $f(X)$. Podoben argument velja za $g(X)$. Tako dobimo $(f(X) + (p))(g(X) + (p)) = f(X) + g(X) + (p) = 0$, kolobar $\mathbb{Z}[X]/_{p\mathbb{Z}[X]}$ ima torej delitelje niča. Ker pa je izomofen $(\mathbb{Z}/_{p\mathbb{Z}})[X] = \mathbb{Z}_p[X]$ in je $\mathbb{Z}_p$ polje je to protislovje. □

Definicija 148: Nekonstanten polinom $f(X) \in \mathbb{Z}[X]$ je nerazcepen, če ga je noremo zapisati kot produkt dveh nelinearnih polinomov iz $\mathbb{Z}[X]$

Izrek 32:
Če je polinom $f(X) \in \mathbb{Z}[X]$ nerazcepen v $\mathbb{Z}[X]$ je nerazcepen tudi v $\mathbb{Q}[X]$.

Opomba: Veljevnost v obratno je trivialna.

Dokaz. $f(X) = g(X)h(X), g(X), h(X) \in \mathbb{Q}[X]$ Izberemo $k, l \in \mathbb{N}$, da velja $kg(X), lh(X) \in \mathbb{Z}[X]$, dobimo $klf(X) = kg(X)lh(X)$, kjer imajo vsi trije koeficiente v $\mathbb{Z}$.
Zapišemo $hg(X) = d_1 g_0(X)$, kjer je d_1 največji skupni delitelj koeficientov $hg(X)$. Potem je g_0 primitiven. Podobno dobimo: $lh(X) = d_2 h_(X), h_0(X)$ je primitiven in $f(X) = df_0(X), f_0(X)$ je primitiven.
$\underbrace{(hld)}_{\in\mathbb{Z}} f_0(X) = \underbrace{(d_1 d_2)}_{\in\mathbb{Z}} \underbrace{g_0(X)h_0(X)}_{\text{primitivna po Gaussovi lemi}}$
Največji skupni delitelj $(hld)f(X)$ j3 kld, za $(d_1 d_2)g_0(X)h_0(X)$ pa $d_1 d_2$ torej $kld = d_1 d_2$.
Pokrajšamo polinoma $f_0(X) = g_0(X)h_0(X) \implies f(X) = df_0(X) = dg_0(X)h_0(X)$, ki pa je nerazcepen v $\mathbb{Z}$. Sledi da je $dg_0(X)$ ali $h_0(X)$ konstanten torej $g(X)$ ali $h(x)$ je konstanten.

□

Posledica:[Eisensteinov kriterij]
Naj bo $n \in \mathbb{N}$ in $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X], a_n \neq 0$. Če obstaja tako praštevilo p, da $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1} \wedge p \nmid a_n \wedge p^2 \nmid a_0$, potem je $f(X)$ nerazcepen v $\mathbb{Q}[X]$.

Dokaz. Po izreku zadošča pokazati, da je $f(X)$ nerazcepen v $\mathbb{Z}[X]$. Naj bo $f(X) = g(X)h(X)$ kjer $g(X) = b_0 + b_1 X + \cdots + b_r X^r, b_r \neq 0$ in $h(X) = c_0 + c_1 X + \cdots + c_s X^s, c_s \neq 0$ $a_0 = b_0 c_0$ in ker $p \mid a, p^2 \nmid a_0 \implies p$ deli natanko eno izmed b_0 in c_0, naj deli b_0. Vemo tudi $a_n = b_r c_s$, $p \nmid a_n \implies p \nmid b_r$. Naj bo $k \leq r$ število z lastnostjo $p \mid b_0, p \mid b, \ldots, p \mid b_{k-1}, p \nmid b_n$, potem $a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$, $p \mid a_n$(ker $k \leq r < n$) in $p \mid b_0, \ldots p \mid b_{n-1}$. Sledi $p \mid b_n c_0 \implies p \mid b_n \vee p \mid c_0$ kar pa je protislovje. □

Primer:
$X^n - p \in \mathbb{Q}[X]$, kjer je p praštevilo je nerazcepen v $\mathbb{Q}[X]$, torej nima ničel, torej $\sqrt[n]{p} \notin \mathbb{Q}$

7 Ničle polinomov in razširitve polj

7.1 Pogled v zgodovino

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \underbrace{\mathbb{Q}}_{\text{ničle } nX-m} \subseteq \underbrace{\mathbb{R}}_{\text{ničle } X^2-1} \subseteq \underbrace{\mathbb{C}}_{\text{ničle } X^2+1}$$

Polinom $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, a_n \neq 0$ ima za poljuben a_i ničlo v $\mathbb{C}$(po osnovnem izreku algebre).
Že Babilonci so (cca. 4000 let naza) znali reševati linearne in kvadratne enačbe.

Ničle kubičnega polinoma so v 16. stoletju znali reševati s pomočjo Cardanovih formul.

$$x^3 + px + q = 0 \implies x = \sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{q})^2 - (\frac{p}{3})^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{(\frac{q}{q})^2 - (\frac{p}{3})^3}}$$

Splošne enačbe tretje in četrte stopnje se da prevesti na to, za $n \geq 5$ pa so Ruffini, Abel in Galois dokazali, da obstajajo polinomi, za katere se rešitev ne da izraziti z njihovimi koeficienti in operacijami: $+, -, *, /, \sqrt[n]{}$.
Primer:
Poleg prejšnjih polj so za raziskovanje pomembna tudi polja:

- $\{a + bi \mid a, b \in \mathbb{Q}\}$
- $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
- $\mathbb{Z}_p$
- $\mathcal{F}[X] \hookrightarrow \mathcal{F}(x)$

7.2 Algebraični in transcedentni elementi

Primer:
$\sqrt{2}$ je algebraično število, saj je ničla $X^2 - 2$, medtem ko število π ni algebraično, je torej transcedentno(dokaz je zelo zahteven).
Opomba: V tem smislu lahko govorimo, da je $\sqrt{2}$ "bližje"$\mathbb{Q}$ kot π.

Definicija 149: Naj bo polje $\mathcal{E}$ razširitev polja $\mathcal{F}$. Pravimo, da je $a \in \mathcal{E}$ **algebraičen nad** $\mathcal{F}$, ča obstaja tak $0 \neq f(X) \in \mathcal{F}[X]$, da velja $f(a) = 0$.

Definicija 150:Če a ni algebraičen nad $\mathcal{E}$, potem rečemo, da je a **transcedenten nad** $\mathcal{F}$.

Opomba: Če je $\mathcal{E} = \mathbb{C}, \mathcal{F} = \mathbb{Q}$, takrat govorimo o algebraičnih oziroma transcedentnih številih.

Definicija 151: Naj bo $a \in \mathcal{E}$ algebraičen nad $\mathcal{F}$, polinom $p(X) \in \mathcal{F}[X]$ je **minimalni polinom** elementa a, če velja:

- $p(X) \neq 0$
- $p(a) = 0$
- vodilni koeficient $p(X)$ je 0
- izmed vseh polinomov, ki imajo a za 0 ima $p(X)$ najmanjšo stopnjo

Opomba: Eksistenca in enoličnost sta očitni
Trditev 55: Naj bo $a \in \mathcal{E}$ algebraičen nad $\mathcal{F}$ in naj bo $p(X) \in \mathcal{F}[X]$ neničelen polinom, da je njegovo vodilni koeficient 0 ter $p(a) = 0$. Naslednje trditve so ekvivalentne:

1. $p(X)$ je minimalen polinom elementa a
2. $p(X)$ je nerazcepen v $\mathcal{F}[X]$
3. $(p(X)) = \{f(X) \in \mathcal{F}[X] \mid f(a) = 0\}$

Dokaz. (i) $\implies$ (ii):
Naj bo $p(X) = g(X)h(X)$, potem $0 = p(a) = g(a)h(a) \implies g(a) = 0 \vee h(a) = 0$, ker pa je $f(X)$ minimalen, potem $st(g(X)) > st(p(X))$, kar pa je protislovje.
(ii) $\implies$ (iii):
naj bo $p(X)$ nerazcepen, $\mathcal{I} := \{f(X) \mid f(a) = 0\}$ je ideal za $\mathcal{F}[X]$, vemo da je $\mathcal{I}$ glavni ideal, tj $\mathcal{I} = (p_1(X))$, torej $p(X) \in \mathcal{I} = p_1(X)g(X)$, ker pa je $p(X)$ nerazcepen je $g(X)$ konstanten polinom in $(p(X)) = (p_1(X))$
(iii) $\implies$ (i):
$f(a) = 0$, $f(X) = p(X)g(X)$, torej ima $p(X)$ izmed vseh polinomov, katerih ničla je a najmanjšo stopnjo.

□

Definicija 152: Elementa $a \in \mathcal{E}$ je **algebraične stopnje** n, če je n stopnja njegovega minimalnega polinoma.

Primer:
1. Elementi $\mathcal{F}$ so algebraične stopnje 1 nad $\mathcal{F}$.
2. Vsak $z \in \mathbb{C}$ je algebraičen nad $\mathbb{R}$, saj je ničla $(X-z)(X-\overline{z}) = X^2-(z+\overline{z})X \in \mathbb{R}[X]$ in če $z \in \mathbb{C} - \mathbb{R}$, je z algebraičen stopnje 2 nad $\mathbb{R}$.
3. $\mathcal{F}, \mathcal{F}[X](= \mathcal{E}$, $X \in \mathcal{F}[X]$ je očitno transcedenten nad $\mathcal{F}$
4. π, e sta transcedentni števili(dokaz je dokaj zahteven, zato navadno transcedentna števila konstruiramo posebej, glej Liouvillova števila).

Opomba: Algebraičnih števil je številno mnogo.
Opomba: Vsota dveh algebraičnih števil je algebraično število.

7.3 Kratnost ničle polinoma

Definicija 153: Naj bo $f(X) \in \mathcal{F}[X]$ neničelen polinom in $a \in \mathcal{F}$ njegova ničla. a je enostavna ničla polinoma $f(X)$, če velja $f(X) = (X-a)g(X)$ in $g(a) \neq 0$.

Definicija 154: Naj bo $f(X) \in \mathcal{F}[X]$ neničelen polinom in $a \in \mathcal{F}$ njegova ničla. a je $k-$kratna ničla polinoma $f(X)$, če velja $f(X) = (X-a)^k g(X)$ in $g(a) \neq 0$.

Trditev 56: Naj bo polje $\mathcal{E}$ razširitev polja $\mathcal{F}$. Polinom $f(X) \in \mathcal{F}[X]$ ima ničlo $a \in \mathcal{E}$ natanko tedaj, ko obstaja $g(X) \in \mathcal{E}[X]$, da velja $f(X) = (X-a)g(X)$.

Dokaz. Za $\mathcal{F} = \mathcal{E}$ to že vemo. Če obravanvamo $f(X)$ kot element $\mathcal{E}[X]$ tako trditev sledi.
V splošnem lahko zapišemo $f(X) = (X-a)^k g(X), g(X) \in \mathcal{E}[X] \wedge g(a) \neq 0$
Tudi $g(X)$ pa ima lahko ničle v $\mathcal{E}$, tako pridemo do zapisa $f(X) = (X - a_1)^{k_1}(X-a_2)^{k_2}\dots(X-a_r)^{k_r} f_(X)$, kjer so $a_i \in \mathcal{E}$ in $f_0(X)$ nima ničel v $\mathcal{E}$.
Opazimo: $st(f(X)) = k_1 + k_2 + \cdots + k_r + st(f_0(X))$ □

Posledica: Število ničel polinoma, štetih z njihovo mnogokratnostjo je kvečjemu manjše od stopnje polinoma
Primer:
$f(X) = X^6 - 3X^2 + 4 \in \mathbb{Q}[X], f(X) = (X^2-2)^2(X^2+1)$ Glede na izbiro polja $\mathcal{E}$ imamo več možnosti:

1. $\mathcal{E} = \mathbb{Q}$: polinom nima ničel, $f_0(X) = f(X)$
2. $\mathcal{E} = \mathbb{R} : a_1 = \sqrt{2}, k_1 = 2; a_2 = -\sqrt{2}, k_2 = 2; f_0(X) = (X^2+1)$
3. $\mathcal{E} = \mathbb{C} : a_1 = \sqrt{2}, k_1 = 2; a_2 = -\sqrt{2}, k_2 = 2; a_3 = i, k_3 = 1; a_4 = -1, k_4 = 1$

7.4 Končne razširitve

$\mathcal{F} \subseteq \mathcal{E}$, tedaj lahko $\mathcal{E}$ obravanavamo kot vektorski prostor nad $\mathcal{F}$. $\mathcal{E}$ je seveda aditivna grupa, za množenje s skalarji pa vzamemo kar damo množenje v $\mathcal{E}$. Tako so vsi aksiomi za vektorske prostore izpolnjeni.

Definicija 155: Naj bo $\mathcal{E}$ razširitev $\mathcal{F}$. Rečemo, da je $\mathcal{E}$ končna razširitev $\mathcal{F}$, če je $\mathcal{E}$ končno razsežen vektorski prostor nad $\mathcal{F}$. Dimanziji $\mathcal{E}$ nad $\mathcal{F}$ pravimo stopnja razširitve in jo označujemo z

$$[\mathcal{E} : \mathcal{F}] := dim_{\mathcal{F}}(\mathcal{E})$$

Primer:
1. $[\mathbb{C} : \mathbb{R}] = 2$, s standardno bazo: $\{1, i\}$

2. $\mathbb{R} nikonnaraziritev \mathbb{Q}$ (Vsaka končna razširitev $\mathcal{Q}$ je števna množica.

Izrek 33:
Naj bo polje $\mathcal{L}$ končna razširitev polja $\mathcal{F}$ in polje $\mathcal{E}$ končna razširitev polja $\mathcal{L}$. Potem je tudi $\mathcal{E}$ končna razširitev $\mathcal{F}$ in velja:

$$[\mathcal{E} : \mathcal{F}] = [\mathcal{E} : \mathcal{L}][\mathcal{L} : \mathcal{F}]$$

Dokaz. Naj bo $\{a_1, \dots a_m\}$ baza $\mathcal{L}$ nad $\mathcal{F}$in $\{b_1, \dots, b_n\}$ baza $\mathcal{E}$ nad $\mathcal{L}$. Trdimo, da je $B := \{a_i b_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ baza $\mathcal{E}$ nad $\mathcal{F}$.
Preverimo, da je ogrodje:
$x \in \mathcal{E} \implies x = c_1 b_1 + \dots + c_n b_n, c_i \in \mathcal{L}$, $c_i = \sum_{j=1}^{m} f_{ij} a_j$

$$x = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} a_j b_i$$

Torej je B ogrodje. Pokažimo, še da je linearno neodvisna.
Denimo $\sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij}(a_j b_i) = 0, f_{ij} \in \mathcal{F}$
Potem $\sum_{i=1}^{n} \underbrace{(\sum_{j=1}^{m} f_{ij} a_j)}_{\in \mathcal{L}} b_i = 0 \implies \sum f_{ij} a_j = 0$, sa so b_i linearno neodvsini nad $\mathcal{L}$. Prav tako pa so tudi a_j linearno neodvisni in torej $f_{ij} = 0$.

□

Posledica: Naj bo $\mathcal{E}$ končna razširitev $\mathcal{F}$. Če je $\mathcal{L}$ podpolje $\mathcal{E}$, ki vsebuje $\mathcal{F}$, potem $[\mathcal{L} : \mathcal{F}]$ deli $[\mathcal{E} : \mathcal{F}]$.

Dokaz. Bralec bo lahko sam razmislil. □

Definicija 156: Polje $\mathcal{E}$ je **algebraična razširitev** polja $\mathcal{F}$, le je vsak element iz $\mathcal{E}$ algebraičen nad $\mathcal{F}$.

Opomba: število a je algebraično natanko tedaj, ko so elementi $1, a, \dots, a^n \in \mathcal{E}$ linearno odvisni nad $\mathcal{F}$.
Trditev 57: Vsaka končna razširitev je algebraična.

Dokaz. Naj bo $[\mathcal{E} : \mathcal{F}] = n$, $a \in \mathcal{E} \implies 1, a, \dots, a^n$ so linearno odvisni nad $\mathcal{F}$, saj jih je $n + 1$, kar je več od dimenzije. To pomeni, da obstaja tak polinom, katerega ničla je a. Torej je a algebraičen. □

Primer:
$[\mathbb{C} : \mathbb{R}] = 2 \implies \mathbb{C}$ je algebraičen nad $\mathbb{R}$, iz dokaza pa sledi, da je poljubno kompleksno število ničla nekega polinoma, stopnje 2 ali manj z realnimi koeficienti $((X - \overline{z})(X + \overline{z}))$.
Opomba: Obstajajo tudi algebraične razširitve, ki niso končne.

Definicija 157: Naj bo $\mathcal{F} \subseteq \mathcal{E}$ in naj bo $\mathcal{A}$ podmnožica $\mathcal{E}$. Z $\mathcal{F}[\mathcal{A}]$ označimo podkolobar $\mathcal{E}$ generiran z $\mathcal{F}$ in $\mathcal{A}$.

Definicija 158: Naj bo $\mathcal{F} \subseteq \mathcal{E}$ in naj bo $\mathcal{A}$ podmnožica $\mathcal{E}$. Z $\mathcal{F}(\mathcal{A})$ označimo podpolje $\mathcal{E}$ generiran z $\mathcal{F}$ in $\mathcal{A}$.

Opomba: Če je $\mathcal{A} = \{a_1, a_2, \dots\}$ pišemo kar $\mathcal{F}[a_1, a_2, \dots]$ ali $\mathcal{F}(a_1, a_2, \dots)$. Največkrat je $\mathcal{A}$ kar singelton torej $\mathcal{F}[a]$ in $\mathcal{F}(a)$.
Primer:
$\mathcal{F}[a] = \{f(a)(= \lambda_0 + \lambda_1 a_1 + \dots \lambda_n a_n) \mid f(X) \in \mathcal{F}[X]\}$
$\mathcal{F}(a) = \{f(a)g(a)^{-1} | f(X), g(X), g(a) \neq 0 \in \mathcal{F}[X]\}$

Definicija 159: Polje $\mathcal{F}(a)$ imenujemo polje, dobljeno s priključitvijo elementa.

Definicija 160:$\mathcal{E}$ je enostavna razširitev $\mathcal{F}$, če obstaja tak $a \in \mathcal{E}$, da je $\mathcal{E} = \mathcal{F}(a)$, tedaj ta a imanujemo primitivni element iz razširitve.

Primer:
1. $\mathbb{C} = \mathbb{R}(i)$, $\mathbb{C}$ je torej enostavna razširitev $\mathbb{R}$, i pa je primer primitivnega elementa.
2. $\mathcal{F} = \mathbb{Q}, \mathcal{E} = \mathbb{C}, a = i$
$\mathbb{Q}[i] = \{f(i) | f(X) \in \mathbb{Q}[X]\} = \{a + bi | a, b \in \mathbb{Q}\}$, kar pa je tudi polje vidmo: $\mathbb{Q}[i] = \mathbb{Q}(i)$

Izrek 34:
Naj bo polje $\mathcal{E}$ razširitev polja $\mathcal{F}$. Če je $a \in \mathcal{E}$ algebraičen stopnje n nad $\mathcal{F}$, potem je $\mathcal{F}(a) = \mathcal{F}[a] = \{\lambda_0 + \lambda_1 a + \dots + \lambda_{n-1} a^{n-1} \mid \lambda_i \in \mathcal{F}\}$ in velja $[\mathcal{F}(a) : \mathcal{F}] = n$

Dokaz. Vsak element iz $\mathcal{F}[a]$ je oblike $f(a)$ za nek $f(X) \in \mathcal{F}[X]$. Denimo: $f(a) \neq 0$, dokazati moramo, da $f(a)^{-1} \in \mathcal{F}[a]$.
Naj bo $p(X)$ minimalen polinom elementa a (stopnje n). $f(a) \neq 0 \implies p(X) \nmid f(X)$, $p(X)$ je nerazcepen, torej sta si $p(X)$ in $f(X)$ tuja. $\exists h(X), k(X) \in \mathcal{F}[X]. h(X)p(X) + k(X)f(X) = 1$. Vsativmo a in dobimo $f(a)k(a) = 1 \implies f(a)^{-1} = k(a) \implies \mathcal{F}[a] = \mathcal{F}(a)$
Za drugi del uporabimo osnovni izrek o deljenju.: $f(X) = q(X)p(X) + r(X) \implies f(a) = \underbrace{q(a)p(a)}_{=0} + r(a) = r(a)$, $r(X) = 0 \vee st(r(x)) < n$ Tako dobimo, da so elementi $1, a, \dots, a^{n-1}$ ogrodje $\mathcal{F}(a)$ nad $\mathcal{F}$, ker pa je a algebraične stopnje n pa so si tudi neodvsini.
Torej je $\{1, a, \dots, a^{n-1}\}$ baza $\mathcal{F}(a)$ nad $\mathcal{F}$ in sledi $[\mathcal{F}(a) : \mathcal{F}] = n$. □

Opomba: V slučaju zgornjega izreka bomo namesto $\mathcal{F}[a]$ raje uporabljali $\mathcal{F}(a)$.
Spomnimo se, da če vzamemo praštevilo p, je potem $\sqrt[n]{p}$ algebraične stopnje n nad $\mathcal{Q}$, saj je njegov minimalni polinom $X^n - p$, ki je po Eisensteinovem kriteriju nerazcepen.

Tako dobimo $\mathbb{Q}(\sqrt[n]{p}) = \{\lambda_0 + \lambda_1 \sqrt[n]{p} + \cdots + \lambda_{n-1} \sqrt[n]{p^{n-1}}, \lambda_i \in \mathbb{Q}\}$
Opomba: Za nek $a \in \mathcal{E}, \mathcal{F} \subseteq \mathcal{E}$, je $\varphi : \mathcal{F}[X] \to \mathcal{F}[a], f(x) \mapsto f(a)$ surjektivni (evalvacijski) homomorfizem in velja:

1. Če je a algebraičen, potem $\mathrm{Ker}(\varphi) = (p(X))$, kjer je $p(X)$ minimalnio polinom za a. Te lepo sledi iz izreka o izomorfizmih:

$$\underbrace{\mathcal{F}[X]/_{(p(X))}}_{\text{je polje, saj je } p(X) \text{nerazcepen}} \cong \mathcal{F}[a]$$

   Tudi od tod bi lahko dobili enakost $\mathcal{F}[a] = \mathcal{F}(a)$

2. Če je a transcedenten, potem $\mathrm{Ker}(\varphi) = \{0\}$ in je zato φ izomorfizem in torej $\mathcal{F}[a] \cong \mathcal{F}[X]$ in velja celo $\mathcal{F}(a) = \mathcal{F}(X)$(to preprosto vidimo tako, da poiščemo razširitev preslikave iz zgornje vrstice) in je zato $\mathcal{F}[a] \subsetneq \mathcal{F}(a)$

Opomba: Izrek pove $[\mathcal{F}(a) : \mathcal{F}]$ je stopnja algebraičnosti elementa a. Naj bo $\mathcal{L}$ razširitev $\mathcal{F}$. Ker je a algebraičen nad $\mathcal{F}$, je algebraičen nad $\mathcal{L}$. Stopnja algebraičnosti nad $\mathcal{L}$ pa je manjša ali enaka kot stopnja algebraičnosti nad $\mathcal{F}$.

$$[\mathcal{L}(a) : \mathcal{L}] \leq [\mathcal{F}(a) : \mathcal{F}]$$

Posledica: Naj bo $\mathcal{E}$ razširitev $\mathcal{F}$. Če so $a_1, \ldots a_n \in \mathcal{E}$ algebraični nad $\mathcal{F}$, potem je polje $\mathcal{F}(a_1, \ldots, a_n)$ končna razširitev $\mathcal{F}$ in velja

$$\mathcal{F}[a_1, \ldots, a_n] = \mathcal{F}(a_1, \ldots, a_n)$$

Dokaz. Dokažemo z indukcijo na n. Za $n = 1$ je to kar osnovni izrek.
Predpostavimo lahko, da je $\mathcal{L} = \mathcal{F}[a_1, \ldots a_{n-1}] = \mathcal{F}(a_1, \ldots, a_{n-1}$ končna razširitev $\mathcal{F}$. Ker je a algebraičen nad $\mathcal{F}$, potem je a tudi algebraičen nad $\mathcal{L}$. Po osnevnem izreku je $\mathcal{L}(a_n)$ končna razširitev $\mathcal{L}$ in ker je $\mathcal{L}$ končna razširitev $\mathcal{F}$ je $\mathcal{L}(a_n)$ končna razširitev $\mathcal{F}$ (Končna razširitev končne razširitve je končna razširitev). Pokazati moramo torej $\mathcal{L}(a_n) = \mathcal{F}(a_1, \ldots, a_n) = \mathcal{F}[a_1, \ldots, a_n]$. Elementi $\mathcal{L}(a_n)$ so oblike $l_0 + l_1 a_1 + \cdots + l_k a_k^k$, vsak l_i pa je oblike $f_i(a_1, \ldots, a_{n-1})$
Sledi: vsak podkolobar, ki vsebuje $\mathcal{F}$ in vse a mora vsebovati $\mathcal{L}(a_n)$, ki je celo polje in ki vsebuje vse a_i in s tem dobimo željeno.

□

Opomba: Če so torej $a_1, \ldots, a_n$ algebraični nad $\mathcal{F}$, je $\mathcal{F}(a_1, \ldots, a_n)$ končna razširitev $\mathcal{F}$. Velja pa tudi obratno. Tako je vsaka kočna razširitev $\mathcal{F}$ oblike $\mathcal{F}(a_1, \ldots, a_n)$ za $a_i \in \mathcal{E}$(Včasih se za zelo pametno izkaže, da izberemo kar elementa iz baze). Izrek o primitivnem elementu nam pove, da če je $\mathrm{Ker}(F) = 0$, potem lahko vse a_i nadomestimo z enim samim elementom a ($\mathcal{F}(a_1, \ldots, a_n) = \mathcal{F}(a)$) in je torej vsaka končna razširitev enostavna.
Primer:
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{2})$, inkluzija v eno smer je očitna, v drugo pa se je potrebno malo bolj potruditi. $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$ in torej $2\sqrt{2} = (\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})$. Tako smo $\sqrt{2}$ izrazili kot $f(\sqrt{2} + \sqrt{3}), f(X) \in \mathbb{Q}$. Podobmo naredimo še za $\sqrt{3}$ in dobimo $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, z malo razmisleka pa lahko ugotovim otudi $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$
Opomba: Naj bo $\mathcal{E}$ razširitev nad $\mathcal{F}$. Množica $\mathcal{A}$ vseh elementov iz $\mathcal{E}$, ki so algebraični nad $\mathcal{F}$ je podpolje polja $\mathcal{E}$ (ki vsebuje polje $\mathcal{F}$).

Dokaz. Pokazati je treba:

$$a, b(\neq 0) \in \mathcal{A} \implies a+b, a-b, ab, b^{-1} \in \mathcal{A}$$

Vemo da velja $\mathcal{F}(a,b) = \mathcal{F}[a,b]$ končna razširitev $\mathcal{F}$ in je zato tudi algebraična. Vsak element iz $\mathcal{F}(a,b)$ je torej algebraičen nad $\mathcal{F}$ in pripada $\mathcal{A}$(posebej $a+b, a-b, ab, b^{-1}$). □

Opomba: Poseben primer: Polje algebraičnih števol $\mathcal{A}$. To je tudi primer algebraične razširitve, ki ni končna, saj $[\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}] = n$ in če bi veljalo $[\mathcal{A} : \mathbb{Q}] \leq \infty$, sledilo: $n \mid [\mathcal{A} : \mathbb{Q}]$ za vsk n (pride iz formule $[\mathcal{E} : \mathcal{F}] = [\mathcal{E} : \mathcal{L}][\mathcal{L} : \mathcal{F}]$), kar pa je protislovje.

7.5 Razpadna polja

Dan je $f(X) \in \mathcal{F}(X)$ in denimo, da nima ničel v $\mathcal{F}$, zanima nas, ali bi obstajala kakšna razširitev, v kateri bi $f(X)$ imel ničlo. (Če je $\mathcal{F} \subseteq \mathbb{C}$ potem nam odgovor da kar osnovni izrek algebre, a nas zanimajo bolj splošna polja).
Primer:
"Ponovno odkrijmo"$\mathbb{C}$. Vemo, da $X^2+1 \in \mathbb{R}$ nima ničel. Radi bi pokazali, da

$$\mathbb{R}[X]/_{(X^2+1)} \cong \mathbb{C}$$

Dokaz.

$$\varphi : \mathbb{C} \to \mathbb{R}[X]/_{(X^2+1)}, \varphi(a+bi) = (a+bX) + \underbrace{(X^2+1)}_{=\mathcal{I}}$$

Preprosto preverimo, da je φ izomorfizem. $i \in \mathbb{C}$ je v smislu tega izmorfizma identifikacija z $X + \mathcal{I}$. □

Izrek 35:
Naj bo $\mathcal{F}$ polje in $f(X) \in \mathcal{F}[X]$ nekonstanten polinom. Potem ima $f(X)$ ničlo v kaki razširitvi $\mathcal{E}$ polja $\mathcal{F}$.

Dokaz. Naj bo $p(X) \in \mathcal{F}[X]$ nerazcepen polinom, ki deli $f(X)$(ta obstaja, saj vemo, da je $F(X)$ produkt nerazcepnih polinomov). $\mathcal{I} = (p(X))$ in ker je $p(X)$ nerazcepen vemo da je

$$\mathcal{E} := \mathcal{F}[X]/_{\mathcal{I}}$$

polje. Tako lahko na $\mathcal{F}$ gledamo kot na podpolje v smislu vložitve $a \mapsto a + \mathcal{I}$ ($a + \mathcal{I} \neq 0$, saj $\mathcal{I}$ ne vsebuje konstantnih polinomov). Tako lahko poljuben element a identificiramo z $a + \mathcal{I} \in \mathcal{E}$. Vzemimo sedaj $g(X) \in \mathcal{F}[X](\subseteq \mathcal{E}[X])$. $g(X) = a_0 + a_1X + \ldots a_nX, a_i \in \mathcal{F}$ in jih zaradi lažje predstave pišimo kot $a_i + \mathcal{I} \in \mathcal{E}$.
$g(X+\mathcal{I})$ je tako vrednost polinoma $g(X) \in \mathcal{E}[X]$ v elementu $X + \mathcal{I} \in \mathcal{E}$. $g(X+\mathcal{I}) = (a_0+\mathcal{I}) + (a_1+\mathcal{I})(X+\mathcal{I}) + \cdots + (a_n+\mathcal{I})(X+\mathcal{I})^n = (a_0 + \mathcal{I}) + (a_1X+\mathcal{I}) + \cdots + (a_nX^n+\mathcal{I}) = g(X)+\mathcal{I}$. Za $g(X) = f(X)$ tako dobimo $f(X+\mathcal{I}) = \underbrace{f(X)+\mathcal{I}=\mathcal{I}}_{f(X)\in\mathcal{I}} = 0$
Tako je $X + \mathcal{I} \in \mathcal{E}$ ničla polinoma $f(X)$. □

Izrek 36:
Naj bo $\mathcal{F}$ polje in $f(X) \in \mathcal{F}[X]$ nekonstanten polinom z vodilnim koeficientom $c \in \mathcal{F}$. Potem obstaja taka razširitev $\mathcal{E}$ polja $\mathcal{F}$, da je $f(X) = x(X - a_1)^{k_1} \dots (X - a_r)^{k_r}$ za neke $a_i \in \mathcal{F}$.

Dokaz. Izrek pove, da obstaja razširitev $\mathcal{E}_1$ in $a_1 \in \mathcal{E}_1 . f(a_1) = 0$. Sledi da $f(X) = (X - a_i)g(X)$ na nek $g(X) \in \mathcal{E}_1[X]$. Potem induktivno obstaja razširitev $\mathcal{E}_2 \supseteq \mathcal{E}_1 \supseteq \mathcal{F}$ in $a_2 \in \mathcal{E}_2 . g(a_2) = 0$. $f(X) = (X - a_1)(X - a_2)h(X), h(X) \in \mathcal{E}_2[X]$. Tako nadaljujemo do konca. □

Opomba: Tako vidimo, da za vsak nekonstanten polinom $f(X) \in \mathcal{F}[X]$ obstaja razširitev, v kateri ima $f(X)$ toliko ničel štetih z njihovo večkratnostjo, kot je njegova stopnja.

Definicija 161: Pravimo, da polinom $f(X) \in \mathcal{F}[X]$ razpade v polju $\mathcal{E}$, le je $f(X)$ produkt lineranih polinomov iz $\mathcal{E}[X]$. Če $f(X)$ razpade v $\mathcal{E}$, ne razpade pa v nobenem podpolju $\mathcal{E}$, $\mathcal{E}$ imenujemo **razpadno polje** $f(X)$.

Izrek 37:
Za vsak nekonstanten polinom $f(X) \in \mathcal{F}[X]$ obstaja razpadno polje.

Dokaz. Naj bo $\mathcal{E}$ polje iz prejšnjega izreka. $f(X) = c(X - a_1)^{k_1} \dots (X - a_r)^{k_r}, a_i \in \mathcal{E}$. Vsako podpolje $\mathcal{E}$, v katerem $f(X)$ razpade mora vsebovati a_i, torej ja to razpadno polje $\mathcal{F}(a_1, \dots, a_n)$ □

Opomba: a_i so ničle $f(X) \in \mathcal{F}[X]$, zato so to algebraični elementi nad $\mathcal{F}$, tako je razpadno polje vselej **končna razširitev**.
Primer:
Kaj je razpadno polje $X^2 + 1$, odgovor je odvisien od izbire $\mathcal{F}$.

- $\mathcal{F} = \mathbb{Q}$ Seveda $X^2 + 1$ razpade v $\mathbb{C}$, razapdno polje pa je že $\mathbb{Q}(i, -i) = \{a + bi |\ a, b \in \mathbb{Q}\}$
- $\mathcal{F} = \mathbb{R}$, razpadno polje je $\mathbb{R}(i) = \mathbb{C}$
- $\mathcal{F} = \mathbb{C}$ $X^2 + 1$ razpade že v $\mathcal{F}$, zato je to že kar razpadno polje.
- $\mathcal{F} = \mathbb{Z}_2$, $(X^2 + 1) = (X + 1)^2$, zato razpade že kar v $\mathcal{F}$

Opomba: Razpadno polje poljubnega nekonstantnega polinoma obstaja, ni pa enolično določeno.

Dokaz. Poljubni razpadni polji istega polnoma sta si izomorfni □

Opomba: Ni dokaza

7.6 Algebraično zaprta polja

Definicija 162: Polje $\mathcal{Z}$ je **algebrično zaprto**, le ima vsak nekonstanten polinom iz $\mathcal{Z}[X]$ vsaj eno ničlo v $\mathcal{Z}$

Opomba: Osnovni izrek algebre: $\mathbb{C}$ je algebraično zaprto polje.
Opomba: Naslednje trditve so si ekvivalentne:

- $\mathcal{Z}$ je algebraično zaprto
- Vsak nekonstanten polinom iz $\mathcal{Z}[X]$ je produkt linearnih faktorjev iz $\mathcal{Z}[X]$, $f(X) = c(X - a_1)^{k_1} \dots (X - a_r)^{k_r}, a_i \in \mathcal{Z}$
- Vsak nekonstanten polinom iz $\mathcal{Z}[X]$ ima toliko ničel štetih z njivovo večkratnostjo, kot je njegovo stopnja.

Trditev 58: Naj bo $\mathcal{L}$ algebraična razširitev $\mathcal{F}$, če je $\mathcal{E}$ razširitev $\mathcal{L}$ i nje $X \in \mathcal{E}$ algebraičen nad $\mathcal{L}$, potem je algebraičen tudi nad $\mathcal{F}$.

Dokaz. Po predpostavki je $a_0 + a_1X + \dots a_nX^n =$ za neke $a_i \in \mathcal{L}$, ki niso vsi 0. Torej je X algebraičen že nad poljen $\mathcal{F}(a_0, \dots, a_n)$, to polje pa je končna razširitev $\mathcal{F}$, saj so $a_i \in \mathcal{L}$ in so zato algebraični nad $\mathcal{F}$. Po znanen izreku je $(\mathcal{F}(a_0, \dots, a_n))(X)$ končna razširitev $\mathcal{F}(a_0, \dots, a_n)$ in ker je končna razširitev končne razširitve spet končna razširitev, je to tudi končna razširitev $\mathcal{F}$, vsak element iz končne razširitve pa je algebraičen, torej tudi X. □

Posledica: Algebraična razširitev algebraične razširitve je sama algebraična.

Definicija 163: Polje $\mathcal{A}$ se imenuje **algebraično zaprtje** poja $\mathcal{F}$, če je algebraična zaprto in je algebraična razširitev $\mathcal{F}$.

Primer:
$\mathbb{C}$ je algebraično zaprtje $\mathbb{R}$, ni pa algebraično zaprtje $\mathbb{Q}$, saj ni algebraična razširitev.
Izrek 38:
Naj bo $\mathcal{F}$ podpolje algebraično zaprtega polja $\mathcal{Z}$. Potem je množica $\mathcal{A}$ vseh elementov iz $\mathcal{Z}$, ki so algebraični nad $\mathcal{F}$ algebraično zaprtje $\mathcal{F}$.

Dokaz. $f(X) \in \mathcal{A}[X]$ naj bo nekonstanten polinom, ker $\mathcal{A} \subseteq \mathcal{Z}$ in je $\mathcal{Z}$ algebraično zaprto ima $f(X)$ ničlo $x \in \mathcal{Z}$. x je torej algebraičen nad $\mathcal{A}$, ki je sam po sebi algebraična razširitev $\mathcal{F}$ in je zato po trditvi x tudi algebraičen nad $\mathcal{F}$. To pomeni, $x \in \mathcal{A}$. □

Posledica: Polje algebraičnih števil je algebraično zaprtje polja $\mathbb{Q}$.
Izrek 39:
Vsako polje ima algebraično zaprtje. Poljubni algebraični zaprtji istega polja sta si izomorfni.

Opomba: Ni dokaza
Opomba: Iz tega izreka seveda sledi obstoj razpadnega polja posameznih polinomov

7.7 Končna polja

Cilj: Klasifikacija vseh končnih polj, od katerih zanekrat poznamo $\mathbb{Z}_p$, kjer je p praštevilo.
Vemo, da ima končno polje končno karakteristiko p vsebuje izomorfno kopijo $\mathbb{Z}_p$, vsako polje s karakteristiko 0 pa kopijo $\mathbb{Z}$, zato smemo predpostaviti, da vsako kočno polje s karakteristiko p vsebuje $\mathbb{Z}_p$

Lema 24. *Če je $\mathcal{E}$ končno polje s karakteristiko p, je $|\mathcal{E}| = p^n, n \in \mathbb{N}$*

Dokaz. $\mathbb{Z}_p \subseteq \mathcal{E}$ in seveda

$$n := [\mathcal{E} : \mathbb{Z}_p] < \infty$$

Naj bo $\{b_1, \ldots, b_n\}$ baza $\mathcal{E}$ nad $\mathbb{Z}_p$. Vsak element iz $\mathcal{E}$ torej lahko zapišemo na en sam način kot $\lambda_1 b_1 + \ldots \lambda_n b_n, \lambda_i \in \mathbb{Z}_p$, število vseh možnih zapisov je torej produkt števila zapisov za vsako komponento $|\mathcal{E}| = p * p \ldots p = p^n$. □

Denimo, da je $|\mathcal{E}| = p^n$, $\mathcal{E}^* - \{0\}$ je množica vseh obrnljivih elementov v $\mathcal{E}$ in je grupa za množenje. Za $x \in \mathcal{E}^*$ velja $x^{|\mathcal{E}^*|} = 1$, torej $x^{p^n-1} = 1$ za neničelne x, če to formulo pomnožimo z x dobimo

$$\forall x \in \mathcal{E}.x^{p^n} = x$$

.
Seveda nas zanima, kako poiskati končna polja. Končne razširitve polja $\mathbb{Z}_p$ bodo končna polja s p^n elementi.
Razpadna polja polinomov so končne razširitve. Načeloma lahko izberemo katerikoli polinom iz $\mathbb{Z}_p[X]$, njegovo rzapadno polje bo končna razširitev. Zato zadošča obravnavati polinom iz naslednje leme:

Lema 25. *Če je $\mathcal{E}$ polje s p^n elementi, potem je $\mathcal{E}$ razpado polje polinoma $X^{p^n} - X \in \mathbb{Z}_p[X]$*

Dokaz. $f(X) = X^{p^n} - X$. Prejšnja lema pove, da je vsak $x \in \mathcal{E}$ ničla $f(X)$. Torej ima $f(X)$ toliko ničel v $\mathcal{E}$ kot je njegova stopnja. Zato $f(X)$ v $\mathcal{E}$ razpade. Ker je $\mathcal{E}$ množica vseh njegovih ničel, $f(X)$ ne more razpasti v pravem podpolju $\mathcal{E}$. Zato je razpadno polje. □

Opomba: Lema pravi, da če polje s p^n elementi obstaja, potej je razpadno polje $f(X)$. Toda ali tako polje sploh obstaja?

Lema 26. *Če je $\mathcal{K}$ komutativen kolobar s karakteristiko p, potem je*

$$\varphi : \mathcal{K} \to \mathcal{K}, \varphi(x) = x^p$$

endomorfizem $\mathcal{K}$

Dokaz. $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$ Za dokaz $\varphi(x+y) = \varphi(x) + \varphi(x)$ pa potrebujemo enakost: $(x+y)^p = x^p + y^p$. Po binomskem izreku vemo da velja:

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + y^p$$

Ker $p \mid \binom{p}{k}; k = 1, \ldots, p-1$, v kolobarju s karakteristiko p velja $\varphi(x+y) = (x+y)^p = x^p + y^p = \varphi(x) + \varphi(y)$ □

Opomba: Zgoraj uporabljeni endomorfizem imenujemo **Frobeniusev endomorfizem**.
Če je $\mathcal{K} = \mathcal{E}$ končno polje, je φ avtomorfizem. Ker je $\mathcal{E}$ polje je $\mathrm{Ker}(\varphi)$ ideal in velja $\mathrm{Ker}(\varphi) = \{0\}$ ali $\mathcal{E}$, torej φ je injektiven in če je $\mathcal{E}$ končen tudi surjektiven. $(\varphi \circ \varphi)(x) = (x^p)^p = x^{pp} = x^{p^2}$ in torej:

$$\varrho(x) = (\underbrace{\varphi \circ \cdots \circ \varphi}_{n-\text{krat}})(x) = x^{p^n}$$

Lema 27. *Razpadno polje polinoma $X^{p^n} - X$ nad $\mathbb{Z}_p$ ima p^n elementov.*

Dokaz. Naj bo $\mathcal{E}$ razpadno polje, torej najmajše polje, ki vsebuje vse ničle tega polinoma. Naj bo $\mathcal{E}_0 := \{x \in \mathcal{E} | x^{p^n} = x\}$ množica vseh ničel tega polnoma v $\mathcal{E}$. ϱ je endomorfizem in $\mathcal{E}_0 = \{x \in \mathcal{E} | \varrho(x) = x\}$ Pokazati moramo, da je $\mathcal{E}_0$ podpolje $\mathcal{E}$. To preprosto poračunamo: $x, y \in \mathcal{E}_0$ $\varrho(x - y) = x - y, 1 \in \mathcal{E}_0, \varrho(xy) = xy, \varrho(x^{-1}) = x^{-1}$ in ato celo $\mathcal{E} = \mathcal{E}_0$ (saj je $\mathcal{E}$ najmanjše ple, ki vsebuje vse ničle, množica $\mathcal{E}_0$ vseh ničel pa je že polje.) Pokažimo še, da velja $|\mathcal{E}| = |\mathcal{E}_0| = p^n$. Ker ima $X^{p^n} - X$ največ toliko ničel kot je njegova stopnja, torej p^n, moramo dokazati, da so vse ničle enostavne. Od tod bo sledilo, da je toliko različnih ničel/elementov v $\mathcal{E}$ kot je spotnja polinoma. Vemo $f(X) = X(X^{p^n-1} - 1)$. 0 je seva enostavna ničla, saj ni ničla $X^{p^n} - 1$. Naj bo $a \in \mathcal{E} - \{0\}$, pokažimo, da je a enostavna ničla $f(X)$. $a^{p^n} = a \implies a^{p^n-1} = 1$, torej $f(X) = X^{p^n} - X = X(X^{p^n-1} - 1) = X(X^{p^{n-1}} - a^{p^n-1}) = X(X - a)(X^{p^n-2} + X^{p^n-3}a + \cdots + Xa^{p^n-3} + a^{p^n-2}) = (X - a)g(X)$, kjer pa $g(a) = -a^{p^n-1} \neq 0 = -1$ □

Opomba: Polje iz zgornje leme (polje z p^n elementi imenujemo **Galoisevo polje** (s p^n elementi) in ga oznalujemo z $\mathcal{GF}(p^n)$
Povzemimo vse z izrekom: **Izrek 40:**
Za vsako praštevilo p in vsako naravno število n obstaja polje $\mathcal{GF}(p^n)$ s p^n elementi. Vsako končno polje je izomorfno enemu izmed teh polj.

Za $n = 1 : \mathcal{GF}(p) = \mathbb{Z}_p$, kako pa računamo v $\mathcal{GF}(p^n)$ za večje n? Kot abelova grupa za $+$ je $\mathcal{GF}(p^n) \cong \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n-\text{krat}}$
Izkaže pa se, da je $\mathcal{GF}(p^n)^*$ ko grupa za noženje vseh neničelnih elementov ciklična. Torej je $\mathcal{GF}(p^n) = \{0, 1, a, a^2, \ldots, a^{p^n-2}\}$
Opomba: Če ima polje karakteristiko p imanjo tudi njegova podpolje in njegove rezširitve karakteristiko p.

7.8 Konstrukcije z ravnilom in šestilom

Iz stare Grčije so se ohranili trije osnovni problemi s šestilom in ravnilom:

1. **Podvojitev kocke**: Ali lahko samo z ravnilom in šestilom iz dane kocke konstruiramo kocko z dvakratno prostornino?

2. **Trisekcija kota**: Ali lahko samo z ravnilom in šestilo vsako kot razdelimo na 3 enake dele.

3. **Kvadratura kroga**: Ali lahko samo z ravnilom in šestilom iz danega kroga konstruiramo kvadrat z isto ploščino?

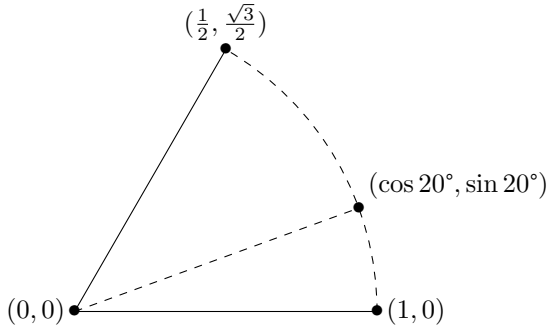
Odgovor je **NE** na vsa vprašanja. Prvega in drugaga je podal P. Wantzel leta 1837, tretjega pa F. von Lindemann leta 1882

Definicija 164: Ravnilo je neoznačeno, s pomočjo ravnila lahko čez dve že obstoječi točki potegnemo premico. S pomočjo šestila lahko naredimo krožnico s središčem v eni izmed obstoječih točk in radijem, ki je enak oddaljenosti središča do katere druge točke. Tako dobimo kot presečišča krožnic in premic nove točke, ki jih lahko uporabimo za konstrukcije nocih objektov.

Da bi lažje delali naše probleme "preoblečemo".

1. Podvojitev kocke poenostavimo, na problem podvojitve kocke z robom 1. Postavimo sedaj kocko v koordinatni sistem: $T_0(0,0,0), T_1(1,0,0)$. Ali lahko sedaj dobimo "podvojeno kocko", ki bo imelo stranico dolžine $\sqrt[3]{2}$. Torej nas zanima, ali lahko iz točk T_0, T_1 s šestilom in ravnilo skonstruiramo $Z(0, \sqrt[3]{2})$

2. Nekatere kote lahko raztretnjinimo (npr $\frac{\pi}{2}$), kaj pa recimo kot 60°? Vzemimo $T_1 = (0,0), T_2 = (1,0), T_3 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ Vprašanje se torej glasi, ali lahko s pomočjo ravnila, šestila in vnaprej postavljenih točk T_1, T_2, T_3 skonstruiramo točko $Z(\cos 20°, \sin 20°)$



Slika 4: Skica konstrukcije

3. Ali lahko z ravnilom in šestilom iz točk $T_1(0,0), T_2(1,0)$ konstuiramo $Z(\sqrt{\pi}, 0)$?

Splošna situacija. Naj bo $\mathcal{T}$ dana množica točk (v naših preimerih $\mathcal{T} = \{T_1, T_2\}$, kakšne so lastnosti vseh točk, ki jih lahko konstruiramo iz $\mathcal{T}$
Bistvo pristopa: Če $\mathcal{T} = \{(a_i, b_i)\}$, potem obravanvamo polje $\mathcal{F}$, ki vsebuje vsa števila a_i, b_i ($\mathcal{F} \subseteq \mathbb{R}$), torej $\mathcal{T} = \mathbb{R} \times \mathbb{R}$ in nas zanimajo lastnosti, ki jih dobimo iz $\mathcal{F} \times \mathcal{F}$. To so v prvem in tretjem problemu $\mathcal{F} = \mathbb{Q}$, v drugem pa $\mathcal{F} = \mathbb{Q}(\sqrt{3})$
V prvem koraku konstrukcije dobimo točko A, za katero velja ena izmed možnosti

1. (pp) A je presečišče dveh premic doblenih iz $\mathcal{T}$

2. (pk) A je presečišče premice in krožnice dobljene iz $\mathcal{T}$

3. (kk) A je presečišče dveh krožnic dobljenih iz $\mathcal{T}$

V drugem koraku torej $\mathcal{T} \cup \{A\}$ dodamo točko B, do katere pridemo na enak način. Tako nadaljujemo in dobimo $\mathcal{T}'$. Zanima nas, do katerih točk pridemo v končno mnogo korakih. Tako dobljene točke $(A, B, \dots)$ imenujemo **konstruirane točke iz množice** $\mathcal{T}$.

Izrek 41:
Naj bo $\mathcal{T}$ množica točk v ravnini in $\mathcal{F}$ tako podpolje $\mathbb{R}$, da je $\mathcal{T} \subseteq \mathcal{F} \times \mathcal{F}$. Če je točka $Z = (a, b)$ konstruirana iz množice $\mathcal{T}$ sta števili a, b algebraični nad $\mathcal{F}$, stopnja algebraičnosti pa je potenca števila 2.

Dokaz. Naj bo A doblena v prvem koraku kot zgoraj. Dokazali bomo, da obstaja tako polje $\mathcal{L}$, da je $A \in \mathcal{L} \times \mathcal{L}$ in $[\mathcal{L} : \mathcal{F}] \in \{1, 2, 4\}$ Ko s tem postopkom nadaljujemo v naslednjem koraku dobimo točko B in polje $\mathcal{M}$: $B \in \mathcal{M} \times \mathcal{M}$ in $[\mathcal{M} : \mathcal{L}] \in \{1, 2, 4\}$ kar nam da $[\mathcal{M} : \mathcal{F}] = 2^u 2^v; u, v \in \{0, 1, 2\}$. Najdaljujmo s postopkom in dobimo polje $\mathcal{E}, Z \in \mathcal{E} \times \mathcal{E}$ in $[\mathcal{E} : \mathcal{F}] = 2^w$. Naj bo $Z(a, b$, $\mathcal{F}(a) \subseteq \mathcal{E}$, ker je $\mathcal{E}$ končna razširitev je $<$ algebraičen nad $\mathcal{F}$ in

$$[\mathcal{F}(a) : \mathcal{F}] \mid [\mathcal{E} : \mathcal{F}] = 2^w \implies \underbrace{[\mathcal{F}(a) : \mathcal{F}]}_{\text{stopnja slgebraičnosti } a} = 2^k$$

Če je premica dobljena iz $\mathcal{T}$, je njena enačba

$$y = \alpha x + \beta \text{ ali } x = \gamma; \alpha, \beta, \gamma \in \mathcal{F} \tag{95}$$

$\alpha = \frac{y_2 - y_1}{x_2 - x_1}, x_i, y_i \in \mathcal{F}$
Če pa je krožnica dobljena iz $\mathcal{T}$, je njena enačba

$$x^2 + y^2 = \delta x + \epsilon y + \zeta;\ \delta, \epsilon, \zeta \in \mathcal{F} \tag{96}$$

Dokazati moramo, da so presečišča posameznih objektov spet točke s komponentami v $\mathcal{F}$

1. Presečišče premice z enačbo od prej in premice z enačbo: $y = \alpha' x + \beta'$ ali $x = \gamma'$ je točka s komponentama v $\mathcal{F}$

2. Presečišče premice in krožnice z zgornjima enačbama je točka $A(x, y)$, kjer za x velja kvadratna enačba, ki ima koeficiente v $\mathcal{F}$:

   $$x^2 + (\alpha x + \beta)^2 = \delta x + \epsilon(\alpha x + \beta) + \zeta$$

   Imamo dve možnosti: če je $x \in \mathcal{F}$ smo končali, če pa $x \neq \mathcal{F}$ potem je algebraične stopnje 2 nad $\mathcal{F}$ torej $[\mathcal{F}(x) : \mathcal{F}] = 2$, podoben sklep naredimo za y in dobimo $\mathcal{L} := \mathcal{F}(x, y)$, za katerega velja: $[\mathcal{L} : \mathcal{F}] = [(\mathcal{F}(x))(y) : \mathcal{F}(x)][\mathcal{F}(x) : \mathcal{F}] \in \{1, 2, 4\}$

3. Presečišče krožnice z enačbo od prej in krožnice z enačbo: $x^2 + y^2 = \delta' x + \epsilon' y + \zeta'$: Enačbi odštejemo in dobimo

   $$(\delta - \delta')x + (\epsilon - \epsilon')y + (\zeta - \zeta') = 0$$

   Če privzamemo, da sta krožnici različni, smo s tem prevedli problem na presečišče premice in krožnice.

□

Posledica: Iz dane kocke z ravnilom in šestilom ne moremo konstruirati ocke z dvakratno prostornino.

Dokaz. Če bi lahko konstruirali bi $Z = (\sqrt[3]{2}, 0)$ lahko konstruirali iz $\mathcal{T} = \{(0,0,0),(1,0,0);\ \mathcal{F} = \mathbb{Q}$. Po izreku bi porem $\sqrt[3]{2}$ bilo algebraično število stopnje 2^k, stopnja $\sqrt[3]{2}$ pa je 3, saj je $X^3 - 2 \in \mathbb{Q}[X]$ nerazcepen. □

Posledica: Kota 60°z ravnilom in šestilom ne moremo razdeliti na 3 enake dele.

Dokaz. Pokazati moramo, do točke $Z(\cos 20°, \sin 20°)$ ne moremo konstruirati iz $\mathcal{T} = \{(0,0),(1,0),(\frac{1}{2}, \frac{\sqrt{3}}{2}\}$; $\mathcal{F} = \mathbb{Q}(\sqrt{3})$. Pokazali bomo, da $\cos 20°$ ni algebraično število stopnje 2^k nad $\mathbb{Q}(\sqrt{3})$, natančneje, število je algebraične stopnje 3. $\cos 3x + i \sin 3x = (\cos x + i \sin x)^3$, realni del: $\cos 3x = (\cos x)^3 - 3\cos x(1 - \cos^2 x) = 4\cos^3 x - 3\cos x$ Vstavimo $x = 20°$in $v = \cos x\ \frac{1}{2} = 4v^3 - 3v$ torej $8v^3 - 6v - 1 = 0$ Vzemimo torej polinmo $1 + 6X - 8X^3 \in \mathbb{Q}[X] \subseteq \mathbb{Q}(\sqrt{3})[X]$ in pokažimo, da je to minimalni polinom nad $\mathbb{Q}(\sqrt{3})$, torej da nima ničle v $\mathbb{Q}(\sqrt{3})$(ker ima stopnjo 3 to pomeni, da j nerazcepen). Recimo, da je a ničla. $b := 2a \in \mathbb{Q}(\sqrt{3})$. Dobimo $1 + 3b - b^3 = 0$, in $b = p + r\sqrt{3}; p, r \in \mathbb{Q}$, $1 + 3q - q^3 - 9qr^2 = 0$ in $r(1 - q^2 - r^2) = 0$ torej $r = 0$ ali $1 - q^2 - r^2 = 0$. Če $r = 0$, $1 + 3q - q^3 = 0$, $q = \frac{m}{n}$, dobimo $1 + 3\frac{m}{n} - \frac{m^3}{n^3} = 0 \implies n^3 + 3mn - m^3 = 0$ kar pomeni, da $m = \pm 1, n = \pm 1$, kar pa je protislovje. Če pa $r^2 = 1 - q^2$ potem velja $1 - 3s + s^3 = 0, s \in \mathbb{Q}$, kar pa je spet protislovje. □

Opomba: Točka, ki jih lahko konstruiramo iz $\mathcal{T} = \{(0,0),(1,0)\}$ imenujemo **konstruktibilne točke**, njihove komponente pa **konstruktibilna števila**.
Posledica: Iz danega kroga z ravnilom in šestilom ne moremo konstruirati kvadrata z isto ploščino.

Dokaz. Če bi lahko bi $Z(\sqrt{\pi}, 0)$ lahko konstrirali iz $\mathcal{T} = \{(0,0),(1,0)\}$, kar bi pomenilo, da je $\sqrt{\pi}$ algebraično število in torej tudi π algebraično število, kar pa ni res, saj je π transcedentno. □