

1. Deljivost v komutativnih klobarjih

$$xy = yx$$

$$1 \in K$$

Gaussova štetila!

Primeri: $\mathbb{Z}$, $\mathbb{F}[X]$, $\mathbb{Z}_n$, $\mathbb{Z}[i] = \{a+bi; a, b \in \mathbb{Z}\}$

Cel klobar - komutativen klobar, brez deliteljev
nič

Osnovni izrek aritmetike $n \in \mathbb{N}$. $n = p_1 p_2 \dots p_s$

$p_1, \dots, p_s \in \mathbb{P}$ prastevila enolično določena

v $\mathbb{F}[X]$: $f(x) = p_1(x) \dots p_s(x)$, kjer so $p_1 \dots p_s$ nerazcepni
enolično določeni:

1.1 osnovni pojmi

Definicija: Naj bo K komutativen kolobar.

1. Element $b \neq 0 \in K$ **deli** element $a \in K$, če

$$a = gb \text{ za nek } g \in K$$

(a je **deljiv** z b , b je **delitelj** a)

2. nenulna elementa $a, b \in K$ sta **asociirana**, če delita drug drugega ali $1 \mid b$ ali $a \mid 1$

3. **Največji skupni delitelj** elementov $a, b \in K$, ki nista 0 , je tak element $d \in K$, da velja

$$a) d \mid a \wedge d \mid b$$

$$b) c \mid a \wedge c \mid b \Rightarrow c \mid d$$

Elemente sta **tujca**, če je njun največji skupni delitelj enak 1 ^(n.s.d.)

4. Element $p \in K$ je **nerazcepen**, če:

$$a) p \neq 0 \wedge p \text{ ni obrnljiv}$$

$$b) p = ab \Rightarrow a \text{ je obrnljiv} \vee b \text{ je obrnljiv}$$

Element je **razcepen**

$$a) p \neq 0 \wedge p \text{ ni obrnljiv}$$

$$b) \text{ ni nerazcepen}$$

Odslej: K je cel

Trditev: Naj bo K cel kolobar. $a, b \in K$ $a \neq 0$
 $b \neq 0$ sta asociirana $\Leftrightarrow \exists u \in K$ obrnljiv, da
je $a = ub$

Dokaz: $(\Leftarrow) a = ub \wedge b = u^{-1}a$

$$(\Rightarrow) a = kb \wedge b = ga \Rightarrow a = kga \Rightarrow$$

$$a(1 - kg) = 0 \Rightarrow 1 - kg = 0 \Rightarrow 1 = kg$$

$$\uparrow \text{ni delitelj ni } a \Rightarrow k = g^{-1}$$

Opomba: Največji skupni delitelj ne obstaja nujno.
Če obstaja pa ni nujno enolično določen.

Dva n.s.d. istega para sta vedno asociirana

Primer: Ali je 2 nerazcepen element? Odvisno od
kolobarja

$$K = \mathbb{Z}: \text{Ja}$$

$$K = \mathbb{Z}[X]: \text{Da}$$

$$K = \mathbb{R}[X]: \text{Ne}$$

$$K = \mathbb{Z}[i]: 2 = (1+i)(1-i) \text{ Ne}$$

$\nwarrow$ katera koli polje

(3 pa ni razcepan)

1.2 Glavni kolobarji:

$$I \text{ ideal: } \bullet I \leq (K, +) \\ \bullet KI, IK \subseteq I$$

K komutativ

Definicija: Naj bo $a \in K$, množica $(a) = \{ax; x \in K\}$

je glavni ideal (generiran z a)

(ideal je glavni, če je generiran z enim elementom)

$$b|a \Leftrightarrow (a) \subseteq (b)$$

$$\Rightarrow a = gb$$

$$ax = b(gx) \Rightarrow ax \in (b) \Rightarrow (a) \subseteq (b)$$

$$\Leftarrow a \in (a) \subseteq (b) \Rightarrow a = gb$$

$$a \text{ in } b \text{ asociirana} \Leftrightarrow (a) = (b)$$

Primer: 1) $\{0\} = (0)$

2) $K = (1)$

$$K = (a) \Leftrightarrow a \text{ je obrnljiv}$$

Ideal je **konageneriran**, če je generiran s končno množico

Če je I generiran z $\{a_1, \dots, a_n\}$ ga označimo z $(a_1, \dots, a_n)$

Opazimo: $(a_1, \dots, a_n) = (a_1) + (a_2) + \dots + (a_n)$

$$(a_1, \dots, a_n) = \{a_1x_1 + a_2x_2 + \dots + a_nx_n; x_i \in K\}$$

Primer: 1. kaj je $(4, 6) \vee \mathbb{Z}$? $(4, 6) = (2) = 2\mathbb{Z}$

Edini ideali: $\mathbb{Z}$ so $n\mathbb{Z}$ (glavni ideali)

2. $\vee F[X]$ ideali?

polinomi s konstantnim členom 0 (X)

$\vee$ si ideali so glavni

3. $I \triangleleft \mathbb{Z}[X]$

$I = \{p(x); \text{konstantni člen je sod}\} = (2, X)$

Ali je I glavni ideal?

npr $I = (f(x))$

$2 = f(x)g(x) \Rightarrow f(x)$ je lahko samo

konstanten $f(x) = a_0 \in 2\mathbb{Z}$

$x \in I \Rightarrow x = a_0h(x)$

$\nwarrow$ sod

$\times$

$\nwarrow x$ ni sod

4) $\vee F[X, Y]$ ideal iz polinomov s konstantnim

členom z 0 (X, Y) tudi ta ideal

ni glavni

Definicija: Cel kolobar K je **glavni kolobar**,
če je vsak njegov ideal glavn; (PID)

↑
principle ideal domain
↑?
ni deliteljav nič

Prime: $\mathbb{Z}$, $F[X]$, $\mathbb{Z}[X]$

Definicija: Cel kolobar K je **evklidski kolobar**, če
 $\exists \delta: K \setminus \{0\} \rightarrow \mathbb{N}_0$ z naslednjimi lastnostima

a) Za $\forall a, b \in K, b \neq 0, \exists q, r \in K, a = qb + r$
in je $r = 0$ ali pa $\delta(r) < \delta(b)$

b) $\delta(a) \leq \delta(ab) \quad \forall a, b \in K \setminus \{0\}$

Izreki: Naslednji kolobarji so evklidski:

a) $\mathbb{Z}$

b) $F[x]$, F polje

c) $\mathbb{Z}[i]$

Dokaz:

a) $\delta: m \mapsto |m|$

b) $\delta(f(x)) = \deg(f(x))$ (0 nima definirane stopnje)

c) $\delta: m+ni \mapsto m^2+n^2$

b) $\checkmark$ Vemo da je to kvadrat absolutne vrednosti.

$$\mathbb{Z} \mid |w| = |zw| \quad |w| \neq 0 \Rightarrow |w| \geq 1$$

a) $a, b \in \mathbb{Z}[i]$, $b \neq 0$

$$a = qb + r$$

$$c = b^{-1}a \in \mathbb{Q}$$

$$c = u + iv \quad u, v \in \mathbb{R}$$

Izberimo $k, l \in \mathbb{Z}$. $|k-u| \leq \frac{1}{2} \wedge |l-v| \leq \frac{1}{2}$

$$g = k + li \in \mathbb{Z}[i]$$

$$r := a - gb \quad r = 0 \vee \delta(r) < \delta(b)$$

$$|r|^2 < |b|^2$$

$$|r|^2 = |a - gb|^2 = |cb - gb|^2 =$$

$$= |c - g|^2 |b|^2 = \left(\underbrace{(u-k)^2}_{\frac{1}{4}} + \underbrace{(v-l)^2}_{\frac{1}{4}} \right) |b|^2$$

$$\leq \frac{1}{2} |b|^2 < |b|^2$$

Izrek: V evklidski kolobar je glavni kolobar

Dokaz: K naj bo evklidski z δ . $I \triangleleft K$

$$I = \{0\} \Rightarrow I = (0)$$

$$I \neq \{0\}. \exists a \in K. (a) = I$$

Naj bo $a \in K$ element, ki ima najmanjšo vrednost δ od vseh $u \in I$

$$(a) \subseteq I \text{ trivialno}$$

Naj bo $x \in I$ poljuben

$$x = \underbrace{a}_\in I + r \quad \forall \quad r \in I \Rightarrow \delta(r) \geq \delta(a) \quad \forall \quad r=0$$

$$\Rightarrow a \mid x$$

glavni $\Rightarrow$ evklidski
kolobar kolobar

Izrek: Naj bosta $a, b \in K$ glavnega kolobarja
 $(a \neq 0 \vee b \neq 0)$. Potem $\exists$ največji skupni delitelj
 obstaja in je oblike

$$d = ax + by \text{ za neke } x, y \in K$$

Dokaz:

Vzemimo ideal $(a, b) = \{ax + by; x, y \in K\} \overset{\text{K je glavni}}{=} (d)$
 $\exists d \in K. (a, b) = (d)$
 $d \neq 0$

$$a \in (a, b) = (d) \Rightarrow d \mid a$$

$$b \in (a, b) = (d) \Rightarrow d \mid b$$

Reamo da $\exists c \in K. c \mid a \wedge c \mid b$

$$d \in (a, b) \Rightarrow d = \underset{c \mid z}{\underset{\parallel}{a}}x + \underset{c \mid w}{\underset{\parallel}{b}}y = c(zx + wy) \Rightarrow c \mid d$$

Izreki: Naj bo $p \neq 0$ EK afektivni koobar.

Naslednji pogoji so ekvivalentni:

- i) $\Leftrightarrow p$ je nerazcepen
- ii) $\Leftrightarrow (p)$ je maksimalni ideal
- iii) $\Leftrightarrow K/(p)$ je polje

Dokaz: ii) $\Leftrightarrow$ iii) Algebra 2

M je **maksimalni ideal** $\Leftrightarrow M \neq K \wedge M \subseteq I \subseteq K \Rightarrow I = K$
 $\forall M = I$

i) $p = ab \Rightarrow a$ obrnljiv ali b obrnljiv,
 p ni obrnljiv

ii) (p) je maksimalen $\Rightarrow (p) \neq K \Leftrightarrow p$ ni obrnljiv

$(p) \subseteq (a) \subsetneq K \Rightarrow (p) = (a) \Rightarrow p|a \wedge a|p$

$p = ab$ in a ni obrnljiv $\Rightarrow$
 b je obrnljiv

i) in ii) utiriva poveske isto

1.3 Endolčna faktorizacija

$$a \neq p_1 p_2 \dots p_n$$

Lema: Naj bo K cel kolobar. Domimo da element $a \in K$ ni enak produktu nerazcepnih elementov. $a \neq 0$ in a ni deljiv. Potem K vsebuje tako neskončno zaporedje elementov $a = a_1, a_2, \dots$ da je $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$ (Neskončno strogo naraščajoče zaporedje glavnih idealov)

Dokaz:

a ni nerazcepen

$a_1 = a_2 b_2$ a_2 in b_2 nista deljiva

Vsej eden izmed njiju (npr a_2) ni produkt nerazcepnih

$a_2 = a_3 b_3$; a_3 ni produkt nerazcepnih

$(a_1) \subsetneq (a_2)$ saj če $(a_1) = (a_2) \Rightarrow a_1 = a_2 u$

$\Rightarrow u = b_2$ je deljiv $\times$

Definicija: Komutativen kolobar K je **noetrd**, če se v naraščajoči verigi idealov

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ ustavi.

Torej $I_n = I_{n+1} = \dots$ od nekoga n naprej

Lema: $\forall$ glavni; kolebar je noetrski

Dokaz: Naj bo $I_1 \subseteq I_2 \subseteq \dots$

$I := \bigcup_{i \in \mathbb{N}} I_i$ to je ideal (v splošnem unija ni)
 $K \subseteq I$ oziroma (ponavadi ni grupa za
 $u, v \in I$ seštevanje)

$u - v \in I$
.....

$u \in I_n, v \in I_m, n \geq m \Rightarrow u - v \in I_n \subseteq I$

I je glavni, zato je $I = (a)$ za nek $a \in I$

$\Rightarrow a \in I_n$ za nek $n \in \mathbb{N} \Rightarrow I \subseteq I_n \Rightarrow$

Od nekega naprej so vsi ideali $I \subseteq I_{n+1} \subseteq I$

Hilbertov izrek o bazi

K noetrski $\Rightarrow K[x]$ noetrski

Primer: $K[x, y]$ ni glavni

$\parallel$
 $\underbrace{K[x][y]}_{\text{glavni}}$
 $\underbrace{\hspace{1.5cm}}_{\text{ni glavni}}$

prejšnji: dve lemi $\Rightarrow$ v glavnem kolobarju
je vsak element produkt nerazcepnih

Definicija: Naj bo K komutativen kolobar.

$p \in K$ je **praelement** $p \neq 0$, pri obrnljiv in
velja $p|ab \Rightarrow pa \vee pb \quad \forall a, b \in K$

Lema: Naj bo K cel. Vsak praelement je nerazcepen.
če je K glavni velja tudi obrat

Dokaz: Naj bo p praelement. $p = xy$

1)

$$p|xy \Rightarrow p|x \vee p|y.$$

$$\text{Recimo da } p|x \Rightarrow x = pu \Rightarrow p = puy \Rightarrow$$

$$uy = 1$$

2) Naj bo K glavni

$\Rightarrow y$ je obrnljiv

p naj bo nerazcepen. p praelement

$p|ab$. Recimo da $p|a \Rightarrow$

p in a sta si tuja (to pomeni da je največji
skupni delitelj 1)

$$1 = px + ay$$

$$b = pbx + (ab)y = p(\dots) \Rightarrow p|b$$

Definicija: Cel kolobar K imenujemo kolobar z enolično faktORIZACIJO (UFD), če se za vsak $a \neq 0$, ni obrnljiv, velja:

- obstajajo taki nerazcepni elementi p_i ,
da je $a = p_1 \dots p_s$
- ta faktorizacija je enolična do asociiranosti
in vrstnega reda faktorjev natanko
to pomeni: $a = q_1 \dots q_t$; q_i nerazcepni
 $\Rightarrow s = t \quad \exists \pi \in S_n, \exists \pi(i)$ asociiran z p_i

Izreke: V glavnem kolaber je kolaber z enolično bakterizacijo

Dokaz: $a \neq 0$ n: obrniti v.

Vemo iz prvih dveh lema: a je produkt nerazcepnih

$$a = p_1 \dots p_s \text{ recimo da je kad } a = g_1 \dots g_t$$

$$p_1 | a \Rightarrow p_1 | z_1 \dots z_i \Rightarrow \text{Field. } p_1 | z_i \text{ BSZS } p_1 | z_i$$

↑
nerazcepan + glavni klobas → proslavet

I_1 hergestellt $\Rightarrow p_1$ in I_1 ist 8; also eintraue

$$p_i / p_1 \dots p_s = p_1 u_2 \dots u_t$$

$p_2 \dots p_s = u_2 \dots u_s$ p -slope pairing

S=t: $S \geq t \Rightarrow u = \underbrace{p_{i+1} \dots p_s}_{\text{negaz cef } n_i} \text{ kes } n_i \text{ mozaere}$

2. Modeli

2.1. Caylyjev izrek za kolobarje

$$\begin{array}{ll} G \longrightarrow G & \varphi: G \longrightarrow \text{Sym } G \\ L_a: x \longmapsto ax & a \longmapsto L_a \end{array}$$

M aditivna grupa

$\text{End}(M) =$ množica vseh endomorfizmov $M \rightarrow M$

$$\varphi \in \text{End } M \iff \varphi: M \rightarrow M; \varphi(u+v) = \varphi(u) + \varphi(v)$$

$\text{End } M$ je kolobar če vpeljemo

$$\varphi + \psi, \varphi\psi: M \rightarrow M$$

$$(\varphi + \psi)u = \varphi(u) + \psi(u)$$

$$(\varphi \cdot \psi)(u) = \varphi(\psi(u))$$



Izrek: $\forall$ klobar lahko vložimo v klobar
endomorfizmov neke aditivne grupe

Dokaz: K klobar

$$a \in K. \quad l_a: K \rightarrow K \\ x \mapsto ax$$

$$l_a(x+y) = l_a(x) + l_a(y)$$

$$l_a \in \text{End}(K) \\ K \text{ kot grupa za } +$$

$$\varphi: K \rightarrow \text{End} K$$

$$a \mapsto l_a$$

$$\varphi(a+b) = l_{a+b} = l_a + l_b = \varphi(a) + \varphi(b)$$

$$(a+b)x = ax + bx$$

$$\varphi(ab) = l_{ab} = l_a \circ l_b = \varphi(a) \varphi(b)$$

$$(ab)x = a(bx)$$

$$\varphi(1) = 1 = \text{id} = l_1$$

injektivnost:

$$a \in \ker \varphi \Leftrightarrow l_a = 0 \Leftrightarrow ax = 0 \quad \forall x \Leftrightarrow a = 0 \quad (\text{ker } x = 1)$$

Fija

Gaybey

E

(unle)

Naj bo A algebra nad poljem F

V vektorski prostor nad F

$\text{End}_F(V)$

Napodoben rezultat dokazemo

Izrek: $\forall$ algebra nad F lahko vložimo v
algebra endomorfizmov nekakega vekt. prostora
nad poljem F .

$\dim A = n$ $\swarrow$ matrike $n \times n$ nad F
 $\dim A < \infty$ $M_n(F)$

$A \hookrightarrow \text{End}_F(A) \cong M_n(F)$ A lahko vložimo v algebra lin. operatorjev
končno razsežnega prostora

Posledica: $\forall$ končno razsežna algebra A nad F lahko vložimo v algebra $n \times n$ matrik za nek $n \in \mathbb{N}$
 $M_n(F)$

Primer: A končno razsežna algebra nad F
Ali ta algebra lahko vsebuje take elemente s in t
da je $st - ts = 1$

ekvivalentno: ali obstajata taki matriki S in T , da
je $ST - TS = I$

$$\text{sl}(ST - TS) = \text{sl}(I) = n$$

$$\begin{array}{ccc} \parallel & & \parallel \\ \text{sl}(ST) - \text{sl}(TS) & = & 0 \end{array}$$

če je $\text{char} F = 0$ je to protislovje

2.2 Definicija module

Definicija: Naj bo K kolobar. Množica M

skupaj z binarno operacijo $(a, u) \mapsto au$

in $K \times M \rightarrow M$ in binarno operacijo

$M \times M \rightarrow M : (u, v) \mapsto u+v$ je **modul nad K**

ali **K -modul**, če velja:

- 1) $(M, +)$ je abelova grupa
- 2) $(a+b)u = au + bu \quad \forall a, b \in K, \forall u \in M$
- 3) $a(u+v) = au + av \quad \forall a \in K, \forall u, v \in M$
- 4) $(ab)u = a(bu) \quad \forall a, b \in K, \forall u \in M$
- 5) $1 \cdot u = u \quad \forall u \in M$

Operaciji $(a, u) \mapsto au$ pravimo množenje s skalari:

ali tudi **modulsko množenje**

Opomba: Pojem K -modula M je ekvivalenten

pojmu homomorfizma kolobarjev $K \rightarrow \text{End}(M)$

Dokaz: Naj bo M K -modul

$$\varphi: K \rightarrow \text{End}(M): a \mapsto (u \mapsto au)$$

Naj bo φ homomorfizem. $\varphi: K \rightarrow \text{End}(M)$

postane M K -modul, če definiramo

$$a \cdot u = \varphi(a)(u)$$



Definirali smo **levi modul nad K** . Poznamo
tudi desne, namesto au imamo ua in podobno

Naj bo M levi K -modul. Če definiramo
 $ua := au$ je to potem desni K -modul, če je
 K komutativen

Odslej modul = levi modul

Primeri:

1. $K=F$ potem je F -modul = vek. prostor nad F

2. Vseke M aditivne skupine (= abelove grupe) je $\mathbb{Z}$ -modul, če definiramo

$$n \cdot u = \underbrace{u + \dots + u}_{n\text{-krat}}$$

$$(-n) \cdot u = n \cdot (-u)$$

$$0 \cdot u = 0$$

3. $\forall$ kolobar K postane modul nad semimnozbo, če definiramo $a \cdot u$ kot običajni produkt $a \cdot u \in K$

4. Naj bo I levi ideal K

I je K -modul, če je $a \cdot u$ običajni produkt

5. Naj bo K podkolobar K' . Če $a \cdot u$ označuje množenje v K' , je K' K -modul

6. $K = M_n(F)$ $M = F^n$

$A \cdot u$ = običajno množenje matrike z vektorji

7. Trivialni ali ničelni modul

2.3 Osnovni pojmi teorije moduler

Podmoduli

Podmodul je podmnožica, ki je za isti operaciji sama modul.

Če je $N \subseteq M$ je N podmodul, če

$$1) (N, +) \leq (M, +) \quad (u, v \in N \rightarrow u - v \in N)$$

$$2) KN \subseteq N \quad (\forall a \in K, \forall n \in N, a \cdot n \in N)$$

Primeri:

1. če je V vekt. prostor nad F je podmodul = podprostor

2. Podmodul $\mathbb{Z}$ -modula so podgrupe

3. Podmodul K -modula K so levi ideali

če sta N_1 in N_2 podmoduli je tudi
 $N_1 \cap N_2$ in $N_1 + N_2$ podmoduli

Def: Če sta R in M edini podmoduli M
rečemo da je M **enostaven**

Primeri:

1. V. prostor je enostaven kot modul $\Leftrightarrow$ je 1-razsečen

2. Aritmetična grupa je enostaven kot $\mathbb{Z}$ -modul $\Leftrightarrow \cong \mathbb{Z}_p$

3. $M = M_n(F)$ $M = n \times n$

$$M \subseteq F^M$$

$$N \neq \{0\}; 0 \neq u \in N$$

$$Au \in N \text{ za } \forall A \in M_n(F) \quad \{A \mid A \in M_n(F)\} = F^n$$

M je enostaven modul nad matrikami;

Homomorfizmi: modula

M, N K -moduli

$\varphi: M \rightarrow N$ je homomorfizem K -modula, če

velja $\varphi(u+v) = \varphi(u) + \varphi(v) \quad \forall u, v \in M$ in

$$\varphi(au) = a\varphi(u) \quad \forall a \in K, \forall u \in M$$

oziroma ekvivalentno $\varphi(au+bv) = a\varphi(u) + b\varphi(v)$

Rečemo jim tudi K -linearne preslikave

$$\ker \varphi = \{u \in M; \varphi(u) = 0\} \quad \text{im } \varphi = \{\varphi(a); a \in M\}$$

sta podmodula M oz. N

$$\ker \varphi = \{0\} \Leftrightarrow \varphi \text{ injektivna}$$

$$M \cong N = \text{izomorfizem } M$$

(obstaja izomorfizem)

Primeri: $K = F \Rightarrow$ homomorfizmi so linearne preslikave

2) $K = \mathbb{Z}$: homomorfizmi so preslikave ki ohranjajo vsoto

3) I levi ideal K

$$u_0 \in I \quad \varphi: I \rightarrow I \quad \swarrow \text{desna množenje}$$

$$u \mapsto uu_0 \in I$$

$$\varphi(au) = auu_0 = a(uu_0) = a\varphi(u)$$

φ je endomorfizem K modula I

Kolobarji endomorfizmov

V vek. pr. $\text{End}_F(V)$

M aditivna grupa $\subseteq \text{End}(M)$

$\text{End}_K(M) = \{ \psi; \text{endomorfizmi } K\text{-modula } M \}$

je kolobar če vpišemo

$$(\psi + \varphi)(u) = \psi(u) + \varphi(u)$$

$$(\psi \cdot \varphi)(u) = \psi(\varphi(u))$$

Schurova lema: Če je M enostaven K -modul,
je kolobar $\text{End}_K(M)$ obseg n zi elementov
in dovoljiv:

Dokaz:

Naj bo $0 \neq \varphi \in \text{End}_K(M)$

$\ker \varphi$ in $\text{im } \varphi$ sta φ -modula in M je enostaven

$$\Rightarrow \ker \varphi = \{0\} \quad (\ker \varphi \neq 0) \quad \text{in} \\ \text{im } \varphi = M$$

$\Rightarrow \varphi$ je bijekcija, zato je dovoljiv element

Kvocietni; modeli

M K -model

N podmodel

$$M/N := \{u+N; u \in M\}$$

$$(u+N) + (v+N) = (u+v)+N$$

$$a(u+N) = au+N$$

S tem postane M/N K -model
inenujemo ga kvocietni model.

Primeri:

1. $K=F \Rightarrow$ kvocietni vektor.

2. $K=\mathbb{Z} \Rightarrow$ kvocietni grupa

3) I levi ideal $K \Rightarrow K/I = \{a+I; a \in K\}$

$$(a+I) + (b+I)$$

$$a(b+I) = ab+I \quad \swarrow \text{dovodj je levi ideal}$$

Izrek o izomorfizmu

$$\varphi: M \rightarrow N \Rightarrow M/\ker \varphi \cong \text{Im } \varphi$$

Direktne vsote modulov

$M_1, \dots, M_s$ K -moduli:

Množica $M_1 \times \dots \times M_s$ postane K -modul,
če definiramo

$$(u_1, \dots, u_s) + (v_1, \dots, v_s) = (u_1 + v_1, \dots, u_s + v_s)$$

$$a(u_1, \dots, u_s) = (au_1, \dots, au_s)$$

Imenujemo ga **direktna vsota** modulov
 $M_1, \dots, M_s$ in pišemo $M_1 \oplus \dots \oplus M_s$

Natančneje: Zunanja direktna vsota

Naj bo sedaj M modul in $M_1, \dots, M_s$ njegovi podmoduli:

če velja

a) $M = M_1 + \dots + M_s$ kroz M :

b) $\forall i \in [s]. \quad M_i \cap (M_1 + \dots + M_s) = \{0\}$

potem M imenujemo **(notranja) direktna vsota** podmodulov $M_1, \dots, M_s$

b) je ekvivalenten da iz $v_1 + v_2 + \dots + v_s = 0$ sledi:
 $v_i = 0$ za $\forall i \in [s]$

Če je M nekranja direktna vsota $N_1 \dots N_s$ je
 $M \cong N_1 \oplus \dots \oplus N_s$

Izomorfizem je podan z $v_1 + \dots + v_s \mapsto (v_1, \dots, v_s)$
 $\leftarrow$

ker je $v_1 + \dots + v_s$ enoličen zgornj

Tudi natr. dir. vsot. označimo z

$$N_1 \oplus \dots \oplus N_s$$

Naj bo N podmodul M . Zanimata je
 N **direktni sumant**, če ^{obstaja} ~~obstaja~~ tak
podmodul N' , da je $M = N \oplus N'$

Primer

1. $K = \mathbb{F}$ ^{ust.} je ~~je~~ ^{podprostor} je direktni sumant

$$2. K = \mathbb{Z} : M = \mathbb{Z}$$

Podmoduli (= podgrupe) so $n\mathbb{Z}$ ($n \in \mathbb{N}_0$)

Direktna sumanda sta le $\{0\}, n\mathbb{Z}$

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \neq \{0\}$$

Generiranje modulov

M K -modul

$u \in M$

$Ku = \{au; a \in K\}$ je podmodul M , ki
gotovo vsebuje u . Rečemo da je Ku
generiran z u

Podmodul generiran z enim samim
elementom se imenuje **ciklični podmodul**

Ciklični modul je generiran z enim samim
elementom

Primeri:

1. $K = F$ 1-razsežni podprostorji in $\mathbb{Z}$ -m
 2. $K = \mathbb{Z}$: ciklični $\mathbb{Z}$ modul so $\mathbb{Z}$ ciklične grupe
 3. K komutativen kolobar ... ~~ide~~ glavn
- $u \in I$ lev: ideal $K/I = \{a+I; a \in K\}$

K/I je ciklični modul generiran z $1+I$

Naj bo $X \subseteq M$. Podmodul generiran
z X je množica vseh linearnih
kombinacij

Če je podmodul generiran s X , cel M ,
pomeni da množica X generira M
 M je končno generirana

2.4 Prosti moduli

Definicija: Podmnostica B K -modula M je **linearno neodvisna**, če za vse različne elemente $e_1, \dots, e_s \in B$ in vse $a_1, \dots, a_s \in K$ in $a_1 e_1 + \dots + a_s e_s = 0$ sledi $a_1 = \dots = a_s = 0$.
Če je B neskončna podmnožica je linearno neodvisna, če je vsaka končna podmnožica lin. neodvisna.

Če je B linearno neodvisna in generira M je ta **Baza** modula M .

a b c d e f g h i j k l
m n o p r s t u v x y z

Opomba: Če je B baza M , za $\forall u \in M$ obstaja $e_1, \dots, e_s \in B$, da je $u = a_1 e_1 + \dots + a_s e_s$ kjer so a_i enolično določeni el. iz K .

Pišemo $u = \sum a_i e_i$.

Primeri:

1) $K=F$: vsi vek. prost. imajo bazo

2) $K=\mathbb{Z}$ G katera abelova grupa

$u \in G$ že žuž n : lin neodvisne

ker je $n \cdot u = 0$ kjer je n red grupe

Edina linearno neodvisna množica je prazna množica

3) $K=\mathbb{Z}$ $G=\mathbb{Z}$

bazis $\emptyset$ sta $1, 12, \dots, n, n+1, \dots$

Definicija: Modul, ki ima bazo se imenuje
Prosti modul

Primeri: 1) Vsek vek. gr. je prost (kot F modul)

2) K klobč, polni je

$\underbrace{K \oplus \dots \oplus K}_s \text{ sumanda} = K^s$ je prost K modul

3) $\mathbb{Z}^s$ je prosta abelova grupa $\equiv$ abelova grupa, ki
je kot $\mathbb{Z}$ modul prosta

Vespa

$0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$ je kratko eksaktno
 zaporedje $\varphi \text{ inj}, \psi \text{ sur } \text{Im} \varphi = \text{Ker} \psi \quad (\psi \varphi = 0)$

L podmodul M

$$0 \rightarrow L \rightarrow M \rightarrow M/L \rightarrow 0$$

$$L \cong \text{Im} \varphi \quad \text{ker je inj}$$

$$L \cong \text{Im} \varphi \cong \text{Ker} \psi$$

$$N \cong M/\text{Im} \varphi \cong M/L$$

$$0 \rightarrow L \xrightarrow{i_L} L \oplus N \xrightarrow{\pi_N} N \rightarrow 0$$

$$t \mapsto (t, 0)$$

$$(t, v) \mapsto v$$

n -tho eksaktno zaporedje razpade, če zaporedje

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0 \quad \text{izgleda kot}$$

$$0 \rightarrow L \rightarrow L \oplus N \rightarrow N \rightarrow 0$$

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

$$\downarrow i_L \quad \downarrow \sigma \quad \downarrow i_N$$

$$0 \rightarrow L \rightarrow L \oplus N \rightarrow N \rightarrow 0$$

$\exists \sigma$ izomorfizem
 da ta diagram
 komutira

$$\sigma \varphi = i_L \quad \sigma(\varphi(t)) = (t, 0)$$

$$\pi_N \sigma = \psi \quad \pi_N = \psi \sigma^{-1} : \varphi(\sigma^{-1}(t, v)) = v$$

Izreki: Za katrsko eksaktno zaporedje

$0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$ so naslednji pogoji ekvivalentni:

$\Leftrightarrow$ zaporedje je razpadno

$\Leftrightarrow \exists$ homomorfizem $\varphi': M \rightarrow L$, da je $\varphi'\varphi = \text{id}_L$

$\Leftrightarrow \exists$ homomorfizem $\psi': N \rightarrow M$, da je $\psi\psi' = \text{id}_N$

Dokaz

ii) $\Rightarrow$ i) $\sigma(u) = (\varphi'(u), \psi(u))$

σ je res izomorfizem in uveljavlja pogoj

σ je homomorfizem obeh

$u \in \ker \sigma \Rightarrow \varphi'(u) = 0 \wedge \psi(u) = 0$

$\Rightarrow u \in \ker \varphi = \text{Im } \psi \Rightarrow u = \psi(t)$

$\Rightarrow \varphi'(\psi(t)) = 0 = t \Rightarrow u = 0$ torej je injektivno

σ surj $(t, v) \in L \oplus N$

$\exists u \in M. (t, v) = \sigma(u) = (\varphi'(u), \psi(u))$

$\Rightarrow \varphi'(u) = t, \psi(u) = v$

$\psi(u) = v \Rightarrow \exists u_0 \in M: \psi(u_0) = v$

$\psi(u_0 + \psi(l)) = v$ ker je $\ker \psi = \text{Im } \varphi$ za $\forall l \in L$

Poiščemo $t \in L$, da bo $\varphi'(u_0 + \psi(l)) = t$

$\varphi'(u) + \varphi'(\psi(l)) = t$

$\varphi'(u) + l = t$

$l = t - \varphi'(u)$

enačbe

$\sigma(\psi(t)) = (\varphi'(\psi(t)), \psi(\psi(t))) = (t, 0)$ ✓

$\pi_N(\sigma(u)) = \pi_N(\varphi'(u), \psi(u)) = \psi(u)$ ✓

iii) $\Rightarrow$ i)

$\sigma': L \oplus N \rightarrow M$

$\sigma'(t, v) = \varphi(t) + \psi'(v)$

σ' je homomorfizem

σ' je izomorfizem

$(t, v) \in \ker \sigma' \Rightarrow \varphi(t) + \psi'(v) = 0 \Rightarrow$

$\underbrace{\varphi(t)}_0 + \underbrace{\psi'(v)}_v = 0 \Rightarrow v = 0$

$\varphi(t) + \underbrace{\psi'(v)}_0 = 0 \Rightarrow t = 0$ ker je φ inj

surj

$u \in M$

$u = \varphi(t) + \psi'(v)$

$\psi(u) = 0 + v \Rightarrow v = \psi(u)$

$u = \varphi(t) + \psi'(\psi(u))$

$\varphi(t) = u - \psi'(\psi(u))$

cilj je pokazati da $u - \psi'(\psi(u)) \in \text{Im } \varphi$

vemo: $\text{Im } \varphi = \ker \psi$

$\psi(u - \psi'(\psi(u))) = \psi(u) - \psi(u) = 0$ ✓

Naj bo $\sigma = \sigma^{-1}$

$\sigma t = i_L \quad \varphi(t) = \sigma'(t, 0) = \varphi(t)$ ✓

drugi pogoj:

i) $\Rightarrow$ ii) in iii)

$\sigma: M \rightarrow L \oplus N$

$\varphi' = \pi_L \sigma \quad \psi' = \sigma^{-1} i_N$

pogledano definicije in vidimo da je vrsto

2.6 Projekтивni moduli:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow \vartheta & & \searrow \psi & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array}$$

φ surjektiven

Definicija: Modul P je **projekтивен**, če za φ homomorfizem $\varphi: P \rightarrow N$ in vsek epim. $\varphi: M \rightarrow N$ obstaja tak homomorfizem $\vartheta: P \rightarrow M$ da je $\varphi\vartheta = \varphi$

Lema: Vsek prost modul je projekтивен

Dokaz: P prost

$$\begin{array}{ccccc} & & P & & \\ & \swarrow \vartheta & & \searrow \psi & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array}$$

P ima bazo B

$\varphi(e) = \varphi(u_e)$ za nek $u_e \in M$

$\vartheta: e \rightarrow u_e$

ϑ je z delovanjem na bazi enolično določen in $\varphi\vartheta = \varphi$

Izrek: Za modul P so naslednje trditve ekvivalentne

$\Leftrightarrow P$ je projekcijski modul

$\Leftrightarrow \forall$ kratko eksaktno zaporedje W se konča s P , razpade $0 \rightarrow L \rightarrow M \xrightarrow{\psi} P \rightarrow 0$

$\Leftrightarrow$ obstaja modul L , da je $L \oplus P$ prost

Dokaz:

i) $\Rightarrow$ ii) P proj. $\begin{array}{c} \psi \\ \swarrow \downarrow id \\ 0 \rightarrow L \rightarrow M \rightarrow P \rightarrow 0 \end{array}$

$\exists \psi$ da je $\psi \psi = id_P$

ψ' je ψ in tako zaporedje razpade

ii) $\Rightarrow$ iii) Vsak modul (tudi P) je nemnožična slika prostega modula, ki ga označuje z M

$L \rightarrow M \xrightarrow{\psi} P \rightarrow 0$
definiramo
 $L := \ker \psi$

$0 \rightarrow \ker \psi \xrightarrow{id} M \xrightarrow{\psi} P \rightarrow 0$

ker to zaporedje razpade sledi:

$M \cong L \oplus P$

$L \oplus P$ je tudi prost

ii) $\Rightarrow$ i) $L \oplus P$ je prost za nek L P je projekcijski

$\begin{array}{c} L \oplus P \xrightarrow{\pi_P} P \\ \swarrow \theta \downarrow \psi \\ M \xrightarrow{\psi} P \rightarrow 0 \end{array}$ $\psi := \theta \pi_P$

$\psi \psi = \psi$ $\psi \psi = \psi \theta \pi_P = \psi \pi_P \pi_P = \psi id_P = \psi$

Primer: želimo najti projektiivni modul k ki ni prost

K je prost k -modul

k je komutativen in obstaja $e = e^2 \neq 0, 1$ idempotent

$P := eK = \{ex; x \in K\}$ je podmodul ($\perp$ -ideal)

$$1-e \in K \Rightarrow (1-e)ex = 0 \text{ za } \forall x \in K$$

$\Rightarrow \{ex\}$ nikoli ni linearne neodvisen:

$$\left\{ \begin{array}{l} K_1, K_2 \text{ kolobarja } K := K_1 \times K_2 \\ e = (1, 0) \end{array} \right.$$

$$K = eK \oplus (1-e)K$$

$$x = ex + (1-e)x$$

$$ex = (1-e)y \quad /e$$

$$ex = 0 \Rightarrow x = 0 \text{ podobno } y = 0 \text{ torej } eK \cap (1-e)K = \{0\}$$

torej je P projektiivni: produkt (kot direktni
sumand prostega), k ni prost

2.7 Tenzorski produkti

$M \otimes N$ K -moduli, kjer je K komutativen kolobar

Moduli bodo nad komutativnim kolobarjem K

N, M K -moduli

Množica $M \times N$ vzemimo prosti modul, ki ima za bazo $M \times N$. Označimo ga z $\mathcal{F} = \mathcal{F}_{M,N}$

Maj bo $\mathcal{N} = \mathcal{N}_{M,N}$ podmodul generiran z vsemi elementi dolike $(au + a'u', v) - a(u, v) - a'(u', v)$,
 $(u, av + a'v') - a(u, v) - a'(u, v')$, kjer $a, a' \in K$

$u, u' \in M, v, v' \in N$

Definicija: **Tenzorski produkt** modulov M in N je modul $\mathcal{F}/\mathcal{N}$. Označimo ga z simbolom

$$M \otimes N = (M \otimes_K N)$$

Preslikava $\Phi: M \times N \rightarrow L$ je bilinearna, če je linearna v vsakem argumentu

$$(\Phi(au + a'u', v) = a\Phi(u, v) + a'\Phi(u', v) \text{ in isto v drugem argumentu})$$

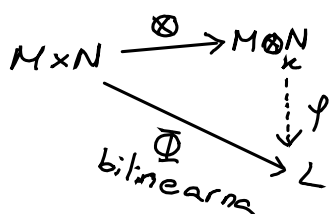
Primeri:

Skalarni produkt, vektorski produkt v $\mathbb{R}^3$, produkt v vsaki

algebri: $(x, y) \mapsto xy$,

produkt matrik $M_{m,n}(F) \times M_{n,p}(F) \rightarrow M_{m,p}(F)$

Izreki: (univerzalna lastnost tenzorskega produkta)



za $\forall$ modula M in N nad
komutativnim klobarjem K , $\exists$ take
bilinarna preslikava $M \times N \rightarrow M \otimes_K N$,
 $(u, v) \mapsto u \otimes v$, za katero velja,

za $\forall$ bilinarno preslikavo $\Phi: M \times N \rightarrow L$, kjer je
 L poljubni K -modul, $\exists$ enolično določena

Linearna preslikava $\varphi: M \otimes_K N \rightarrow L$, da

je $\varphi(u \otimes v) = \Phi(u, v)$ za $\forall u, v \in M \times N$

S to lastnostjo je tenzorski produkt natančno in
enolično določen.

Dokaz $\Rightarrow$

Dokaz: Vpeljimo $u \otimes v := (u, v) + \mathcal{N}$

$$(au + a'u', v) - a(u, v) - a'(u', v) \in \mathcal{N}$$

$\Leftrightarrow$

$$(au + a'u', v) + \mathcal{N} = a(u, v) + \mathcal{N} + a'(u', v) + \mathcal{N}$$

$$(au + a'u') \otimes v = a(u \otimes v) + a'(u' \otimes v)$$

Podobno izpeljemo linearnost preslikave $\otimes$ v drugem argumentu

$\Phi: M \times N \rightarrow L$ bilinearna preslikava.

Iščemo linearno preslikavo φ ^{endolizna}

$\mathcal{F}$ ima bazo $M \times N$, zato lahko Φ razširimo do

lin. preslikave $F: \mathcal{F} \rightarrow L$ $F(u, v) = \Phi(u, v)$.

Ker je Φ bilinearna, $\ker F$ vsebuje podmodul $\mathcal{N}$

$$\left(\begin{aligned} &F(au + a'u', v) - a(u, v) - a'(u', v) \text{ se slika v?} \\ &= F(au + a'u', v) - aF(u, v) - a'F(u', v) = \\ &= \Phi(au + a'u', v) - a\Phi(u, v) - a'\Phi(u', v) = 0 \end{aligned} \right)$$

Zato je $\varphi: M \otimes N \rightarrow L$
 $x + \mathcal{N} \mapsto F(x)$ dobro definirana

Ker je F linearna je tudi φ linearna

$$\varphi(u \otimes v) = \varphi((u, v) + \mathcal{N}) = F(u, v) = \Phi(u, v)$$

φ in Φ se ujemata na $u \otimes v$, torej mora slediti, da se ujemata povsod (ker je φ linearna in Φ bilinearna).

Endoliznost

Naj bo tudi T modul z enako lastnostjo kot $M \otimes N$

ker je $\otimes$ bilinearna, $\exists$

linearna preslikava $\varphi: M \otimes N \rightarrow T$

taka da je $\varphi(u \otimes v) = u \odot v$

Analogno obstaja linearna preslikava

$$\psi: T \rightarrow M \otimes N, \psi(u \odot v) = u \otimes v$$

$(\psi\varphi)(u \otimes v)$ za $\forall$ enostavni tenzor $u \otimes v \Rightarrow \psi\varphi = \text{id}_{M \otimes N}$

$\psi\varphi = \text{id}_T$ analogno

"ujemanje na bazi"



"Praktična" definicija tenzorskega produkta

- $\forall u \in M, \forall n \in \mathbb{N}, \exists u \otimes v \in M \otimes N, \tau$ imenujemo **enostavni** tenzor.
Vsek drug element je vsda teh enostavnih tenzorjev

- $(u+u') \otimes v = u \otimes v + u' \otimes v$

$$u \otimes (v+v') = u \otimes v + u \otimes v'$$

$$(au) \otimes v = u \otimes (av) = a(u \otimes v)$$

$$\text{Zato } 0 \otimes v = u \otimes 0 = 0$$

$$M \times N \xrightarrow{\otimes} M \otimes N$$

$$\varphi(u \otimes v) := \Phi(u, v)$$

$$\searrow \Phi \quad \downarrow \varphi$$

$$\varphi(\sum u_i \otimes v_j) = \sum \Phi(u_i, v_j)$$

Sporočilo izreka je, da je φ dobro definirana

^{Definicija}
 φ, ψ nej. bodlin. preslikave $\varphi: M \rightarrow M'$ in $\psi: N \rightarrow N'$

$$M \times N \longrightarrow M \otimes N$$

$(u, v) \mapsto \varphi(u) \otimes \psi(v)$ je bilinearne preslikave.

Zato $\exists$ linearna preslikava, kijo označimo $\varphi \otimes \psi$, ki

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$$

Imenujemo jo **tenzorski produkt** $\varphi \otimes \psi$

$$(\varphi_1 + \varphi_2) \otimes \psi = \varphi_1 \otimes \psi + \varphi_2 \otimes \psi \text{ in podobno drugi faktor}$$

$$a(\varphi \otimes \psi) = (a\varphi) \otimes \psi = \varphi \otimes (a\psi)$$

$$(\varphi_1 \otimes \varphi_2)(\psi_1 \otimes \psi_2) = (\varphi_1 \psi_1) \otimes (\varphi_2 \psi_2)$$

$$\varphi, \psi \text{ izomorfizme} \Rightarrow \varphi \otimes \psi \text{ bij}$$

$$(\varphi \otimes \psi)^{-1} = \varphi^{-1} \otimes \psi^{-1}$$

Izrek. Naj bodo M, N, R moduli. Potem velja

a) $M \otimes N \cong N \otimes M$

b) $(M \otimes N) \otimes R \cong M \otimes (N \otimes R)$

c) $(M \otimes N) \otimes R \cong M \otimes R \oplus N \otimes R$

d) $M \otimes K \cong M$

Dokaz:

$$M^{\otimes n} = \underbrace{M \otimes \dots \otimes M}_{n\text{-krat}}$$

a) $M \times N \rightarrow N \otimes M$

$(u, v) \mapsto v \otimes u$ je bilinearna.

Zato $\exists$ linearna preslikava $u \otimes v \mapsto v \otimes u$

Ali je bijektivna? Iščemo inverz.

$\exists$ lin. preslikava ^{Analogno} $v \otimes u \mapsto u \otimes v$. "Očitno" sta si preslikavi inverz

d) $M \otimes K \rightarrow M$
 $u \otimes a \mapsto au$
 $M \xrightarrow{M \otimes K}$
 $u \mapsto u \otimes 1$

Ker je linearna, je dobro definirana
 preslikavi sta druga drugi inverz

b) Radi bi videli, da je preslikava $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$

dobro definirana linearna preslikava

Analogno definiramo $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$
 ki bo njen inverz.

Fiksirajmo $w \in R$

$u \otimes v \mapsto u \otimes (v \otimes w)$ je bilinearna preslikava

Zato $\exists$ linearna preslikava $u \otimes v \mapsto u \otimes (v \otimes w)$

Zato lahko definiramo bilinearno preslikavo

$\Phi: (M \otimes N) \times R \rightarrow M \otimes (N \otimes R)$

$\Phi(\sum u_i \otimes v_i, w) = \sum u_i \otimes (v_i \otimes w)$

$\exists$ seena linearna preslikava ki sliko

$(M \otimes N) \otimes R \rightarrow M \otimes (N \otimes R)$



2.8 Tenzorski produkti prostih modulov

Primer:

$$\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathbb{Z}_2$$

"Kaj je $\mathbb{Z}_3 \otimes \mathbb{Z}_2$. Če je kaj pravice na svetu je to $\mathbb{Z}_6$, ampak vsi uemo da na svetu ni pravice"

$$u \otimes v = (3u - 2u) \otimes v = -2u \otimes v = -u \otimes 2v = 0$$

$$\Rightarrow \mathbb{Z}_3 \otimes \mathbb{Z}_2 = 0$$

$$\mathbb{Z}_n \otimes \mathbb{Z}_m = 0, \text{ če sta } n \text{ in } m \text{ tuji}$$

Izrek: Naj bo M prost K -modul z bazo $\{e_i : i \in I\}$
in N poljuben K -modul.

Potem vsak element $M \otimes N$ lahko enolično zapisemo kot
 $\sum e_i \otimes v_i$

To razumemo: vsi razen končno mnogo $v_i = 0$

Dokaz: $u \in M, v \in N$

$$u \otimes v = (\sum a_i e_i) \otimes v = \sum (a_i e_i \otimes v) = \sum e_i \otimes \underbrace{(a_i v)}_{v_i}$$

$\uparrow$
za neke $a_i \in K$

endičnost:

Ker je vsak element $M \otimes N$ vsota enostavnih tenzorjev,
je res vsak element oblike $\sum e_i \otimes v_i$

Zadošča dokazati: $\sum e_i \otimes v_i = 0 \Rightarrow v_i = 0 \ \forall i \in I$

Izberimo $i_0 \in I$

če uspemo najti tako linearno preslikavo $\varphi: M \otimes N \rightarrow M$

da bo $\varphi(e_i \otimes v_i) = 0$ razen za $i = i_0$

in $\varphi(e_{i_0} \otimes v_{i_0}) = v_{i_0}$; potem bo sledilo

$$0 = \varphi(0) = \varphi(\sum e_i \otimes v_i) = \sum \varphi(e_i \otimes v_i) = v_{i_0}$$

Izberimo linearno preslikavo $\varphi_0: M \rightarrow K$

$$\varphi_0: e_i \mapsto 0; i \neq i_0$$

$$e_{i_0} \mapsto 1$$

Taka preslikava obstaja, ker je
 $\{e_i\}$ baza, in lahko to enolično
razširimo na M

Definirajmo $\Phi: M \times N \rightarrow N$

$$(u, v) \mapsto \varphi_0(u) \cdot v \text{ je bilinearna,}$$

zato ∃ linearna preslikava $\varphi: M \otimes N \rightarrow N$ taka, da je

$$\varphi(u \otimes v) = \Phi(u, v)$$

$$\varphi(e_i \otimes v_i) = \varphi_0(e_i) v_i = \begin{cases} v_{i_0} & i = i_0 \\ 0 & \text{sicer} \end{cases}$$

Opomba: Podobni izrek velja, če je N prost
z bazo $\{f_j\}$

Izrek: Najbo M prosti K -modul z bazo $\{e_i\}$ in
 N prosti K -modul z bazo $\{f_j\}$. Potem je
tudi tenzorski produkt prosti modul, z
bazo $\{e_i \otimes f_j; i \in I, j \in J\}$

Dokaz: Vek. $e \in M \otimes N$ je oblike $\sum_i e_i \otimes v_i =$

$$= \sum e_i \otimes (\sum_j a_{ij} f_j) = \sum_{i \in I} \sum_{j \in J} a_{ij} (e_i \otimes f_j)$$

Linearne neodvisnost?

$$0 = \sum_{i,j} a_{ij} (e_i \otimes f_j) = \sum_i e_i \otimes (\sum_j a_{ij} f_j) \Rightarrow \sum_j a_{ij} f_j = 0 \quad \text{za } \forall i$$

↑
ker $\sum e_i \otimes v_i$ je enoličen

$$\Rightarrow a_{ij} = 0 \quad \forall i, j \in I \times J$$

↑
f. baze

■

Posledica: Če je U vek. pr. nad F z bazo $\{e_i\}$ in
 V vek. prost nad F z bazo f_j , je $U \otimes V$ vek. pr. nad F
z bazo $e_i \otimes f_j$. Če sta U in V končno
razsežna, je torej $\dim(U \otimes V) = \dim U \cdot \dim V$

Primer: V vekt. pr. nad F , $v \in V$, $f \in V^*$ $\xleftarrow{\text{dual } V}$
 $\xleftarrow{\text{lin funkcional}}$

$$v \otimes f: V \rightarrow V$$

$$(v \otimes f)u = f(u) \cdot v$$

Primeri iz zvezi v učeniku

2.9 Tenzorski produkt algebr

Algebra nad F :

- vek. pr nad F
- kolobar
- $a(xy) = (ax)y = x(ay)$

Splānejsi pojemi: Algebra nad komutativnim kolobarjiem

K je definēta enako. Torej je to K -modul

skupis ar množējēnu (za kēterēu je kolobar) un ē

$$a(xy) = (ax)y = x(ay)$$

Primeri:

1. $\forall$ Kolobar je algebra nad $\mathbb{Z}$
2. $\forall$ kolobar je algebra nad $Z(K)$ (center)
3. $K \subseteq C$ kom. kol. C je K -algebra

Izrek: Naj bosta A in B K -algebri:

Potem K -modul $A \otimes B$ postane K -algebra, če vpeljemo množenje s predpisom

$$(u \otimes v)(t \otimes w) = ut \otimes vw$$

Opomba: prava definicija množenja je

$$\left(\sum u_i \otimes v_i\right) \left(\sum t_j \otimes w_j\right) = \sum \sum u_i t_j \otimes v_i w_j$$

Dokaz: Problem je dobra definirana množenja

$\forall z \in A \vee B \quad \rho_z(x) = xz$ je K -linearna preslikava na vsaki algebri:

$$z \in A \vee w \in B$$

$$\rho_z: A \rightarrow A \quad \rho_w: B \rightarrow B \quad \rho_z \otimes \rho_w: A \otimes B \rightarrow A \otimes B$$

$$((\rho_z \otimes \rho_w)(u \otimes v) = \rho_z(u) \otimes \rho_w(v))$$

$$\Phi: A \times B \rightarrow \text{End}(A \otimes B) \quad \begin{array}{l} \leftarrow \text{enkrat je samo } K\text{-modul} \\ (z, w) \mapsto \rho_z \otimes \rho_w \end{array}$$

če je $A \otimes B$ K -modul, je $\text{End}(A \otimes B)$ K -algebra

$$\Phi \text{ je bilinearna zato } \exists \text{ lin. pres. } \gamma: A \otimes B \rightarrow \text{End}(A \otimes B) \\ (z \otimes w) \mapsto \rho_z \otimes \rho_w$$

Definirajmo množenje v $A \otimes B$

$$r \cdot s := \gamma(s) \cdot r$$

Ki je to naša definicija množenja?

$$\begin{aligned} (u \otimes v)(z \otimes w) &= \gamma(z \otimes w)(u \otimes v) = \\ &= (\rho_z \otimes \rho_w)(u \otimes v) = uz \otimes vw \end{aligned}$$

Produkt je bilinearen:

$$(ar + a'r') \otimes s = a(rs) + a'(r's)$$

$$r(\dots) = r_{\dots} + r_{\dots} \quad \text{itd}$$

asoc: očitno

enota: $1 \otimes 1$

Izrek: Za K -algebre A, B, C velja

a) $A \otimes B \cong B \otimes A$

b) $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$

c) $(A \times B) \otimes C \cong (A \otimes C) \times (B \otimes C)$

d) $A \otimes K \cong A$

direktni produkt
in direktna vsota
algebr sta ekvivalentna

Dokaz: isto kot za module

Primer:

- $K[X]$ je kolobar in je cela K algebra

$$a(\sum a_i x^i) = \sum a a_i x^i$$

- A K algebra

$A[X]$ je K -algebra

- $A \otimes K[X] \cong A[X]$

$K[X]$ je prosti K modul z bazo $\{1, x, x^2, \dots\}$
Elementi v $A \otimes K[X]$ so torej oblike

$$\sum_{i \geq 0} a_i \otimes x^i \leftarrow \text{enclizen zapis (prejeto izreki)}$$

$$\sum_{i \geq 0} a_i \otimes x^i \mapsto \sum_{i \geq 0} a_i x^i \text{ je izomorfizem}$$

- A poljubna K -Algebra

$M_n(K)$ je kolobar in je tudi K -Algebra, če

definiramo $a \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$

lahko definiramo

$$M_n(A) \otimes K \stackrel{?}{\cong} M_n(A)$$

Vse elemente v $M_n(A) \otimes K$ je oblike

$$\sum_{i=1}^n \sum_{j=1}^n E_{ij} \otimes u_{ij}; u_{ij} \in A$$

Vpeljemo $\varphi: M_n(A) \otimes A \longrightarrow M_n(A)$

$$\sum E_{ij} \otimes u_{ij} \mapsto \begin{bmatrix} u_{11} & \dots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \dots & u_{nn} \end{bmatrix}$$

$$\text{torej } E_{ij} \otimes u = u \cdot E_{ij}$$

$$\varphi(E_{ij} \otimes u \cdot E_{kl} \otimes v) = \varphi(\delta_{jk} E_{il} \otimes uv) = \delta_{jk} uv E_{il}$$

$$\varphi(\dots) \cdot \varphi(\dots) = u E_{ij} \cdot v E_{kl} = uv \cdot E_{il} \delta_{jk}$$

$$M_n(K) \otimes M_m(K) = M_n(M_m(K)) \cong M_{n \cdot m}(K)$$

$\nwarrow$ bloke matrice

$$S = \begin{bmatrix} s_{11} & \dots & s_{1m} \\ \vdots & & \vdots \\ s_{m1} & \dots & s_{mm} \end{bmatrix} \in M_m(K)$$

$T \in M_n(K)$

$$S \otimes T = \sum_i \sum_j s_{ij} E_{ij} \otimes T =$$

$$= \sum_i \sum_j E_{ij} \otimes s_{ij} T \mapsto \begin{bmatrix} s_{11} T & \dots & s_{1m} T \\ \vdots & & \vdots \\ s_{m1} T & \dots & s_{mm} T \end{bmatrix}$$

2.10 Razširitev skalarjev

Naj bo A realna, končnodimenzionalna algebra

Naj bo $\{e_1, \dots, e_n\}$ njena baza

$$\text{Rešimo } e_i e_j = \sum_k \alpha_{ijk} e_k \quad \alpha_{ijk} \in \mathbb{R} \quad *$$

$A_{\mathbb{C}}$ naj bo kompleksen prostor z enako označeno bazo $\{e_1, \dots, e_n\}$, množenje pa naj bo definirano z isto formulo

Primeri:

1. $M_n(\mathbb{R})_{\mathbb{C}} \cong M_n(\mathbb{C})$

2. $\mathbb{H}_{\mathbb{C}} \cong M_2(\mathbb{C})$

* morda delitev ni $\cong$ zato ne more biti $\cong \mathbb{H}$

K, C komutativna klobarja

$\alpha: K \rightarrow C$ homomorfizem

M K -modul

C postane K modul, če definiramo $k \cdot c = \alpha(k) \cdot c$

$$\begin{aligned}(k_1 \cdot k_2) c &= \alpha(k_1 k_2) c = \alpha(k_1) \alpha(k_2) c = \alpha(k_1) k_2 c = \\ &= k_1 (k_2 \cdot c)\end{aligned}$$

Lahko definiramo $M_c := C \otimes M$

(M_c je odvisen od α !)

K modul M_c postane C modul, če definiramo

$$c \cdot (d \otimes u) = (cd \otimes u)$$

To množenje je dobro definirano.

$l_c: C \rightarrow C$ levo množenje je K -linearne
 $d \mapsto cd$

$$cy = (l_c \otimes \text{id}_M)(y) \quad \begin{matrix} \forall c \in C \\ \forall y \in M_c \end{matrix}$$

nesporne definicija $\Rightarrow$ množenje
je dobro definirano

$c \otimes u = c(1 \otimes u) \Rightarrow$ Modul M_c temelji na
linearnih kombinacij elementov $1 \otimes u; u \in M$

Primer:

$$\alpha: K \rightarrow C \quad K \text{ podkolobar } C \\ k \mapsto k$$

$$M_C = C \otimes M \quad \text{elementi so } 1 \otimes u \text{ u } C \otimes M$$

Naj bo A K -algebra

A_C je C -modul

$C \otimes A$ je tudi K -algebra saj sta C in A K -algebr.

Z množenjem

$$C(d \otimes u) = cd \otimes u \text{ je } A_C \text{ } C\text{-algebra}$$

Elementi so C -linearne kombinacije $1 \otimes e_i$,

kjer so $\{e_i; i \in I\}$ baza A .

$\{1 \otimes e_i\}$ so baza za A_C

Če je množenje v K -algebri A določeno z množenjem

$$b \rightarrow n \text{ vektorjev } e_i e_j = \sum_k \alpha_{ijk} e_k, \text{ j}$$

$$(1 \otimes e_i)(1 \otimes e_j) = (1 \otimes e_i e_j) = \sum_k \alpha_{ijk} (1 \otimes e_k)$$

Primer: K komutativan kelobar

Naj bo I maksimalni ideal $K \Rightarrow \overset{,,C}{K/I}$ je polje

$$\text{npr } K = \mathbb{Z} \quad I = p\mathbb{Z} : K/I \cong \mathbb{Z}_p$$

$$\alpha: K \rightarrow C$$

$$k \mapsto k+I \quad \text{Tako iz } K \text{ modula } M \text{ dobivamo}$$

vektorski prostor M_C nad C

Izrek: Naj bo K komutativen kolobar. Potem
 $iz\ K^S \cong K^T \Rightarrow S=T$

(Vemo od prej:
 $K^n = K \times K \dots \times K$ je prosti K modul.
 $\forall K$ -modul z bazo z n elementi je izomorfen temu).

Dokaz:

Naj bo C polje kot v prejšnjem primeru.

za $n \in \mathbb{N}$ definiramo $(K^n)_C \leftarrow$ To razširitev
 skalarjev

To je vektorski prostor nad C z bazo

$1 \otimes e_1, \dots, 1 \otimes e_n$; če je $e_1, \dots, e_n$ baza K^n

Ta prostor je n dimenzionalen $\dim_C(K_C) = n$

Recimo da $K^S \cong K^T$

$\Phi: K^S \rightarrow K^T$ izomorfizem K -modulov

$\text{id}_C \otimes \Phi: (K^S)_C \rightarrow (K^T)_C$ je K linearne, v našem
 primeru je tudi C -linearne

$$(\text{id}_C \otimes \Phi)(cd \otimes u) = cd \otimes \Phi(u) = c(d \otimes \Phi(u)) =$$

in tudi bijektivne $\Rightarrow$ je izomorfizem $C(\text{id}_C \otimes \Phi)(d \otimes u)$
 vektorskih prostorov nad C

ker sta K^S in K^T vektorske prostora, je $S=T$

2.11. Končno generirane Abelove grupe

Naj bo K cel klobar in M K -modul

Definiramo

$$\text{tr}(M) = \{ u \in M ; \exists a \in K \text{ i.o. } a u = 0 \}$$

torzijski podmodul

To je podmodul

$$u, v \in \text{tr}(M)$$

$$a u = 0 \quad b v = 0$$

$$a b (u - v) = b a u - a b v = 0 - 0 = 0$$

$$u \in \text{tr } M \quad b \in K \quad a u = 0$$

$$\Rightarrow a b u = b a u = 0$$

M je torzijsko prost če je $\text{tr}(M) = \{0\}$

$M / \text{tr}(M)$ je torzijsko prost

$$\begin{aligned} a(u + \text{tr}(M)) = 0 &\Rightarrow a u + \text{tr}(M) = 0 \Rightarrow a u \in \text{tr}(M) \\ &\Rightarrow \exists b \in K. \quad b a u = 0 \Rightarrow u \in K. \ker(b a) u = 0 \\ &\Rightarrow u + \text{tr } M = 0 \end{aligned}$$

V posebnem primeru: $K = \mathbb{Z}$

$\text{tor}(G) =$ torzijske podgrupe abelove (additivne) grupe G

Pokaželi smo, $G / \text{tor}(G)$ je torzijsko prosta Grupa

...vsi elementi razen 0 imajo neskončen red

kanone $\Rightarrow$ kanono generirane

$$|G| < \infty ; G \cong \mathbb{Z}_{r_1} \oplus \dots \oplus \mathbb{Z}_{r_n} \quad r_i = p_i^{k_i}$$

$$\mathbb{Z} \oplus \mathbb{Z}$$

$\nwarrow$ kanone abelova

$$\mathbb{Z}^s \oplus K \cong \mathbb{Z}^s \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{k_r}} \quad \text{bomo dežel:}$$



kanonogenerirane abelova grupa

Lema: Končno generirana torzijsko prosta abelova grupa je prosta

Dokaz: Naj bo H k.g.t.p. Abelove

Naj bo $m \in \mathbb{N}$ taka. H generirana z n elementi, ne pa manj

Denimo da H ni prosta

Izmed vseh množic z m elementi, ki generirajo

H , izberimo „najmanjšo“ ($\{a_1, \dots, a_m\}$ generirajo H ,

$\exists k_1, \dots, k_m \in \mathbb{Z}, k_1 a_1 + \dots + k_m a_m = 0$ in

$\sum_{i=1}^m |k_i|$ minimalno število (če je $\{b_1, \dots, b_m\}$ tudi

množica generatorjev in je $\sum l_i b_i = 0 \Rightarrow \sum |l_i| \geq \sum |k_i|$)

H tor. prosta, sta vsej dva $k_i \neq 0$

reimo da sta to k_1 in k_2

BSZS. $|k_1| \geq |k_2| > 0$

$k_1 = 2k_2 + r$; $0 < r < |k_2|$ oz $|k_1 - 2k_2| < |k_2|$

$0 = k_1 a_1 + k_2 a_2 + \dots + k_n a_n =$

$= (k_1 - 2k_2) a_1 + k_2 (a_2 + 2a_1) + k_3 a_3 + \dots + k_n a_n$

$|k_1 - 2k_2| < |k_2| \leq |k_1|$

$|k_1 - 2k_2| + |k_2| + \dots + |k_n| < \sum |k_i|$

ker $a_1, (a_2 + 2a_1), a_3, \dots, a_n$ tudi generirajo H

Izrek: G končno generirana abelova grupa.

Potem je njena torzijska podgrupa T končna
in $G \cong \mathbb{Z}^s \oplus T$, za nek endično določen: $s \geq 0$

Dokaz: G obravnavamo kot $\mathbb{Z}$ modul

G/T je torzijsko prosta zato je prosta

$\Rightarrow G/T \cong \mathbb{Z}^s$ za nek endično določen: $s \geq 0$

Ker je G končno generirana je k.g. tudi G/T

G/T je prost $\mathbb{Z}$ modul $\Rightarrow G/T$ je projektiven

$$\Rightarrow 0 \longrightarrow T \xrightarrow{\iota} G \xrightarrow{\pi} G/T \longrightarrow 0$$

To zaporedje razpade $\Rightarrow G \cong G/T \oplus T \cong \mathbb{Z}^s \oplus T$

T končna

$T \cong \frac{T \oplus \mathbb{Z}^s}{\{0\} \oplus \mathbb{Z}^s}$ T je zato končno generirana, saj je $T \oplus \mathbb{Z}^s$ k.g.

Naj bo $\{t_1, \dots, t_r\}$ množica generatorjev T

Vsi elementi so oblike

$$m_1 t_1 + m_2 t_2 + \dots + m_r t_r \quad m_i \in \mathbb{Z}$$

$\forall t_i$ ima končen red, zato je takih različnih zapisov le končno mnogo.

Posledica: V končno generirane abelove grupe, je
oblike $\mathbb{Z}^s \oplus \mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_r}^{k_r}$

s, p_i, k_i so endično določeni:

Enak izrek velja za module nad glavnim
kolobarjem

3. Prezentacije grup in algebr

3.1 Proste grupe in prezentacije grup

Neformalno: kaj je prosta grupa na množici X

$$|X|=1 \Rightarrow F_X \cong \mathbb{Z}$$

$$|X|=2 \quad X=\{x, y\}$$

$$F_X = \{1, x, y, x^2, x^{-1}, xy, yx, x^3y^{-3}x^{-5}y^4x, \dots\}$$

Vse besede iz x, y, x^{-1}, y^{-1}

Različni; zepisi daje vedno različne elemente

$$xyx^{-2} \cdot yx^{-1}y^{-1}x^2 = xyx^{-2}yx^{-1}x^2$$

Formalno: X poljubna množica

Definirajmo grupo F_X na X

$$X = \emptyset \Rightarrow F_X = \{1\}$$

$X \neq \emptyset \Rightarrow$ označimo X^{-1} množica z isto kardinalnostjo

$$\text{kot } X, X^{-1} = \{x^{-1}; x \in X\}$$

$\nwarrow$ samo oznake

Zaporedje $(x_1, x_2, \dots); x_i \in X \cup X^{-1} \cup \{1\}$, kjer so

od nekega naprej vsi členi enaki 1 pravimo **beseda**

Npr $(1, 1, \dots) = 1$ je beseda, ki ji pravimo **prazna beseda**

če sta izpolnjena pogoja

1) Elementa x, x^{-1} nikoli ne nastopata zaporedoma

$$x_i = x \Rightarrow x_{i+1} \neq x^{-1} \quad \wedge \quad x_i = x^{-1} \Rightarrow x_{i+1} \neq x$$

2) če je nek $x_n = 1$ velja $x_{n+i} = 1 \quad \forall i \in \mathbb{N}$

potem besedi pravimo **reducirane besede**

Zaporedje $(x_1^{e_1}, x_2^{e_2}, \dots, x_n^{e_n}, 1, \dots)$ $e_i \in \{1, -1\}$

pišemo kot $x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$

$$\left(\text{Namesto } (xxy^{-1}y^{-1}x^{-1} = x^2y^{-2}x^{-1}) \right)$$

kot množica je F_X množica reduciranih besed

Vpeljimo operacijo

Vzemimo dve reducirani besedi

$$x_1^{e_1} x_2^{e_2} \dots x_m^{e_m} \text{ in } y_1^{\mu_1} y_2^{\mu_2} \dots y_n^{\mu_n} \quad e_i, \mu_i \in \{1, -1\}$$

in naj bo $m \leq n$

$$x_i, e_i \in X$$

$$x_1^{e_1} \dots x_m^{e_m} y_1^{\mu_1} \dots y_n^{\mu_n} =$$

nejvečji
k najmanjše da
 $y_k \neq x_{m-k+1}$ in $e_{m-k+1} \neq \mu_k$

$$\begin{cases} x_1^{e_1} \dots x_{m-k+1}^{e_{m-k+1}} y_k^{\mu_k} \dots y_n^{\mu_n} & k \leq m \\ y_{k+1}^{\mu_{k+1}} \dots y_n^{\mu_n} & k = m+1 \quad m < n \\ 1 & k = m+1 \quad m = n \end{cases}$$

$$k = m+1 \quad m = n$$

F_X je grupa

1 je enota

$$(x_1^{e_1} \dots x_n^{e_n})^{-1} = x_n^{-e_n} \dots x_1^{-e_1}$$

F_X imenujemo **Prosta grupa** na množici X

$$X \subseteq F_X$$

$\nwarrow$ neformalno

Izrek: Naj bo X množica in F_X najbo prosta grupa na X in $i: X \rightarrow F_X \quad x \mapsto x$

Za $\forall f: X \rightarrow G$, kjer je G poljubna grupa

$\exists$ homomorfizem $\varphi: F_X \rightarrow G$. da je $\varphi(i(x)) = f(x)$
 $\quad \quad \quad \forall x \in X$

$$\begin{array}{ccc} X & \xrightarrow{i_X} & F_X \\ & \searrow f & \downarrow \varphi \\ & & G \end{array}$$

Dokaz: $\varphi(x_1^{e_1} x_2^{e_2} \dots x_m^{e_m}) = f(x_1)^{e_1} \dots f(x_m)^{e_m}$

Izrek: $\forall$ grupe je homomorfna slik: proste grupe

Dokaz: Naj bo G grupa. Naj bo $X \subseteq G$ množica, ki

G generira. Na X gledamo kot množico, zgradimo prosto grupo F_X na X . Po prejšnjem izreku

$\exists$ homomorfizem $\varphi: F_X \rightarrow G$ (če vzamemo $\varphi(x) = x$)
 $x \mapsto x$

φ je surjektivna, ker je $\text{im } \varphi \leq G$ in $X \subseteq \text{im } \varphi$
generatorji

Posledica:

$$F_X / \ker \varphi \cong G$$

Definicija: Naj bo X množica in naj bo R podmnožica reduciranih besed v X

Pravimo, da je G definirana z generatorji $x \in X$, in relacijami $r=1 \quad r \in R$, če je $G \cong F_X / N_R$,

kjer je N_R edinke generirane z vsemi elementi iz R

V tem primeru rečemo, da je par $\langle X | R \rangle$ **prezentacija**
 G

Naj bo $\langle X | R \rangle$ prezentacija

$N = N_R$ F_X / N je generirana z odseki $x_i N$; $x_i \in X$

$$r \in R \quad r = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$$

$$(x_1 N)^{e_1} \dots (x_n N)^{e_n} = (x_1^{e_1} \dots x_n^{e_n}) N = r N = N = 1$$

G je **končno prezentirana**, če obstaja končna množica X in končna množica R , da je $\langle X | R \rangle$ prezentacija G . Takrat pišemo

$$\langle X | R \rangle = \langle x_1, \dots, x_m \mid r_1 = \dots = r_n = 1 \rangle$$

Primeri:

1) Prezentacija proste grupe

$$\langle x | \emptyset \rangle$$

$$2) \langle x | x^n = 1 \rangle \cong \mathbb{Z}_n$$

$$3) \langle x, y | xy = yx \rangle = \mathbb{Z} \oplus \mathbb{Z}$$

$$4) D_{2n} = \langle 1, r, \dots, r^{n-1}, z \rangle$$

$$\langle r, z | r^n = 1 = z^2 = (rz)^2 \rangle$$

$$\langle x, y | x^n = y^2 = (xy)^2 = 1 \rangle$$

Nedinke gen. $z, x^n, y^2, (xy)^2$

Naj bo G kakor koli grupa generirana z $\langle u, v \rangle$

$$k: \text{zadešče } u^n = v^2 = (uv)^2 = 1$$

D_{2n} je taka grupa, pravi tudi $F_{\{x,y\}}/N$ je taka

$$(u=xN, v=yN)$$

1. korak: G je homom. $F_{\{x,y\}}/N$

2. korak: G ima največ 2n elementov

Denimo da je ta res. Potem po 1. koraku

$$\exists \text{ epimorfizem } \varphi: F_{\{x,y\}}/N \rightarrow D_{2n}$$

2. korak pravi, da če za G izhaja $\frac{F_{\{x,y\}}}{N}$ ima $\leq 2n$ elementov $= |D_{2n}| \Rightarrow$

φ je bijektiven

1. korak

Vemo: $\exists \text{ homom. } F_{\{x,y\}} \rightarrow G$

$$x \mapsto u$$

$$y \mapsto v$$

$\ker \varphi$ vsebuje $x^n, y^2, (xy)^2$

$$\Rightarrow N \leq \ker \varphi$$

$$\text{zato } \exists \text{ homomorfizem } F_{\{x,y\}}/N \rightarrow F_{\{x,y\}}/\ker \varphi \stackrel{\text{imp}}{\cong} G$$

$$\omega N \mapsto \omega \ker \varphi$$

2. korak

$$u^{m_1} v^{n_1} u^{m_2} \dots v^{n_r} \quad m_i, n_i \in \mathbb{Z}$$

$\S$

$$m_i \in \mathbb{Z}, 1 \leq i \leq r, n_i \in [n]$$

$$v u^m v = (v u v)^m = (u^{-1})^m = u^{-m}$$

Edini možni elementi so

$$1, u, \dots, u^{n-1}, v, uv, \dots, u^{n-1}v \Rightarrow \text{jele } 2n$$

3.2. Proste algebre in prezentacije algebr

Algebra naj bo nad poljem F

Elementi proste algebre so nekomutativni polinomi.

X, Y dve spremenljivki

$$\{1, X, Y, XY, YX, XY - YX, 3 + 7X^2Y - 9YX^4Y, \dots\}$$

Naj bo X množica. Elementi *proste monoida*

$$X^* \text{ so besede: zaporedja } (X_1, X_2, \dots, X_m, 1, 1, \dots) \\ = X_1 X_2 \dots X_m$$

$$XXYYX = X^2Y^2X$$

Upetemo množenje $X_1 \dots X_n \cdot Y_1 \dots Y_m = X_1 \dots X_n X_{n+1} \dots X_{n+m}$
1 je enota za množenje

X^* s tem postane monoid. Rečemo mu
prosti monoid

$F\langle X \rangle$ naj bo vektorski prostor nad F z bazo X^*

$F\langle X \rangle$ postane algebra, če definiramo

$$(\sum \lambda_i w_i) (\sum \mu_j w_j) := \sum \nu_k w_k$$

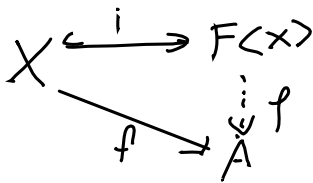
$$w_i w_j = w_k$$

$$\nu_k = \sum \lambda_i \mu_j$$

$$w_i w_j = w_k$$

$F\langle X \rangle$ imenujemo *prosta algebra* na množici X

$$i: X \rightarrow F\langle X \rangle \\ x \mapsto x$$



Izrek: Naj bo X množica in A algebra in $f: X \rightarrow A$. Potem $\exists!$ homomorfizem $\varphi: F\langle X \rangle \rightarrow A$,
 da diagram komutira $\varphi \circ i = f$

Dokaz: $\varphi(f(x_1, \dots, x_m)) := \varphi(f(x_1), \dots, f(x_m))$
 To je res homomorfizem

(t.j. prosta algebra je prosti objekt v kategoriji:
 algebr nad F)

Posledica: Vsaka algebra je homeomorfna s sliko
 neke proste algebre

Dokaz: Naj bo A algebra $X \subseteq A$ $\langle X \rangle = A$ polarna množica generaterja

Naj bo $f: X \rightarrow A$
 $x \mapsto x$

Po izreku: $\exists \varphi: F\langle X \rangle \rightarrow A$
 $x \mapsto x$

$X \subseteq_{\text{imp}} \Rightarrow A \subseteq_{\text{imp}} \Rightarrow A =_{\text{imp}}$
 $A \cong \frac{F\langle X \rangle}{I} \quad I = \ker \varphi$

Definicija: Najbo $X \neq \emptyset$, naj bo F polje in naj bo R množica nekomutativnih polinomov iz X

Pravimo da je algebra A definirana z generaterji

$x \in X$ in relacijami: $p=0 \quad p \in R$, če je

$$A \cong \frac{F\langle X \rangle}{(R)}$$

kideal proste algebre generiran z R

V tem primeru rečemo da je $\frac{F\langle X \rangle}{(R)}$ **prezentacija**
algebre A

A je **končno generirana**, če sta X in R

končni. Potem pišemo $\frac{F\langle X \rangle}{(R)} = F\langle x_1 \dots x_m \mid r_1 = \dots = r_n = 0 \rangle$

Primeri:

1. Pivota algebra $\langle X | \emptyset \rangle$

2. $F\langle X, Y | XY = YX \rangle = F[X, Y]$

3. $F\langle X, Y | XY = 1 \rangle$

4. $F\langle E_{12}, E_{21} | E_{1,2}^2 = E_{2,1}^2 = 0 \rangle$

$$\left. \begin{array}{l} \\ E_{11} = E_{12}E_{21} \end{array} \right\} I = E_{12}E_{21} + E_{21}E_{12}$$

$$E_{22} = E_{21}E_{12}$$

Ugibamo: prezentacija je F

$$F\langle X, Y | X^2 = Y^2 = 0, XY + YX = 1 \rangle$$

NEKOMUTATIVNA ALGEBRA

Direktni produkt kolobarjev in direktne vsote idealov

$K_1, \dots, K_s$ kolobarji: $K = K_1 \times \dots \times K_s$ direktni produkt

$$(x_1, \dots, x_s) + (y_1, \dots, y_s) = (x_1 + y_1, \dots, x_s + y_s)$$

$$(x_1, \dots, x_s) \cdot (y_1, \dots, y_s) = (x_1 y_1, \dots, x_s y_s)$$

$\tilde{K}_1 = K_1 \times \{0\} \times \dots \times \{0\}$ je ideal

$$K = \tilde{K}_1 \oplus \dots \oplus \tilde{K}_s$$

$e \in K$ je idempotent če $e^2 = e$

$e \in Z(K) \Rightarrow e$ je centralni idempotent

Idempotenta e, f sta ortogonalna če $ef = fe = 0$

Primer: e in $1-e$ sta ortogonalna

$$K = K_1 \times \dots \times K_s$$

$e_i = (0 \dots 1 \dots 0)$ je centralni idempotenti

parama so si ortogonalni. $e_1 + \dots + e_s = 1$

$$\tilde{K}_i = e_i K$$

Opomba: e centralni idempotent $\Rightarrow eK \triangleleft K$ je
kolobar z enoto e

Izrek: Naj bodo $I_1, \dots, I_s$ ideali kakega $K \Rightarrow$
 $(K = I_1 \oplus \dots \oplus I_s \Leftrightarrow \exists e_1, \dots, e_s \text{ param. ort. cent. idem.})$
 $e_1 + \dots + e_s = 1 \wedge I_j = e_j K$
 $\forall$ tem primeru je $K \cong I_1 \times \dots \times I_s$

Dokaz:

($\Rightarrow$)

$$1 \in K \Rightarrow \exists (e_1, \dots, e_s) \in I_1 \times \dots \times I_s. 1 = e_1 + \dots + e_s$$

$$I_1 I_j \subseteq I_1 \cap I_j = \{0\}$$

$$\text{Zato: } e_i u_j = u_j e_i = 0 \text{ za } u_j \in I_j, j \neq i$$

$$u_i = u_i \cdot 1 = u_i e_1 + \dots + u_i e_s = u_i e_i \quad \text{za } u_i = e_i$$

$$\Rightarrow u_i = u_i e_i = e_i u_i \quad \text{za } \forall u_i \in I_i \Rightarrow e_i^2 = e_i$$

$$x \in K \Rightarrow x = u_1 + \dots + u_s$$

$$x e_i = u_1 e_i + \dots + u_s e_i = e_i u_i = e_i x \Rightarrow e_i \in Z(K)$$

$$I_j \triangleleft K \Rightarrow e_j K \subseteq I_j$$

$$u_j = e_j u_j \Rightarrow I_j \subseteq e_j K \Rightarrow e_j K = I_j$$

$$(\Leftarrow) I_j = e_j K \wedge e_1 + \dots + e_s = 1$$

$$\forall x \in K. x = 1 \cdot x = \underbrace{e_1 x}_{\in I_1} + \dots + \underbrace{e_s x}_{\in I_s}$$

$$I_j \cap (I_1 \cap \dots \cap I_s) = \{0\}$$

$$\text{Recimo da } e_j u = e_1 x_1 + \dots + e_s x_s \quad \checkmark \text{ brez j} \quad \begin{matrix} x_1, \dots, x_s \in K \\ u \in K \end{matrix}$$

$$\Rightarrow e_j u = 0 \quad / \cdot e_j$$

$$K \cong I_1 \times \dots \times I_s$$

$$\varphi: I_1 \times \dots \times I_s \longrightarrow K$$

$$(u_1, \dots, u_s) \longmapsto u_1 + \dots + u_s$$

$$\varphi \text{ je bijekcija ker } \forall x \in K. x = e_1 x + \dots + e_s x$$

$$\text{in ker } I_j \cap (\text{ostali}) = \{0\}$$

počitno ohranjanje vsote

$$\varphi(u_1, \dots, u_s) \varphi(v_1, \dots, v_s) = (u_1 + \dots + u_s)(v_1 + \dots + v_s)$$

$$\forall i, u_j \in I_i, I_j \subseteq I_i \cap I_j = \{0\} \text{ za } i \neq j$$

$$\Rightarrow \varphi(\dots) \varphi(\dots) = u_1 v_1 + \dots + u_s v_s = \varphi(u_1 v_1, \dots, u_s v_s)$$

Posledica: Če ima K take paroma ortogonalne idempotentne $e_1, \dots, e_s$ ki je $e_1 + \dots + e_s = 1$
 $\Rightarrow K \cong e_1 K \times \dots \times e_s K$

Primeri: $\mathbb{Z}_6 = \{0, 3\} \oplus \{0, 2, 4\} = 3\mathbb{Z}_6 \oplus 4\mathbb{Z}_6$

Enostavni kolobarji

Definicija: Kolobar K je **enostaven**, če $K \neq \{0\}$ in sta edina njegova ideala $\{0\}$ in K

Opomba: $I \triangleleft K$, $a \in I$ obrnljiv $\Rightarrow I = K$

Primer: 1) D obseg $\Rightarrow M_n(D)$ enostaven

$$E_{ij} A E_{kl} = a_{jk} E_{il} \quad \text{Naj bo } \{0\} \neq I \triangleleft M_n(D)$$

$$0 \neq A \in I \Rightarrow a_{jk} E_{il} \in I \text{ za nek } a_{jk} \neq 0$$

$$I \ni (a_{jk}^{-1} I) a_{jk} E_{il} = E_{il}$$

$$I \ni E_{1i} \cdot E_{il} E_{l1} = E_{11} \quad \text{podobno } E_{ii} \in I$$

$$\Rightarrow I \in I$$

$S \subseteq K$ $a, b \in K$

aSb

Možnost 1 in 2 sta ideala. z JL označimo
grupo za seštevanje, generirano z elementi oblike jL

Kak je podgrupa za seštevanje

$$M_{n_1}(D_1) \times \dots \times M_{n_s}(D_s)$$

$M_{n_1}(D_1) \times \{0\} \times \dots \times \{0\}$ je ideal

Ne vem zakaj je to tukaj napisan

Lemma: K kolobar. MSE:

$$i) \Leftrightarrow \forall a \in K, aKa = \{0\} \Rightarrow a = 0$$

$$ii) \Leftrightarrow \forall L \text{ lev: ideal } L, L^2 = \{0\} \Rightarrow L = \{0\}$$

$$iii) \Leftrightarrow \forall I \triangleleft K, I^2 = \{0\} \Rightarrow I = \{0\}$$

Dokaz:

$$i) \Rightarrow ii) \text{ Naj bo } L \text{ lev: ideal } L^2 = \{0\}$$

$$a \in L \Rightarrow \underbrace{aKa}_{\substack{\cap \\ L}} = \{0\} \Rightarrow a = 0 \Rightarrow L = \{0\}$$

$$ii) \Rightarrow iii) \text{ trivialno}$$

$$iii) \Rightarrow i) \quad aKa = 0$$

$$(Kak)^2 = \left(\sum x_i a y_i \right) \left(\sum z_j a w_j \right) = 0 \Rightarrow (Kak)^2 = 0 \Rightarrow$$

$$Kak = \{0\} \Rightarrow 0$$

$\uparrow$
 $1 \in K$

Definicija: Kolobar K je **polprakolobar**, če
zadaja pogojem iz leme (na prejšnji strani.)

Primer: Kolobar brez deliteljev nič je polprakolobar

Lema: $I \triangleleft K_1 \times \dots \times K_s \Leftrightarrow I = I_1 \times \dots \times I_s$ za neke $I_j \triangleleft K_j$

Dokaz: $u = (u_1, \dots, u_s) \in I \Leftrightarrow (0, \dots, 0, u_i, 0, \dots, 0) \in I \quad \forall i$

$$(0, \dots, 0, u_i, 0, \dots, 0) = e_i \cdot u \in I$$

Posledica: $K_1, \dots, K_s$ polprakolobarji $\Rightarrow K_1 \times \dots \times K_s$
polprakolobar

Dokaz: $I^2 = \{0\} \Leftrightarrow I_j^2 = \{0\}$

Primeri

1) Enostevni kolobarji so polprekolobarji:

Tudi $M_{n_1}(D_1) \times \dots \times M_{n_s}(D_s)$ je polprekolobar

2) $T_n(K) = \left\{ \begin{bmatrix} * & & \\ 0 & * & \\ & & x_i \end{bmatrix} \right\}$ ni polprekolobar

$$I = \left\{ \begin{bmatrix} 0 & * \end{bmatrix} \right\}$$

Definicija: Kolobar K je **levi artinski kolobar**,
če ^{se} vsaka padajoča veriga njegovih levih
idealov $L_1 \supseteq L_2 \supseteq \dots$ ustavi
($\exists n \in \mathbb{N}. L_n = L_{n+1} = \dots$)

Primer: 1. Vse končnorazsežne algebre so levi artinski kolobarji.

Levi ideali so podprostorji, saj $\lambda l = (\lambda \cdot 1)l \in L$

2. Za obseg D je $M_n(D)$ levi artinski kolobar

3. $K_1, \dots, K_s$ levi artinski kolobarji $\Rightarrow K_1 \times \dots \times K_s$ L. artinski kol.

Levi ideal je oblike $L_1 \times \dots \times L_s$ $L_i \triangleleft K_i$ levi ideal

4) $\mathbb{Z}$ ni levi artinski kolobar

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \dots$$

$e \in K$ idempotent $\Rightarrow eke = \{exe ; x \in K\}$ kolobar z $e \neq 0$
..... *koln: kolobar*

Primer:

$$E = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} \quad EAE = \begin{bmatrix} * & 0 \\ 0 & 0 \end{bmatrix}$$

Lema:

1) K polprazkolabar $\Rightarrow eKe$ polprazkolabar

2) K levi artinski $\Rightarrow eKe$ levi artinski

Dokaz:

1) $eae \in eKe$

$$eae \cdot eae \cdot eae = 0$$

$\parallel$ $\nearrow$ predprazkolabar

$$(aek \cdot aka = \{0\} \Rightarrow a = 0)$$

$$(eae) \times (eae) \Rightarrow eae = 0 \Rightarrow eKe \text{ polprazkolabar}$$

$\uparrow$
 K polprazkolabar

2)

$$L_1 \supseteq L_2 \supseteq \dots \text{ levi ideali } \vee eKe$$

$$KL_1 \supseteq KL_2 \supseteq \dots \dots \text{ levi ideali } \vee K$$

$$\Rightarrow KL_n = KL_{n+1} = \dots$$

$$\Rightarrow eKe \cdot L_n = eKe L_{n+1} = \dots \Rightarrow L_n = L_{n+1} = \dots$$

??

Lema

e in $f \neq 0$ ortogonale idempotente hebben $\Rightarrow K(1-e) \supset K(1-e-f)$

Datēzi:

$$\supseteq: x(1-e-f) = x(1-e-f)(1-e) \quad x \in K$$

$$\neq: e \in K(1-e)$$

$$f = f(1-e) \quad f = x(1-e-f)$$

$$\Rightarrow f = f^2 = x(1-e-f)f = 0 \quad \Rightarrow f \notin K(1-e-f)$$

Definicija: Množica $\{e_{ij}; 1 \leq i, j \leq n\}$ je
 množica $n \times n$ matricnih enot kolobarja K ,
 če velja $e_{ij} \cdot e_{kl} = \delta_{jk} e_{il}$ $\wedge$ $e_{11} + \dots + e_{nn} = 1$

Primer: 1. Standardne matricne enote
 2. $\{S E_{ij} S^{-1}\}$

Lema: Naj bo $\{e_{ij}; 1 \leq i, j \leq n\}$ množica $n \times n$
 matricnih enot kolobarja K . Potem velja
 $K \cong M_n(e_{11} K e_{11})$

Dokaz:

$$a \in K \quad a_{ij} := e_{1i} a e_{j1} = e_{11} e_{1i} a e_{j1} e_{11} \in e_{11} K e_{11}$$

$$\varphi: K \longrightarrow M_n(e_{11} K e_{11})$$

$$a \longmapsto a_{ij}$$

$$\underline{\varphi(ab) = \varphi(a)\varphi(b)}$$

$$(i, j)\text{-ti člen od } \varphi(a)\varphi(b) = \sum_{k=1}^n e_{1i} a e_{k1} \underbrace{e_{k1} e_{j1}}_{e_{1j}} b e_{j1}$$

$$e_{1i} a \left(\sum_{k=1}^n e_{kk} \right) b e_{j1} = e_{1i} a b e_{j1} = (i, j)\text{-ti člen od } \varphi(ab)$$

Lema: če ima kolobar K take parametre
 ortogonalne idempotentne $e_{11}, \dots, e_{nn}$, da je
 $\sum_{i=1}^n e_{ii} = 1$ in elemente $e_{1i} \in e_{11} K e_{ii}$ in
 $e_{i1} \in e_{ii} K e_{11}$, da je $e_{1i} \cdot e_{i1} = e_{11}$ in $e_{i1} e_{1i} = e_{ii}$,
 potem lahko množico te dopolnimo do množice
 $n \times n$ matričnih enot.

Dokaz: $e_{ij} := e_{i1} e_{1j}$ preveri lemma

Definicija: $L = \{0\}$ je **minimalni levi ideal**, če za
vsak levi ideal J iz $\{0\} \subseteq J \subseteq L \Rightarrow J = \{0\} \vee J = L$

Primer: 1. $\forall M_n(D)$ je $L = \left\{ \begin{bmatrix} * & \\ & 0 \end{bmatrix} \right\}$ minimalni levi ideal

$$L = KE_{11} \text{ in } E_{11}KE_{11} \cong D$$

2) $\mathbb{Z}$ nima minimalnega levega ideala

Lema: Levi artinski kolobar ima minimalni levi ideal

Dokaz: Naj bo $L_1 \neq \{0\}$ levi ideal, če ni minimalni;

$\exists L_2: \{0\} \subset L_2 \subset L_1$, če ta ni minimalni, tako nadaljujemo

$L_1 \supset L_2 \supset L_3 \dots$ ta veriga se nekoč ustavi. $\blacksquare$

Lema: Naj bo L min. Levi ideal polpraktolobarja K . Potem K vsebuje tak element e , da je $L = Ke$ in eKe obseg.

Dokaz: $L \neq \{0\}$ ker je K polpraktolobar

$$\exists y \in L. Ly \neq \{0\}, \{0\} = Ly \leq L$$

$$\Rightarrow Ly = L \Rightarrow \exists e \in L. ey = y$$

$M = \{z \in L; zy = 0\}$ je Levi ideal

$$\{0\} \subseteq M \subseteq L \xrightarrow{M \neq L} M = \{0\} \quad e-1 \in M \Rightarrow e-1=0$$

$$\Rightarrow e^2 = e$$

???

$$\underline{L = Ke}$$

$$e \in L \Rightarrow Ke \subseteq L$$

$$\{0\} \subset Ke \subseteq L \Rightarrow Ke = L$$

eKe je obseg

$$0 \neq eae \in eKe$$

$$\{0\} \subset Keae \subseteq L \Rightarrow Keae = L$$

$$e = beae \text{ za nek } b \in K$$

$$e = ebe \cdot eae \quad ebe \text{ je Levi inverz za } a$$

b ima iz enakega razloga Levi inverz ece

$$\Rightarrow b \text{ ima inverz}$$

Lemma: Naj bosta e, f tak par ortogonalnih idempotentov polprakovoberja K , da sta eKe in fKf obsega in $eKf \neq \{0\}$. Potem $\exists$ taka $u \in eKf$ in $v \in fKe$, $uv = e$ in $vu = f$

Dokaz: $\exists a \in K, eaf \neq 0 \Rightarrow \exists b \in K, eaf \cdot b \cdot eaf \neq 0$.

$$0 \neq eaf \cdot b \cdot e \in eKe$$

$$eKe \text{ obseg} \Rightarrow \exists a \in K, \underbrace{eaf}_{u} \cdot \underbrace{f \cdot b \cdot e}_{v} \cdot ece = e$$

$$(vu)^2 = v \underbrace{u \cdot v}_{e} u = vu$$

$vu \in fKf$, fKf obseg

Edine idempotentne sta 0 in f

$$vu \neq 0 \text{ ker } vu = 0 \Rightarrow uvu = eu = e = 0$$

$$\Rightarrow vu = f$$

QED

Lema: Naj bodo $e_1, \dots, e_n$ različni ortogonalni idempotenti polprakovarja K .

Denimo, da je $e_i K e_i$ domag in $e_i K e_i \neq \{0\}$ za $\forall i$.

Potem za idempotent $e = e_1 + \dots + e_n$ velja $e K e \cong M_n(e_i K e_i)$

Dokaz:

Prejšnja lema

$\exists e_{i,1} \in e_i K e_i, \exists e_{i,1} \in e_i K e_i, e_{i,1} \cdot e_{i,1} = e_i, e_{i,1} \cdot e_{i,1} = e_i$
 $e_{i,1} \cdot e_i$

Izpolnjeni so vsi pogoji neke prejšnje leme.

Izrek (Wedderburn-Artimov)

Naj bo $K \neq \{0\}$ kolobar. NSE.

1. $\Leftrightarrow K$ je polprakovolbar in levi artinski kolobar

2. $\Leftrightarrow \exists$ obsegi $D_1, \dots, D_s$ in $n_1, \dots, n_s$. $K \cong M_{n_1}(D_1) \times \dots \times M_{n_s}(D_s)$

Dokaz:

2) $\Rightarrow$ 1) smo že

1) $\Rightarrow$ 2) K polprakovolbar in levi artinski.

Torej ima minimalni levi ideal

Po eni lemi: $\exists e = e^2$. eK je obseg

$e = 1 \Rightarrow$ smo končali ($K \cong M_1(K)$)

Naj bo $e \neq 1$

Pa neki lemi: $K \supset K(1-e)$

$(1-e)K(1-e)$ je levi artinski polprakovolbar
(po lemi 2 (nekeje))

lema 4: $\exists e_2 = e_2^2 \in (1-e)K(1-e)$. $e_2(1-e)K(1-e)e_2$ je obseg

e_1, e_2 sta ortogonalna, ker

$$e_2 e (1-e) K (1-e)$$

lema 3 $K(1-e_1) \supset K(1-e_1-e_2)$

lema 4: $\exists e_3 \in (1-e_1-e_2)K(1-e_1-e_2)$.

$e_3(1-e_1-e_2)K(1-e_1-e_2)e_3$ je ob

al: pa $1 = e_1 + e_2$ ker pa je dovolj

e_3 je ortogonalen na e_1 in e_2

ker je K levi artinski se postopek po končno mnogo kratkih korakov

Torej $\exists$ paroma ortogonalni idempotenti $e_1, \dots, e_n \in K$.

$e_i K e_j$ so obsegi V_i in $e_1 + \dots + e_n = 1$

$E = \{e_1, \dots, e_n\}$ vpeljimo relacijo

$$e_i \sim e_j \Leftrightarrow e_i K e_j \neq \{0\}$$

To je ekvivalenca

• $e_i K e_i \neq \{0\}$ ker je obseg (z0? nima enote)

• $e_i \sim e_j \Leftrightarrow e_j \sim e_i$

Recimo da $e_j K e_i = \{0\}$

$$\text{potem } (e_i K e_j) K (e_i K e_j) = 0 \Rightarrow e_i K j = 0 \quad \times$$

$e_i \sim e_j$ $e_j \sim e_i$

ker je polprakovolbar

$$e_i K e_j \neq 0 \Rightarrow \exists u \in e_i K e_j \exists v \in e_j K e_i$$

lema 5

$$uv = e_i \wedge vu = e_j$$

$$uv = e_i \Rightarrow ue_j v = e_i \quad ve_i u = e_j \quad (\text{ker } e_i u = u \text{ } u \in e_i K e_i)$$

Recimo da $e_i K e_n = \{0\} \Rightarrow e_j K e_n =$

$$= ve_i u K e_n = \{0\} \quad \times$$

$$\underbrace{\quad}_k = 0$$

$E_1, \dots, E_s$ naj bodo ekvivalentni razredi

Naj bo f vsota vseh idempotentov v E_i

$$f_i^2 = f_i \text{ in } f_i \cdot f_j = 0$$

$$f_1 + \dots + f_s = 1$$

$$f_i x = f_i x 1 = f_i x (f_1 + \dots + f_s) = f_i x f_i$$

$$\text{podobno } x f_i = f_i x f_i \Rightarrow f_i \in Z(K)$$

$$\text{po km: } 1 \Rightarrow K \cong f_1 K \times \dots \times f_s K$$

$$f_i K \cong M_{n_i}(D_i)$$

$$\hookrightarrow D_i = e_i K e_i$$

Posledica: Neničelni, levi kolobar K je levi artinski

$$\Leftrightarrow K \cong M_n(D) \text{ za nek } n \in \mathbb{N} \text{ in obseg } D$$

Posledica: (Wedderburnov izrek)

Naj bo A neničelna konzorazsežna algebra.

Potem je A polpraa algebra $\Leftrightarrow A \cong M_{n_1}(D_1) \times \dots \times M_{n_s}(D_s)$

kjer so $n_i \in \mathbb{N}$ in D_i obsegi in konzorazsežne algebre

Definicija: Kolobar je **polenostaven** če zadošča

ekvivalentnega pogoja Wedderburn-Artinovega izreka

Lema: Naj bo D končnorazsežna algebra nad algebrsko zaprtim poljem F . Če je D obseg $\Rightarrow D \cong F$

Dokaz: $n = \dim_F D$ $a \in D \Rightarrow 1, a, a^2, \dots, a^n$ so lin. odv.

$$\lambda_0 + \lambda_1 a + \dots + \lambda_n a^{n-1} + a_n = 0 \Rightarrow$$

$f(a)$ je polinom stopnje n $f(x) = F[x]$

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n) \quad \alpha_i \in F$$

$$0 = f(a) = (a - \alpha_1 \cdot 1) \dots (a - \alpha_n \cdot 1) = 0$$

en izmed teh mora biti 0, ker v obsegu
ni deliteljev nič $\Rightarrow a = \alpha_i \cdot 1$

$$\Rightarrow n=1$$

Posledica: Kompleksna končnorazsežna algebra A je
polpra algebra $\Leftrightarrow A \cong M_{n_1}(\mathbb{C}) \times \dots \times M_{n_s}(\mathbb{C})$

Naj bo D končno-razsežna realna algebra, ki je obseg

Primeri: $\mathbb{R}, \mathbb{C}, \mathbb{H}, \dots$?

Lema 1:

$$\forall x \in D, \exists \alpha, \beta \in \mathbb{R}. x^2 + \beta x + \alpha \cdot 1 = 0$$

Dokaz: Isto kot prejšnja lema + $\forall$ realen polinom je produkt linearnih in kvadratnih

Dogovor: Namesto $\alpha \cdot 1$ pišemo samo α

$\mathbb{R} \cdot 1 = \mathbb{R}$ $\mathbb{R}$ je enorazsežna podalgebra D

$$V := \{v \in D. v^2 \underset{\uparrow}{\leq} 0\}$$

(to pomeni: $v^2 = \alpha \cdot 1 \wedge \alpha \leq 0$)

Lemma 2: Če sta $u, v \in V$ lin. neodv. $\Rightarrow u, v, 1$ lin. neodv. $\leftarrow$ iz prejšnjestrani

Dokaz: Denimo da so $u, v, 1$ lin. odv.

$$\exists \alpha, \beta \in \mathbb{R}. \quad 1 + \alpha u = \beta v$$

$$1 + 2\alpha u + \alpha^2 u^2 = \beta^2 v^2 \quad \swarrow \text{če je } \alpha = 0$$

$$\Rightarrow 2\alpha u \in \mathbb{R} \Rightarrow u \in \mathbb{R} \quad \forall v \in \mathbb{R}$$

$$\Rightarrow u^2 = 0 \Rightarrow u = 0$$

ali:

$$v^2 = 0 \Rightarrow v = 0$$

Ze elementa $u, v \in V$ $\swarrow$ lahko je tudi keti i keti kolobar
 $u \circ v = uv + vu$ jordansti produkt
(ni asociativen, je pa komutativen)

u, v antikomutirata če $u \circ v = 0$

Lemma 3. Za $\forall u, v \in V$. $u \circ v \in \mathbb{R}$



Dokaz: Če sta u, v lin odvisna, je to očitno

$$v = \alpha u \quad u \circ v = 2\alpha u^2 \in \mathbb{R}$$

Drugače:

$W = \text{Lin}\{u, v, 1\}$ ima dimenzijo 3

$$(x+y)^2 = x^2 + x \circ y + y^2$$

Po 1.lem: $x \in W \Rightarrow x^2 \in W$

Zato $x \circ y = (x+y)^2 - x^2 - y^2 \in W$ (zaprteost za jordanovski produkt)

$A: W \rightarrow W$

$$w \mapsto w \circ u$$

A je linearna in dimenzija je 3

$\Rightarrow A$ ima realno lastno vrednost λ

$$w \circ u = \lambda w \quad wu + uw = \lambda w \quad \text{za nek } w \neq 0$$

$$\Rightarrow \overset{w^{-1}}{w^{-1}uw} = \lambda - u \quad /^2$$

$$u^2 = w^{-1}u^2w = \lambda^2 - 2\lambda u + u^2$$

$\uparrow$
ker $u^2 \in \mathbb{R}$ komutira z vsem

$$\Rightarrow 2\lambda u \in \mathbb{R} \Rightarrow \lambda = 0$$

$$\Rightarrow uw + wu = 0$$

$$w = \lambda_1 + \lambda_2 u + \lambda_3 v \Rightarrow 2\lambda_2 u + 2\lambda_3 u^2 + \lambda_3(u \circ v) = 0$$

$$\Rightarrow \lambda_3 \neq 0 \Rightarrow u \circ v \in \text{Lin}\{1, u\}$$

$$\text{podobno } u \circ v \in \text{Lin}\{1, v\} \Rightarrow u \circ v \in \text{Lin}\{1\}$$

$$\Rightarrow u \circ v \in \mathbb{R}$$

Lema 4: Če je $x \in D$ tak, da $x^2 \in \mathbb{R}$. Potem $x \in V$
 ali: $x \in \mathbb{R}$

Dokaz: $x \notin V \Rightarrow x^2 > 0 \Rightarrow x^2 = y^2$ za nek $y \in \mathbb{R}$
 $\Rightarrow (x-y)(x+y) = 0 \Rightarrow x = \pm y \in \mathbb{R}$

Lema 5: V je vektorski prostor in $D = \mathbb{R} \oplus V$

Dokaz: $u \in V$ poljučen

$$\underline{\underline{\alpha u \in V}}$$

$$(\alpha u)^2 = \alpha^2 u^2 \leq 0$$

$$\underline{\underline{u+v \in V}}$$

Predpostavimo da sta u in v lin neodvisna.

$$(u+v)^2 = \underbrace{u^2}_0 + \underbrace{uov}_{\in \mathbb{R}} + \underbrace{v^2}_0 \in \mathbb{R}$$

Po lemi 4. $u+v \in \mathbb{R}$ $\vee$ $u+v \in V$

Ker so $u, v, 1$ linearno neodvisni, velja $u+v \in V$

$$\underline{\underline{\mathbb{R} \oplus V}}$$

$$x^2 + \beta x \in \mathbb{R} \Rightarrow (x + \frac{\beta}{2})^2 \in \mathbb{R} \Rightarrow x + \frac{\beta}{2} \in V \vee x + \frac{\beta}{2} \in \mathbb{R}$$

$$x + \frac{\beta}{2} \in V \Rightarrow x = (x + \frac{\beta}{2}) - \frac{\beta}{2}$$

$$\downarrow \in \mathbb{R}$$

Vpeljemo skalarni produkt v V

$$\langle u, v \rangle = -\frac{1}{2} uov$$

Lemma 6: $n=1 \Rightarrow D \cong \mathbb{R}$. Če je $n=2 \Rightarrow D \cong \mathbb{C}$

$n \geq 2 \Rightarrow D$ vsebuje kvaternione (homomorfno kopije)

Dokaz: $n=1$ ✓

$$n \geq 1: \dim V = n-1 \geq 1$$

Naj bo i enotski vektor v V glede na $\langle \dots \rangle$

(to pomeni: $i^2 = -1$)

$n=2 \Rightarrow$ dvazgazen prostor, ima 1 in i , velja vsestranskost.

$n \geq 3 \Rightarrow \dim V \geq 2$. Naj bo j ortogonalna na i :

točej $ij = -ji$ in naj bo j enotski: $j^2 = 1$

$$\text{Vpeljemo } k := ij \quad k^2 = ijij = -i^2j^2 = (-1) \cdot (-1) = -1$$

$$k \cdot i = iji = -i^2j = j \quad \text{itd itd}$$

linearna neodvisnost

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

če $\underbrace{\quad}_{=0} \underbrace{\quad}_{=0} \Rightarrow a, b, c, d = 0$

Izrek: Frobeniusov izrek

V končno razsežen realni obsegu je izomorfen $\mathbb{R}, \mathbb{C}$ ali $\mathbb{H}$

Dokaz:

$$n > 4 \Rightarrow \dim V > 3$$

$$\dim(\text{Lin} \{i, j, k\}) = 3$$

Naj bo e endski vektor ortogonalen na ta prostor

$$\text{traj: } e i = -i e \quad \text{ona ko } z j \text{ in } k$$

$$e j = -j e$$

$$e k = -k e \quad e k = e i j = -i e j = i j e = k e = -k e$$

$$e k = 0 \Rightarrow e = 0 \quad \forall k = 0 \quad \text{ampak } e \text{ in } k$$

sklenatda

*

~~Q~~

oktenioni niso asociativni

Wedderburnov izrek:

V končen obseg je polje.

4.3 Grupna algebra

$G = \{g_1, g_2, \dots, g_n\}$ grupa

F polje

$F[G]$ Grupna algebra je vektorski prostor nad F z bazo G in množenjem

$$\left(\sum_i \lambda_i g_i\right) \left(\sum_j \mu_j g_j\right) = \sum_i \sum_j \lambda_i \mu_j g_i g_j$$

$F[G]$ je res algebra nad F

V konč. razs. vekt. pr. $T: V \rightarrow V$ lin. preslikava

$\text{tr}(V), \dots$ sled linearne preslikave = sled matrike prirejeni T glede na neko bazo

(to je dobro definirano, ker sta matriki glede na različni bazi podobni)

Izrek: (Maschkejev izrek)

Naj bo G končna grupa in F polje.

Potem je $F[G]$ polipralgebra (in tudi polenostavna, ker je končno razsežna), razen kadar je karakteristika polja F praštevilo p , ki deli $\text{red}(G)$

če je $p \nmid |G|$ potem $F[G]$ ni polipralgebra

Dokaz:

$$a \in F[G]$$

$$\rho: F[G] \rightarrow F$$

$$\rho(a) = \text{tr}(L_a)$$

$$L_a: F[G] \rightarrow F[G]$$

$$x \mapsto ax$$

ρ je torej linearni funkcional

$$g_1 = 1$$

$$\rho(g_1) = \rho(1) = \text{tr}(I) = \dim F[G] = \text{red}(G) = n$$

$$L_{g_2}(g_j) = g_2 g_j \neq g_j \quad \forall j$$

če za bazo izberemo G imamo matrice

L_{g_2} na diagonal: same ničle

$$\Rightarrow \rho(g_2) = 0 \quad \text{podobno } \rho(g_i) = 0 \quad \forall i \neq 1$$

Naj bo $I \triangleleft F[G]: I^2 = \{0\}$ in $I \neq \{0\}$

$$\text{Naj bo } 0 \neq a \in I = \lambda_1 g_1 + \lambda_2 g_2 + \dots + \lambda_n g_n$$

BŠZS. $\lambda_1 \neq 0$ (sicer a pomnožimo z $g_i^{-1} a \in I$ kjer $\lambda_i \neq 0$)

$$\rho(a) = \rho(\lambda_1 g_1 + \dots + \lambda_n g_n) = \lambda_1 \rho(g_1) + \dots + \lambda_n \rho(g_n) =$$

$$= \lambda_1 \rho(g_1) + 0 + \dots + 0$$

$$= \lambda_1 n$$

$$a \in I \Rightarrow a^2 = 0 \Rightarrow L_{a^2} = 0 \Rightarrow (L_a)^2 = 0$$

$$\rho(a) = \text{tr } L_a = 0$$

$\hookrightarrow$ sled nilpotentne matrice = 0

(spravimo v Jordanovo formo

nad algebraično zaprtim poljem $\bar{F}$)

$$0 = n\lambda_1 \Rightarrow n = 0 \Rightarrow p \mid n$$

Dokaz dodatni:

$$V = g_1 + \dots + g_n \in F[G]$$

$$V g_i = V = g_i V \Rightarrow F_V \triangleleft F[G]$$

$$V^2 = V(g_1 + \dots + g_n) = V + \dots + V = n \cdot V$$

$$p \mid n \Rightarrow nV = 0 \Rightarrow V^2 = 0$$

$$I = F_V \neq \{0\} \quad F_V^2 = 0$$

Skupaj z Wederburgovim rezultatom dobimo posledico

Posledica: $|G| < \infty$. Potem je $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \dots \times M_{n_s}(\mathbb{C})$

Na tem temelji upodobitev grup

$$\text{Primer: } \mathbb{C}[S_3] \cong M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}$$