

1. Deljivost v komutativnih klobarjih

$$xy = yx$$

$$1 \in K$$

Gaussova izreka!

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 endižno določena

v $\mathbb{F}[X]$: $f(x) = p_1(x) \dots p_s(x)$, kjer so p_1, \dots, p_s nerazcepni
endižno 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 $a \mid b$

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

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

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

Elementa sta **tuja**, 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: $(\Leftarrow) a = ub \wedge b = u^{-1}a$

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

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

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

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 \mathbb{Z} nerazcepen element? Odvisno od kolobarja

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

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

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

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

\nearrow katero koli polje

(3 pa ni razcepan)

1.2 Glavni kolobarji:

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

K komutativan

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) $\mathbb{Z} \text{ o } \mathbb{Z} = (0)$

2) $K = (1)$

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

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

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

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

$$(a_1, \dots, a_n) = \{a_1 x_1 + a_2 x_2 + \dots + a_n x_n; x_i \in K\}$$

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)

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

$x \in I \Rightarrow x = a_0 h(x)$ \times
 \uparrow sod $\uparrow x$ 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 delitelj nič

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

Izreki: Naslednji kolobarji so evklidski:

a) \mathbb{Z}

b) $F[x]$, F polje

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

Dokaz:

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

b) $\delta(fg) = \delta f \delta g$ (0 nima definirane stopnje)

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

b) \checkmark Vemo da je to kvadrat absolutne vrednosti:

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

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 $|l-v| \leq \frac{1}{2}$
 $g = k+li \in \mathbb{Z}_i$

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

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

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

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

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

Izrek: V evklidski kolobar je glavni kolobar

Dokaz: Naj bo evklidski z δ . $I \subseteq K$

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

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

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

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

Naj bo $x \in I$ poljuben

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

$$\Rightarrow a \mid x$$

glavni ~~≠~~ evklidski
kolobar kolobar

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

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

Dokaz:

Vzemimo ideal $(a, b) = \{ax + by; x, y \in K\} \stackrel{\text{kje glavni}}{=} (d)$

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

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

$$\exists d \in K. (a, b) = (d) \\ d \neq 0$$

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

$$d \in (a, b) \Rightarrow d = \underset{cz}{\parallel} ax + \underset{cw}{\parallel} by = c(zx + wy) \Rightarrow c \mid d$$

Izreki: Naj bo $p \neq 0 \in K$ glavnih deliteljev.

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

$$i) p = ab \Rightarrow a \text{ deljiv ali } b \text{ deljiv,} \\ p \text{ ni deljiv}$$

$$ii) (p) \text{ je maksimalen} \Rightarrow (p) \neq K \Leftrightarrow p \text{ ni deljiv}$$

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

$$p = ab \text{ in } a \text{ ni deljiv} \Rightarrow \\ b \text{ je deljiv}$$

i) in ii) utrdita pravzeto 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 delnjiv. 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 delnjiva

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 **noetrski**, če se \nexists naraščajoča veriga idealov

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

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

Lema: V glavnih klobar je noetrski

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

$I := \bigcup_{i \in \mathbb{N}} I_i$ to je ideal (vsplānem unija ni)
(ponavedi ni grupa za seševanje)

$u, v \in I$

$u-v \in I$

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

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 nekele 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
 $\underbrace{K[x][y]}_{\text{glavni}}$
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 $plab \Rightarrow pla \vee plb \quad \forall a, b \in K$

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

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

1)

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

$$\text{Recimo da } p \mid x \Rightarrow x = pu \Rightarrow p = pu y \Rightarrow$$

$$uy = 1$$

2) Naj bo K glavni

$$\Rightarrow y \text{ je obrnljiv}$$

p ne bo nerazcepen. p praelement

$$plab. \text{ Recimo da } p \nmid a \Rightarrow$$

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

$$1 = px + ay$$

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

Definicija: Cet kolobar K imenujemo kolobar z enolično faktorizacijo (UFD),

če se za vsak $a \neq 0$, ni obrnljiv, velja:

- obstajajo kti 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: $a = z_1 \dots z_t$; z_i nerazcepni
 $\Rightarrow s = t \quad \exists \pi \in S_n$. $z_{\pi(i)}$ asociiran z p_i

Izrek: V glavnem kolobar je kolobar z enolično faktorizacijo

Dokaz: $a \neq 0$ ni obrnljiv.

Vemo iz prvih dveh lemm: a je produkt nerazcepnih

$a = p_1 \dots p_s$ recimo da je tudi $a = z_1 \dots z_t$

$p_1 | a \Rightarrow p_1 | z_1 \dots z_t \Rightarrow \exists i \in [t]. p_1 | z_i$. BSZS $p_1 | z_i$
 \uparrow
 nerazcepen + glavni kolobar \Rightarrow praelement

z_1 nerazcepen $\Rightarrow p_1$ in z_1 sta si asociirana

$p_1 / p_1 \dots p_s = p_1 u_2 \dots z_t$

$p_2 \dots p_s = u_2 \dots z_t$ p - obroke ponovimo

$s = t$. $s > t \Rightarrow u = p_{t+1} \dots p_s$ ker ni moze
 $\underbrace{a \neq 0 \text{ ni obrnljiv}}_{\text{nerazcepen!}}$

2. Modeli

2.1. Caylyjev izrek za kolobarje

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

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

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

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

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

Cay R



Izrek: \forall kolobar lahko vložimo v kolobar
endomorfizmov neke aditivne grupe

Dokaz: K kolobar

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

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

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

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

$$a \mapsto l_a$$

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

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

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

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

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

injektivnost:

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

Fija

Glej

\mathbb{F}

(univ)

Naj bo A algebra nad poljem F

V vektorski prostor nad F

$$\text{End}_F(V)$$

Napodoben namir dokazemo

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

$$\dim A = n \quad \swarrow \text{matrice } n \times n \text{ nad } F$$

$$\dim A < \infty$$

$$M_n(F)$$

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

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

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

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

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

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

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

2.2 Definicija modula

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) $a(au) = au + au \quad \forall a \in K, \forall u, v \in M$
- 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 $K \rightarrow \text{End}(M)$

Dalje: 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 = vekt. prostor nad F
2. Vseke M additive skupine (= abelova grupa) 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 klobar K postane modul nad semimrebo, 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 podklobar 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

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

$$2) KN \subseteq N \quad (\forall a \in K. \forall n \in N. an \in N)$$

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 $\{0\}$ 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 $K = M_n(F)$ $M = \mathbb{F}^n$

$$M \subseteq F^M$$

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

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

M je enostaven modul nad matrikami;

Homomorfizmi: moduli

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

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

sta podmoduli M oz. N

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

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

(obstaja izomorfizem)

Kolobarji endomorfizmi

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

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

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

Schurava lemma: Če je M enostaven K -modul,
je kolobar $\text{End}_K(M)$ obseg (vsi elementi
so obrnljivi)

Dokaz:

Možbo $0 = \varphi \in \text{End}_K(M)$

$\ker \varphi$ in $\text{im } \varphi$ sta podmodula in M je enostaven

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

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

Kvocienčni modeli

M K -modul

N podmodul

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

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

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

S tem postane M/N K -modul
imenujemo ga kvocienčni modul.

Primeri:

1. $K=F \Rightarrow$ kvocienčni vekt. pr.

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

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

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

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

Izreki 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 N_1, \dots, N_s njegovi podmoduli:

če velja

$$a) M = N_1 + \dots + N_s \quad \text{brez } M:$$

$$b) \forall i \in [s]. \quad N_i \cap (N_1 + \dots + N_s) = \{0\}$$

potem M imenujemo **(notranja) direktna vsota** podmodulov N_1, \dots, N_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 notranja direktna vsota $N_1 \dots N_s$ je
 $M \cong N_1 \oplus \dots \oplus N_s$

izomorfizem je podan z $v_1 + \dots + v_s \mapsto (v_1, \dots, v_s)$
ker je $v_1 + \dots + v_s$ enoličen zapis

Tudi notr. dir. vsot. označimo z

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

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

Primer

1. $K = F$ ^{vsota} je ~~podprostor~~ ^{podprostor} je direktni sumant

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

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

Direktni sumandi so $\{0\}, n\mathbb{Z}$

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

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}
2. $K = \mathbb{Z}$: ciklični \mathbb{Z} modul so ~~ga~~ ciklične grupe
3. K komutativen kolobar ... ~~in~~ glej
4. 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 kanono generirana

2.4 Prosti moduli

Definicija: Podprostor B K -modula M je

linearno neodvisen, 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 $a_1 = \dots = a_s = 0$

Lč je B nezkonen ptem je linearno neodvisen, če je vsaka konena podmnožica lin. neodvisna

Če je B linearno neodvisen 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

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 d. 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) $K=\mathbb{Z}$ $G=\mathbb{Z}$
baza: 1 : $\mathbb{Z} = \mathbb{Z} \cdot 1$

Definicija: Modul, ki ima bazo se imenuje
Prosti modul

- Primeri:
- 1) Vsek vek. pr. je prost (kot F modul)
 - 2) K ketober, polen je
 $\underbrace{K \oplus \dots \oplus K}_{s \text{ sumandov}} = K^s$ je prost K modul
 - 3) \mathbb{Z}^s je prosta abelova grupa \iff abelova grupa, ki
je kot \mathbb{Z} modul prosta

Vespaña

$0 \rightarrow L \xrightarrow{f} M \xrightarrow{\psi} N \rightarrow 0$ je **kratko eksaktno zaporedje** $f \circ \eta_j, \psi \circ \eta_j \implies \text{Im } f = \text{Ker } \psi \quad (\psi \circ f = 0)$

L podmodul M

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

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

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

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

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

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

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

kratko eksaktno zaporedje **razpada**, če zaporedje

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

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

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

$$\downarrow \text{id} \quad \downarrow \sigma \quad \downarrow \text{id}$$

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

$\exists \sigma$ izomorfizem
da ta diagram
komutira

$$\sigma \circ f = i_L \quad \sigma(\psi(t)) = (t, 0)$$

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

Izrek: Za katko eksaktno zaporedje

$$0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0 \quad \text{so naslednji pogoji}$$

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 velja j^o pogoj

σ je homomorfizem oostre

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

$\Rightarrow u \in \ker \varphi' = \text{im } \varphi \Rightarrow u = \varphi(t)$

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

Svoj $(t, v) \in L \oplus N$

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

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

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

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

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

$\varphi'(u) = \varphi'(u_0) + \varphi'(\varphi(l)) = t$

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

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

enako

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

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

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

Svoj

$u \in M$

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

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

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

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

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

veno: $\text{im } \varphi = \ker \psi$

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

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

$\sigma f = \text{id} \quad \varphi(t) = \sigma'(t, 0) = \varphi(t)$

drugi p^o

i) \Rightarrow ii) in iii)

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

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

pregledano definicije in vidimo da je vreda

2.6 Projektiivni modul:

$$\begin{array}{ccc} & P & \\ \swarrow \vartheta & \downarrow \psi & \\ M & \xrightarrow{\psi} N & \rightarrow 0 \end{array}$$

ψ surjektiv

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

Lema: Vsek prost modul je projektiiven

Dokaz: P prost

$$\begin{array}{ccc} & P & \\ \swarrow \vartheta & \downarrow \psi & \\ M & \xrightarrow{\varphi} N & \rightarrow 0 \end{array}$$

P ima bazo B

$$\varphi(e) = \varphi(u_e) \text{ za nek } u_e \in P$$

$$\vartheta: e \rightarrow u_e$$

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

Izrek: Za modul P so naslednje trditve ekvivalentne

$\Leftrightarrow P$ je projekcijski modul

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

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

Dokaz:

i) \Rightarrow ii) P proj. $\begin{array}{ccccccc} & & & & P & & \\ & & & \nearrow \psi & \downarrow \text{id} & & \\ 0 & \rightarrow & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & P \rightarrow 0 \end{array}$

$\exists \vartheta$ da je $\varphi \vartheta = \text{id}_P$

φ' je ϑ in tako zaporedje razpade

ii) \Rightarrow iii) Vseki modul (tudi P) je konomotorni sledi prostega modula, ki ga označuje z M

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

$0 \rightarrow \ker \varphi \xrightarrow{\text{id}} M \xrightarrow{\varphi} P \rightarrow 0$

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

$\begin{array}{ccc} & L \oplus P & \swarrow \text{projektivna} \\ \theta \nearrow & \downarrow \pi_P \uparrow i_P & \\ & P & \\ \downarrow \varphi & & \\ M & \xrightarrow{\varphi} & M \rightarrow 0 \end{array}$
 $\vartheta := \theta i_P$

$\varphi \vartheta = \varphi$ $\varphi \vartheta = \varphi \theta i_P = \varphi \pi_P i_P = \varphi \text{id}_P = \varphi$

Primer: želimo najti projekcijski modul k 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 (e -ideal)

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

$\Rightarrow \{ex\}$ nikoli ni linearna neodvisna:

$$\{k_1, k_2 \text{ kolobarja } K := K_1 \times K_2 \\ e = (1, 0)\}$$

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

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

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

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

torej je P projekcijski modul (kot direktna sornad prostora), k ni prost

2.7 Tenzorski produkti

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

Moduli bodo nad komutativnim kolobarjem K

M, N K -moduli

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

Naj bo $\mathcal{N} = \mathcal{N}_{M,N}$ podmodul generiran z vsemi elementi dolžke $(a(u + a'u), v) - a(u, v) - a'(u', v)$,
 $(u, a(v + a'v)) - a(u, v) - a'(u, v')$, 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

$(\Phi(a(u + a'u), v) = a\Phi(u, v) + a'\Phi(u', v)$ 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)

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_K N \\ & \searrow \Phi & \downarrow \varphi \\ & & L \end{array}$$

bilinearna

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

za \forall bilinearno 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

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

$\parallel \qquad \qquad \parallel \qquad \qquad \parallel$

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

Podobno izpeljemo linearnost preslikave \otimes v drugem argumentu

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

Iščemo linearno preslikavo φ enolizno

\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).

Enoliznost

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

Analogno obstaja linearna preslikava

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

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

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

"ujemanje na bazi"



"Praktična" definicija tenzorskega produkta

- $\forall u \in M, \forall n \in \mathbb{N}, \exists u \otimes v \in M \otimes N$. T. imenujemo **enostavni** tenzor.
Vsak drug element je vsota 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 definirano

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

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

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

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** φ in ψ

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

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

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

φ, ψ izomorfizma $\Rightarrow \varphi \otimes \psi$ 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) $M \otimes K \cong M$

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

Dokaz:

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) $M \otimes K \rightarrow M$
 $u \otimes a \mapsto au$

$M \rightarrow M \otimes K$
 $u \mapsto u \otimes 1$

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

b) Radi bi videli, če 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 $\alpha: u \otimes v \mapsto u \otimes (v \otimes w)$

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 \exists seena linearna preslikava ki slik

$(M \otimes N) \otimes R \rightarrow M \otimes (N \otimes R)$ \ddot{u}



2.8 Tenzorci produkti prostih modula

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 , a morda vsi vemo 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 poljučen K -modul.

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

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

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

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

↑
za neke $a_i \in K$

enoličnost:

Ker je V element $M \otimes N$ vsake enostavnih tenzorjev, je res V element oblike $\sum e_i \otimes v_i$.

Zato da 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 $\varphi: M \otimes N \rightarrow N$

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 $\Phi: M \otimes N \rightarrow N$

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

zato \exists 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: Podoben izrek velja, če je N prost
z bazo $\{f_j\}$

Izreki: Naj bo 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: Velemen je oblike $\sum_i e_i \otimes v_i =$

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

Linearne neodvisnost?

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

česar $\sum e_i \otimes v_i$ je enoličen

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

\nearrow f. baza

□

Posledica: Če je U vekt. pr. nad F z bazo $\{e_i\}$ in
 V vekt. prost nad F z bazo f_j , je $U \otimes V$ vekt. 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 , $v \in V$, $f \in V^*$ ^{\leftarrow dual V}
 _{\leftarrow lin funkcional}

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

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

Primeri: n izdeli v učeniku

2.9 Tenzorski produkt algebr

Algebra nad F :

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

Splāšējais priems: Algebra nad komutatīvu kolobarju K je definēta enāko. Torej je to K -modul
skupis Z množenjum (za katera je kolobar) in se
akšam $a(xy) = (ax)y = x(ay)$

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 definiranoost množenja

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

$$z \in A \quad w \in B$$

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

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

$$\Phi: A \times B \rightarrow \text{End}(A \otimes B) \quad \left(\begin{array}{l} \text{enkrat je samo} \\ K\text{-modul} \end{array} \right)$$

$(z, w) \mapsto \rho_z \otimes \rho_w$ če je $A \otimes B$ K -modul, je $\text{End}(A \otimes B)$ K -algebra

Φ je bilinearna zato \exists 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:

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

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

asoc: očitno

enota: $1 \otimes 1$

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

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

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

direktni produkt
in direktna vsota
algebr sta ekvivalentna

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

$$d) A \otimes K \cong A$$

Dokaz: isto kot za module

Primer:

- $K[X]$ je kolebar in je celo 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 kolebar in je tudi K -Algebra, če

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

lahko definiramo

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

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

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

$$\text{Vpeljemo } \varphi: M_n(A) \otimes A \longrightarrow M_n(A)$$

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

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

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

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

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

\uparrow
bloke matrike

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

$T \in M_n(K)$

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

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

2.10 Razširitev skalarjev

Naj bo A realna, konvencionalna algebra

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

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

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

Primer:

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

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

* izdelike niza :: zato nemore biti $\cong \mathbb{H}$

K, C komutativna klobarja

M K -modul

$\alpha: K \rightarrow C$ homomorfizem

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

$$(k_1 \cdot k_2) c = \alpha(k_1 k_2) c = \alpha(k_1) \alpha(k_2) c = \alpha(k_1) k_2 c = k_1 (k_2 c)$$

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
 $d \mapsto cd$

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

↑
nesparne 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:

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

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

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

$$C(1 \otimes u) = C1 \otimes u \text{ je } A_C \text{ } C\text{-algebra}$$

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

$$\text{bazijskih vektorjev } e_i e_j = \sum_k \alpha_{ijk} e_k, \text{ je}$$

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

Primer: K komutativan kelobar

Naj bo I maksimalni ideal $K \Rightarrow K/I$ je polje

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

$$\alpha: K \rightarrow C$$

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

vektorski prostor M nad C

Zreke: 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

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

in tudi bijektivne \Rightarrow je izomorfizem $C(\text{id}_C \otimes \Phi)(c \otimes u)$
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

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

torzijski podmodul

To je podmodul

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

$$au = 0 \quad bv = 0$$

$$ab(u-v) = b au - abv = 0 - 0 = 0$$

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

$$\Rightarrow abu = b au = 0$$

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

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

$$a(u + \text{tor}(M)) = 0 \Rightarrow au + \text{tor}(M) = 0 \Rightarrow au \in \text{tr}(M)$$

$$\Rightarrow \exists b \in K. b au = 0 \Rightarrow u \in K. \ker(ba)u = 0$$

$$\Rightarrow u + \text{tor } M = 0$$

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

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

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

...Vsí elementi razen 0 imajo neskončen red

kanone \Rightarrow kanono generirane

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

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

$\mathbb{Z}^s \oplus K \leftarrow$ kanone abelava

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



kanono generirane abelava grupe

Lema: Končno generirana torzijsko prosta abelova grupa je prosta

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

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

Denimo da H ni prosta

Izmed vseh množic z m elementi, ki generirajo
 H , raberimo „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 vsaj 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

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

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

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

Vti ima končen red, zato je takih različnih zapisov le končno mnogo.

Posledica: V kanonično generirani abelovi grupi, 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 enolično določeni:

Enak izrek velja za module nad glavnim
kolebarjem

3. Prezentacije grup in algebr

3.1 Proste grupe in prezentacije grup

Neformalno: kaj je prosta grupa na množici X

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

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

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

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

Različni; zapiši da jo vedno različne elemente

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

Formelno: 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, kjer 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 $(x_1^{e_1}, x_2^{e_2}, \dots, x_n^{e_n}, 1, \dots) \quad e_i \in \{1, -1\}$

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

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

$x_i, y_i \in X$

in naj bo $m \leq n$

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

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

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

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 naj bo 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 $\varphi(i(x)) = f(x)$
 $\forall x \in X$

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

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 grupa je homomorfna slik: proste grupe

Dokaz: Naj bo G grupa. Naj bo $X \in G$ 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 ideal generirana 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

$N = N_R \quad F_X / N$ 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

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

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

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

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

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

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

$$N \text{ edinka gen. z } x^n, y^2, (xy)^2$$

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

$$\text{ki zadošča } u^n = v^2 = (uv)^2 = 1$$

D_{2n} je take grupe, pa tudi $F_{\{x,y\}}/N$ je take

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

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

2. korak: G ima največ 2n elementov

Denimo da je to res. Potem po 1. koraku

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

2. korak pavi, da če za G izberemo $\frac{F_{\{x,y\}}}{N}$

$$\text{ima } \leq 2n \text{ elementov} = |D_{2n}| \Rightarrow$$

φ je bijektiven

1. korak

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

$$x \mapsto u$$

$$y \mapsto v$$

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

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

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

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

2. korak

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

\S

$$m_i \in \mathbb{Z}, n_i \in [n]$$

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

Edini možni elementi so

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

3.2. Proste algebre in prezentacije algebr

Algebra naj bo nad poljem F

Elementi proste algebre so nekomutativni; polinom.
 X, Y dve spremenljivki

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

Naj bo X množica. Elementi *proste monoida*

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

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

Vpeljemo 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

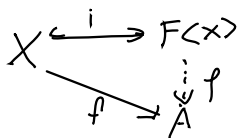
$F\langle X \rangle$ naj bo vektorski prostor nad F z bazo X^*

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

$$(\sum \lambda_i w_i) (\sum \mu_j w_j) := \sum V_k w_k \\ w_i w_j = w_k \\ V_k = \sum_{w: w_j = w_k} \lambda_i \mu_j$$

$F\langle X \rangle$ 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: $\varphi(p(x_1, \dots, x_m)) := p(f(x_1), \dots, f(x_m))$
 To je res homomorfizem

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

Posledica: Vsaka algebra je homeomorfna sliki
 neke proste algebre

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

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

$$A \cong F\langle X \rangle / (R)$$

kideal proste algebre generiran z R

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

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

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

Primer:

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

$$\uparrow \\ E_{11} = E_{12}E_{21}$$

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

$$I = E_{12}E_{21} + E_{21}E_{12}$$

Ugibamo: prezentacija je F

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