

1. Deljivost v komutativnih kolobarjih

$$xy = yx$$

$\lambda \in K$

polje

Gaussova števila!

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

Cel kolobar - komutativen kolobar, brez delitljiv
niza

Osnovni izrek aritmetike $n \in \mathbb{N}$. $n = p_1 p_2 \dots p_s$
 $p_1, \dots, p_s \in \mathbb{P}$ prstevila andicna delocna

v $F[X]$: $f(x) = p_1(x) \dots p_s(x)$, kjer so $p_1 \dots p_s$ nerazložni
enolično delocni:

1.1 osnovni pojmi

Definicija: Naj bo K komutativen kolobar.

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

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

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

2. nancelna elementa $a, b \in K$ sta asocirana, če delita drug druga ali $a | b$ ali $b | a$

3. Največji skupni delitelj elementov $a, b \in K$, ki niste ena o, je tak element $d \in K$, da velja

a) $d | a \wedge d | b$

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

Elemente sta tuja, če jenžu največji skupni delitelj enak 1
(n.s.d.)

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

a) $p \neq 0 \wedge p$ ni obrnljiv

b) $p = ab \Rightarrow a$ je obrnljiv $\wedge b$ je obrnljiv

Element je razcegen

a) $p \neq 0 \wedge p$ ni obrnljiv

b) p ni nerazcegen

Odslej: k je cel

Trditv: Naj bo k cel kolobar. $a, b \in k$ a $\neq 0$
 $b \neq 0$ sta asocirana \Leftrightarrow Esek obrniljiv, 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
ni delitelj ju niza $\Rightarrow k = g^{-1}$

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

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

Primer: Ali je \mathbb{Z} nerazcegen element? Odrisno od kolobarja

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

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

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

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

Katero kol. pošte

(3 pa n; razcegen)

1.2 Glavni kolobarji:

I : ideal: • $I \subseteq (K, +)$
• $KI, IK \subseteq I$

K komutativen

Definicija: Maj 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)

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

$$\Rightarrow a = \underbrace{gb}_{\alpha x = b(gx)}$$

$$\alpha x \in (b) \Rightarrow a \in (b) \Rightarrow (a) \subseteq b$$

$$\Leftarrow a \in (a) \subseteq (b) \Rightarrow a = \underbrace{gb}_{\alpha x = b(gx)}$$

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

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

2) $K = (1)$

$$k = (a) \Leftrightarrow a \text{ je obrnjiv}$$

Ideal je konanageneriran, če je generiran s konano množico

če je I generiran z $\{a_1, \dots, a_n\}$ ali označimo
 $= (a_1, \dots, a_n)$

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

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

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

Edim ideal: \mathbb{Z} so $n\mathbb{Z}$ (glevni: ideal!)

2. $\vee F[\mathbb{X}]$ ideal?

polinomi s konstantnim členom o (X)

vsj ideali so glejni!

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

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

Ali je I glejni ideal?

$$\text{npr } I = (f(x))$$

$2 = f(x) \text{ gesd} \Rightarrow f(x) \text{ je lahko samo}$

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

$$x \in I \Rightarrow x = a_0 h(x)$$

\nwarrow sod \times \nearrow ni sod

4) $\vee F[\mathbb{X}, Y]$ ideal iz polinomov s konstantnim členom z o (X, Y) tudi ta ideal ni glejni:

Definicija: Cel kolobar K je glavn; kolobar,
če je vsek njegov ideal glavn; (PID)

↑
principle ideal domain
↗?
n; delitelj nica

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

Izreči: Naslednji kolobarji so arklidski:

- a) \mathbb{Z}
- b) $F[X]$, F polje
- c) $\mathbb{Z}[i]$

Dokaz:

- a) $\delta: m \mapsto |m|$
- b) $\delta(f(x)) = \delta(f(x))$ (O nime definirane stopnje)
- c) $\delta: m+n \mapsto m^2+n^2$

b) ✓ Vemo da je to kvadrat absolutne vrednosti.

$$\delta(|w|) = |zw| \quad |w| \neq 0 \Rightarrow |w| \geq 1$$

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

$$a = \underbrace{b}_r + \underbrace{r}_{\dots}$$

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

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

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

$$z = k + l i \in \mathbb{Z};$$

$$r := a - \underbrace{zb}_r \quad r = 0 \vee \delta(r) < \delta(b)$$

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

$$|r|^2 = |a - \underbrace{zb}_r|^2 = |cb - \underbrace{zb}_r|^2 =$$

$$= |c - \underbrace{z}_r|^2 |b|^2 = ((u-k)^2 + (v-l)^2) |b|^2$$

$$\begin{matrix} \nearrow \\ \frac{1}{4} \\ \end{matrix} \quad \begin{matrix} \nearrow \\ \frac{1}{4} \\ \end{matrix}$$

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

Izrek: Aevklidski kolobar je glavn; kolobar

Dokaz: K nej bo evklidski $\Rightarrow \sigma$. Iak

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

$$I \neq \{0\}. \exists a \in I, a \neq 0$$

Naj bo aek element, ki ima najmanjso vrednost v σ od vsek $a \in I$

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

Naj bo $x \in I$ poluben

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

glavni \Rightarrow evklidski
kolobar kolobar

Izrek: Nej bosta $a, b \in K$ glavne klobarje ($a \neq 0 \vee b \neq 0$). Potem \exists največji skupni delitelj obstaja in je obliko

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

Dokaz:

\forall pomimo ideal $(a, b) = \{ax + by; x, y \in K\} \overset{k \in \text{glavn.}}{\supseteq} (d)$

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

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

\exists del. $(a, b) \nsubseteq (d)$
 $d \neq 0$

Reamo da $\exists c \in K, c \neq 0 \wedge c | b$

$$\begin{aligned} d \in (a, b) &\Rightarrow d = \underset{c|z}{\cancel{a}x} + \underset{c|w}{\cancel{b}y} = c(zx + wy) \Rightarrow c | d \end{aligned}$$

Izrek: Maj bo $p \neq 0$ ek afavniholobar.

Navednj; poagni so ekvivalentni:

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

Dokaz: ii) \Leftrightarrow iii) Algebra 2

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

$$\vee M = I$$

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

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

$(p) \subseteq (a) \not\subseteq K \Rightarrow (p) = (a) \Rightarrow p | a \wedge a | p$

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

i) in ii) ustvarju prav tako isto

1.3 Endična faktorizacija

$a \neq p_1 p_2 \dots p_n$

Lemma: Nej bo K cel klobar. Dovimo da element a ni enak produktu razceganih elementov. $a \neq 0$ in a ni obrnjiv. Potem K vsebuje tako neskonano zaporedje elementov $a = a_1, a_2, \dots$ da je $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$
(Neskonano strogo naraščajoče zaporedje glavnih idealov)

Dokaz:

a ni razcegan

$a_1 = a_2 b_2$, a_2 in b_2 nista obrnjiva

Vsih eden izmed njiju (npr a_2) ni produkt razceganih

$a_2 = a_3 b_3$; a_3 ni produkt razceganih

$(a_1) \subsetneq (a_2)$ saj $\exists e(a_2) = (a_2) \Rightarrow a_1 = a_2 e$

$\Rightarrow u = b_2$ je obrnjiv \times

Definicija: Komutativen klobar K je **neotsko**, 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

Lemma: \forall glavn; koločar je načrtov.

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

$I := \bigcup_{i \in \mathbb{N}} I_i$ to je ideal (v sklopu enem unija n)
 $KI \subseteq I$ oziroma (ponavadi n ; grupa α sestavljanje)
 $u, v \in I$

$\frac{u-v \in I}{\dots}$

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

I je glavn;, zato je $I = (\alpha)$ za nek $\alpha \in I$

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

Od nekod nekej sa vsi ideali $I \subseteq I_{n+1} \subseteq I$

Hilbertov izrek o bazi

K načrtni $\Rightarrow K[x]$ načrtni

Primer: $K[x, y]$ n; glavn;

||

$K[x][y]$

glavn;

n ; aglavn;

preženji: dve leme \Rightarrow v glavnem kolabaju
je \forall element produkt nerazcegenih

Definicija: Nej bo K komutativen kolobar.

$p \in K$ je **praelement** $p \neq 0$, p ni obrniljiv in
velja $p|ab \Rightarrow p|a \vee p|b$ $\forall a, b \in K$

Leme: Nej bo K cel. Vsak praelement je nerazcen.
če je K glavn. velja tudi obrat

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

$$\stackrel{1)}{\rightarrow} p|x y \Rightarrow p|x \vee p|y.$$

$$\text{Recimo da } p|x \Rightarrow x = pu \Rightarrow p = puy \Rightarrow \\ u = 1$$

$\stackrel{2)}{\Rightarrow}$ Nej bo K glavn. $\Rightarrow y$ je obrniljiv

p nej bo nerazcen. p praelement

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

p in a sta si tja (to pomeni da je najvecji
skupni delitelj 1)

$$1 = px + ay$$

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

Definicija: Čet kolaber k imenujemo
kolaber z enolichen faktorizacijo (UFD),

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

- obstajajo tako nerazcepni elementi p_i ,
da je $a = p_1 \dots p_s$
 - ta faktorizacija je enolična do asociiranosti
in vrstnega reda faktorjev natančno
- To pomeni: $a = g_1 \dots g_t$; g_i nerazcepni;
 $\Rightarrow s = t$ in $\exists \{e_{i,j}\}$, $g_{T(i)}$ asociiran z p_j .

Izrek: V glavnih kolaberi je kolaber z enolichen faktorizacijo.

Dokaz: $a \neq 0$ ni obrnljiv.

Vemo iz prvih dveh lem: a je produkt nerazcepnih
 $a = p_1 \dots p_s$ recimo da je tudi $a = g_1 \dots g_t$

$$p_1 | a \Rightarrow p_1 | g_1 \dots g_t \Rightarrow \text{Fakt. } p_1 | g_i \cdot \text{BSZS } p_1 | g_i$$

↑
nerazcepen + glavni kolaber \Rightarrow prvi element

$\exists i$ nerazcepen $\Rightarrow p_1 \mid g_i$ str. 8; asociiran

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

$$p_2 \dots p_s = u_2 z_2 \dots z_t \quad p - \text{slopek paravine}$$

$$\underline{s=t:} \quad \underline{s>t} \Rightarrow \underline{u = p_{t+1} \dots p_s} \quad \text{ker ni možete}$$

$\overbrace{\text{atnljiv}}$ $\overbrace{\text{nerazcepen}}$

2. Modeli:

2.1. Cayleyjev izrek za kolaboraciju

$$\begin{array}{ccc} G & \longrightarrow & G \\ L_a: x & \mapsto & ax \\ & & a \mapsto L_a \end{array} \quad \varphi: G \longrightarrow \text{Sym } G$$

M aditivne grupe

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

$$\varphi \in \text{End } M \Leftrightarrow \varphi: M \rightarrow M, \quad \varphi(u+v) = \varphi(u) + \varphi(v)$$

$\text{End } M$ je kolobar če veljame

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

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

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

Cay R



Izrek: Ako k je tihko vložimo u k homomorfizmov neke aditivne grupe

Dokaz: K je k

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

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

$l_a \in \text{End}(K)$
K je k let grupa za +

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

$$a \mapsto l_a$$

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

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

Fija

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

$$\begin{matrix} l \\ (ab)x = a(bx) \end{matrix}$$

$$\varphi(1) = 1 = id = l_1$$

Gayley
()

(wyl) wyl

injektivnost:

$$a \in K \Leftrightarrow l_a = 0 \Leftrightarrow ax = 0 \forall x \Leftrightarrow a = 0 \quad (\ker x = 1)$$

Naj bo A algebra nad poljem F

V vektorski prostor nad F

$\text{End}_F(V)$

Napodoben nečim dokazemo

Izrek: A algebra nad F lahko vložimo v
algebra endomorfizmov nekega vekt. prostora
nad poljem F .

$$\dim A \stackrel{n}{<} \infty \quad M_n(F) \xrightarrow{\text{matrice nxn nad } F}$$
$$A \hookrightarrow \text{End}_F(A) \cong A \text{ lahko vloženo v algebra lin. operatorjev}$$

končno razsežnosti prostora

Posledica: A končna razsežna algebra nad F lahko vložimo v algebra n × n matrik za neki $M_n(F)$

Primer: A končna razsežna algebra nad F
Ali ta algebra lahko vsebuje tako elemente s in t

$$\text{da je } st-ts=1$$

ekvivalentno: ali obstajata tako matrike S in T, da

$$st-ts=I$$

$$\operatorname{sl}(st-ts) = \operatorname{sl}(F) = n$$

$$\operatorname{sl}(st) - \operatorname{sl}(ts) = n$$

$$\operatorname{sl}(st) - \operatorname{sl}(ts) = 0$$

če je $\operatorname{char} F = 0$ je to pravilno

2.2 Definicija module

Definicija: Naj bo K kolobar. Množica M

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

in $K \times M \cup M$ in binarna operacija

$M \times M \rightarrow M : (u, v) \mapsto u+v$ 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 števaji:

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 levi imamo rea in podobno

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

Odgovor modul = levi modul!

Primeri:

1. $\lambda = F$ potem je F -modul = vektori prostor nad F

2. Vsecke M additive grupe (=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. Če k je postopek modul nad semimedjo, če definiramo $a \cdot u$ kot običajni produkt $a \cdot u \in K$

4. Napiši bo I lev: ideal K

I je K -modul, če je av običajni produkt

5. Napiši bo K podmodul K' . če av označi množenje v K' , jo K' K -modul

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

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

7. trivialni: ali nizdimen modul

2.3 Osnovni pojmi teorije modula

Podmoduli

Podmodul je podmnožica, ko je za iste operacije
sama modul.

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

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

$$2) KN \subseteq N \quad (\forall k \in K, n \in N, kn \in N)$$

Primeri:

1. Če je V vektorična nad F je podmodul = podprostori

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

3. Podmodul K -modula K so levi ideali

če sta N_1 in N_2 podmodule tudi

$N_1 \cap N_2$ in $N_1 + N_2$ podmodule

Def: Ce sta zgozi in M edina podmodule tudi
recemo da je M enostaven

Primer:

1. V. prostor je enostaven test modul \Rightarrow je 1-rozsečen

2. Aritmetični prostor je enostaven kot \mathbb{Z} -modul $\Rightarrow \cong \mathbb{Z}_p$

3. $M = M_n(F)$ $M = F^n$

$$N \subseteq F^n$$

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

$$A \in N \Leftrightarrow \forall A \in M_n(F) \quad \{A \in M_n(F)\} - F^n$$

M je enostaven modul nad matridom;

Homomorfizm: modulov

M, N K -module

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

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

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

$$\text{oz: rama ekvivalentna } \varphi(au+bv) = a\varphi(u) + b\varphi(v)$$

Rečemo jim tudi K -linearne preslike/av

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

stan podmodula M oz. N

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

$M \cong N = \exists \text{ :izomorfija } N$

(obstaja :izomorfizam)

Kolobarji endomorfizmov

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

M aktivne grupe $\text{End}(M)$

$\text{End}_k(M) = \{ \varphi; \text{endomorfizm; } k\text{-modula } M \}$

je kolobar ce vjetrene

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

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

Schurova lema: Če je M enosteven k -modul,
je kolobar $\text{End}_k(M)$ obseg (zsi elementi
en doonljiv:)

Dokaz:

$$\text{Naj bo } 0 = \varphi \in \text{End}_k(M)$$

ker φ in im φ ste podmoduli 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 doonljiv element

Kvocientni moduli

M K-modul

N podmodul

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

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

$$\alpha(u+N) = \alpha u + N$$

S tem postavljene $\frac{M}{N}$ K-modul
imenujemo ga kvocientni modul.

Primeri:

1. $K = F \Rightarrow$ kvocientni vektori pr.

2. $K = \mathbb{Z} \Rightarrow$ kvocientna grupa $\mathbb{Z}/n\mathbb{Z}$

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

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

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

Izrek o izomorfizmu

$$\gamma: M \rightarrow N \Rightarrow M_{\text{ker } \gamma} \cong \text{Im } \gamma$$

Direktne vsote modulov

M_1, \dots, M_s k-moduli:

Unazice $M_1 \times \dots \times M_s$ 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: zunanjja direktna vsota

Naj bo sedaj M modul in N_1, \dots, N_s njegovi podmoduli:

če velja

$$a) M = N_1 + \dots + N_s \quad \checkmark \quad \text{rez } N:$$

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

potem M imenujemo (natančno) direktna vsota podmodulov N_1, \dots, N_s

b) je ekvivalenten da iz $v_1 + v_2 + \dots + v_s = 0$ sledi

$$v_i = 0 \quad \forall i \in \mathbb{N}$$

Ce je M nebrana direktna vsota $N_1 \dots N_s$ je
 $M \cong N_1 \oplus \dots \oplus N_s$

Karakterizem je poden $\cong V_1 \oplus \dots \oplus V_s \xrightarrow{\text{iff}} (V_1 \dots V_s)$
ker je $V_1 \oplus \dots \oplus V_s$ en direktni zopis

Tudi matr. dir. vsot. označimo z
 $N_1 \oplus \dots \oplus N_s$

Naj bo N podmodul M. Zatem pa je
N direktni sumant, če obstaja tak
podmodul N' , da je $M = N \oplus N'$

Primer

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

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

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

Direktne sumande stale zopis: $n\mathbb{Z}$

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

Generiranje modulov

M K-modul

$u \in M$

$Ku = \{au : a \in K\}$ je podmodul M, ki ga tako vsebuje u. Rečeno pa je ku generiran z u

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

Ciklični modul je generiran z enim samim elementom

Priimer:

1. $K = \mathbb{F}$: 1-rezultanti podmoduli in \mathbb{Z}^3

2. $K = \mathbb{Z}$: ciklični Z-modul so ~~ne~~ ciklične grupe

3. K komutativen kolobar ... ~~je~~ glede na

$u \in I$ lev.: ideal $K/\underline{I} = \{a + I : a \in K\}$

K/\underline{I} je ciklični modul generiran z $1+I$

Naj bude $X \subseteq M$. Podmnožina generirana
z X je množica vseh linearnih
kombinacij

če je podmnožina generirana s X , cel M ,
recemo da množica X generirana M
 M je končno generirana

2.4 Prosti moduli

Definicija: Podmnožica 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 enoti t_1, \dots, t_s sledi: $a_1e_1 + \dots + a_se_s = 0$ sledi $a_1 = \dots = a_s = 0$
Če je B neprazna podmnožica M je linearno neodvisna, če je vsaka končna podmnožica lin. neodvisna.

Če je B linearno neodvisna in generira M je ta **baze** modula M

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

Spomembba: Če je B baza M , za vsak element $x \in M$ obstajajo $a_1, \dots, a_s \in K$, deje $x = a_1e_1 + \dots + a_se_s$ kjer so a_i enotne deloženosti x iz K

$$\text{Pišemo } x = \sum a_i e_i$$

Primer:

- 1) $K = F$: vsi vek. prost. imajo bazo
- 2) $K = \mathbb{Z}$ G končna abelova grupe
nega je Že Že n: lin neadvise
ker je $n \cdot u = 0$ kjer je n red grupe

Edina linearna neadvise množica je pravimo

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

baze: ~~je~~ sta $\{1\}$: n $\{1\}$

ZDefinicija: Model, ki ima bazo se imenuje
prosti model

Primer: 1) Vsak vek.-pr. je prost (kot F model)

- 2) K kolobar, polom je

$$\underbrace{K + \dots + K}_{s \text{ sumandov}} = K^s \text{ je prost k model}$$

- 3) \mathbb{Z}^s je prosta abelova grupe = abelova grupe, ki
je kot \mathbb{Z} model prost

✓ *españa*

$0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$ je krate eksaktna
 zaporedje φ inj, ψ sur $\text{Im } \varphi = \ker \psi$ ($\psi \circ \varphi = 0$)

L podmodul M

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

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

$$L \cong \text{im } \varphi \cong \text{ker } \psi$$

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

$$\begin{aligned}
 0 \rightarrow L &\xrightarrow{i_L} L \oplus N \xrightarrow{\pi_N} N \rightarrow 0 \\
 t &\mapsto (t, 0) \\
 (t, v) &\mapsto v
 \end{aligned}$$

Krate eksaktna zaporedje razpade, če zaporedje

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0 \quad \text{izpelje krate}$$

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

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

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

$\exists \sigma$ izomorfizem
 deto diagramen
 komutativ

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

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

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

Izrek: Za karte eksaktno razpadlj

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

ekvivalentni:

\Leftrightarrow razpadlj je razpadno

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

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

Dokaz

$$\text{i)} \Rightarrow \text{ii)} \quad \sigma(u) = (\varphi(u), \psi(u))$$

σ je res izomorfizem in velja v pogoj!

σ je homomorfizem ostvar

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

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

$$\Rightarrow \varphi(\varphi(f)) = 0 = f \Rightarrow u = 0 \quad \text{torej je injektivne}$$

$$\text{S. n. j. } (t, v) \in L \oplus N$$

$$\exists u \in M: (t, v) = \sigma(u) = (\varphi(u), \psi(u))$$

$$\Rightarrow \varphi(u) = t, \psi(u) = v$$

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

$$\psi(u_0 + \varphi(f)) = v \quad \text{kerje koprime} = \ker \varphi \subset \ker \psi$$

$$\text{Poščemo t. l., da bo } \varphi(u_0 + \varphi(f)) = t$$

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

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

$$\text{enako} \quad l = t - \varphi(u)$$

$$\sigma(\varphi(f)) = (\varphi(\varphi(f)), \psi(\varphi(f))) = (t, 0)$$

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

$$\text{iii)} \Rightarrow \text{i)}$$

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

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

σ' je homomorfizem

σ' je izomorfizem

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

$$\underbrace{\varphi(t)}_0 + \underbrace{\psi(v)}_0 = 0 \Rightarrow v = 0$$

$$\varphi(t) + \underbrace{\psi(v)}_0 = 0 \Rightarrow t = 0 \quad \text{kerje \psi inj}$$

S. n. j.

$u \in M$

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

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

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

$$\varphi(t) = u - \psi(\psi(v))$$

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

vemo: $\varphi \circ \varphi = \text{id}_M$

$$\varphi(u - \varphi(\varphi(v))) = \varphi(u) - \varphi(\varphi(v)) = 0$$

Naj bo $\sigma \Rightarrow \text{ii)}$

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

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

po slednji definiciji izvidno da je vreda

$$\text{i)} \Rightarrow \text{ii)} \text{ in iii)}$$

2.6 Projekтивни модел:

$$\begin{array}{ccccc} & P & & & \varphi \text{ surjektiven} \\ & \swarrow \vartheta & \downarrow \varphi & & \\ M & \xrightarrow{\varphi} & N & \rightarrow O & \end{array}$$

Dekinicija: Model P je **projektiven**, če za V homomorfizem $\varphi: P \rightarrow N$ in vsake epim. $\psi: M \rightarrow N$ obstaja tak homomorfizem $\vartheta: P \rightarrow M$ da je $\psi \vartheta = \varphi$

Lema: Vsek prost model je projektiven

Dokaz: P prost

$$\begin{array}{ccc} & P & \text{Prima baza } B \\ & \swarrow \vartheta & \downarrow \varphi \\ M & \xrightarrow{\varphi} & N \rightarrow O \\ & \psi(e) = \varphi(v_e) \text{ za nek. } v_e \in e \\ & \vartheta: e \rightarrow v_e & \end{array}$$

ϑ je z delovanjem na bazi enotično določen in

$$\psi \vartheta = \varphi$$

- Izrek: Za modul P so naslednje trditev ekvivalentne
- $\Leftrightarrow P$ je projektivni modul
 - $\Leftrightarrow \forall$ kritko eksaktna razpredelje L se konča s P , razpade $0 \rightarrow L \rightarrow M \rightarrow P \rightarrow 0$
 - \Leftrightarrow obstaja modul L , da je $L \oplus P$ prost

Dokaz:

$$i) \Rightarrow ii) \quad P \text{ proj.} \quad \begin{array}{c} \varphi \\ \downarrow id \end{array} \quad \begin{array}{c} P \\ \downarrow \end{array}$$

$$0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} P \rightarrow 0$$

$\exists \vartheta$ da je $\vartheta \varphi = id_P$

ϑ je ϑ in tako razpredelje razpade

ii) \Rightarrow iii) vsak modul (tudi $??$) je nemonostrški prost modul, ki ga označuje $\cong M$

$$L \xrightarrow{\varphi} M \xrightarrow{\psi} P \rightarrow 0$$

determinira

$L := \ker \varphi \quad 0 \rightarrow \ker \varphi \xrightarrow{id} M \xrightarrow{\psi} P \rightarrow 0$
 ker to razpredelje razpade sledi:

$$M \cong L \oplus P$$

$L \oplus P$ je tudi prost

iii) \Rightarrow i) $L \oplus P$ je prost \Leftrightarrow nek L $??$ je projektivni

$$\begin{array}{ccc} & \swarrow \text{projektivni} & \\ L \oplus P & \downarrow \pi_P \circ \vartheta & \vartheta := \theta \circ \varphi \\ \theta \swarrow & \downarrow \varphi & \\ M & \xrightarrow{\varphi} & N \rightarrow 0 \end{array}$$

$$\vartheta \varphi = \varphi \quad \vartheta \varphi = \vartheta \circ \varphi = \vartheta \circ \pi_P \circ \vartheta = \pi_P \circ \vartheta = id_P = \varphi$$

✓

Primer: Zelimo naći projektivni modul K u n ; prost

K je prost K -modul

K je komutativen i obsteja $e = e^2 \neq 0, 1$: demotiv

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

$$1 - e \in K \Rightarrow (1 - e)ex = 0 \in P \cap eK$$

$\Rightarrow \{ex\}$ niholi ni linearne neodvisan:

$\underbrace{\begin{array}{l} K_1, K_2 \text{ kolaboraju } K := K_1 \times K_2 \\ e = (1, 0) \end{array}}$

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

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

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

$$ex = 0 \Rightarrow x = 0 \text{ podloži } y = 0 \text{ te } e \in eK \cap (1 - e)K = \{0\}$$

te e je P projektivni modul (not direktni sumand prostog), K ni prost

2.7 Tensorski 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 $\mathcal{F} = \mathcal{F}_{M,N}$

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

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

Definicija: **Tensorski produkt** modulov M in N je modul \mathcal{F}/\mathcal{A} . 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, vektori produkt v \mathbb{R}^3 , produkt v vektoru

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

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

Izrek: (univerzalna lastnost tensorškega produkteta)

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

za \forall modela M in N nad komutativnim telesom k , \exists tako bilinearna preslikava $M \times N \rightarrow M \otimes N$, $(u,v) \mapsto u \otimes v$, za katero velja,

za \forall bilinearna preslikavo $\bar{\Phi}: M \times N \rightarrow L$, kjer je

L poljuben k -model, \exists enolično določena

linearna preslikava $\varphi: M \otimes N \rightarrow L$, da

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

S to lastnostjo je tensorški produkt natančno in enolično določen.

Dokaz \Rightarrow

Dokaz: Vpeljimo $u \otimes v := (u, v) + \alpha'$

$$(au + a'u, v) - a(u, v) - a'(u, v) \in \alpha'$$

$$\Leftrightarrow$$

$$(au + a'u, v) + \alpha' = a(u, v) + \alpha' \quad \text{||} \quad a'(u, v) + \alpha' \quad \text{||}$$

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

Podobno izpeljemo linearnost preslikave \otimes v drugem argumentu

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

Izšemo linearno preslikavo φ enako

F ima bazo $M \times N$, zato lahko Φ razčrimo do

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

Ker je Φ bilinearna, ker F vsebuje podmodul α'

$$\left\{ \begin{array}{l} F(au + a'u, v) - a(F(u, v)) - a'(F(u', v)) \text{ se sliči } v ? \\ = F(au + a'u, v) - aF(u, v) - a'F(u', v) = \\ = \Phi(au + a'u, v) - a\Phi(u, v) - a'\Phi(u', v) = 0 \end{array} \right.$$

Zato je $\varphi: M \otimes N \rightarrow L$ $x + \alpha' \mapsto F(x)$ dobro definirana

Ker je F linearne je tudi φ linearne

$$\varphi(u \otimes v) = \varphi((u, v) + \alpha') = F(u, v) = \Phi(u, v)$$

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

Enakost

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

ker je \otimes bilinearna, \exists

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

taka da je $\psi(u \otimes v) = u \otimes v$

Analogno obstaja linearne preslikave

$$\Psi: T \rightarrow M \otimes N \quad \Psi(u \otimes v) = u \otimes v$$

$$(\Psi \circ \varphi)(u \otimes v) = \text{A enakostni tensor } u \otimes v \Rightarrow \Psi \circ \varphi = \text{id}_{M \otimes N}$$

$$\Psi \circ \varphi = \text{id}_T \text{ analogno}$$

"ujemanje na bazi"



"Praktična" definicija tenzorskega produkta

- $\forall u \in M, v \in N, \exists u \otimes v \in M \otimes N$. T. menujemo ga **enostavni tensor**. Vsak drug element je vsota teh enostavnih tensorjev.
- $(u+u') \otimes v = u \otimes v + u' \otimes v$

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

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

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

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \searrow \Phi & \downarrow \varphi \\ & & L \end{array}$$
$$\varphi(u \otimes v) := \Phi(u, v)$$
$$\varphi\left(\sum u_i \otimes v_j\right) = \sum \Phi(u_i, v_j)$$

Sporazilo izreka je, da je φ dobro definirana

Definicija
 φ, ψ nej bodelin. 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 bilinearna preslikava.

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

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

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

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

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

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

φ, ψ izomorfisme $\Rightarrow \varphi \otimes \psi$ bij

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

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

- $M \otimes N \cong N \otimes M$
- $(M \otimes N) \otimes R \cong M \otimes (N \otimes R)$
- $(M \otimes N) \otimes R \cong M \otimes R \otimes N \otimes R$
- $M \otimes k \cong M$

Dokaz:

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

- $M \times N \rightarrow N \otimes M$
 $(u, v) \mapsto v \otimes u$ je bilinearna.

Zato \exists linearna preslikave $u \otimes v \mapsto v \otimes u$
Ali je bijektivna? Če smo inverz.

\exists lin preslikave $v \otimes u \mapsto u \otimes v$. "Očitno" sta si
preslikavi inverz

- $M \otimes k \rightarrow M$
 $u \otimes 1 \mapsto u$ ker je linearna, je dobro definirana
 $M \rightarrow M \otimes k$
 $1 \mapsto u \otimes 1$ preslikavi sta drugi drugi inverz

- Radi bi videli, da je preslikava $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$
dobro definirana linearna preslikava
Analogni 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 bilinearna preslikava
 $\Phi: (M \otimes N) \times R \rightarrow M \otimes (N \otimes R)$

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

$\Leftrightarrow \exists$ 3 linearne preslikave u_i sicer

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



2.8 Tensorski 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 pravica ne sledi
je to \mathbb{Z}_6 , ampak vsi vrednosti
svetlu 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 V element M $\otimes N$ lahko enocno zapisemo kot
 $\sum e_i \otimes v$:

To razumemo: vsi razen končna množic $v_i = 0$

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

$$u \otimes v = (\sum a_i e_i) \otimes v = \sum (a_i e_i) \otimes v = \sum e_i \underbrace{\otimes (a_i v)}_{v_i} \quad \begin{matrix} \uparrow \\ \text{za neke } a_i \in K \end{matrix}$$

enocnost:

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

Zadostna dokazi

$$\sum e_i \otimes v_i = 0 \Rightarrow v_i = 0 \quad \forall i \in I$$

Izberimo $i_0 \in I$

če uspemo najti tako linearne preslikave $\varphi: M \otimes N \rightarrow N$
 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 linearne preslikave $\varphi_i: M \rightarrow K$

$$\varphi_i: e_i \mapsto 0, i \neq i_0$$

$e_{i_0} \mapsto 1$
 Tačka preslikava obstaja, ker jo
 imamo bazo, in lahko te enocno
 razširimo na M

Definirajmo $\bar{\Phi}: M \times N \rightarrow N$

$$(u, v) \mapsto \varphi_i(u) \cdot v \quad \text{je bilinear,}$$

zato \exists linearne preslikave $\varphi: M \otimes N \rightarrow N$ taka, da je
 $\varphi(u \otimes v) = \bar{\Phi}(u, v)$

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

Opomba: Podoben izrek velja, če je N prost
z bazo $\{f_i\}$

Izrek: 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: Vsi elementi v obliki $\sum_i e_i \otimes v_i =$

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

Linearna neodvisnost?

$$0 = \sum_{i,j} a_{ij} (e_i \otimes f_j) = \sum_i e_i \otimes (\sum_j a_{ij} f_j) \xrightarrow{\text{zapis } \sum_i e_i \otimes v_i \text{ je enoten}} \sum_j a_{ij} f_j = 0$$

zapis $\sum_i e_i \otimes v_i$ je enoten

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

f_j baza

■

Posledica: Če je U vektor. prostor nad F z bazo $\{e_i\}$ in
 V vektor. prostor nad F z bazo f_j , je $U \otimes V$ vektor. prostor nad F
z bazo $e_i \otimes f_j$. Če sta U in V končni
razsežni, je torej $\dim(U \otimes V) = \dim U \cdot \dim V$

Primer: V vek. pr. nad F , $v \in V$, $f \in V^*$ $\xleftarrow{\text{dual } V}$
 $\xleftarrow{\text{in funk. anal}}$

$v \otimes f: V \rightarrow V$

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

Primeri in izredu v učbenikom

2.9 Tensorski produkt algebr

Algebra nad F :

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

Složnejši pojem: Algebra nad komutativnim kolobarjem K je definirana enako. Torej je to K -modul skupaj z množenjem (za katero je kolobar) in sčemanjem $a(xy) = (ax)y = x(ay)$

Primeri:

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

Izrek: Naj bosta A in B K -algebre:

Potem K -model $A \otimes B$ postane K -algebra, če veljajo 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 definicija množenja

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

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

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

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

$$\begin{aligned} \bar{\Phi} : A \times B &\longrightarrow \text{End}(A \otimes B) && \text{enkrat je samo} \\ (z, w) &\mapsto \rho_z \otimes \rho_w && \text{K-model} \\ &&& \text{če je } A \otimes B \text{ K-model, je } \text{End}(A \otimes B) \\ \bar{\Phi} \text{ je bilinearna} &\text{ zato } \exists \text{ lin. pres. } f : A \otimes B \rightarrow \text{End}(A \otimes B) \\ (z \otimes w) &\mapsto \rho_z \otimes \rho_w && \text{K-algebra} \end{aligned}$$

Deklinirajmo množenje v $A \otimes B$

$$r \cdot s = \varphi(s) \cdot r$$

Ki je to neska definicija množenja?

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

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

Produkt je bilinearen:

$$(a_1 r + a_2 r') s = a_1 (r s) + a_2 (r' s)$$

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

asoc: očitno

enota: $1 \otimes 1$

Izrek: Za K -algebri 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 direktni vseote
algebre so ekvivalentne

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 kolobar in je cela K -algebra

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

- A je 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

$$\sum_{i \geq 0} a_i \otimes X^i \leftarrow enakem napis (preprost: zrcali)$$

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

- A poljubna K -Algebra

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

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

Lahko determinamo

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

V elementu v $M_n(A) \otimes K$ je oblike

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

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

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

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

$$\varphi(E_{ij} \otimes u_{ij} \cdot E_{kl} \otimes v_{kl}) = \varphi(\delta_{j,k} \delta_{l,i} \otimes uv) = \delta_{j,k} \delta_{l,i} uv E_{ij}$$

$$\varphi(\dots) \cdot \varphi(\dots) = u_{ij} \cdot v_{kl} E_{ij} \otimes E_{kl} = uv \cdot E_{ij} \delta_{j,k} \delta_{l,i}$$

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

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

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

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

2.10 Razširitev skalarjev

Naj bo A realna, končnodimenzionalna algebra.

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

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

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

Primer:

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

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

• izmedlikej niza i^z zato nemore biti $\cong H$

K, C komutativne kategorije

M K -model

$\alpha: K \rightarrow C$ homomorfizem

C postane K model, će definiramo $K \cdot C = \alpha(K) \cdot C$

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

Lekko definiramo $M_C := C \otimes M$

(M_C je odvisen od α !)

K model M_C postane C model, će definiramo

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

To množenje je dobra definiranost.

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

$$cy = (l_C \otimes id_M)(y) \quad \forall c \in C \quad \forall y \in M_C$$

nesporne definicije \Rightarrow množenje
je dobro definirano

$c \otimes u = c(1 \otimes u) \Rightarrow$ Model M_C temelji na
linearnih kombinacij elementov $1 \otimes u : u \in M$

Primer:

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

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

Naj bo A K -algebra

A_C je C -modul

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

Z množenjem

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

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

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

$\{1 \otimes e_i\}$ je baza $\otimes A_C$

Če je množenje v K -algebi: A določeno z množenjem

$$\text{ločni vektorji } e_i e_j = \sum_k \alpha_{ijk} e_k, \quad \text{je}$$

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

Priimeš: K komutativan keločar
Naj bo I nelesimelni ideal $K \Rightarrow \frac{K}{I}$ je polje

npr $K = \mathbb{Z}$ $I = p\mathbb{Z} : \frac{K}{I} \cong \mathbb{Z}_p$

$\alpha: K \rightarrow C$
 $k \mapsto k + I$ Tako iz K modula M dobimo
vektorski prostor M_0 nad C

Izrek: Nej bo K komutativen kolobar. Potem je $K^s \cong K^t \Rightarrow s=t$

$\left(\begin{array}{l} \text{Vemo od prej:} \\ K^n = K \times K \times \dots \times K \text{ je prosti } K \text{ modul.} \\ \forall K\text{-modul z bazo z n elementi je izomorfen temu} \end{array} \right)$

Dokaz:

Nej bo C polje kot v prejšnjem primeru.

za $n \in \mathbb{N}$ definiramo $(K^n)_C \xleftarrow[\text{skalarjev}]{} \text{To je razširitev}$

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

To prostor je n -dimensionalen $\dim_C(K^n) = n$

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 -linearna, v nasem primeru je tudi C -linearna

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

je izomorfizem C -linearnih prostorov nad C

ker sta K^s in K^t vektorski prostori, je $s=t$

2.11. Konano generirane Abelove grupe

Naj bo K celočrkovar in M K -modul

Definiramo

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

torzijasti podmodul

To je podmodul

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

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

$$ab(u - v) = bau - abv = 0 - 0 = 0$$

$$u \in \text{tr}(M) \text{ b. e. } au = 0$$

$$\Rightarrow abu = bau = 0$$

M je torzijasto prost ce je $\text{tr}(M) = \{0\}$

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

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

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

$\text{tr}(G) = \text{torzijaste podgrupe abelove (aditivne) grupe } G$

Pokazati smo, $G/\text{tr}(G)$ je torzijasto prosta grupa

... vsi elementi razen 0 imajo reskencen red

konone \Rightarrow konoro generirane

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

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

$$\mathbb{Z}^s \oplus K \cong \mathbb{Z}^s \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{k_r}}$$

lomo dekorat.

\Updownarrow

konrogenerirane abelova grupe

Lema: Končno generirana torzjska prostota abelove grupe je prostota

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

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

Preimoma da H ni prostota

Izmed vseh množic z m elementi, ki generirajo H , izberimo „najmanjšo“ ($\{a_1, \dots, a_m\}$ generirajo H ,

$\exists k_1, \dots, k_m \in \mathbb{Z}, k_1a_1 + \dots + k_ma_m = 0$ 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. prostota, sta vsaj dva $k_i \neq 0$

Preimoma da sta to k_1 in k_2

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

$$k_1 = gk_2 + r; \quad 0 < r < |k_2| \text{ oz } |k_1 - gk_2| < |k_2|$$

$$0 = k_1a_1 + k_2a_2 + \dots + k_ma_m =$$

$$= (k_1 - gk_2)a_1 + k_2(a_2 + ga_1) + k_3a_3 + \dots + k_ma_m$$

$$|k_1 - gk_2| < |k_2| \leq |k_1|$$

$$|k_1 - gk_2| + |k_2| + \dots + |k_d| < \sum |k_i|$$

ker $a_1, (a_2 + ga_1), a_3, \dots, a_n$ 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 obračunavamo 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 generirane je k.g tudi G/T

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

$$\Rightarrow 0 \longrightarrow T \xrightarrow{\quad} G \xrightarrow{\quad} G/T \longrightarrow 0$$

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

T končna

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

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 imata končen red, zato je tehih različnih zapisa le končno množje.

Posledica: A 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 določen:

Enak izrek velja za module nad glavnim
keldarjem

3. Prezentacija grup in algebre

3.1 Proste grupe in prezentacije grupe

Neformalno: kaj je prostă grupa na množici X

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

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

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

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

Različni zapisi dejajo 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} množico z isto kardinalnostjo

$$\text{ket } X, X^{-1} = \{x^{-1} : x \in X\}$$

↑ samo označke

Zaporedje (x_1, x_2, \dots) ; $x_i \in X \cup X^{-1} \cup \{1\}$, kjer so od nekaj naprej vsi temi enaki 1 pravimo beseda

Npr $(1, 1, \dots) = 1$ je beseda, kjer pravimo prazna beseda

če sta izpolnjena pogoja

1) Elementi 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 besed: pravimo reducirana besed

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

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

((Namesto $(x x y^{-1} y^{-1} x^{-1}) = x^2 y^{-2} x^{-1}$))

kot množica je F_X množica reduciranih besed

Vpeljimo operacijo

Vzemimo dve reducirani besedi:

$x_1^{e_1} x_2^{e_2} \dots x_m^{e_m}$ in $y_1^{\mu_1} y_2^{\mu_2} \dots y_n^{\mu_n}$ $e_i, \mu_j \in \{-1, 1\}$
in nujno $m \leq n$ $x_i, e_i \in X$

$x_1^{e_1} \dots x_m^{e_m} y_1^{\mu_1} \dots y_n^{\mu_n} =$ $\begin{cases} \text{nugajti:} \\ \text{k negajti de} \\ y_k \neq x_{m+k} \text{ in } e_{m+k} \neq \mu_k \end{cases}$

$\left\{ \begin{array}{l} x_1^{e_1} \dots x_{m-k+1}^{e_{m-k+1}} y_k^{\mu_k} \dots y_n^{\mu_n} \\ y_{k+1} \dots y_n \end{array} \right.$ $k \leq m$

;

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

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

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

$$X \subseteq F_X$$

↑ neformalno

Izrek: Naj bo X množica in F_X naj bo prostota grupe na X in $i: X \rightarrow F_X$ $x \mapsto x$
 za $\forall f: X \rightarrow G$, kjer je G poljubna grupa
 $\exists!$ homomorfizem $\varphi: F_X \rightarrow G$. dej 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: Ako je grupe je homomorfna slik: proste grupe

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

G generira. Na X glejmo kot množico, zgradimo
prosto grujo F_X na X . Po prejšnjem izreku

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

φ je surjektiven ker je $\text{im } \varphi \leqslant G$ in $X \subseteq \text{im } \varphi$
*generatorji

Posledica:

$$\cancel{F_X}_{\text{ker } \varphi} \cong G$$

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: $r=1$ $r \in R$, če je $G \cong \frac{F_X}{N_R}$,

kjer je N_R edinke 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

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

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

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

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

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

Prímo:

1) Prezentácia prosté grupe

$$\langle x | \phi \rangle$$

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

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

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

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

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

$$\text{Nedlinke gen. } \geq x^n, y^2, (xy)^2$$

Naj bo G hetero kelingrupa generácie $\langle u, v \rangle$

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

D_{2n} je teke grupe, pretože $F_{\langle x, y \rangle}/N$ je tele
($u = xN, v = yN$)

1. kerak: G je homeo. $F_{\langle x, y \rangle}/N$

2. kerak: G má najviac $2n$ elementov

Definície je to res. Potom je 1. kerak

Homomorfizmus $\varphi: F_{\langle x, y \rangle}/N \rightarrow D_{2n}$

2. kerak pove, že φ je G izomorf $\frac{F_{\langle x, y \rangle}}{N}$

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

φ je bijectívny

1. kerak

Vemo: \exists homomorfizmus $F_{\langle x, y \rangle}/N \rightarrow G$

$$x \mapsto u$$

$$y \mapsto v$$

Kerf vsetkých $x^n, y^2, (xy)^2$

$$\Rightarrow N \leq \text{kerf}$$

zato \exists homomorfizmus $F_{\langle x, y \rangle}/N \xrightarrow{\varphi} F_{\langle x, y \rangle}/\text{kerf} \cong G$

$$wN \mapsto w \text{kerf}$$

2. kerak

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

ξ

$$m_i \in \mathbb{Z}, \forall n_i \in [r].$$

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

Edim možné elementy so

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

3.2. Proste algebре и презентације алгебре

Алгебра јеј ће бити полје над F

Елементи просте алгебре су некомутативни полиноми.

X, Y две спременљиве

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

Над \mathbb{X} ће бити мношка. Елементи **простог монида**

\mathbb{X}^* су бројеви: разредја $(X_1, X_2, \dots, X_m, 1, 1, \dots)$

$$= X_1 X_2 \dots X_m$$

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

$$\text{Употребимо мозајкје } X_1 \dots X_n \cdot Y_1 \dots Y_m = X_1 \dots X_n Y_1 \dots Y_m$$

1 је едино ∞ мозајко

$\bar{\mathbb{X}}$ је такође монид. Речимо му **прости монид**

$F(\mathbb{X})$ јеј ће бити векторски простор над F са базом \mathbb{X}^*

$F(\mathbb{X})$ постаније алгебра, ако дефинирамо

$$(\sum \lambda_i w_i) (\sum \mu_j v_j) := \sum V_k w_k$$

$$w_i w_j = w_k$$

$$V_k = \sum_{w_i w_j = w_k} \lambda_i \mu_j$$

$F(\mathbb{X})$ именујемо **проста алгебра** на мноштву: \mathbb{X}^*

$$i: \mathbb{X} \rightarrow F(\mathbb{X})$$
$$x \longmapsto x$$

$$\begin{array}{ccc} X & \xrightarrow{i} & F(x) \\ & \searrow f & \downarrow f \\ & A & \end{array}$$

Izrek: Naj bo X množica in A algebra in
 $f: X \rightarrow A$. Potem $\exists!$ homomorfizem $\varphi: F(x) \rightarrow A$,
 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. preste algebra je presti objekt v kategoriji:
 algebr nad F)

Postedica: Vsaka algebra je homeomorpha slike
 neke preste algebre

Dokaz: Naj bo A algebra $X \subseteq A$ $\langle \underset{\text{generatorji}}{x} \rangle = A$

$$\begin{array}{c} \text{Naj bo } f: X \rightarrow A \\ x \mapsto x \end{array}$$

Po izrek: $\exists \varphi: F(x) \rightarrow A$
 $x \mapsto x$

$$X \subseteq \text{im } f \Rightarrow A \subseteq \text{im } f \Rightarrow A = \text{im } f$$

$$A \cong \frac{F(x)}{I} \quad I = \ker f$$

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

Pravimo da je algebra A definisana z generatorji $x \in X$ in relacijami: $p=0$ $p \in R$, če je

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

ideal pravte algebre generiran z R

V tem primeru recemo da je $\frac{F\langle X \rangle}{\langle R \rangle}$ prezentacija algebre A

A je končno generirana, če sta X in R

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

Primer:

$$1. \text{ Picasta algebra } \langle x | \emptyset \rangle$$

$$2. F\langle x, y | xy = yx \rangle = F[x, y]$$

$$3. F\langle x, y | xy = 1 \rangle$$

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

$$\begin{array}{l} E_1 = E_{12}E_{21} \\ E_{22} = E_{21}E_{12} \end{array} \quad I = E_{12}E_{21} + E_{21}E_{12}$$

Vazibam: prezantacija je F

$$F\langle x, y | x^2 = y^2 = 0, xy + yx = 1 \rangle$$