1. Deljivost v komutativnih kolobarjih

$xy = yx$

$1 \in K$

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

Cel kolobar - komutativen kolobar, brez deliteljev ničla

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

$p_1, \dots p_n \in \mathbb{P}$ praštevila enolično določena

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

1.1 osnovni pojmi

Definicija: Naj bo K komutativen kolobar.

1. element $b \neq 0 \in K$ **deli** element $a \in K$, če
$a = gb$ za nek $g \in K$
(a je **deljiv** z b, b je **delitelj** a)

2. neničelna elementa $a, b \in K$ sta **asociirana**, če delita drug drugega $a|b \wedge b|a$

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

   Elementa sta **tuja**, če je njun največji skupni delitelj (n.s.d) enak 1

4. Element $p \in K$ je **nerazcepen**, če:
   a) $p \neq 0 \wedge p$ ni obrnljiv
   b) $p = ab \Rightarrow a$ je obrnljiv $\vee$ b je obrnljiv

   Element je **razcepen**
   a) $p \neq 0 \wedge p$ ni obrnljiv
   b) ni nerazcepen

Odsek: K je cel

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

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

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

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

↑ ni deliteljev niča $\Rightarrow k = g^{-1}$

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

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

Primer: Ali je 2 nerazcepen element? odvisno od kolobarja

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

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

↑ katero koli polje (3 pa ni razcepen)

1.2 Glavni kolobarji:

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

K kom utativen

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)

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

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

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

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

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

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

Ideal je konačnogeneriran, če je generiran s končno množico

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

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

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

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

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

2. V $F[x]$ ideali?

polinomi s konstantnim členom 0 (x)

Vsi ideali so glavni

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

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

Ali je I glavni ideal?

npr $I = (f(x))$

$2 = f(x)g(x) \Rightarrow f(x)$ je lahko samo konstanten $f(x) = a_0 \in 2\mathbb{Z}$

$x \in I \Rightarrow x = a_0 h(x)$ $\not\Rightarrow$

$\uparrow$ sod $\quad \uparrow x$ ni sod

4) V $F[x,y]$ 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 glavni (PID)

principle ideal domain

?

ni delitelja ničla

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

Izreki: Naslednji kolobarji so evklidski

a) $\mathbb{Z}$

b) $F[x]$, F polje

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

Dokaz:

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

b) $\delta(f(x)) = \text{st}(f(x))$ (O ničemu definirane stopnje)

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

b) ✓ Vemo da je to kvadrat absolutne vrednosti:

$|z||w| = |zw|$ $\quad |w| \neq 0 \Rightarrow |w| \geq 1$

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

$a = qb + r$

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

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

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

$q = k + li \in \mathbb{Z}_i$

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

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

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

$= |c-q|^2 |b|^2 = \left((u-k)^2 + (v-l)^2\right)|b|^2$

$(u-k)^2 \leq \frac{1}{4}$, $(v-l)^2 \leq \frac{1}{4}$

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

Izrek: Vsak evklidski kolobar je glavni kolobar

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

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

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

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

$I = (a)$ $\quad (a) \subseteq I$ trivialno

Naj bo $x \in I$ poljuben

$x = aq + r$ v K $\Rightarrow r \in I \Rightarrow \delta(r) \geq \delta(a)$ v $r = 0$
$\in I$

$\Rightarrow a \mid x$

glavni kolobar $\not\Rightarrow$ evklidski kolobar

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

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

Dokaz:

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

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

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

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

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

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

Izrek: Naj bo $p \neq 0 \in K$ algebrsko število.

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 če $M \neq K \wedge M \subseteq I \trianglelefteq K \Rightarrow I = K \vee M = I$

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

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

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

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

i) in ii) ubistvu povsem isto

1.3 Enolična faktorizacija

$a \neq p_1 p_2 \cdots p_n$

Lema: Naj bo K cel kolobar. Recimo da element $a \neq 0$ ni enak produktu nerazcepnih elementov. $a \neq 0$ in a ni obrnljiv. Potem K vsebuje tako neskončno zaporedje elementov $a = a_1, a_2, \ldots$ da je $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$

(Neskončno strogo naraščajoče zaporedje glavnih idealov)

Dokaz:

a ni nerazcepen

$a_1 = a_2 b_2$ a_2 in b_2 nista obrnljiva

Vsaj 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 obrnljiv $\lightning$

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

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

Tako $I_n = I_{n+1} = \ldots$ od nekega n naprej

Lema: V glavni kolobar je noetrski

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

$I := \bigcup_{i \in \mathbb{N}} I_i$ to je ideal (v splošnem unija ni) (ponovi: ni grupa za seštevanje)

$KI \subseteq I$ očitno

$u, v \in I$

$u - v \in I$

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

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

Hilbertov izrek o bazi

K noetrski $\Rightarrow K[x]$ noetrski

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

$=$

$K[x][y]$

glavni

ni glavni

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

Definicija: Naj bo K komutativen kolobar.
$p \in K$ je praelement $p \neq 0$, p ni obrnljiv in velja $p \mid ab \Rightarrow p \mid a \vee p \mid b$ $\forall a, b \in K$

Lema: Naj bo K cel. $\forall$ sak praelement je nerazcepen. Če je K glavni velja tudi dorat

Dokaz: 1) Naj bo p praelement. $p = xy$

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

Recimo da $p \mid x \Rightarrow x = pu \Rightarrow p = puy \Rightarrow uy = 1$

2) Naj bo K glavni $\Rightarrow y$ je obrnljiv

p naj bo nerazcepen. p praelement.

$p \mid ab$. 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: Cel kolobar K imenujemo kolobar z enolično faktorizacijo (UFD), če se za vsak $a \neq 0$, ni obrnljiv, velja:

- obstajajo taki nerazcepni elementi p_i, da je $a = p_1 \cdots p_s$
- ta faktorizacija je enolična do asociiranosti in vrstnega reda faktorjev natančno

To pomeni: $a = q_1 \cdots q_t$; q_i nerazcepni
$\Rightarrow s = t$ $\exists \pi \in S_n$. $q_{\pi(i)}$ asociiran z p_i

Izrek: V glavni kolobar je kolobar z enolično faktorizacijo

Dokaz: $a \neq 0$ ni obrnljiv.

Vemo iz prvih dveh lem: a je produkt nerazcepnih
$a = p_1 \cdots p_s$ recimo da je tudi $a = q_1 \cdots q_t$

$p_1 | a \Rightarrow p_1 | q_1 \cdots q_t \Rightarrow \exists i \in \overline{1,t}.\ p_1 | q_i$. BSZS $p_1 | q_1$
(p_1 nerazcepen + glavni kolobar $\Rightarrow$ praelement)

q_1 nerazcepen $\Rightarrow$ p_1 in q_1 sta si asociirana

Pri: $p_1 \cdots p_s = p_1 u q_2 \cdots q_t$

$p_2 \cdots p_s = u q_2 \cdots q_t$ p - skopek ponavljamo

$s = t$: $s > t \Rightarrow u = p_{t+1} \cdots p_s$ ker ni mogoče
(obrnljiv) (nerazcepni)

15.10

2. Modeli

2.1. Cayleyjev izrek za kolobarje

$G \longrightarrow G$
$L_a : x \longmapsto ax$

$\varphi : G \longrightarrow \mathrm{Sym}\, G$
$a \longmapsto L_a$

M aditivna grupa
$\mathrm{End}(M)$ = množica vseh endomorfizmov $M \longrightarrow M$

$\varphi \in \mathrm{End}\, M \Leftrightarrow \varphi : M \to M \,;\ \varphi(u+v) = \varphi(u) + \varphi(v)$

$\mathrm{End}\, M$ je kolobar če vpeljemo
$\varphi + \psi,\ \varphi \circ \psi : M \to M$
$(\varphi + \psi)u = \varphi(u) + \psi(u)$
$(\varphi \cdot \psi)(u) = \varphi(\psi(u))$

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

Dokaz: K kolobar

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

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

$$l_a \in End(K)^*$$

$*$ K kot grupa za $+$

$$\varphi : K \to End K, \quad a \mapsto l_a$$

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

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

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

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

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

injektivnost:

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

Fija

Gay bey

$\Updownarrow$

Cuy ley

Naj bo A algebra nad poljem F

V vektorski prostor nad F

$End_F(V)$

Napodoben neskončen dokažemo

Izrek: Vsako algebro nad F lahko vložimo v algebro endomorfizmov nekega vekt. prostora nad poljem F.

$\dim A = n < \infty$ $\quad$ $M_n(F)$ ← matrike nxn nad F

$A \hookrightarrow End_F(A) \cong M_n(F)$ Algebro lahko vložimo v algebro lin. operatorjev končno razsežnega prostora

Posledica: $\forall$ končnorazsežno algebro A nad F lahko vložimo v algebro $n \times n$ matrik za neki n $M_n(F)$

Primer: A končno razsežna algebra nad F

Ali ta algebra lahko vsebuje taka elementa s in t da je $st - ts = 1$

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

$$sl(ST - TS) = sl(I) = n$$

$$\| \qquad\qquad \|$$

$$sl(ST) - sl(TS) = 0$$

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

2.2 Definicija modula

Definicija: Naj bo K kolobar. Množica M skupaj z binarno operacijo $(a,u) \mapsto au$ in $K \times M \to M$ in binarno operacijo $M \times M \to M : (u,v) \mapsto u+v$ 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 skalarji ali tudi **modulsko množenje**

Opomba: Pojem K-modula M je ekvivalenten pojmu homomorfizma kolobarjev $K \to End(M)$

Dokaz: Naj bo M K-modul

$$\varphi : K \to End(M) : a \mapsto (u \mapsto au))$$

Naj bo φ homomorfizem $\varphi : K \to End(M)$ postane M K-modul, če definiramo

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

■

Definirali smo levi modul nad K. Poznamo tudi desne. namesto ax imamo xa in podobno

Naj bo M levi K-modul. Če definiramo xa:= ax 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. Vsaka M aditivna grupa (= 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. $\forall$ kolobar K postane modul nad samim seboj, če definiramo au kot običajni produkt $a.u$ v K

4. Naj bo I levi ideal K
I je K-modul, če je $a.u$ običajen produkt

5. Naj bo K podkolobar K'. če au označuje množenje v K', je K' K-modul

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

Au = običajno množenje matrike z vektorji

7. Trivialni ali ničelni modul

2.3 Osnovni pojmi teorije modulov

Podmoduli

Podmodul je podmnožica, ki je za isti operacji 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 vek. 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 podmodula sta tudi

$N_1 \cap N_2$ in $N_1 + N_2$ podmodula

Def: če sta $\{0\}$ in M edina podmodula M rečemo da je M enostaven

Primer:

1. V. prostor je enostaven kot modul $\Leftrightarrow$ je 1-razsežen
2. Abelova grupa je enostavna kot $\mathbb{Z}$-modul $\Leftrightarrow \cong \mathbb{Z}_p$
3. $K = M_n(F)$ $\quad M = F^n$

$N \subseteq F^n$

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

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

M je enostaven modul nad matrikami;

Homomorfizm modulov

M, N K-modula

$\varphi: M \to N$ 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

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

sta podmodula M oz. N

$\ker\varphi = \{0\} \iff \varphi$ injektivna

$M \cong M : M$ **izomorfna** N

(obstaja **izomorfizem**)

Kolobarji endomorfizmov

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

M aditivna grupa $End(M)$

$\mathrm{End}_K(M) = \{$vs; endomorfizmi; K-modula $M\}$

je kolobar če vpeljemo

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

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

Schurova lema: Če je M enosteven K-modul, je kolobar $\mathrm{End}_K(M)$ obseg (vsi elementi so obrnljivi:)

Dokaz:

Naj bo $0 = \varphi \in \mathrm{End}_K(M)$

$\ker\varphi$ in $\mathrm{im}\varphi$ sta podmodula in M je enosteven

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

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

Kvocientní moduli

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 kvocientni modul.

Primeri:

1. $K = F \Rightarrow$ kvocientni vek. pr.
2. $K = \mathbb{Z} \Rightarrow$ kvocientna grupa
3) I levi ideal $K \Rightarrow K/I = \{a+I;\ a \in K\}$

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

$$a(b+I) = ab+I$$ ← dovolj je levi ideal

Izrek o izomorfizmu

$\varphi: M \to N \Rightarrow M/\ker\varphi \cong \mathrm{Im}\varphi$

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 $M_1 \oplus \dots \oplus M_s$

Notacija: zunanja direktna vsota

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

če velja

a) $M = N_1 + \dots + N_s$

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

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 $v_1 + \dots + v_s \longmapsto (v_1, \dots, v_s)$

ker je $v_1 + \dots + v_s$ enolično zapis

Tudi notr. dir. vsot. označujemo z

$N_1 \oplus \dots \oplus N_s$

Naj bo N podmodul M. Rečemo da je N direktni sumand, če obstaja podmodul N', da je $M = N \oplus N'$

Primer

1. $K = F$ vsak podprostor je direktni sumand
2. $K = \mathbb{Z}$: $M = \mathbb{Z}$

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

Direktna sumanda sta le $\{0\}$ in $\mathbb{Z}$

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

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-rezsežni podprostori in $\{0\}$
2. $K = \mathbb{Z}$: ciklični $\mathbb{Z}$ modul so ciklične grupe
3. K komutativen kolobar ... glavni

u 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, 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 $a_1 e_1 + \dots + a_s e_s = 0$ sledi $a_1 = \dots = a_s = 0$

(Če je B neskončna pa je linearno neodvisna, če je vsaka končna podmnožica lin. neodvisna)

Če je B linearno neodvisna in generira M je to Baza modula M

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

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

Pišemo $u = \sum a_i e_i$

Primer:

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

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

$u \in G$ že $\exists n$: lin neodvisna

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

Edina linearna neodvisna množica je prazna množica

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

bazni [illegible] $\{1\}$: $n \mathbb{Z}$

Definicija: Modul, ki ima bazo se imenuje

Prosti modul

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

2) K kolobar, potem je

$\underbrace{K \oplus \dots \oplus K}_{s \text{ sumandov}} = K^s$ je prost K modul

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


España

$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ je kratko eksaktno zaporedje φ inj, ψ sur $\operatorname{Im}\varphi = \ker\psi$ $(\psi\varphi = 0)$

L podmodul M

$0 \to L \to M \to M/L \to 0$

$L \cong \operatorname{im}\varphi$ ker je inj

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

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

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

$t \mapsto (t, 0)$

$(t, v) \to v$

Kratko eksaktno zaporedje razpade, če zaporedje $0 \to L \to M \to N \to 0$ izgleda kot

$0 \to L \to L \oplus N \to N \to 0$

$$\begin{array}{ccccccccc} 0 & \to & L & \to & M & \to & N & \to & 0 \\ & & \downarrow \mathrm{id} & & \downarrow \sigma & & \downarrow \mathrm{id} & & \\ 0 & \to & L & \to & L \oplus N & \to & N & \to & 0 \end{array}$$

$\exists \sigma$ izomorfizem da ta diagram komutira

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

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

Izrek: Za kratko eksaktno zaporedje

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

$\Leftrightarrow$ zaporedje je razpadno

$\Leftrightarrow \exists$ homomorfizem $\varphi' : M \to L$, da je $\varphi'\varphi = id_L$

$\Leftrightarrow \exists$ homomorfizem $\psi' : N \to M$, da je $\psi\psi' = id_N$

Dokaz

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

σ je res izomorfizem in ustreza pogoju!

σ je homomorfizem očitno

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

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

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

σ surj $(t, v) \in L \oplus N$

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

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

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

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

Poiščimo še l, da bo $\varphi'(u_0 + \varphi(l)) = t$

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

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

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

enačbe

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

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

iii) $\Rightarrow$ i)

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

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

σ' je homomorfizem

σ je injektivna

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

$\psi\varphi(t) + \psi\psi'(v) = 0$

$0 \qquad v \qquad \Rightarrow v = 0$

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

surj:

$u \in M$

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

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

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

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

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

velja $\operatorname{im}\varphi = \ker\psi$

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

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

$\sigma\varphi = i_L \quad \varphi(t) = \sigma^{-1}(t, 0) = \varphi(t)$ ✓

drugi pogoj:

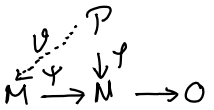
i) $\Rightarrow$ ii) in iii)

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

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

poglejmo definicije in vidimo da je vredu

2.6 Projektivni modul:

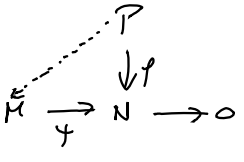


ψ surjektivna

Definicija: Modul P je projektiven, če za $\forall$ homomorfizem $\varphi: P \to N$ in vsak epim. $\psi: M \to N$ obstaja tak homomorfizem $\vartheta: P \to M$ da je $\psi\vartheta = \varphi$

Lema: Vsak prost modul je projektiven

Dokaz: P prost



P ima bazo B

$\varphi(e) = \psi(u_e)$ za neke $u_e \in M$

$\vartheta: e \to u_e$

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

Izrek: Za modul P so naslednje trditve ekvivalentne

$\Leftrightarrow P$ je projektivni modul

$\Leftrightarrow \forall$ kratko eksaktno zaporedje ki se končna s P, razpade $\quad 0 \to L \to M \to P \to 0$

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

Dokaz:

i) $\Rightarrow$ ii) P proj. $\quad 0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} P \to 0$, $P \xrightarrow{id} P$, $P \xrightarrow{\vartheta} M$

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

ψ je ϑ in tako zaporedje razpade

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

$L \to M \xrightarrow{\psi} P \to 0$

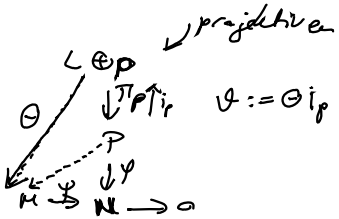
definirano $L := \ker\psi$ $\qquad 0 \to \ker\psi \xrightarrow{id} M \xrightarrow{\psi} P \to 0$

ker to zaporedje razpade sledi:

$M \cong L \oplus P$

$L \oplus P$ je tudi prost

iii) $\Rightarrow$ i) $L \oplus P$ je prost za nek L $\quad P$ je projektiven



$\varphi\vartheta = \varphi$ $\qquad \varphi\vartheta = \varphi\Theta i_P = \varphi\pi_P i_P = \varphi\, id_P = \varphi$

$\square$

Primer: Želimo najti projektivni modul ki ni prost

K je prost K-modul

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

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

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

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

(K_1, K_2 kolobarja $K := K_1 \times K_2$, $e = (1,0)$)

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

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

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

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

Torej je P projektivni modul (not direct summand prostaga), ki ni prost

2.7 Tenzorski produkti

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

Moduli bodo nad komutativnim kolobarjem K

N, M K-modula

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 oblike $(au + a'u', v) - a(u,v) - a'(u',v')$,

$(u, av + a'v') - a(u,v) - a'(u,v')$, kjer $a, a' \in K$

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

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

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

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

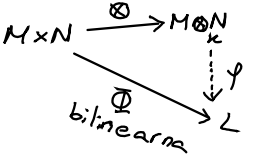
($\Phi(au + a'u', v) = a\Phi(u,v) + a'\Phi(u',v)$ in isto v drugem argumentu)

Primeri:

Skalarni produkt, vekt. produkt v $\mathbb{R}^3$, produkt v vsaki algebri: $(x,y) \mapsto xy$,

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

Izrek: (univerzalna lastnost tenzorskega produkta)



Za $\forall$ modula M in N nad komutativnim kolobarjem K, $\exists$ taka bilinearna preslikava $M \times N \to M \otimes N$, $(u,v) \mapsto u \otimes v$, za katero velja, za $\forall$ bilinearno preslikavo $\Phi: M \times N \to L$, kjer je L poljuben K-modul, $\exists$ enolično določena linearna preslikava $\varphi: M \otimes N \to L$, 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 >>

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

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

$\Leftrightarrow$

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

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

Podobno izpeljemo linearnost preslikave $\otimes$ v drugem argumentu

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

Iščemo linearno preslikavo φ

$\mathcal{F}$ ima bazo $M \times N$, zato lahko Φ (enolično) razširimo do lin. preslikave $F : \mathcal{F} \to L$ $\quad F(u,v) = \Phi(u,v)$.

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

$F(au + a'u', v) - a(u,v) - a'(u',v)$ se slika v ?

$= F(au + a'u', v) - aF(u,v) - a'F(u',v) =$

$= \Phi(au + a'u', v) - a\Phi(u,v) - a'\Phi(u,v) = 0$

Zato je $\varphi : M \otimes N \to L$, $x + \mathcal{N} \mapsto F(x)$ 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.

Enoličnost

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

ker je $\odot$ bilinearna, $\exists$ linearna preslikava $\psi : M \otimes N \to T$ taka da je $\psi(u \otimes v) = u \odot v$

Analogno obstaja linearna preslikava $\Psi : T \to M \otimes N$. $\Psi(u \odot v) = u \otimes v$

$(\Psi\psi)(u \otimes v)$ za $\forall$ enostavni tenzor $u \otimes v \Rightarrow \Psi\psi = id_{M \otimes N}$ (↑ "ujemanje na bazi")

$\psi\Psi = id_T$ analogno

□

"Praktična definicija tenzorskega produkta

- $\forall u \in M. \forall n \in M. \exists u \otimes v \in M \otimes N.$ T. imenujemo ga enostavni tenzor.

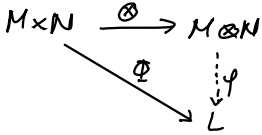
  Vsak drug element je vsota teh enostavnih tenzorjev

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

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

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

  Zato $0 \otimes v = u \otimes 0 = 0$



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

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

Sporočilo izreka je, da je φ dobro definirana

Definicija
φ, ψ naj bodeta lin. preslikava $\varphi: M \to M'$ in $\psi: N \to N'$

$M \times N \longrightarrow M \otimes N$
$(u,v) \longmapsto \varphi(u) \otimes \psi(v)$ 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 φ in ψ

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

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

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

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

d) $M \otimes K \cong M$

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

Dokaz:

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

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

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

Ali je bijektivna? Iščemo inverz.

$\exists$ lin preslikava $v \otimes u \longmapsto u \otimes v$. "Očitno" sta si preslikavi inverz (Analogno)

d) $M \otimes K \to M$

$u \otimes a \longmapsto au$ ker je linearna, je dobro definirana

$M \longrightarrow M \otimes K$

$u \longmapsto u \otimes 1$ preslikavi sta druga drugi inverz

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

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

Fiksirajmo $w \in R$

$u \otimes v \longmapsto u \otimes (v \otimes w)$ je bilinearna preslikava.

Zato $\exists$ linearna preslikava $^{\alpha}$ $u \otimes v \longmapsto u \otimes (v \otimes w)$

Zato lahko definiramo bilinearno preslikavo

$\Phi : (M \otimes N) \times R \longrightarrow M \otimes (N \otimes R)$ ($\in$ naraden $\times$)

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

$\Leftrightarrow \exists$ šcena linearna preslikava ki slika

$(M \otimes N) \otimes R \longrightarrow M \otimes (N \otimes R)$ ü

□

2.8 Tenzorski produkti prostih modulov

Primer:

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

" Kaj je $\mathbb{Z}_3 \otimes \mathbb{Z}_2$. Če je kaj pravi cena sveda je to $\mathbb{Z}_6$, amkak ker vsi vemo da ne sveta ni pravice "

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

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

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

Izrek: Naj bo M prost K-modul z bazo $\{e_i : i \in I\}$ in N poljuben K-modul.
Potem $\forall$ element $M \otimes N$ lahko enolično zapišemo kot

$$\sum e_i \otimes v_i$$

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

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

$$u \otimes v = \Big(\sum \underbrace{a_i}_{\text{za neke } a_i \in K} e_i\Big) \otimes v = \sum (a_i e_i) \otimes v = \sum e_i \otimes \underbrace{(a_i v)}_{v_i}$$

enoličnost:
Ker je $\forall$ element $M \otimes N$ vsota enostavnih tenzorjev, je res $\forall$ element oblike $\sum_i e_i \otimes v_i$
Zadošča dokazati $\sum_i e_i \otimes v_i = 0 \Rightarrow v_i = 0$ za $\forall i \in I$

Izberimo $i_0 \in I$
če uspemo najti tako linearno preslikavo $\varphi : M \otimes N \to N$
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
$0 = \varphi(0) = \varphi\left(\sum e_i \otimes v_i\right) = 0 \sum \varphi(e_i \otimes v_i) = v_{i_0}$

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

$$\varphi_0 : e_i \mapsto 0 \; ; \; i \neq i_0$$
$$e_{i_0} \mapsto 1$$

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

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

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

zato $\exists$ linearna preslikava $\varphi : M \otimes N \to N$ 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 $\{f_j\}$

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: $\forall el. \in M \otimes N$ je oblike $\sum_i e_i \otimes v_i =$

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

Linearna neodvisnost:

$$0 = \sum_{ij} a_{ij} (e_i \otimes f_j) = \sum_i e_i \otimes \left(\sum_j a_{ij} f_j\right) \Rightarrow \sum a_{ij} f_j = 0 \text{ za } \forall i$$

(zapis $\sum e_i \otimes v_i$ je enoličen)

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

(f_j baza)

■

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

Primer: V vek. pr. nad F, $v \in V$, $f \in V^*$ (dual V ← lin funk cons)

$v \otimes f : V \longrightarrow V$

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

Primeri in izreki v učbeniku

2.9 Tenzorski produkt algebr

Algebra nad F:

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

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

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 definiranost množenja

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

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

$$\varphi_z : A \to A \quad \varphi_w : B \to B \quad \varphi_z \otimes \varphi_B : A \otimes B \to A \otimes B$$

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

$\Phi : A \times B \longrightarrow End(A \otimes B)$ ← za enkrat je samo K-modul
$(z, w) \longmapsto \varphi_z \otimes \varphi_w$ če je $A \otimes B$ K-modul, je $End(A \otimes B)$ K-algebra

Φ je bilinearna zato $\exists$ lin. pres. $\varphi : A \otimes B \to End(A \otimes B)$
$(z \otimes w) \longmapsto \varphi_z \otimes \varphi_w$

Definirajmo množenje v $A \otimes B$

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

Ali je to res definicija množenja?

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

$$= (\varphi_z \otimes \varphi_w)(u \otimes v) = uz \otimes vw$$

Produkt je bilinearen:

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

$r(\ldots) = r_{\ldots} + r_{\ldots}$ itd

asoc: očitno

enota: $1 \otimes 1$

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

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

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

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

d) $A \otimes K \cong A$

direktni produkt in direktna vsota algebr sta ekvivalentna

Dokaz: isto kot za module

Primer:

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

$$a\left(\sum a_i X^i\right) = \sum a a_i X^i$$

- 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

  $\sum_{i \geq 0} a_i \otimes X^i$ ← enolično zapis (preštej: izreki)

  $\sum_{i \geq 0} a_i \otimes X^i \longmapsto \sum_{i \geq 1} a_i X^i$ je izomorfizem

- A poljubna K-Algebra

  $M_n(K)$ je kolobar in je tudi K-Algebra, če definiramo $a \begin{bmatrix} a_{11} \dots a_{1n} \\ \vdots \\ a_{n1} \dots a_{nn} \end{bmatrix}$

  Lahko definiramo

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

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

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

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

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

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

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

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

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

  ← bločne matrike

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

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

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

2.10 Razširitev skalarjev

Naj bo A realna, končnodimenzionalna algebra

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

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

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

Primer:

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

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

   $\uparrow$ ima delitelje niča $\Rightarrow$ zato ne more biti $\cong \mathbb{H}$

K, C komutativna kolobarja $\qquad M$ K-modul

$\alpha : K \to C$ homomorfizem

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

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

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.

$l_c : C \to C$ levo množenje je K-linearna
$d \mapsto cd$

$$cy = (l_c \otimes id_M)(y) \quad \begin{matrix} \forall c \in C \\ \forall y \in M_C \end{matrix}$$

↑ lesparna 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:

$\alpha: K \to C$ $\quad$ K podkolobar C

$k \mapsto k$

$M_C = C \otimes M$ elementi so $1 \otimes u$ $u \in M$

Naj bo A K-algebra

A_C je C-modul

$C \otimes A$ je tudi K-algebra s $c \mapsto c \otimes 1_A$ K algebri

z množenjem

$c(d \otimes u) = cd \otimes u$ je A_C C-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

baznih vektorjev $e_i e_j = \sum_k \alpha_{ijk} e_k$, 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 komutativen kolobar

Naj bo I maksimalni ideal $K \Longrightarrow K/I = C$ je polje

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

$\alpha : K \longrightarrow C$

$k \mapsto k + I$ Tako iz K modula M dobimo

vektorski prostor M_C nad C

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

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

Dokaz:

Naj bo C polje kot v prejšnjem primeru.
Za $n \in \mathbb{N}$ definiramo $(K^n)_C$ ← To z razširitvijo 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 $K^s \cong K^t$
$\Phi : K^s \longrightarrow K^t$ izomorfizem K-modulov

$id_C \otimes \Phi : (K^s)_C \longrightarrow (K^t)_C$ je K linearna, v našem primeru je tudi C-linearna
$(id_C \otimes \Phi)(c d \otimes w) = cd \otimes \Phi(w) = c(d \otimes \Phi w) =$
$= c(id \otimes \Phi)(d \otimes w)$
in tudi: bijektivna $\Rightarrow$ je izomorfizem vektorskih prostorov nad C

Ker sta K^s in K^t vektorska prostora, je $s = t$

2.11. Končno generirane Abelove grupe

Naj bo K celi kolobar in M K-modul

Definiramo

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

torzijski podmodul

To je podmodul

$u, v \in tor(M)$

$au = 0 \quad bv = 0$

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

$u \in tor\ M \quad b \in K \quad au = 0$

$\Rightarrow abu = bau = 0$

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

$M/tor(M)$ je torzijsko prost

$a(u + tor(M)) = 0 \Rightarrow au + tor(M) = 0 \Rightarrow au \in tor(M)$

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

$\Rightarrow u + tor M = 0$

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

$tor(G)$ = torzijska podgrupa abelove (aditivne) grupe G

Pokazali smo, $G/tor(G)$ je torzijsko prosta grupa

...vsi elementi razen 0 imajo neskončen red

končna ⇒ končno generirana

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

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

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

bomo dokazali:

⇕

končnogenerirana abelova grupa

Lema: Končno generirana torzijsko prosta abelova grupa je prosta

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

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

Denimo da H ni prosta

Izmed vseh množic z m elementi, ki generirajo H, izberimo „najmanjšo" ($\{a_1 \dots a_m\}$ generirajo H, $\exists k_1 \dots k_m \in \mathbb{Z}$. $k_1 a_1 + \dots + k_m a_m = 0$ in $\sum_{i=1}^{m} |k_i|$ minimalno število (zaj $\{b_1 \dots b_m\}$ 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 $k_i \neq 0$

Recimo da sta to k_1 in k_2

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

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

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

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

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

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

ker $a_1, (a_2 + q a_1), a_3, \dots, a_n$ 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 enolično 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 enolično določen: $s \geq 0$
ker je G končno generirana je k.g tudi: G/T

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

$$\Rightarrow 0 \longrightarrow T \underset{\hookrightarrow i}{\longrightarrow} G \underset{\pi}{\longrightarrow} G/T \longrightarrow 0$$

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

T končna

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

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

Vsi elementi so oblike

$m_1 t_1 + m_2 t_2 + \ldots m_r t_r \qquad m_i \in \mathbb{Z}$

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

Posledica: V končno generirana abelova grupa, 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 kolobarjem

3. Prezentacije grup in algeber

3.1 Proste grupe in prezentacije grup

Neformalno: kaj je prosta grupa na množici X

F_X

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

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

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

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

Različni zapisi dajo vedno različne elemente

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

Formalno: X poljubna množica

Definirajmo grupo F_X na X

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

$X\neq\emptyset \Rightarrow$ označimo X^{-1} množica z isto kardinalnostjo kot X, $X^{-1}=\{x^{-1}; x\in X\}$ ← samo oznaka

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

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

Če sta izpolnjena pogoja

1) Elementa X, X^{-1} nikoli ne nastopata zaporedoma
$x_i = x \Rightarrow x_{i+1} \neq x^{-1} \wedge x_i = x^{-1} \Rightarrow x_{i+1} \neq x$

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

potem besedi pravimo reducirana beseda

Zaporedje $(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \dots, x_n^{\varepsilon_n}, 1, \dots)$ $\varepsilon_i \in \{1,-1\}$

pišemo kot $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$

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

kot množica je F_X množica reduciranih besed

Vpeljimo operacijo

Vzemimo dve reducirani besedi:

$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m}$ in $y_1^{\mu_1} y_2^{\mu_2} \dots y_n^{\mu_n}$ $\varepsilon_i, \mu_i \in \{-1,1\}$ $x_i, e_i \in X$

in naj bo $m \leq n$

$x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \cdot y_1^{\mu_1} \dots y_n^{\mu_n} =$

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

$$\begin{cases} x_1^{\varepsilon_1} \dots x_{m-k+1}^{\varepsilon_{m-k+1}} y_k^{\mu_k} \dots y_n^{\mu_n} & k \leq m \\ y_{k+1} \dots y_n & k = m+1 \quad m < n \\ 1 & k = m+1 \quad m = n \end{cases}$$

F_X je grupa

1 je enota

$(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1}$

F_X imenujemo Prosta grupa na množici X

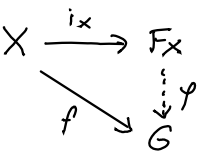
$X \subseteq F_X$

↑ neformalno

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

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

$\exists!$ homomorfizem $\varphi: F_X \to G$. Velja $\varphi(i(x)) = f(x)$ za $\forall x \in X$



Dokaz: $\varphi(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m}) = f(x_1)^{\varepsilon_1} \cdot \dots \cdot f(x_m)^{\varepsilon_m}$

Izrek: $\forall$ grupa je homomorfna slika: proste grupe

Dokaz: Naj bo G grupa. Naj bo $X \subseteq G$ množica, ki G generira. Na X gledmo kot množico, zgradimo prosto grupo F_X na X. Po prejšnjem izreku $\exists$ homomorfizem $\varphi: F_X \to G$, $x \mapsto x$ (ker vzamemo $f(x)=x$)

φ je surjektiven ker je $\operatorname{im}\varphi \leq G$ in $X \subseteq \operatorname{im}\varphi$ 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: $r = 1$ $r \in R$, če je $G \cong F_X / N_R$, kjer je N_R edinka 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 odseki $x_i N$; $x_i \in N$

$r \in R$ $r = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$

$$(x_1 N)^{\varepsilon_1} \dots (x_n N)^{\varepsilon_n} = (x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) N = rN = N = 1$$

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

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

Primer:

1) Prezentacija proste grupe

$\langle X \mid \emptyset \rangle$

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

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

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

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

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

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

Naj bo G neka druga dieedrska grupa generirana z $\langle u, v \rangle$ ki zadošča $u^n = v^2 = (uv)^2 = 1$

D_{2n} je taka grupa, pa tudi $F_{\{x,y\}}/N$ je taka ($u = xN$, $v = yN$)

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

2. korak: G ima največ $2n$ elementov

Denimo da je to res. Potem po 1. koraku

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

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

φ je bijektiven

1. korak

Velmo: $\exists$ homomorfizem Φ iz $F_{\{x,y\}}$ v G

$x \mapsto u$

$y \mapsto v$

Ker φ vsebuje x^n, y^2 in $(xy)^2$

$\Rightarrow N \leq \ker\varphi$

zato $\exists$ homomorfizem $F_{\{x,y\}}/N \to F_{\{x,y\}}/\ker\varphi \overset{\text{izo}}{=} G$

$wN \mapsto w\ker\varphi$

2. korak

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

$\{$

$m_i \in \{0, 1\}$ $n_i \in [n]$.

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

Edini možni elementi so

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

3.2. Proste algebre in prezentacije algebr

Algebra naj bo nad poljem F

Elementi proste algebre so nekomutativni polinomi.

X, Y dve spremenljivki

$\{1, X, Y, XY, YX, XY-YX, 3+7x^2y-9yx^4y, \ldots\}$

Naj bo X množica. Elementi prostega monoida X^* so besede: zaporedja $(x_1, x_2, \ldots x_m, 1, 1, \ldots)$

$= x_1 x_2 \ldots x_m$

$xxyyx = x^2y^2x$

Vpeljemo množenje $x_1 \ldots x_n \cdot y_1 \ldots y_m = x_1 \ldots x_n y_1 \ldots y_m$

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^*

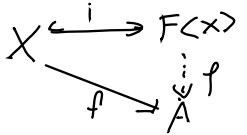
$F\langle X \rangle$ postane algebra, če definiramo

$$\left(\sum \lambda_i w_i\right) \overset{e X^*}{\left(\sum \mu_j w_j\right)} := \sum_{w_i w_j = w_k} v_k w_k$$

$$v_k = \sum_{w_i : w_j = w_k} \lambda_i \mu_j$$

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

$$i : X \longrightarrow F\langle X \rangle$$
$$x \longmapsto x$$



Izrek: Naj bo X množica in A algebra in $f: X \to A$. Potem $\exists!$ homomorfizem $\varphi: F\langle X\rangle \to A$, 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 $X \subseteq A$ $\langle X\rangle = A$ (podalgebra, ki jo generatorja)

Naj bo $f: X \to A$, $x \mapsto x$

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

$X \subseteq \operatorname{im}\varphi \Rightarrow A \subseteq \operatorname{im}\varphi \Rightarrow A = \operatorname{im}\varphi$

$A \cong \frac{F\langle X\rangle}{I}$ $I = \ker\varphi$

Definicija: Naj bo $X \neq \emptyset$, naj bo F polje in naj bo R množica nekomutativnih polinomov iz X. Pravimo da je algebra A definirana z generatorji $x \in X$ in relacijami $p = 0$ $p \in R$, če je

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

$\curvearrowleft$ ideal 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. Prosta algebra $\langle X \mid \emptyset \rangle$
2. $F\langle X, Y \mid XY = YX \rangle = F[X, Y]$
3. $F\langle X, Y \mid XY = 1 \rangle$
4. $F\langle E_{12}, E_{21} \mid E_{1,2}^2 = E_{21}^2 = 0$

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

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

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

Vajbarnova prezentacija je F

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