1. Deljivost v komutativnih kolobarjih

$xy = yx$

$1 \in K$

Gaussova števila!

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

Cel kolobar - komutativen kolobar, brez deliteljev niča

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 niste 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 (n.s.d) delitelj 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

Odslej: K je cel

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

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

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

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

ni delitelja 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

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

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

kateko koli polje

(3 pa ni razcepen)

1.2 Glavni kolobarji

I ideal: $\bullet\ I \leq (K,+)$

$\bullet\ KI, IK \subseteq I$

K komutativen

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)

$$\boxed{b \mid a \Leftrightarrow (a) \subseteq (b)}$$

$\Rightarrow$ $a = gb$

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

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

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

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

2) $K = (1)$

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

Ideal je končnogeneriran, 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: $(a_1 \dots a_n) = (a_1) + (a_2) + \dots + (a_n)$

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

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

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

Ali je I glavni ideal?

npr $I = (f(x))$

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

$x \in I \Rightarrow x = a_0 h(x)$ $\cancel{\;}$

$\uparrow$ 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 deliteljev niča

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

Izrek: Naslednji kolobarji so evklidski

a) $\mathbb{Z}$

b) $F[x]$, F polje

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

Dokaz:

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

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

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

b) ✓ vemo da je to kvadrat absolutne vrednosti

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

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

$\underline{a = qb + r}$

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

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

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

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

$r := a - qb$ $\underline{r = 0 \vee \delta(r) < \delta(b)}$

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

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

$$= |c-q|^2 |b|^2 = \big(\underbrace{(u-k)^2}_{\leq \frac{1}{4}} + \underbrace{(v-l)^2}_{\leq \frac{1}{4}}\big)|b|^2$$

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

Izrek: $\forall$ evklidski kolobar je glavni kolobar

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

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

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

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

$\underline{I = (a)}$ $\qquad (a) \subseteq I$ trivialno

Naj bo $x \in I$ poljuben

$x = \underbrace{aq}_{\in I} + r$ v K $\Rightarrow r \in I \Rightarrow \delta(r) \geq \delta(a) \vee r = 0$

$\Rightarrow a \mid x$

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 obstaja in je oblike

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

Dokaz:

K je glavni

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

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

$d \neq 0$

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

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

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

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

Izrek: Naj bo $p \neq 0 \in K$ glavni kolobar..

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 $M \neq K \wedge M \subseteq I \triangleleft K \Rightarrow I = K$
$\vee M = I$

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

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

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

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

i) in ii) ustrezata povesta isto

1.3 Enolična faktorizacija

$a \neq p_1 p_2 \cdots p_n$

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

Dokaz:

a ni nerazcepen

$a_1 = a_2 b_2$ $\quad a_2$ 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

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

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

Definicija: Komutativen kolobar K je noetrski, če se $\forall$ naraščajoča veriga idealov

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

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

Lema: $\forall$ 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)

(ponavadi ni grupa za seštevanje)

$KI \subseteq I$ očitno

$u, v \in I$

$u - v \in I$

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

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 $\quad I \subseteq I_{n+1} \subseteq I$

Hilbertov izrek o bazi

K noetrski $\Rightarrow K[x]$ noetrski

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

$\quad\quad\ \ \ \|$

$\underbrace{\underbrace{K[x]}_{\text{glavni}}[y]}_{\text{ni glavni}}$

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

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

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

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

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

Recimo da $p | x \Rightarrow x = pu \Rightarrow p = puy \Rightarrow uy = 1 \Rightarrow y$ je obrnljiv

2) Naj bo K glavni

p naj bo nerazcepen. p praelement

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

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

$1 = px + ay$

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

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: $\forall$ 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 $a = q_1 \cdots q_t$

$p_1 | a \Rightarrow p_1 | q_1 \cdots q_t \Rightarrow \exists i \in [t]. \; p_1 | q_i$. BSZS $p_1 | q_1$

nerazcepen + glavni kolobar $\Rightarrow$ praelement

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

$p_1 \cdot /$ $\quad p_1 \cdots p_s = p_1 u q_2 \cdots q_t$

$p_2 \cdots p_s = u q_2 \cdots q_t$ postopek ponovimo

$s = t$: $\quad s > t \Rightarrow \underbrace{u}_{\text{obrnljiv}} = \underbrace{p_{t+1} \cdots p_s}_{\text{nerazcepni}}$ ker ni mogoče

15.10

2. Moduli

2.1. Caylyjev izrek za kolobarje

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

M aditivna grupa

$\mathrm{End}(M)$ = množica vseh endomorfizmov $M \to M$

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

$\mathrm{End}\, M$ 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

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

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

$l_a \in End(K)$ ← K kot grupa za $+$

$\varphi : K \to End K$
$\qquad a \mapsto l_a$

$$\varphi(a+b) = l_{a+b} = l_a + l_b = \varphi(a) + \varphi(b)$$
$$\Uparrow$$
$$(a+b)x = ax + bx$$

Fija

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

Gay bey

$\Updownarrow$

Luy ley

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

injektivnost:

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

Naj bo A algebra nad poljem F

V vektorski prostor nad F

$End_F(V)$

Na podoben način dokažemo

Izrek: $\forall$ algebro nad F lahko vložimo v algebro endomorfizmov nekega vekt. prostora nad poljem F.

$\dim A \overset{= n}{<} \infty$

matrike $n \times n$ nad F

$A \hookrightarrow End_F(A) \cong M_n(F)$ A 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 nek 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 $ST - TS = I$

$$
\begin{array}{ccc}
sl(ST - TS) = sl(I) = & n \\
\| & \| \\
sl(ST) - sl(TS) = & 0
\end{array}
$$

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

2.2 Definicija modula

Definicija: Naj bo K kolobar. Množica M skupaj z binarno operacijo $(a,u) \mapsto au$ iz $K \times M$ v 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

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

$\blacksquare$

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

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

Odslej modul = levi modul

Primeri:

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

2. 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 sabo, če definiramo au kot običajni produkt $a \cdot u$ v K

4. Naj bo I levi ideal K
   I je K-modul, če je au običajni 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 operaciji sama modul.

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

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

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

Primeri:

1. če je V 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. Aditivna grupa je enostavna kot $\mathbb{Z}$-modul $\Leftrightarrow$ $\cong \mathbb{Z}_p$
3. $R = M_n(F)$ $\quad M = F^n$

$N \subseteq F^n$

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

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

M je enostaven modul nad matrikami;

Homomorfizmi modulov

M, N K-modula

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

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

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

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

Rečemo jim tudi K-linearne preslikave

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

sta podmodula M oz. N

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

$M \cong N$: M izomorfna N

(obstaja izomorfizem)

Kolobarji endomorfizmov

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

M aditivna grupa $\mathrm{End}(M)$

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

je kolobar če vpeljemo

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

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

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

Dokaz:

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

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

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

$\operatorname{im}\varphi = M$

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

Kvocientni 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

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

Direktne vsote modulov

$M_1, \ldots, M_s$ K-moduli

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

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

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

Imenujemo ga direktna vsota modulov $M_1 \ldots M_s$ in pišemo $M_1 \oplus \ldots \oplus M_s$

Natančneje: zunanja direktna vsota

Naj bo sedaj M modul in $N_1 \ldots N_s$ njegovi podmoduli: če velja

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

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

potem M imenujemo (notranja) direktna vsota podmodulov $N_1 \ldots N_s$

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

Če je M notranja direktna vsota $N_1 \ldots N_s$ je
$M \cong N_1 \oplus \ldots \oplus N_s$

Izomorfizem je podan z $v_1 + \ldots + v_s \longleftrightarrow (v_1 \ldots v_s)$
ker je $v_1 + \ldots + v_s$ enolični zapis

Tudi notr. dir. vsot. označimo z
$N_1 \oplus \ldots \oplus N_s$

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

Primer
1. $K = F$ ~~je~~ 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 cikličen podmodul

Ciklični modul je generiran z enim samim elementom

Primeri:

1. $K = F$ 1-razsežni podprostori in $\{0\}$
2. $K = \mathbb{Z}$: ciklični $\mathbb{Z}$ modul so ciklične grupe
3. K komutativen kolobar ... ~~ideal~~ glavni
4. I levi 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, rečemo 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 $a_1e_1 + \dots + a_se_s = 0$ sledi $a_1 = \dots = a_s = 0$

(če je B neskončna potem 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 $\forall u \in M$ obstaja $e_1, \dots, e_s \in B$, da je $u = a_1e_1 + \dots + a_se_s$ kjer so a_i enolično določeni el. iz K

Pišemo $u = \sum a_ie_i$

Primer:

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

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

$u \in G$ že $\{u\}$ ni lin neodvisna

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

Edina linearnoneodvisna množica je prazna množica

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

bazi sta $\{1\}$ in $\{-1\}$

Definicija: Modul, ki ima bazo se imenuje

Prosti modul

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

2) K kolobar, potem je

$\underbrace{K \oplus \ldots \oplus K}_{s \text{ sumanda}} = K^s$ je prost K modul

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

$\forall$ españa

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

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

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

$\exists \sigma$ izomorfizem ~~kom~~ da ta diagram komutira

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "id"] & M \arrow[r] \arrow[d, "\sigma"] & N \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & L \arrow[r] & L \oplus N \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

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

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

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 velja pogoj

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

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

Poiščimo tak 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 izomorfizem

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

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

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

surj

$u \in M$

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

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

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

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

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

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

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

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

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

drugi pogoj:

...

i) $\Rightarrow$ ii) in iii)

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

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

pogledamo definicije in vidimo da je vredu

2.6 Projektivni moduli:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\vartheta"'] \arrow[d, "\varphi"] & \\ M \arrow[r, "\psi"] & N \arrow[r] & 0 \end{tikzcd}$$

ψ surjektiven

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

$$\begin{tikzcd} & P \arrow[dl, dashed] \arrow[d, "\varphi"] & \\ M \arrow[r, "\psi"'] & N \arrow[r] & 0 \end{tikzcd}$$

P ima bazo B

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

$\vartheta: e \to u_e$

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 konča s P, razpade $0 \to L \to M \to P \to 0$

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

Dokaz:

i) $\Rightarrow$ ii) P proj.

$$\begin{tikzcd} & & & P \arrow[dl, dashed, "\vartheta"'] \arrow[d, "id"] & \\ 0 \arrow[r] & L \arrow[r, "\varphi"] & M \arrow[r, "\psi"] & P \arrow[r] & 0 \end{tikzcd}$$

$\exists \vartheta$ 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

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

definiramo

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

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 $\qquad$ P je projektiven

projektiven

$$\begin{tikzcd} L \oplus P \arrow[dd, bend right, "\Theta"'] \arrow[d, shift right, "\pi_P"'] & \\ P \arrow[u, shift right, "i_P"'] \arrow[dl, dashed, "\vartheta"'] \arrow[d, "\varphi"] & \\ M \arrow[r, "\psi"] & N \arrow[r] & 0 \end{tikzcd}$$

$\vartheta := \Theta i_P$

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

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)

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

$\Rightarrow \{ex\}$ nikoli ni linearno 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 (kot direktni sumand prostega), ki ni prost

2.7 Tenzorski produkti

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

Moduli bodo nad komutativnim kolobarjem K

N, M K-modula

Množica $M \times N$ $\quad$ 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

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

Primeri:

Skalarni produkt, vek. 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)

$$\begin{tikzcd} M \times N \arrow[r, "\otimes"] \arrow[dr, "\Phi"', "\text{bilinearna}"] & M \otimes_k N \arrow[d, dashed, "\varphi"] \\ & L \end{tikzcd}$$

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 <u>Linearna</u> 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 natanočno in enolično določen.

Dokaz >>

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

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

$\Longleftrightarrow$

$$\underbrace{(au + a'u', v) + \mathcal{N}}_{(au+a'u')\otimes v} = a\underbrace{\left((u,v) + \mathcal{N}\right)}_{u\otimes v} + a'\underbrace{\left((u',v) + \mathcal{N}\right)}_{u'\otimes v}$$

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

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 $\mathcal{N}$

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

Zato je $\varphi : \begin{aligned} M \otimes N &\to L \\ x + \mathcal{N} &\mapsto F(x) \end{aligned}$ 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 $M \otimes M$

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

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

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

"ujemanje na bazi"

$\varphi\psi = id_T$ analogno

$\square$

"Praktična" definicija tenzorskega produkta

- $\forall u\in M.\ \forall v\in N.\ \exists\, u\otimes v\in M\otimes N$. 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 $0\otimes v = u\otimes 0 = 0$

$$\begin{tikzcd}
M\times N \arrow[r, "\otimes"] \arrow[dr, "\Phi"'] & M\otimes N \arrow[d, dashed, "\varphi"] \\
 & L
\end{tikzcd}$$

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

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

Sporočilo izreka je, da je φ dobro definirana

Definicija

φ, ψ naj bo stelin. 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) $M \otimes k \cong M$

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

Dokaz:

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

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

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

Ali je bijektivna? Iščemo inverz.

$\exists$ lin preslikava $\overset{\text{Analogno}}{v \otimes u \mapsto u \otimes v}$. "očitno" sta si preslikavi inverz

d) $M \otimes k \to M$

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

$M \longrightarrow M \otimes k$

$u \mapsto u \otimes 1$ 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 $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$ ki bo njen inverz.

Fiksirajmo $w \in R$

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

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

Zato lahko definiramo bilinearno preslikavo

$\Phi : (M \otimes N) \overset{\text{navaden }\times}{\times} R \longrightarrow M \otimes (N \otimes R)$

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

$\Downarrow$ $\exists$ sedaj linearna preslikava ki slika

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

$\square$

2.8 Tenzorski produkti prostih modulov

Primer:

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

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

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

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

$\mathbb{Z}_n \otimes \mathbb{Z}_m = 0$, 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: $u \in M, v \in N$

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

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

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

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

$(u, v) \mapsto \varphi_0(u) \cdot v$ 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?

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

zapis $\sum e_i \otimes v_i$ je enoličen

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

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 torej $\dim (U \otimes V) = \dim U \cdot \dim V$

Primer: V vek. pr. nad F, $v \in V$, $f \in V^*$ ← dual V
← lin funkcional

$v \otimes f : V \longrightarrow V$

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

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

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

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

$\rho_z : A \to A$ $\rho_w : B \to B$ $\rho_z \otimes \rho_B : A \otimes B \to A \otimes B$

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

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

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

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

Definirajmo množenje v $A \otimes B$

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

Ali je to naša definicija množenja?

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

Produkt je bilinearen:

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

$r(\dots) = r_{\dots} + r_{\dots}$ 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 kolabar 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

  $\sum_{i \geq 0} a_i \otimes X^i$ ← enolični zapis (prejšnji izrek)

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

- A poljubna K-Algebra

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

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

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

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

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

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

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

  ↖ bločne matrike

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

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

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

2.10 Razširitev skalarjev

Naj bo A realna, končnodimenzionalna algebra

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

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

$A_\mathbb{C}$ 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. $\mathbb{H}_\mathbb{C} \cong M_2(\mathbb{C})$
   ima delitelje niča :(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
$d \mapsto cd$

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

Konsporna 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:

$\alpha: \mathbb{R} \to \mathbb{C}$ $\quad$ $\mathbb{R}$ podkolobar $\mathbb{C}$

$k \mapsto k$

$M_{\mathbb{C}} = \mathbb{C} \otimes M$ elementi so $1 \otimes u$ $u \in M$

Naj bo A $\mathbb{R}$-algebra

$A_{\mathbb{C}}$ je $\mathbb{C}$-modul

$\mathbb{C} \otimes A$ je tudi $\mathbb{R}$-algebra saj sta $\mathbb{C}$ in A $\mathbb{R}$ algebri

z množenjem

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

Elementi so $\mathbb{C}$-linearne kombinacije $1 \otimes e_i$, kjer so $\{e_i ; i \in I\}$ baza A.

$\{1 \otimes e_i\}$ so baza za $A_{\mathbb{C}}$

Če je množenje v $\mathbb{R}$-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 $K \implies \overset{C}{\overset{\shortparallel}{K/I}}$ 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

$(id_C \otimes \Phi)(c\, d \otimes u) = cd \otimes \Phi(u) = c\,(d \otimes \Phi u) = c\,(id \otimes \Phi)(d \otimes u)$

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 cel kolobar in M K-modul

Definiramo

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

torzijski podmodul

To je podmodul

$u, v \in tr(M)$

$au = 0 \quad bv = 0$

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

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

$\Rightarrow abu = bau = 0$

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

<u>$M/tor(M)$ je torzijsko prost</u>

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

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

$\Rightarrow u + tor M = 0$

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

3.12

končne $\Rightarrow$ končno generirane

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

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

končna abelova

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

$\Updownarrow$

končnogenerirane abelove grupe

Lema: Končno generirana torzijsko prosta abelova grupa je prosta

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

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

Denimo da H ni prosta

Izmed vseh množic z m elementi, ki generirajo H, izberimo „najmanjšo" ($\{a_1 \dots a_m\}$ generirajo H, $\exists k_1 \dots k_m \in \mathbb{Z}$. $k_1 a_1 + \dots + k_m a_m = 0$ in $\sum_{i=1}^{m} |k_i|$ minimalno število (če je $\{b_1 \dots b_m\}$ tudi množica generatorjev in je $\sum l_i b_i = 0 \Rightarrow \sum |l_i| \geq \sum |k_i|$)

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

Recimo da sta to k_1 in k_2

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

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

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

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

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

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

ker $a_1, (a_2 + g a_1), a_3, \dots, a_n$ 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 določeni $s \geq 0$

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 določeni $s \geq 0$

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

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

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

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

T končna

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

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

Vsi elementi so oblike

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

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

Posledica: $\forall$ 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 $\underbrace{\text{prosta grupa}}_{F_X}$ na množici X

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

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

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

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

Različni 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 besede

Npr $(1, 1, \dots) = 1$ je beseda, kiji 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 $(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \dots, x_n^{\varepsilon_n}, 1, \dots)$ $\quad \varepsilon_i \in \{1, -1\}$

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

((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

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

in naj bo $m \leq n$ $\quad x_i, e_i \in X$

$x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \cdot y_1^{\mu_1} \dots y_n^{\mu_n} =$ $\quad$ k ~~najmanjši~~ največji da $y_k \neq x_{m-k+1}$ in $\varepsilon_{m-k+1} \neq \mu_k$

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

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 naj bo 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 $\varphi: F_X \to G$, da je $\varphi(i(x)) = f(x)$ za $\forall x \in X$

$$\begin{tikzcd}
X \arrow[r, "i_X"] \arrow[dr, "f"'] & F_X \arrow[d, dashed, "\varphi"] \\
& G
\end{tikzcd}$$

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 glejmo 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

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

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

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

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

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

Primeri:

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 katera koli 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 homom. $F_{\{x,y\}}/N$

2. korak: G ima največ $2n$ elementov

Denimo da je to res. Potem po 1. koraku

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

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

Vemo: $\exists$ homom. iz $F_{\{x,y\}}$ v G

$x \mapsto u$

$y \mapsto v$

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

$\Rightarrow N \leq \ker \varphi$

zato $\exists$ homomorfizem $F_{\{x,y\}}/N \longrightarrow F_{\{x,y\}}/\ker \varphi \overset{\operatorname{im} \varphi}{\cong} G$

$wN \longmapsto w \ker \varphi$

2. korak

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

$\wr$

$m_i \in \{0, 1\} \ n_i \in [n]_0$

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

Edini možni elementi so

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

$\{1, x, y, xy, yx, xy-yx, 3+7x^2y-9yx^4y, \dots\}$

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

$xxyyx = x^2y^2x$

Upeljemo množenje $x_1 \dots x_n \cdot y_1 \dots y_m = x_1 \dots x_n y_1 \dots y_m$

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

$$\Big(\sum \lambda_i w_i\Big)\Big(\sum \mu_j w_j\Big) := \sum V_k w_k \qquad w_i \in X^*$$

$$w_i w_j = w_k$$

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

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

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

$$x \longmapsto x$$

$$\begin{tikzcd} X \arrow[r, hook, "i"] \arrow[dr, "f"'] & F\langle X\rangle \arrow[d, dashed, "\varphi"] \\ & A \end{tikzcd}$$

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

Dokaz: $\varphi(p(x_1 \dots x_m)) := p(f(x_1), \dots f(x_m))$

To je res homomorfizem

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

Posledica: Vsaka algebra je homomorfna sliki neke proste algebre

Dokaz: Naj bo A algebra $X \subseteq A$ $\langle X\rangle = A$ poljubna množica generatorjev

Naj bo $f: X \longrightarrow A$
$x \longmapsto x$

Po izreku: $\exists\, \varphi: F\langle X\rangle \longrightarrow A$
$x \longmapsto x$

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

$A \cong F\langle X\rangle / I \quad I = \ker\varphi$

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

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

← 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 $F\langle X \rangle / (R) = F\langle x_1 \dots x_m \mid r_1 = \dots = r_n = 0 \rangle$

Primeri:

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

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

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

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

Ugibamo: prezentacija je F

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

NEKOMUTATIVNA ALGEBRA

Direktni produkt kolobarjev in direktne vsote idealov

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

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

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

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

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

$e \in K$ je idempotent če $e^2 = e$

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

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

Primer: • e in $1-e$ sta ortagonalna

• $K = K_1 \times \dots \times K_s$

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

paroma so si ortagonalni. $e_1 + \dots + e_s = 1$

$\tilde{K}_i = e_i K$

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

Izrek: Naj bodo $I_1 \dots I_s$ ideali kolobarja K $\Rightarrow$

$\Big(K = I_1 \oplus \dots \oplus I_s \Leftrightarrow \exists e_1 \dots e_s$ paroma ort. cent. idem.
$e_1 + \dots e_s = 1 \wedge I_j = e_j K \Big)$

V tem primeru je $K \cong I_1 \times \dots \times I_s$

Dokaz:

$(\Rightarrow)$

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

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

Zato: $e_i u_j = u_j e_i = 0$ za $u_j \in I_j\ \ j \neq i$

$u_i = u_i \cdot 1 = u_i e_1 + \dots + u_i e_s = u_i e_i$ za $u_i = e_i$

$\Rightarrow u_i = u_i e_i = e_i u_i$ za $\forall u_i \in I_i \Rightarrow e_i^2 = e_i$

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

$x e_i = u_i e_i = e_i u_i = e_i x \Rightarrow e_i \in Z(K)$

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

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

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

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

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

brez j $\qquad x_1, \dots x_s \in K$, $u \in K$

Recimo da $e_j u = e_1 x_1 + \dots + e_s x_s \qquad / \cdot e_j$

$\Rightarrow e_j u = 0$

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

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

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

φ je bijekcija ker $\forall x \in K .\ x = e_1 x + \dots + e_s x$
in ker $I_j \cap (\text{ostali}) = \{0\}$

φ očitno ohranja vsote

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

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

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

Posledica: Če ima K take parama ortogonalne idempotente $e_1, \dots, e_s$ da je $e_1 + \dots + e_s = 1$

$\Rightarrow \quad K \cong e_1 K \times \dots \times e_s K$

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

Enostavni kolobarji

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

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

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

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

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

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

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

$\Rightarrow I \in I$

$S \subseteq R \quad a, b \in R$

$a S b$

Naj bosta J in L leva ideala. z JL označimo grupo za seštevanje, generirano z elementi oblike jl

Kak je podgrupa za seštevanje

$M_{n_1}(D_1) \times \dots \times M_{n_2}(D_s)$

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

Ne vem zakaj je to tuki napisan

Lema: K kolobar. NSE:

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

ii) $\Leftrightarrow$ $\forall$ levi ideal $L.\ L^2 = \{0\} \Rightarrow L = \{0\}$

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

Dokaz:

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

$$a \in L \Rightarrow a\underbrace{Ka}_{\subseteq L} = \{0\} \Rightarrow a = 0 \Rightarrow L = \{0\}$$

ii) $\Rightarrow$ iii)

trivialno

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

$(KaK)^2$

$$\left(\sum x_i a y_i\right)\left(\sum z_i a w_i\right) = 0 \Rightarrow (KaK)^2 = 0 \Rightarrow$$

$$KaK = \{0\} \Rightarrow 0$$

$1 \in K$

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

Primer: Kolobar brez deliteljev niča je polprakolobar

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

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

$(0 \ldots 0, u_i, 0 . 0) = e_i u \in I$

Posledica: $K_1 \ldots K_s$ polprakolobarji $\Rightarrow K_1 \times \ldots \times K_s$ polprakolobar

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

Primeri

1) Enostavni kolobarji so polprakolobarji:

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

2) $T_n(K) = \left\{ \begin{bmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & & * \end{bmatrix} \right\}$ ni polprakolobar

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

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

Primer: 1. Vse končnorazsežne algebre so levi artinski kolobarji.
Levi ideali so podprostori, saj $\lambda l = (\lambda \cdot 1) l \in L$

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

3. $K_1, \dots K_s$ levi artinski kolobarji $\Rightarrow K_1 \times \dots \times K_s$ l. artinski kol.
Levi ideal je oblike $L_1 \times \dots \times L_s$ $\quad L_i \triangleleft K_i$ levi ideal

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

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

$e \in K$ idempotent $\Rightarrow eKe = \{exe \,;\, x \in K\}$ kolobar z enoto e

..... kotni kolobar

Primer:

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

Lema:

1) K polpraktolobar $\Rightarrow eKe$ polpraktolobar

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

Dokaz:

1) $eae \in eKe$

$$eae \cdot exe \, eae = 0 \quad (a \in K.\ aKa = \{0\} \Rightarrow a = 0)$$

predpostavke

$$\| $$

$$(eae)x(eae) \Rightarrow eae = 0 \Rightarrow eKe \text{ polpraktolobar}$$

K polpraktolobar

2)

$L_1 \supseteq L_2 \supseteq \ldots$ levi ideali v eKe

$KL_1 \supseteq KL_2 \supseteq \ldots$ levi ideali v K

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

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

??

Lema

e in $f \neq 0$ ortogonalna idempotenta kolobarja K

$\Rightarrow \quad K(1-e) \supset K(1-e-f)$

Dokaz:

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

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

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

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

Primer: 1. Standardne matrične enote

2. $\{S E_{ij} S^{-1}\}$

Lema: Naj bo $\{e_{ij}\,;\ 1 \leq i,j \leq n\}$ množica $n \times n$ matričnih enot kolobarja K. Potem velja

$$K \cong M_n(e_{11} K e_{11})$$

Dokaz:

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

$$\varphi : K \longrightarrow M_n(e_{11} K e_{11})$$
$$a \longmapsto a_{ij}$$

$\varphi(ab) = \varphi(a)\varphi(b)$

(i,j)-ti člen od $\varphi(a)\varphi(b) = \sum_{k=1}^{n} e_{1i}\, a \underbrace{e_{ki} e_{ik}}_{e_{kk}} b e_{ji}$

$e_{1i}\, a \big(\underbrace{\sum_{k=1}^{n} e_{kk}}_{=1}\big) b e_{ji} = e_{1i}\, ab\, e_{ji} =$ (i,j)-ti člen od $\varphi(ab)$

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

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

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

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

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

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

Lema: Levi artinski kolobar ima minimalni levi ideal

Dokaz: Naj bo $L_1 \neq \{0\}$ levi ideal. Če ni minimalni
$\exists L_2 . \{0\} \subset L_2 \subset L_1$. Če ta ni minimalni tako nadaljujemo
$L_1 \supset L_2 \supset L_3 \ldots$ ta veriga se nekoč ustavi $\blacksquare$

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

Dokaz: $L^2 \neq \{0\}$ ker je K polprakolobar

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

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

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

$\{0\} \subseteq M \subseteq L \overset{M \neq L}{\Rightarrow} M = \{0\}$ $\qquad e-1 \in M \Rightarrow e-1=0$

$\Rightarrow e^2 = e$

???

$L = Ke$

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

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

eKe je obseg

$0 \neq eae \in eKe$

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

$e = beae$ za nek $b \in K$

$e = ebe \cdot eae$ $\quad ebe$ je levi inverz za a

b ima iz enakega razloga levi inverz ece

$\Rightarrow b$ ima inverz

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

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

$0 \neq eafbe \in eKe$

eKe obseg $\Rightarrow \exists c \in K.\ \underbrace{eaf}_{u} \cdot \underbrace{f \cdot be \cdot ece}_{v} = e$

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

$vu \in fKf$, fKf obseg

Edina idempotenta sta 0 in f

$vu \neq 0$ ker $vu = 0 \Rightarrow uvu = eu = e = 0$

$\Rightarrow vu = f$

$\blacksquare$

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

Denimo, da je $e_i K e_i$ obseg in $e_1 K e_i \neq \{0\}$ za $\forall i$.

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

Dokaz:

Prejšnja lema

$\exists e_{1i} \in e_1 K e_i \; \exists e_{i1} \in e_i K e_1 . \; e_{1i} \cdot e_{i1} = e_1, \; e_{i1} \cdot e_{1i} = e_i$

$e_{ii} := e_i$

Izpolnjeni so vsi pogoji neke prejšnje leme.

Izrek (Wederburn-Artinov)

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

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

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

Dokaz:

2) $\Rightarrow$ 1) smo že

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

Torej ima minimalni levi ideal

Po eni lemi^4 $\exists e = e^2$. eKe je obseg

$e_1 = 1 \Rightarrow$ smo končali ($K \cong M_1(K)$)

naj bo $e_1 \neq 1$

Po neki lemi^3 $K \supset K(1-e_1)$

$(1-e_1)K(1-e_1)$ je levi artenski polpraskolobar (po lemi 2 (nekje))

lema4: $\exists e_2 = e_2^2 \in (1-e_1)K(1-e_1)$. $e_2(1-e_1)K(1-e_1)e_2$ je obseg

e_1, e_2 sta ortogonalna, ker

$e_2 \in (1-e_1)K(1-e_1)$

Lema3 $K(1-e_1) \supset K(1-e_1-e_2)$

lema4: $\exists e_3 \in (1-e_1-e_2)K(1-e_1-e_2)$.

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

ali pa $1 = e_1 + e_2$ ker pa je dovolj

e_3 je ortogonalen na e_1 in e_2

Ker je K levi artinski se postopek po končno mnogo korakih konča

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

e_iKe_i so obsegi $\forall i$ in $e_1 + \dots + e_n = 1$

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

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

To je ekvivalenca

- $e_iKe_i \neq \{0\}$ ker je obseg ($\{0\}$ nima enote)
- $e_i \sim e_j$ $e_j \sim e_i$

Recimo da $e_jKe_i = \{0\}$

potem $\underbrace{(e_iKe_j)K(e_iKe_j)}_{=0} = 0 \Rightarrow e_iKe_j = 0$ $\times$

ker je polpraskolobar

$e_i \sim e_j$ $e_j \sim e_k$ $e_i \sim e_k$

$e_iKe_j \neq 0 \xRightarrow{\text{lema5}} \exists u \in e_iKe_j \; \exists v \in e_jKe_i$.

$uv = e_i \wedge vu = e_j$

$uv = e_i \Rightarrow ue_jv = e_i$ $\quad ve_iu = e_j$ (ker $e_iu = u$, $u \in e_iKe_j$)

Recimo da $e_iKe_k = \{0\} \Rightarrow e_jKe_k =$

$= ve_i\underbrace{uKe_k}_{K} = \{0\}$ $\times$

$=0$

$E_1 \dots E_s$ naj bodo ekvivalenčni razredi

Naj bo f_i vsota vseh idempotentov v E_i

$f_i^2 = f_i$ in $f_i \cdot f_j = 0$

$f_1 + \dots + f_s = 1$

$f_ix = f_ix1 = f_ix(f_1 + \dots + f_s) = f_ixf_i$

podobno $xf_i = f_ixf_i \Rightarrow f_i \in Z(K)$

po lemi 1 $\Rightarrow K \cong f_1K \times \dots \times f_sK$

$f_iK \cong M_{n_i}(D_i)$

$\hookrightarrow D_i = e_iKe_i$

Posledica: Neničelni levi kolobar K je levi artinski

$\Leftrightarrow K \cong M_n(D)$ za nek $n \in \mathbb{N}$ in obseg D

Posledica: (Wedderburnov izrek)

Naj bo A neničelna končnorazsežna algebra.

Potem je A polpraalgebra $\Leftrightarrow A \cong M_{n_1}(D_1) \times \dots \times M_{n_s}(D_s)$

kjer so $n_i \in \mathbb{N}$ in D_i obsegi in končnorazsežne algebre

Definicija: Kolobar je polenostaven če zadošča

ekvivalentnima pogojema Wedderburn-Artinovega izreka

Lema: Naj bo D končnorazsežna algebra nad algebraično zaprtim poljem F. Če je D obseg $\Rightarrow D \cong F$

Dokaz: $n = \dim_F D$ $\quad a \in D \Rightarrow 1, a, a^2 \dots a^n$ so lin. odv.

$\lambda_0 + \lambda_1 a + \dots + \lambda_n a^{n-1} + a_n = 0 \Rightarrow$

$f(a)$ je polinom stopnje n $\quad f(x) = F[x]$

$f(x) = (x - \alpha_1) \dots (x - \alpha_n) \quad \alpha_i \in F$

$0 = f(a) = (a - \alpha_1 \cdot 1) \dots (a - \alpha_n \cdot 1) = 0$

en izmed teh mora biti 0, ker v obsegu ni deliteljev niča $\Rightarrow a = \alpha_i \cdot 1$

$\Rightarrow n = 1$

Posledica: Kompleksna končnorazsežna algebra A je polpraalgebra $\Leftrightarrow A \cong M_{n_1}(\mathbb{C}) \times \dots \times M_{n_s}(\mathbb{C})$

Naj bo D končno-razsežna realna algebra, ki je obseg

Primer: $\mathbb{R}, \mathbb{C}, \mathbb{H}, \dots ?$

Lema 1:

Za $\forall x \in D . \exists \alpha, \beta \in \mathbb{R} . x^2 + \beta x + \alpha \cdot 1 = 0$

Dokaz: Isto kot prejšnja lema + $\forall$ realen polinom je produkt linearih in kvadratnih

Dogovor: Namesto $\alpha \cdot 1$ pišemo samo α

$\mathbb{R} \cdot 1 = \mathbb{R}$ $\quad \mathbb{R}$ je enorazsežna podalgebra D

$V := \{ v \in D . v^2 \leq 0 \}$

(to pomeni: $v^2 = \alpha \cdot 1 \wedge \alpha \leq 0$)

iz prejšnje strani

Lema 2: Če sta $u,v \in V$ lin. neodv. $\Rightarrow u,v,1$ lin. neod

Dokaz: Denimo da so $u,v,1$ lin odv.

$$\exists\, \alpha,\beta \in \mathbb{R}.\quad 1+\alpha u = \beta v$$

$$1+2\alpha u+\alpha^2u^2=\beta^2v^2$$

če je $\alpha=0$

$$\Rightarrow 2\alpha u \in \mathbb{R} \Rightarrow u\in\mathbb{R} \vee v\in\mathbb{R}$$

$$\Rightarrow u^2=0 \Rightarrow u=0$$

ali

$$v^2=0 \Rightarrow v=0$$

$\blacksquare$

lahko je tudi kateri koli kolobar

Za elementa $u,v \in V$ $\quad u\circ v = uv+vu$ jordanski produkt

(ni asociativen, je pa komutativen)

u,v antikomutirata če $u\circ v=0$

Lema 3. Za $\forall u,v \in V$. $u \circ v \in \mathbb{R}$

Dokaz: Če sta u,v lin odvisna, je to očitno

$v = \alpha u \quad u \circ v = 2\alpha u^2 \in \mathbb{R}$

Drugače:

$W = \mathrm{Lin}\{u, v, 1\}$ ima dimenzijo 3

$(x+y)^2 = x^2 + x \circ y + y^2$

Po 1. lemi: $x \in W \Rightarrow x^2 \in W$

Zato $x \circ y = (x+y)^2 - x^2 - y^2 \in W$ (zaprtost za jordanski produkt)

$A : W \longrightarrow W$

$w \longmapsto w \circ u$ A je linearna in dimenzija je 3

$\Rightarrow$ A ima realno lastno vrednost λ

$w \circ u = \lambda w \qquad wu + uw = \lambda w$ za nek $w \neq 0$

$\Rightarrow \quad \overset{w^{-1}}{\cancel{w}}{}^{-1} u w = \lambda - u \quad /^2$

$u^2 = w^{-1} u^2 w = \lambda^2 - 2\lambda u + u^2$

ker $u^2 \in \mathbb{R}$ komutira z vsem

$\Rightarrow 2\lambda u \in \mathbb{R} \Rightarrow \lambda = 0$

$\Rightarrow uw + wu = 0$

$w = \lambda_1 + \lambda_1 u + \lambda_2 v \Rightarrow 2\lambda_0 u + 2\lambda_1 u^2 + \lambda_2 (u \circ v) = 0$

$\Rightarrow \lambda_2 \neq 0 \Rightarrow u \circ v \in \mathrm{Lin}\{1, u\}$

podobno $u \circ v \in \mathrm{Lin}\{1, v\} \Rightarrow u \circ v \in \mathrm{Lin}\{1\}$

$\Rightarrow u \circ v \in \mathbb{R}$