1. Deljivost v komutativnih kolobarjih

$xy = yx$

$1 \in K$

Gaussova števila!

polje

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

Cel kolobar - komutativen kolobar, brez deliteljev niča

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

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

v $F[X]$: $f(x) = p_1(x) \ldots p_s(x)$, kjer so $p_1 .. p_s$ 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 asocirana, 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 (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: $(\Leftarrow)$ $a = ub \wedge b = u^{-1}a$

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

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

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

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

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

$\nwarrow$ katero koli polje $\qquad$ (3 pa ni razcepen)

1.2 Glavni kolobarji

I ideal: • $I \leq (K,+)$

• $KI, IK \subseteq I$

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)

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

$\Rightarrow$ $a = gb$

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

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

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

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

$x \in I \Rightarrow x = \underset{\nwarrow \text{ sod}}{a_0} h(x)$ $\quad \underset{\nwarrow x \text{ ni sod}}{\times}$

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

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

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

$\underline{a = qb + r}$

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

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

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

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

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

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

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

$= |c-q|^2|b|^2 = (\underset{\frac{1}{4}}{\underset{\wedge|}{(u-k)^2}} + \underset{\frac{1}{4}}{\underset{\wedge|}{(v-l)^2}})|b|^2$

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

Izrek: $\forall$ evklidski kolobar je glavni kolobar

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

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

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

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

$\underline{I=(a)}$ $\quad$ $(a) \subseteq I$ 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:

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

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

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

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

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

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 $M \neq K \land M \subseteq I \triangleleft K \Rightarrow I = K \lor M = I$

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

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

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

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

i) in ii) ubistvu 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 $a = a_1, a_2, \ldots$ da je $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$
(Neskončno strogo naraščajoče zaporedje glavnih idealov)

Dokaz:

a ni nerazcepen

$a_1 = a_2 b_2$ $\quad a_2$ 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

$(a_1) \subsetneq (a_2)$ 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
$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ ustavi:

Torej $I_n = I_{n+1} = \ldots$ 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

$u, v \in I$

$\underline{u - v \in I}$

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

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

Hilbertov izrek o bazi

K noetrski $\Rightarrow K[x]$ noetrski

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

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

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

Definicija: Naj bo K komutativen kolobar.
$p \in K$ je praelement $p \neq 0$, p ni 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 $a = q_1 \cdots q_t$

$$\underbrace{p_1 | a \Rightarrow p_1}_{\text{nerazcepen + glavni kolobar} \Rightarrow \text{praelement}} | q_1 \cdots q_t \Rightarrow \exists i \in [t].\ p_1 | q_i \text{ . BSZS } p_1 | q_1$$

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

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

$p_2 \cdots p_s = u q_2 \cdots q_t$ 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 $M \to M$

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

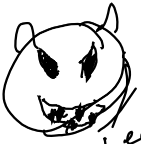
$\mathrm{End}\, M$ je kolobar če vpeljemo

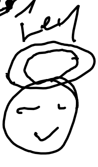
$$\varphi + \psi, \; \varphi \circ \psi : M \to M$$

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

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

Cay R





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

Dokaz: K kolobar

$a \in K.\ l_a : K \to K$

$x \mapsto ax$

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

$l_a \in End(K)$ ↖ K kot grupa za $+$

$\varphi : K \to End K$

$a \mapsto l_a$

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

$\uparrow$

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

Fija

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

$\uparrow$

$(ab)x = a(bx)$

Gay bey

$\downarrow$

Cay 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

$\mathrm{End}_F(V)$

Na podoben način dokažemo

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

$$\dim A \overset{=n}{<} \infty \qquad \overset{\swarrow \text{ matrike } n\times n \text{ nad } F}{M_n(F)}$$

$$A \hookrightarrow \mathrm{End}_F(A) \cong$$

A lahko vložimo v algebro lin. operatorjev končno razsežnega prostora

Posledica: $\forall$ končnorazsežno algebro A nad F lahko vložimo v algebro n×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 $(a,u) \mapsto au$ in $K\times M$ 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 $K \to \mathrm{End}(M)$

Dokaz: Naj bo M K-modul

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

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

$a\cdot u = \varphi(a)(u)$ ∎

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

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

Odslej modul = levi modul

Primeri:

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

2. Vsaka M aditivna grupa (=abelova grupa) je $\mathbb{Z}$-modul, če definiramo

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

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

$$0\cdot u = 0$$

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 $a \cdot u$ 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 operaciji sama modul.

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

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

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

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

Primeri:

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. $k = M_n(F)$ $\quad M = F^n$

$N \subseteq F^M$

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

$Au \in N$ 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

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

sta podmodula M oz. N

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

$M \cong N$: M izomorfna N

(obstaja izomorfizem)