

# 1. Deljivost v komutativnih klobarjih

$$xy = yx$$

$$1 \in K$$

Gaussova izreka!

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

Cel klobar - komutativen klobar, brez deliteljev  
nič

Osnovni izrek aritmetike  $n \in \mathbb{N}$ .  $n = p_1 p_2 \dots p_s$   
 $p_1, \dots, p_s \in \mathbb{P}$  prastevila endižno določena

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

## 1.1 osnovni pojmi

Definicija: Naj bo  $K$  komutativen kolobar.

1. element  $b \neq 0 \in K$  **deli** element  $a \in K$ , če

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

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

2. nenulna elementa  $a, b \in K$  sta **asociirana**,  
če delita drug drugega ali  $a \mid b$

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

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

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

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

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

$$a) p \neq 0 \wedge p \text{ ni obrnljiv}$$

$$b) p = ab \Rightarrow a \text{ je obrnljiv} \vee b \text{ je obrnljiv}$$

Element je **razcepen**

$$a) p \neq 0 \wedge p \text{ ni obrnljiv}$$

$$b) \text{ ni nerazcepen}$$

Odslej:  $K$  je cel

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

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

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

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

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

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

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

Primer: Ali je  $\mathbb{Z}$  nerazcepan element? Odvisno od kolobarja

$K = \mathbb{Z}$ : Ja

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

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

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

$\nearrow$  ker to koli pojje

(3 pa ni razcepan)

## 1.2 Glavni kolobarji:

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

$K$  komutativan

Definicija: Naj bo  $a \in K$ , množica  $(a) = \{ax; x \in K\}$

je glavni ideal (generiran z  $a$ )

(ideal je glavni, če je generiran z enim elementom)

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

$$\Rightarrow a = gb$$

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

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

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

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

2)  $K = (1)$

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

Ideal je **konageneriran**, 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  $(4, 6) \vee \mathbb{Z}$ ?  $(4, 6) = (2) = 2\mathbb{Z}$   
Edini ideali:  $\mathbb{Z}$  so  $n\mathbb{Z}$  (glavni ideali)

2.  $\vee F[X]$  ideali?

polinomi s konstantnim členom 0  $(X)$

$\vee$ si ideali so glavni

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

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

Ali je  $I$  glavni ideal?

npr  $I = (f(x))$

$2 = f(x)g(x) \Rightarrow f(x)$  je lahko samo

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

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

4)  $\vee F[X, Y]$  ideal iz polinomov s konstantnim členom z 0  $(X, Y)$  tudi ta ideal ni glavni

Definicija: Cel kolobar  $K$  je glavni kolobar,  
če je vsak njegov ideal glavn: (PID)

↑  
principle ideal domain  
↑?  
ni delitelj nič

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

Izreki: Naslednji kolobarji so evklidski:

a)  $\mathbb{Z}$

b)  $F[x]$ ,  $F$  polje

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

Dokaz:

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

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

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

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

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

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

$$a = qb + r$$

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

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

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

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

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

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

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

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

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

Izrek: V evklidski kolobar je glavni kolobar

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

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

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

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

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

Naj bo  $x \in I$  poljuben

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

$$\Rightarrow a \mid x$$

glavni ~~≠~~ evklidski  
kolobar kolobar



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

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

Dokaz:

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

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

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

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

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

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

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

Naslednji pogoji so ekvivalentni:

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

Dokaz: ii)  $\Leftrightarrow$  iii) Algebra 2

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

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

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

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

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

i) in ii) utrdva poveske isto

### 1.3 Endolčna faktorizacija

$$a \neq p_1 p_2 \dots p_n$$

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

Dokaz:

$a$  ni nerazcepen

$a_1 = a_2 b_2$   $a_2$  in  $b_2$  nista delnjiva

Vsej eden izmed njiju (npr  $a_2$ ) ni produkt nerazcepnih

$a_2 = a_3 b_3$ ;  $a_3$  ni produkt nerazcepnih

$(a_1) \subsetneq (a_2)$  saj če  $(a_1) = (a_2) \Rightarrow a_1 = a_2 u$   
 $\Rightarrow u = b_2$  je deljiv  $\times$

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

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

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

Lema: V glavnih klobar je noetrski

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

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

$u, v \in I$

$u-v \in I$

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

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

Hilbertov izrek o bazi

$K$  noetrski  $\Rightarrow K[x]$  noetrski

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

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

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

Definicija: Naj bo  $K$  komutativen kolobar.

$p \in K$  je **praelement**  $p \neq 0$ , pri obrnljiv in  
velja  $plab \Rightarrow pla \vee plb \quad \forall a, b \in K$

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

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

1)

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

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

$$uy = 1$$

2) Naj bo  $K$  glavni

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

$p$  ne bo nerazcepen.  $p$  praelement

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

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

$$1 = px + ay$$

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

Definicija: Cel kolobar  $K$  imenujemo **kolobar z evolično faktorizacijo (UFD)**,

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

- obstajajo kti nerazcepni elementi  $p_i$ ,  
da je  $a = p_1 \dots p_s$
- ta faktorizacija je evolična do asociiranosti  
in vrstnega reda faktorjev natanko
- To pomeni:  $a = z_1 \dots z_t$ ;  $z_i$  nerazcepni  
 $\Rightarrow s = t \quad \exists \pi \in S_n$ .  $z_{\pi(i)}$  asociiran z  $p_i$

Izrek: V glavnem kolobar je kolobar z evolično faktorizacijo

Dokaz:  $a \neq 0$  ni obrnljiv.

Vemo iz prvih dveh lemm:  $a$  je produkt nerazcepnih

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

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

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

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

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

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

## 2. Modeli

### 2.1. Caylyjev izrek za kolobarje

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

Aditivna grupa

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

$$\varphi \in \text{End } M \iff \varphi: M \rightarrow M; \varphi(u+v) = \varphi(u) + \varphi(v)$$

$\text{End } M$  je kolobar če vpeljemo

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

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

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

Cay R



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

Dokaz:  $K$  kolobar

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

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

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

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

$$a \mapsto l_a$$

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

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

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

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

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

injektivnost:

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

Fija

Glej

$\mathbb{F}$

(univ)



Naj bo  $A$  algebra nad poljem  $F$

$V$  vektorski prostor nad  $F$

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

Napodoben namir dokazemo

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

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

$$\dim A < \infty$$

$$M_n(F)$$

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

Posledica:  $\forall$  končno razsežna algebra  $A$  nad  $F$  lahko vložimo v algebra  $n \times n$  matrike za nek  $n \in \mathbb{N}$   
 $M_n(F)$

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

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

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

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

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

## 2.2 Definicija modula

Definicija: Naj bo  $K$  kolobar. množica  $M$

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

in  $K \times M \rightarrow M$  in binarno operacijo

$M \times M \rightarrow M : (u, v) \mapsto u+v$  je **modul nad  $K$**

ali  **$K$ -modul**, če velja:

- 1)  $(M, +)$  je abelova grupa
- 2)  $(a+b)u = au + bu \quad \forall a, b \in K, \forall u \in M$
- 3)  $a(u+v) = au + av \quad \forall a \in K, \forall u, v \in M$
- 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 skalari:

ali tudi **modulsko množenje**

Opomba: Pojem  $K$ -modula  $M$  je ekvivalenten

pojmu homomorfizma kolobarjev  $K \rightarrow \text{End}(M)$

Dalje: Naj bo  $M$   $K$ -modul

$$\varphi: K \rightarrow \text{End}(M): a \mapsto (u \mapsto au)$$

Naj bo  $\varphi$  homomorfizem.  $\varphi: K \rightarrow \text{End}(M)$

postane  $M$   $K$ -modul, če definiramo

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



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

Naj bo  $M$  levi  $K$ -modul. Če definiramo

$ua := au$  je to potem desni  $K$ -modul, če je  
 $K$  komutativen

Odslej modul = levi modul

Primeri:

1.  $K=F$  potem je  $F$ -modul = vekt. prostor nad  $F$
2. Vseke  $M$  additive skupine (= abelova grupa) je  $\mathbb{Z}$ -modul, če definiramo

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

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

$$0 \cdot u = 0$$

3.  $\forall$  klobar  $K$  postane modul nad semim območje, če definiramo  $a \cdot u$  kot običajni produkt  $a \cdot u \in K$

4. Naj bo  $I$  levi ideal  $K$

$I$  je  $K$ -modul, če je  $a \cdot u$  običajni produkt

5. Naj bo  $K$  podklobar  $K'$ . Če  $a \cdot u$  označuje množenje v  $K'$ , je  $K'$   $K$ -modul

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

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

7. Trivialni ali ničelni modul

## 2.3 Osnovni pojmi teorije moduler

### Podmoduli

Podmodul je podmnožica, ki je za isti operaciji sama modul.

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

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

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

Primeri:  
1. če je  $V$  vekt. prostor nad  $F$  je podmodul = podprostor

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

3. Podmodul  $K$ -modula  $K$  so levi ideali

če sta  $N_1$  in  $N_2$  podmoduli je tudi  
 $N_1 \cap N_2$  in  $N_1 + N_2$  podmoduli

Def: če sta  $\{0\}$  in  $M$  edini podmoduli  $M$   
rečemo da je  $M$  **enostaven**

Primeri:

1. V. prostor je enostaven modul  $\Leftrightarrow$  je 1-rozsečen

2. Aritmetična grupa je enostaven kot  $\mathbb{Z}$ -modul  $\Leftrightarrow \cong \mathbb{Z}_p$

3  $K = M_n(F)$   $M = J^n$

$$M \subseteq F^n$$

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

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

$M$  je enostaven modul nad matrikami;

## Homomorfizmi: moduli

$M, N$   $K$ -moduli

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

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

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

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

Rečemo jim tudi  $K$ -linearne preslikave

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

sta podmoduli  $M$  oz.  $N$

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

$$M \cong \ker \varphi \oplus \text{izobarizem } M$$

(obstaja izomorfizem)