1. Deljivost v komutativnih kolobarjih

$xy = yx$

$1 \in K$

Gaussova števila!

polje

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

Cel kolobar – komutativen kolobar, brez deliteljev niča

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

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

v $F[X]$: $f(X) = p_1(X) \cdots p_s(X)$, 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: $(\Leftarrow)$ $a = ub$ $\wedge$ $b = u^{-1}a$

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

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

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

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

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

Primer: Ali je 2 nerazcepen element? Odvisno od kolobarja

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

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

ker je to kdi 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)

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

$\Rightarrow a = gb$

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

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

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

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

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

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

$x \in I \Rightarrow \underset{\text{ni sod}}{x} \not= \underset{\text{sod}}{a_0} h(x)$

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

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