Lineare Algebra II

- Kuhlmann -

- 5. Vorlesung -

Am 30.04.2012.

Definition 1. Ein K-Unterraum $M \subseteq K[x]$ ist ein **Ideal** wenn gilt:

$$\forall f \in K[x],\ g \in M \text{ ist } fg \in M.$$

Bsp 0 $M = K[x]$; $M = \{0\}$ sind Ideale

Bsp 1 Sei $d \in K[x]$, $d \neq 0$

$$M := dK[x] = \{df ;\ f \in K[x]\}$$

ist ein Ideal s.d. $1 \in M$, $c \in K$ } Unterraum

$$\underbrace{c(df)}_{\in M} - \underbrace{dg}_{\in M} = \underbrace{d(cf-g)}_{\in M}.$$

$f \in K[x]$ $dg \in M \Rightarrow f(dg) = \underbrace{d(fg)}_{\in M}$ ∎

Definition 2 $dK[x]$ heißt **Hauptideal** (mit Erzeuger d).

Bsp 2 (endlich erzeugtes Ideal)

Seien $d_1, \dots, d_\ell \in K[x]$

$$M := d_1 K[x] + \dots + d_\ell K[x]$$

ist K-Unterraum. Es ist ein Ideal:

Sei $p \in M$; $p = d_1 f_1 + \dots + d_\ell f_\ell$; sei $f \in K[x]$
$f_1, \dots, f_\ell \in K[x]$

dann ist $pf = d_1 \underbrace{(f_1 f)}_{\in K[x]} + \dots + d_\ell \underbrace{(f_\ell f)}_{\in K[x]} \in M$

Definition 3 M ist endlich erzeugtes Ideal (mit Erzeugern $d_1, \dots, d_\ell$).

weitere Beispiele: siehe ü B.

Satz 1. Sei $0 \neq M \subseteq K[x]$ Ideal.

$\exists!$ normierte Polynom $d \in K[x]$ s.d.

$M = d K[x]$

Beweis $\exists^z$: Sei $d \neq 0$; $d \in M$; $\deg d$ minimal, und $\in$ d normiert.

Sei $f \in M$. (DA) $\Rightarrow$ $f = dq + r$ $\quad \overbrace{r = f - dq}^{\in M}$
$r = 0$ oder $\deg r < \deg d$. Aber

Also muss $r = 0$ und damit $f = dq$ ∎

∃! : Sei g normiert s.d $M = gK[x]$

Also ∃ $0 \neq p, q \in K[x]$ s.d

$$\left.\begin{array}{l} d = gp \text{ und} \\ g = dq \end{array}\right\} \text{ also } d = dqp;$$

es folgt: $\deg d = \deg d + \deg p + \deg q$.

Also $\deg p = \deg q = 0$; p, q sind Skalarpolynome. Nun sind g und d normiert, also $p = q = 1$, also $d = g$. ∎

Korollar 1 Das normierte Erzeugerd vom Ideal

$$p_1 K[x] + \dots + p_\ell K[x]$$

ist der $ggT(p_1, \dots, p_\ell)$; d.h.

$d \mid p_i$ $1 \leq i \leq \ell$ und aus $d_0 \mid p_i$ $d_0 \in K[x]$ $1 \leq i \leq \ell$ folgt $d_0 \mid d$.

Beweis $dK[x] = p_1 K[x] + \dots + p_\ell K[x]$

also $d \mid p_i$ $1 \leq i \leq \ell$. Ferner $d \in M$ also

$$d = p_1 q_1 + \dots + p_n q_n$$

$$= d_0 [g_1 q_1 + \dots + g_n q_n] \quad \square$$

Definition 4 $p_1, \dots, p_e$ seien relativ prim wenn

$$ggT(p_1, \dots, p_e) = 1$$

(äquiv: $p_1 K[x] + \dots + p_e K[x] = K[x]$)

§ Primzerlegung (Primfaktorisierung)

Definition 5 $f \in K[x]$ ist reduzible über K wenn es $g, h \in K[x]$ gibt, $\deg g \geq 1$, $\deg h \geq 1$ und $f = gh$

Sonst ist f irreduzible. Ist f irreduzible und $\deg f \geq 1$ so nennen wir f Primpolynome über K.

Bem f reduzible $\Rightarrow \deg f \geq 2$

Bsp $f = x^2 + 1$ reduzible über $\mathbb{C}$

$= (x+i)(x-i)$

aber irreduzible über $\mathbb{R}$.

Satz 2 $p, f, g \in K[x]$, p Primpol.

Aus $p \mid fg$ folgt $p \mid f$ oder $p \mid g$

Beweis OE p normiert, p irreduzible $\Rightarrow$ die einzige

normierte Teiler von p sind 1 und p.

Sei $d := ggT(f, p)$, insbesondere $d = 1$ oder $d = p$.

Falls $d = p$ dann $p \mid f$.

Wenn $d = 1 \Rightarrow 1 = p_0 p + f_0 f$

$p_0, f_0 \in K[x]$ also

$$g = f_0 fg + p_0 pg$$

und $p \mid fg$, $p \mid p(p_0 g)$ $\Rightarrow p \mid g$. ∎

Korollar 2 p Prumpol, $p \mid f_1 \cdots f_\ell$

$\Rightarrow \exists i \in \{1, \ldots, \ell\}$ sd $p \mid f_i$.

Satz 3 Sei $f \in K[x]$, f normiert, $\deg f \geq 1$.

Dann ist f Produkt von normierten Prumpolynomen.

Diese Darstellung ist eindeutig, bis auf

Umnumerierung.

Beweis: $\exists^Z$ $\deg f = 1 \Rightarrow f$ irred. nichts weiter z.Z.

Sei nun $\underbrace{\deg f}_{:= n} > 1$. Beweis per Induktion nach n.

Ist f irreduz. dann nichts weiter z.z.

Sonst $f = gh$ $\quad n > \deg g \geq 1$

$\quad n > \deg h \geq 1$

IA gilt für g, h und damit bekommen wir eine Faktorisierung für f.

Eindeutigkeit. Sei

$$f = p_1 \cdots p_\ell = q_1 \cdots q_s.$$

p_i, q_i normierte prim.

Also $p_\ell \mid q_1 \cdots q_s$; es folgt

$p_\ell \mid q_j$ für ein gewisses $1 \leq j \leq s$

p_ℓ, q_j normierte prim $\Rightarrow q_j = p_\ell$

OE nach Umnummerierung bekommen wir

$$p_\ell = q_s \quad (*)$$

und somit

$$P := p_1 \cdots p_{\ell-1} = q_1 \cdots q_{s-1}$$

$\deg(P) < n$, also IA gilt

d.h $q_1, \dots, q_{s-1}$ ist Umnumerierung von

$P_1, \dots, P_{\ell-1}$. Diese Tatsache zusammen mit ⊛

beweist unsere Behauptung. ∎