5. Script zur Vorlesung: Lineare Algebra II

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory

SS 2012: 30. April 2012

Definition 1 Ein K-Unterraum $M \subseteq K[x]$ ist ein *Ideal*, wenn gilt: Für alle $f \in K[x]$ und $g \in M$ ist $fg \in M$.

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

Beispiel 1 Sei $d \in K[x]$ und $d \neq 0$. $M := dK[x] = \{df; f \in K[x]\}$ ist ein Ideal:

$$\left.\begin{array}{l} d1 \in M; c \in K \\ \underbrace{c(df)}_{\in M} - \underbrace{dg}_{\in M} = \underbrace{d(cf-g)}_{\in M} \end{array}\right\} \text{ Unterraum}$$

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

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

Beispiel 2 (Endlich erzeugtes Ideal)
Seien $d_1, \ldots, d_\ell \in K[x]$. $M := d_1K[x] + \cdots + d_\ell K[x]$ ist ein K-Unterraum. Es ist ein Ideal.

Sei $p \in M, p = d_1f_1 + \cdots + f_\ell f_\ell$ mit $f_1, \ldots, f_\ell \in K[x]$ und sei $f \in K[x]$, dann ist $pf = d_1 \underbrace{(f_1, f)}_{\in K[x]} + \cdots + d_\ell \underbrace{(f_\ell, f)}_{\in K[x]} \in M$.

Definition 3 M ist ein *endlich erzeugtes Ideal* (mit den Erzeugern $d_1, \ldots, d_\ell$).
Weitere Beispiele siehe Übungsblatt.

Satz 1 Sei $0 \neq M \subseteq K[x]$ ein Ideal. Es existiert genau ein normiertes Polynom $d \in K[x]$, so dass $M = dK[x]$.

Beweis **Existenz:** Sei $d \neq 0$ und $d \in M$, deg d ist minimal und ohne Einschränkung d normiert.
Sei $f \in M$. (Divisionsalgorithmus) $\Rightarrow f = dq + r$, mit $r = 0$ oder $\deg r < \deg d$.

Aber $\underbrace{r = f - dq}_{\in M}$. Also muss $r = 0$ und damit $f = dq$ sein.

Eindeutigkeit: Sei g normiert, so dass $M = gK[x]$ ist. Also existieren $0 \neq p, q \in K[x]$, so dass $d = gp$ und $g = dq$, also $d = dqp$ ist. 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 Der normierte Erzeuger d vom Ideal $p_1K[x] + \cdots + p_\ell K[x]$ ist der größte gemeinsame Teiler von $(p_1, \ldots, p_\ell)$ (bezeichnet mit ggT $(p_1, \ldots, p_\ell)$), das heißt $d \mid p_i$ mit $1 = i = \ell$ und aus $d_0 \mid p_i$ mit $d_0 \in K[x]$ und $1 \leq i \leq \ell$ folgt $d_0 \mid d$.

Beweis $dK[x] = p_1K[x] + \cdots + p_\ell K[x]$, also $d \mid p_i$ mit $1 \leq i \leq \ell$. Ferner ist $d \in M$, also $d = p_1q_1 + \cdots + p_nq_n = d_0[g_1q_1 + \cdots + g_nq_n]$.

Definition 4 $p_1, \ldots, p_\ell$ sind *relativprim*, wenn ggT $(p_1, \ldots, p_e) = 1$ ist (äquivalent: $p_1K[x] + \cdots + p_\ell K[x] = K[x]$).

§ 5 Primzerlegung (Primfaktorisierung)

Definition 5 $f \in K[x]$ ist reduzibel über K, wenn es $g, h \in K[x]$ gibt mit deg $g \geq 1$, deg $h \geq 1$ und $f = gh$. Sonst ist f irreduzibel. Ist f irreduzibel und deg $f \geq 1$, so nennen wir f Primpolynome über K.
Bemerkung: f reduzibel $\Rightarrow$ deg $f \geq 2$.

Beispiel $f = x^2 + 1 = (x + i)(x - i)$ ist reduzibel über $\mathbb{C}$, aber irreduzibel über $\mathbb{R}$.

Satz 2 $p, f, g \in K[x]$, p ist ein Primpolynom. Aus $p \mid fg$ folgt $p \mid f$ oder $p \mid g$.

Beweis Ohne Einschränkung ist p normiert, so dass p irreduzibel $\Rightarrow$ die einzigen normierten 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 ist ein Primpolynom. $p \mid f_1 \cdots f_\ell \Rightarrow$ es existiert ein $i \in \{1, \ldots, \ell\}$, so dass $p \mid f_i$.

Satz 3 Sei $f \in K[x]$, f normiert und deg $f \geq 1$. Dann ist f ein Produkt von normierten Primpolynomen. Diese Darstellung ist eindeutig, bis auf Umnummerierung.

Beweis **Existenz:** deg $f = 1 \Rightarrow f$ irreduzibel. Es ist nichts weiter zu zeigen.
Sei nun deg $f > 1 := n$ - Beweis per Induktion nach n. Ist f irreduzibel, dann ist nichts weiter zu zeigen.
Sonst $f = gh$ mit $n >$ deg $g \geq 1$ und $n >$ deg $h \geq 1$. Die Induktionsannahme 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 sind normierte Prim. Also $p_\ell \mid q_1 \cdots q_s$. Es folgt $p_\ell \mid q_j$ für eine gewisse $1 \leq j \leq s$. p_ℓ, q_j sind normierte Prim $\Rightarrow q_j = p_\ell$. Ohne Einschränkung nach Umnummerierung bekommen wir $p_\ell = q_s$ $(*)$
Und somit $P := p_1 \cdots p_{\ell-1} = q_1 \cdots q_{s-1}$. deg $(P) < n$. Also gilt die Induktionsannahme, das heißt $q_1, \ldots, q_{s-1}$ ist die Umnummerierung von $p_1, \ldots, p_{\ell-1}$. Diese Tatsache zusammen mit $(*)$ beweist unsere Behauptung. □