10 Script zur Vorlesung: Lineare Algebra II

Prof. Dr. Salma Kuhlmann

In diesem Skript untersuchen wir weiter den Ring $K[x]$. Wir werden feststellen, das $K[x]$ viele Eigenschaften hat wie der Ring Z. Diese Eigenschaften von Z haben wir in der Vorlesung LA I Skripte 1-4 studiert und bewiesen; die Beweise hier sind sehr ähnlich. Wir zeigen u.a. das jedes Ideal in $K[x]$ ein Hauptideal ist. Dafür werden wir Satz 8.4 (DA) verwenden. In Abschnitt 6 beenden wir vorerst unsere Untersuchung von $K[x]$: Wir etablieren das auch in $K[x]$ die Primfaktorisierung gilt. Somit beenden wir Kapitel I.

Definition 10.1. Seien $p_1, \ldots, p_\ell \in K[x]$. Ein Polynom $d \in K[x]$ ist der *größte gemeinsame Teiler* von $p_1, \ldots, p_\ell$, bezeichnet mit $\mathrm{ggT}(p_1, \ldots, p_\ell)$, wenn:

1. $\forall 1 \leq i \leq \ell$: $d \mid p_i$ und
2. Wenn auch $d_0 \in K[x]$ 1. erfüllt, dann gilt auch $d_0 \mid d$.

Definition 10.2.
$p_1, \ldots, p_\ell$ sind *relativprim*, wenn ggT $(p_1, \ldots, p_\ell) = 1$ ist.

Definition 10.3.
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 10.4.
Sei $d \in K[x]$. Dann ist $M := dK[x] = \{df; f \in K[x]\}$ ein Ideal:

- $df \in M;\ dg \in M;\ c \in K \Rightarrow c(df) - dg = d(cf - g) \in M$, also ist M ein Unterraum.
- $f \in K[x]$ und $dg \in M \Rightarrow f(dg) = d(fg) \in M$.

Definition 10.5.
$< d > := dK[x]$ heißt *Hauptideal* mit Erzeuger d.

Beispiel 10.6.
$K[x] =< 1 >$ und $\{0\} =< 0 >$ sind Hauptideale.

Beispiel 10.7.
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 $p \in M, p = d_1 f_1 + \cdots + d_\ell f_\ell$ 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 10.8.
Das Ideal $d_1K[x] + \cdots + d_\ell K[x]$, bezeichnet mit $< d_1, \ldots, d_\ell >$, ist ein *endlich erzeugtes Ideal*, mit Erzeugern $d_1, \ldots, d_\ell$.

Weitere Beispiele siehe Übungsblatt.

Satz 10.9.
Sei $0 \neq M \subseteq K[x]$ ein Ideal. Es existiert genau ein normiertes Polynom $d \in K[x]$, so dass $M =< d >$.

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

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

Eindeutigkeit: Sei g normiert, so dass $M = gK[x]$ ist. Somit 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. Daher gilt deg $p =$ deg $q = 0$; p, q sind Skalarpolynome. Nun sind g und d normiert, also $p = q = 1$ und damit $d = g$. □

Korollar 10.10.
Der normierte Erzeuger d vom Ideal $< p_1, \ldots, p_\ell >$ ist ggT$(p_1, \ldots, p_\ell)$. Insbesondere, wenn $p_1, \ldots, p_\ell$ relativprim sind, dann ist $< p_1, \ldots, p_\ell >= K[x]$

Beweis:

1. $< d >= dK[x] =< p_1, \ldots, p_\ell >$, also $p_i \in< d >$ für alle $1 \leq i \leq \ell$ und folglich $d \mid p_i$.
2. Sei $d_0 \in K[x]$ so, dass $d \mid p_i$ für alle $1 \leq i \leq \ell$. Es gibt also $g_i \in K[x]$ mit $p_i = d_0 g_i$ für alle $1 \leq i \leq \ell$. Nun ist $d \in< p_1, \ldots, p_\ell >$, also $d = p_1q_1 + \ldots + p_\ell q_\ell = d_0[g_1q_1 + \ldots + g_\ell q_\ell]$.

□

§ 5 Primzerlegung (Primfaktorisierung)

Definition 10.11.
$f \in K[x]$ 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*.
Bemerkung: f reduzibel $\Rightarrow \deg f \geq 2$.

Beispiel 10.12.
$f = x^2 + 1 = (x+i)(x-i)$ ist reduzibel über $\mathbb{C}$, aber irreduzibel über $\mathbb{R}$, weil es keine reellen Nullstellen hat.

Weitere Beispiele siehe Übungsblatt.

Satz 10.13.
Seien $p, f, g \in K[x]$, p ist ein Primpolynom. Aus $p \mid fg$ folgt $p \mid f$ oder $p \mid g$.

Beweis:
Setze $d := \mathrm{ggT}(f, p)$. Ohne Einschränkung ist p normiert und p irreduzibel. Folglich sind 1 und p die einzigen normierten Teiler von p. Damit ist $d = 1$ oder $d = p$. Aus Korollar 10.10 folgt außerdem, dass $p_0, f_0 \in K[x]$ existieren so dass $d = p_0 p + f_0 f$.

- Wenn $d = p$, dann $p \mid f$.
- Wenn $d = 1$, dann ist $1 = p_0 p + f_0 f$, also $g = f_0(fg) + p(p_0 g)$. Nun gilt $p \mid fg$, $p \mid p(p_0)g$ und daraus folgt $p \mid g$. □

Korollar 10.14.
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 10.15.
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 $n := \deg f > 1$ — 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 $f = p_1 \cdots p_\ell = q_1 \cdots q_s$. Nun sind für alle i die p_i, q_i normierte Primpolynome. Also $p_\ell \mid q_1 \cdots q_s$. Es folgt $p_\ell \mid q_j$ für ein gewisses $1 \leq j \leq s$. Da p_ℓ, q_j beide normierte Primpolynome sind folgt $q_j = p_\ell$.
- Ohne Einschränkung nach Umnummerierung bekommen wir $p_\ell = q_s$ $(*)$
  Somit $P := p_1 \cdots p_{\ell-1} = q_1 \cdots q_{s-1}$.
- Die Induktionsannahme gilt für P, weil $\deg(P) < n$. Das heißt $q_1, \ldots, q_{s-1}$ ist eine Umnummerierung von $p_1, \ldots, p_{\ell-1}$.

Diese letzte Aussage zusammen mit $(*)$ beweist unsere Behauptung. □