5 Script zur Vorlesung: Lineare Algebra II (SoSe 2020)

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 $\mathbb{Z}$. Diese Eigenschaften von $\mathbb{Z}$ 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 3.4 (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 5.1.
Seien $P_1, \cdots, p_\ell \in K[x]$. Ein Polynom $d \in K[x]$ ist der *größte gemeinsame Teiler von* $p_1, \ldots, p_\ell$, bezeichnet mit 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 5.2.
$p_1, \ldots, p_\ell$ sind *relativprim*, wenn ggT $(p_1, \ldots, p_e) = 1$ ist

Definition 5.3.
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 5.4.
Sei $d \in K[x]$. Setze $M := dK[x] = \{df \,;\, f \in K[x]\}$ ist ein Ideal:
• $df \in M \,;\, dg \in M \,;\, c \in K \to c(df) - dg = d(cf - g) \in M$, also ist M ein Unterraum.
• $f \in K[x]$ und $dg \in M \Rightarrow f(dg) = d(fg) \in M$.

Definition 5.5.
$< d >:= dK[x]$ heißt *Hauptideal* mit Erzeuger d.

Beispiel 5.6.
$K[x] =< 1 >$ und $\{0\} =< 0 >$ sind Hauptideale.

Beispiel 5.7.
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 $p \in M, p = d_1 f_1 + \cdots + f_\ell f_\ell$ mit $f_1, \ldots, f_\ell \in K[x]$ und sei $f \in K[x]$,
dann ist $pf = d_1 \underbrace{(f_{1f})}_{\in K[x]} + \cdots + d_\ell \underbrace{(f_{\ell f})}_{\in K[x]} \in M$.

Definition 5.8.
Das Ideal $d_1K[x] + \cdots + d_\ell K[x]$, bezeichnet mit $< d_1, \cdots, d_\ell >$, ist ein *endlich erzeugtes Ideal*, mit Erzeugern $d_1, \ldots, d_\ell$.

Weitere Beispiele: siehe Übungsblatt.

Satz 5.9.
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 ist minimal und ohne Einschränkung d ist 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 5.10.
Der normierte Erzeuger d vom Ideal $< p_1, \cdots, p_\ell >$ ist der ggT $(p_1, \ldots, p_\ell)$. Insbesondere, wenn $p_1, \ldots, p_\ell$ relativprim sind, dann ist $< p_1, \cdots, p_\ell >= K[x]$.

Beweis:

1. $< d >= dK[x] =< p_1, \cdots, p_\ell >$, also $p_i \in< d >$ für alle $1 \leq i \leq \ell$, also $d \mid p_i$ für alle $1 \leq i \leq \ell$.
2. Sei $d_0 \in K[x]$ so dass $d_0 \mid p_i$ für alle $1 \leq i \leq \ell$. Es gibt also $g_i \in K[x]$ so dass $p_i = d_0 g_i$ für alle $1 \leq i \leq \ell$. Nun $d \in< p_1, \cdots, p_\ell >$, also $d = p_1 q_1 + \cdots + p_n q_n = d_0[g_1 q_1 + \cdots + g_n q_n]$.

□

§ 5 Primzerlegung (Primfaktorisierung)

Definition 5.11.
$f \in K[x]$ 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 5.12.
$f = x^2 + 1 = (x + i)(x - i)$ ist reduzibel über $\mathbb{C}$, aber irreduzibel über $\mathbb{R}$, weil es keine reelle Nullstellen hat.

Weitere Beispiele: siehe Übungsblatt.

Satz 5.13.
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 $d :=\mathrm{ggT}(f, p)$. OE ist p normiert, und p irreduzibel $\Rightarrow$ die einzigen normierten Teiler von p sind 1 und p. Also ist $d = 1$ oder $d = p$. Aus Korollar 5.10 folgt ausserdem dass: $\exists p_0, f_0 \in K[x]$ so dass $d = p_0p + f_0f$

- Wenn $d = p$, dann $p \mid f$.
- Wenn $d = 1$, dann ist $1 = f_0f + p_0p$, also $g = f_0(fg) + p(p_0g)$. Nun $p \mid fg$, $p \mid p(p_0g) \Rightarrow p \mid g$. □

Korollar 5.14.
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 5.15.
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 eine gewisse $1 \leq j \leq s$. Da p_ℓ, q_j beide normierte Primpolynome sind folgt $q_j = p_\ell$.
- OE nach Umnummerierung bekommen wir $p_\ell = q_s$ $(*)$
Und somit $P := p_1 \cdots p_{\ell-1} = q_1 \cdots q_{s-1}$.
- Die Induktionsannahme gilt für P da $\deg (P) < n$. 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. □