Wichtige Sätze und Definitionen zu
§5: Polynomalgebren und Ideale
aus der Vorlesung:

LV-NR	150 239
Veranstaltung	Diskrete Mathematik II, 4.0 std
Dozent	Holtkamp, R.

5.1
(i) Ist V ablesche Gruppe (bzgl. $+$), K Körper, so heißt V zusammen mit

$$\begin{aligned} \cdot : K \times V &\to V \\ (\lambda, v) &\mapsto \lambda \cdot v \end{aligned}$$

K-Vektorraum *genau dann, wenn*

$$\begin{aligned} \lambda \cdot (v + w) &= \lambda \cdot v + \lambda \cdot w, \\ (\lambda + \mu) \cdot v &= \lambda \cdot v + \mu \cdot v, \\ \lambda \cdot (\mu \cdot v) &= (\lambda\mu) \cdot v, \\ \text{und } 1_K \cdot v &= v \end{aligned}$$

für alle $\lambda \in K,\ v, w \in V$ gilt.

(Homomorphismen: lineare Abbildungen)

(ii) Ein K-Vektorraum V zusammen mit Verknüpfung $\circ : V \times V \to V$ heißt **K-Algebra** *genau dann, wenn $\circ$ assoziativ ist und außerdem K-**bilinear**, d.h.*

$$\begin{aligned} (v_1 + v_2) \circ w &= v_1 \circ w + v_2 \circ w, \\ (\lambda \cdot v) \circ w &= \lambda \cdot (v \circ w), \\ v \circ (w_1 + w_2) &= v \circ w_1 + v \circ w_2, \\ v \circ (\lambda \cdot w) &= \lambda \cdot (v \circ w) \end{aligned}$$

Bemerkung: Also ist V versehen mit einer Ringstruktur (bezüglich der Multiplikation $\circ$, die in jedem Argument linear ist). Meist schreibt man $\cdot$ statt $\circ$.

(Von **K-Algebrahomomorphismen** *verlangt man, dass sie lineare Abbildungen und Ringhomomorphismen sind.)*

5.2
*Ist V K-Vektorraum, $\emptyset \neq B \subseteq V$, so heißt B eine K-**Vektorraumbasis** (kurz K-Basis) von $V \iff B$ ist Erzeugendensystem ($\forall\ v \in V \exists$ Darstellung $v = \sum_{i=1}^{r} \lambda_i w_i, \lambda_i \in K, w_i \in B$) und linear unabhängig ($\sum_{i=1}^{r} \lambda_i w_i = 0 \Longrightarrow \lambda_i = 0 \forall\ i$).*
Bemerkung: Es gilt der Satz : B, B' Basen von $V \Longrightarrow \#B = \#B'$. Man setzt $\dim_K(V) := \#B$.

Beispiel
K^n ist K-Vektorraum mit K-Basis

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0) \\ &\vdots \\ e_n &= (0, 0, \ldots, 1) \end{aligned}$$

Satz 1 (Polynomalgebra $K[x]$)
Sei K Körper.

(i) Es existiert ein K-Vektorraum A mit K-Basis $\{x^i : i \in \mathbb{N}_0\}$.

(ii) $\exists!$ K-bilineare Abbildung $\cdot : A \times A \to A$ mit $x^i \cdot x^j = x^{i+j}$.

(iii) A zusammen mit $\cdot$ ist K-Algebra mit Eins $1 = x^0$. ($K \cong K \cdot x^0 \subset A$)

5.3
Die K-Algebra aus (iii) in Satz 1 heißt K-Algebra der Polynome in einer Variablen x über K und wird mit $K[x]$ bezeichnet.

Beispiel
Ist $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j$, so ist $f = g \iff a_i = b_i \forall\ i$ (wobei a_i, b_j für $i > n, j > m$ Null gesetzt seien).

5.4

a) Sei $f = \sum_{i=0}^{r} a_i x^i \in K[x]$, $a_r \neq 0$, so heißt r auch der Grad $\operatorname{grad}(f)$ von f .
$\operatorname{grad}(0) := -\infty$, d.h. $\operatorname{grad} : K[x] \to \mathbb{N}_0 \cup \{-\infty\}$.

b) $f = \sum_{i=0}^{r} a_i x^i$ mit Grad r heißt normiert $\iff a_r = 1$.

c) $f \in K$-Algebra A heißt Einheit $\iff f$ invertierbar bzgl $\cdot$; man bezeichnet die Gruppe der Einheiten mit A^*.

Satz 2 (Grad)
Es seien $f, g \in K[x]$.

(i) $\operatorname{grad}(f+g) \leq \max(\operatorname{grad}(f), \operatorname{grad}(g))$

(ii) $\operatorname{grad}(f \cdot g) = \operatorname{grad}(f) + \operatorname{grad}(g)$

(iii) $(K[x])^* = K^*$

Zu (ii): $\left(1+x^2\right) \cdot \left(1+x^3\right) = 1 + x^2 + x^3 + x^5$.

5.5
$f \in K[x]$ mit $\operatorname{grad}(f) \geq 1$ heißt **irreduzibel** *in $K[x]$ $:\iff$ wenn $g, h \in K[x]$ und $f = g \cdot h$, so ist stets $g \in K^*$ oder $h \in K^*$.*

Übung 1
$f = x - \lambda \in K[x]$, $\lambda \in K$, ist irreduzibel für alle λ.
$x^2 + 1$, $x^2 + x$ sind nicht irreduzibel in $\mathbb{Z}_2[x]$.
$x^2 + x + 1$ ist irreduzibel in $\mathbb{Z}_2[x]$.

Satz 3 (Division mit Rest und ggT)
$f, g \in K[x]$.

(i) Ist $g \neq 0$ so existieren $q,\ r \in K[x]$ mit $f = q \cdot g + r$, $\operatorname{grad}(r) < \operatorname{grad}(g)$.

(ii) zu $f \neq 0, g \neq 0$ existiert genau ein normiertes Polynom $h \in K[x]$ mit:
h teilt sowohl f als auch g ($h \mid f, h \mid g$), und existiert ein weiteres $\tilde{h} \in K[x]$ mit $\tilde{h} \mid f$ und $\tilde{h} \mid g$, so gilt $\tilde{h} \mid h$.

(iii) Bezeichnet $\mathrm{ggT}(f,g) := h$, dann gilt

$$\mathrm{ggT}(f,g) = \mathrm{ggT}(f, g - q \cdot f) \quad \forall\, q \in K[x]$$

(iv) Es gibt $\tilde{f}, \tilde{g} \in K[x]$ mit

$$\tilde{f} \cdot f + \tilde{g} \cdot g = \mathrm{ggT}(f,g)$$

5.6
$\mathrm{ggT}(f,g) = h$ *wie in (ii) von Satz 3 nennt man* **größten gemeinsamen Teiler** *von* f *und* g.

Übung 2
Division mit Rest für $K = \mathbb{Z}/2\mathbb{Z}$, $f = x^5 + 1$, $g = x^3 + x$, $\mathrm{ggT}(f,g) = x + 1$, $\tilde{g} = x^2 + 1$.

Satz 4 (Zerlegung in Irreduzible)
Sei $f \in K[x]$, $\mathrm{grad}(f) \geq 1$.

(i) f ist Produkt von irreduziblen Polynomen $p_1, \ldots, p_r$ in $K[x]$.

(ii) Diese Darstellung ist eindeutig bis auf die Reihenfolge und bis auf Multiplikation von p_i mit $c_i \in K^*$.

(iii) Ist f normiert, so ist f Produkt von normierten irreduziblen Polynomen $p_1, \ldots, p_r$.

Übung 3
p *irreduzibel in* $K[x]$, $0 \neq g \in K[x]$ *mit* $\mathrm{grad}(g) < \mathrm{grad}(p)$
$\Longrightarrow \quad \mathrm{ggT}(p,g) = 1$

Beispiel
$K = \mathbb{Z}/2\mathbb{Z}$, $p = x^2 + x + 1$, $ggT\left(p, x^3 + x\right) = 1$

Übung 4
$K[x]$ *ist nullteilerfrei*

Satz 5 (Einsetzungshomomorphismus)
A sei K-Algebra mit Eins 1_A und $a \in A \quad \Longrightarrow \quad \exists!K$-Algebrahomomorphismus $\varphi_a : K[x] \to A$ mit

$$\varphi_a(1) = 1_A \text{ und } \varphi_a(x) = a.$$

Man nennet φ_a den **Einsetzungshomomorphismus** und schreibt $f(a) := \varphi_a(f)$.

Beispiel: $\quad \varphi_a\left(\sum_{i=0}^n c_i x^i\right) = \sum_{i=0}^n c_i a^i$

Speziell: Ist $\lambda \in K$, so ist φ_λ Homomorophismus $K[x] \to K$. Man nennt $\lambda \in K$ Nullstelle von f, wenn $f(\lambda) = 0$ ist.

Beispiel
$f = x^3 - x$, $K = \mathbb{Z}/3\mathbb{Z}$. $f(\lambda) = 0\ \forall\ \lambda \in K$, *aber* $f \neq$ *Nullpolynom.*

Übung 5
$0 \neq f \in K[x]$, $\lambda \in K$. *Dann:* $(x - \lambda) \,|\, f \Longleftrightarrow f(\lambda) = 0$.
Nur für $\mathrm{grad}(f) \leq 3$ *gilt:*

$$f \text{ irreduzibel} \Longleftrightarrow f(\lambda) \neq 0 \quad \forall\ \lambda \in K$$

5.7
Sei $I \subseteq K[x]$ nichtleere Teilmenge. I heißt **Ideal** *in $K[x]$ genau dann, wenn*

(i) wenn $f_1, f_2 \in I$, so ist $f_1 + f_2 \in I$

(ii) wenn $f \in I$, $r \in K[x]$, so ist $f \cdot r \in I$

(iii) Ist I Ideal in $K[x]$, $f_1, f_2 \in K[x]$, so schreibt man auch $f_1 \equiv f_2 \mod I$, falls $f_1 - f_2 \in I$.

Beispiel: $xK[x]$. Allgemeiner: für $g \in K[x]$, $I = g \cdot K[x] = \{g \cdot r : r \in K[x]\}$ ist ein Ideal in $K[x]$.

Satz 6 (Hauptidealring)
K Körper, $K[x]$ Polynomalgebra in x über K, I Ideal in $K[x]$, $I \neq \{0\}$
$\Longrightarrow$ $\exists!$ normiertes Polynom $g \in K[x]$ mit $I = g \cdot K[x]$

Übung 6
$K = \mathbb{Z}/3\mathbb{Z}$, $I = \{f \in K[x] : f(1) = f(-1) = 0\}$. Es ist I Ideal in $K[x]$.
Gesucht $g \in I$ mit $I = g \cdot K[x]$. $\rightsquigarrow g = (x-1)(x+1) = x^2 - 1$

Satz 7 (Quotientenalgebra)
Sei I Ideal in $K[x]$, K Körper, $I = g \cdot K[x]$. Dann gilt:
Es existiert eine K-Algebra $A = K[x]/I$ und ein surjektiver K-Algebrahomomorphismus $\pi(= \pi_g) : K[x] \to A$ mit

$$\pi(f_1) = \pi(f_2) \text{ genau dann, wenn } f_1 \equiv f_2 \mod I$$

Weiterhin gilt

(i) $\dim_K A = n$, wenn $g \neq 0$ und $n = \operatorname{grad}(g)$

(ii) A ist Körper $\Longleftrightarrow$ g ist irreduzibel in $K[x]$

(iii) Wenn $\operatorname{grad}(g) = n \geq 1$ und $a := \pi(x) \in A$, so ist $\left\{1, a, a^2, \ldots, a^{n-1}\right\}$ K-Basis von A.

Speziell: wenn K endlich mit $q = \#K$, so ist $\#A = q^n$.

Beispiel
$K = \mathbb{Z}/2\mathbb{Z}$, $g = x^3 + x + 1$ in $K[x]$ ireduzibel, da $g(0) = 1 = g(1)$. $A = K[x]/g \cdot K[x]$ hat K-Basis $1, a, a^2$ mit $a = \pi(x)$. Berechnung von $a^3, a^4, \ldots, a^7$.

Satz 8 (Ableitung und mehrfache Faktoren)
Sei $f \in K[x]$, K Körper. Ist $\operatorname{ggT}(f, f') = 1$, so sind alle irreduziblen Faktoren $p_1, \ldots, p_r$ von f einfach (d.h. ist $p \in K[x]$, $\operatorname{grad}(p) \geq 1$ Faktor, so ist p^2 kein Teiler von f in $K[x]$).

Hierbei ist $f' := \frac{d}{dx}$ die Ableitung von f nach x. Es ist $\frac{d}{dx} : K[x] \to K[x]$ lineare Abbildung, eindeutig bestimmt durch:

(i) $\frac{d}{dx}(x) = 1$

(ii) $\frac{d}{dx}(f \cdot g) = f \cdot \frac{d}{dx}(g) + \frac{d}{dx}(f) \cdot g \quad \forall\, f, g \in K[x]$ (Leibniz- oder Produkt-Regel)

Übung 7
Sei $K = \mathbb{Z}/p\mathbb{Z}$, $f = x^p - x$. $f' = \frac{d}{dx}(f) = px^{p-1} - 1 = -1$.
$\Longrightarrow$ $\operatorname{ggT}(f, f') = 1$
$\Longrightarrow$ $x^p - x = \prod_{\lambda \in K}(x - \lambda)$, $(x - \lambda)^2$ *kein Teiler von $x^p - x$.*