PLENUMSÜBUNG ZUR LINEAREN ALGEBRA II, SS 2020

SIMON MÜLLER

Inhaltsverzeichnis

1. Algebren

Erinnerung: Sei K ein Körper. Eine *K-Algebra* $\mathcal{A}$ ist ein K-Vektorraum $\mathcal{A}$ mit einer Multiplikation von Vektoren

$$\mathcal{A} \times \mathcal{A} \to \mathcal{A},\ (\alpha, \beta) \mapsto \alpha\beta,$$

so dass für alle $\alpha, \beta, \gamma \in \mathcal{A}$ und $c \in K$ gilt:

(a) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(b) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ und $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$.

(c) $c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$.

Falls ein $1 \in \mathcal{A}$ existiert, so dass $1\alpha = \alpha 1 = \alpha$ für alle $\alpha \in \mathcal{A}$ gilt, so heißt die Algebra eine *Algebra mit Einheit.*

Falls $\alpha\beta = \beta\alpha$ für alle $\alpha, \beta \in \mathcal{A}$ gilt, so heißt $\mathcal{A}$ eine *kommuative Algebra.*

Vorsicht: Gleiches Symbol für die Skalar- und die Vektormultiplikation! In der Literatur so üblich. Zur Unterscheidung könnte man etwa $\cdot_K$ und $\cdot_{\mathcal{A}}$ schreiben. Analog sind 1_K und $1_{\mathcal{A}}$ zu unterscheiden.

Beispiel 1.1. Sei K ein Körper.

(1) $M_{n\times n}(K)$, bzw. $L(V, V)$, ist eine nicht kommutative Algebra mit Einheit (siehe Beispiel 1.1 und 1.2).

(2) K ist in kanonischer Weise eine kommutative K-Algebra mit Einheit.

(3) $\mathbb{R}$ ist eine $\mathbb{Q}$-Algebra (kommutativ, mit Einheit).

(4) Sei V ein K-Vektorraum. Dann ist V in kanonischer Weise eine kommutative K-Algebra $\mathcal{A}$ (mit oder ohne Einheit?)

Beweis. Definiere die Vektormultiplikation wie folgt:

$$\mathcal{A} \times \mathcal{A} \to \mathcal{A},\ (\alpha, \beta) \mapsto 0.$$

Diese erfüllt offensichtlich die Axiome (a) - (c) aus der obigen Definition und ist kommutativ. □

Date: 11. Mai 2020.

(5) Sei M eine nichtleere Menge. Dann ist $\mathcal{A} := \{f : M \to K\}$, versehen mit jeweils punktweiser Addition, Vektormultiplikation und Skalarmultiplikation, eine kommutative K-Algebra mit Einheit.

Ein weiteres Beispiel ist die Potenzreihen Algebra (siehe Beispiel 1.3). An dieser Stelle mehr zur Notation. Gemäß Skript 1 ist

$$K^{\mathbb{N}_0} := \{f : \mathbb{N}_0 \to K\},$$

Wir schreiben f_n für $f(n)$ und wir identifizieren f wie folgt mit dem Vektor seiner Funktionswerte:

$$f = (f_n)_{n\in\mathbb{N}_0} = (f_0, f_1, \ldots) = (f(0), f(1), \ldots).$$

Mit folgenden Operationen ist $K^{\mathbb{N}_0}$ eine kommutative Algebra mit Einheit (siehe Proposition 1.4):

- Punktweiser Addition: $f + g := (f_n + g_n)_{n\in\mathbb{N}_0}$.
- Punktweiser Skalarmultiplikation: $cf = (cf_n)_{n\in\mathbb{N}_0}$.
- Produkt: $fg = (\sum_{i=0}^{n} f_i g_{n-i})_{n\in\mathbb{N}_0}$.

$\mathcal{A} = K^{\mathbb{N}_0}$ heißt auch Algebra der Potenzreihen über K. Wir bezeichnen sie auch mit $\mathcal{A} := K[[x]]$. Anstelle von $(f_n)_{n\in\mathbb{N}_0}$ schreiben wir auch $\sum_{i=0}^{\infty} f_n x^n$. Anders als im Polynomring $K[x]$ können hier unendlich viele Koeffizienten von Null verschieden sein.

2. Polynomalgebren

In der ersten Vorlesung wurde der Grad eines Polynoms definiert.

Definition 2.1. Ist $0 \neq f \in K[x]$, so existiert ein $n \in \mathbb{N}_0$ mit $f_n \neq 0$ und $f_k = 0$ für alle $k > n$. In diesem Fall heißt n der *Grad* von f.

Der Grad des Nullpolynoms ist für uns also nicht definiert - wann immer wir über den Grad sprechen, müssen wir das Nullpolynom ausschließen (Vgl. Satz 2.1).

In der Literatur gibt es diesbezüglich keine einheitliche Konvention. Der Einfachheit halber ordnet man dem Nullpolynom gerne (mehr oder weniger willkürlich) einen bestimmten Grad zu, damit einige Aussagen allgemeingültig sind. Weit verbreitet ist die Konvention $\deg(0) = -\infty$. Dies hat unter anderem folgende Vorteile:

- Die Formel $\deg(fg) = \deg(f) + \deg(g)$ (Vgl. Satz 2.1(ii)) bleibt erfüllt.
- Die Formel $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ (Vgl. Satz 2.1(v)) bleibt erfüllt.
- $K[x]_{\leq d}$ ist eine K-Algebra für jedes $d \in \mathbb{N}$.
- Erlauben wir negative Potenzen von x, so ist der Grad von $\sum a_i x^i$ (mit $a_i \in K$) gerade das Supremum über alle i, für welche $a_i \neq 0$.

Als weitere Varianten findet man, aus meist ähnlichen Gründen, $-1, 0$ und $+\infty$.

Unterscheidung von Potenzreihen und Polynomen:
Sei K ein Körper.

Potenzreihen:

- $K[[x]] := K^{\mathbb{N}_0} := \{f : \mathbb{N}_0 \to K\}$, versehen mit den in der Vorlesung definierten Operationen, heißt die **Algebra der Potenzreihen**.
- Eine Potenzreihe über K ist also eine Abbildung $f : \mathbb{N}_0 \to K$.
- Wir identifizieren jedes $f \in K^{\mathbb{N}_0}$ mit dem unendlichen Vektor $(f_n)_{n\in\mathbb{N}_0}$, wobei $f_n := f(n)$.
- Formale Schreibweise: $f = \sum\limits_{n=0}^{n} f_n x^n$.

Polynome:

- $K[x] := \operatorname{span}\{x^k : k \in \mathbb{N}_0\}$.
- Die Elemente aus $K[x]$ heißen **Polynome** und $K[x]$ ein **Polynomring** über K
- In anderen Worten ist ein Polynom eine Potenzreihe $f = \sum_{n=0}^{\infty} f_n x^n$, so dass $f_n = 0$ für alle bis auf endlich viele $n \in \mathbb{N}_0$. Eine Potenzreihe f ist also genau dann ein Polynom, wenn sie als endliche Summe $\sum_{n=0}^{m} f_n x^n$ geschrieben werden kann (Vgl. Skript, Bemerkung 2.0(ii))
- Es gilt somit $K[x] \subseteq K[[x]]$.
- Beispiele:
  (i) $x^2 + 1 \in K[x]$.
  (ii) $\sum\limits_{i=0}^{\infty} x^{2i} = 1 + x^2 + x^4 + \ldots \in K[[x]] \backslash K[x]$.

Nicht zu verwechseln mit Polynomen sind polynomiale Funktionen.

Definition 2.2. (Skript Definition 2.4) Eine Abbildung $f\colon K \to K$ ist eine **polynomiale Funktion**, falls es $c_0, \ldots, c_n \in K$ gibt, so dass $f(x) = c_0 + c_1 x + \ldots c_n x^n$ für alle $x \in K$.

Beispiel 2.3.

(1) Die Abbildung $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + 1$ ist eine polynomiale Funktion. Sie ist kein Polynom und auch keine Potenzreihe.
(2) Die Abbildung $\exp : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sum_{k=0}^{\infty} \frac{x^k}{k!}$ ist weder eine polynomiale Funktion, noch eine Potenzreihe.

Wir erlauben nun, für die Variable x eines Polynoms $f \in K[x]$ bestimmte Werte einzusetzen.

Definition 2.4. (Skript Definition 2.5) Sei $\mathcal{A}$ eine K-Algebra mit 1, sei $\alpha \in \mathcal{A}$ und sei $f = \sum_{i=0}^{n} f_i x^i \in K[x]$. Definiere

$$f(\alpha) := \sum_{i=0}^{n} f_i \alpha^i \in \mathcal{A},$$

wobei $\alpha^0 := 1$.

Beispiel 2.5.

(1) Sei $\mathcal{A} = K[x]$, und seien $f = \sum\limits_{i=0}^{n} a_i x^i$ und $g = \sum\limits_{j=0}^{m} b_j x^j$ in $\mathcal{A}$. Dann gilt

$$f(g) = \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{m} b_j x^j \right)^i .$$

(2) Konkretes Beispiel. Sei $f = 2X^2 + X + 1$ und $g = X + 1$. Dann ist

$$f(g) = 2(X+1)^2 + (X+1) + 1 = 2X^2 + 5X + 4.$$

Auf diese Weise induziert jedes Polynom $f \in K[x]$ eine polynomiale Funktion $\tilde{f}\colon K \to K$. Ist $f = \sum_{i=0}^{n} a_i X^i$, so ist

$$\tilde{f}\colon K \to K, \alpha \mapsto f(\alpha).$$

Notation 2.6. Wir notieren die durch ein Polynom $f \in K[X]$ induzierte polynomiale Abbildung mit $\tilde{f}$ und den K-Vektorraum der polynomialen Funktionen über K mit $K[x]^{\sim}$.

Bemerkung 2.7.

(1) Ist K unendlich, so sind $K[x]$ und $K[x]^{\sim}$ isomorph als K-Algebren (Satz 3.2).
(2) Ist K endlich, so ist dies allerdings nicht allgemeingültig; z.B. ist das Polynom $f = x^3 - x \in \mathbb{F}_3[x]$ von null verschieden, wohingegen $\tilde{f} = 0$.

3. Einschub: Dualraum

Dualräume wurden in der B1 besprochen, siehe das Skript zu Vorlesung 22. In der B2 benutzen wir Dualräume und -basen in einigen Beweisen, siehe Satz 3.0 (Lagrange Interpolation) und Satz 4.5 (Taylor's Formel). Der in diesem Kontext zentrale Satz ist der folgende:

Satz 3.1. *(B1, Satz 22.9) Sei K ein Körper, V ein n-dimensionaler K-Vektorraum und Basis $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ eine Basis von V. Dann existiert genau eine Dualbasis $\mathcal{B}^* = \{f_1, \dots, f_n\}$ für V^*, so dass*

(1) $f_i(\alpha_j) = \delta_{ij}$

(2) $f = \sum_{i=1}^{n} f(\alpha_i) f_i$ *für alle* $f \in V^*$.

(3) $\alpha = \sum_{i=1}^{n} f_i(\alpha)\alpha_i$ *für alle* $\alpha \in V$.

Bemerkung 3.2. Die f_i sind bereits durch Bedingung (1) eindeutig bestimmt, vgl. B1 Vorlesung 22 beziehungsweise Satz 17.8.

Schauen wir uns nun nochmal die Lagrange Interpolation an.

Satz 3.3. *(Lagrange Interpolation) Sei $n \in \mathbb{N}$, sei K ein Körper, sei V der K-Vektorraum $K[x]_{\leq n}$ und seien $t_0, t_1, \dots, t_n$ $n+1$ verschiedene Elemente aus K. Für $0 \leq i \leq n$ sei $L_i \in V^*$ definiert durch $L_i(f) := f(t_i)$. Dann ist $\{L_0, \dots, L_n\}$ eine Basis für V^*.*

Proof. Wir betrachten die Lagrange Polynome

$$P_i := \prod_{j \neq i} \left(\frac{x - t_j}{t_i - t_j} \right) \quad (j = 0, \dots, n).$$

Im Sinne von Satz 3.1 möchten wir, dass $\mathcal{B} := \{P_0, \dots, P_n\}$ eine Basis von V ist und $\mathcal{B}^* := \{L_0, \dots, L_n\}$ die zugehörige Dualbasis. Hierzu genügt es zu zeigen (Vgl. Übungsaufgabe 2.1):

- $L_i(P_j) = \delta_{ij}$ für alle $i, j \in \{1, \dots, n\}$.
- $\{P_0, \dots, P_n\}$ ist eine Basis von V, d.h. zeige $\{P_0, \dots, P_n\}$ ist erzeugend oder linear unabhängig.

Sobald man das hat, bekommt man über Satz 3.1, dass $\{L_0, \dots, L_n\}$ eine Basis von V^* ist.

Zudem erhalten wir die zusätzliche Behauptung

$$\forall f \in V \colon f = \sum_{i=0}^{n} f(t_i) P_i,$$

die im Beweis von Satz 3.2 verwendet wird (und worum es hier eigentlich geht!). In der Tat, nach Satz 3.1(3) gilt für jedes $f \in V$, dass

$$f = \sum_{i=0}^{n} L_i(f) P_i = \sum_{i=0}^{n} f(t_i) P_i.$$

□

Bemerkung 3.4. Die Behauptung $\forall f \in V \colon f = \sum_{i=0}^{n} f(t_i) P_i$ können wir uns auch über die Anzahl der Nullstellen herleiten, siehe Korollar 4.3 im Skript und den Beweis von Satz 3.0 im Abschnitt 5 oder auch das Video zur Plenumsübung 02.

4. Ideale

In der Vorlesung wurden *Ideale* wie folgt definiert (Definition 5.3): ein K-Unterraum $M \subseteq K[x]$ ist ein Ideal, wenn $fg \in M$ für alle $f \in K[x]$ und alle $g \in M$.

Äquivalent dazu ist eine Teilmenge $M \subseteq K[x]$ ein Ideal, falls

(1) $0 \in M$,
(2) $M + M \subseteq M$,
(3) $K[x] \cdot M \subseteq M$ (d.h. $fg \in M$ für alle $f \in K[x]$ und alle $g \in M$).

Bemerkung 4.1. Sei $M \subseteq K[x]$ ein Ideal.

(1) Es gilt $M = K[x] \Leftrightarrow 1 \in M$.
Die Hinrichtung ist trivial, die Rückrichtung folgt aus $K[x] \cdot M \subseteq M$.
(2) M ist insbesondere ein kommutativer Ring.
(3) M ist ein Hauptideal (Satz 5.9), d.h. es existiert ein $d \in K[x]$ so dass $M = dK[x]$.
(4) Schnitte (ÜA) und Summen von Idealen sind wieder Ideale.
(5) Ideale werden in der B3 allgemeiner über beliebigen kommutativen Ringen mit 1 studiert.

Ferner haben wir in der Vorlesung den Begriff der *(Ir-)Reduzibilität* eines Polynoms eingeführt (Definition 5.11). Ein Polynom $f \in K[x]$ ist *reduzibel* über K, wenn es $g, h \in K[x]$ gibt mit $\deg(g), \deg(h) \geq 1$ und $f = gh$. Ansonsten heißt f *irreduzibel.*

Bemerkung 4.2. (1) Jedes Polynom von Grad 1 ist irreduzibel.

Beweis. Ist $f \in K[x]$ von Grad 1 und sind $g, h \in K[x]$ mit $f = gh$, so gilt nach Satz 2.1(ii), dass

$$1 = \deg(f) = \deg(g) + \deg(h).$$

Also $\deg(g) = 0$ oder $\deg(h) = 0$, womit f irreduzibel ist. □

(2) Besitzt ein irreduzibles Polynom eine Nullstelle, so hat es Grad 1.

Beweis. Sei $f \in K[x]$ irreduzibel und $a \in K$ eine Nullstelle von f. Nach dem Divisionsalgorithmus finden wir $q, r \in K[x]$ mit $f = q(x-a) + r$ und $r = 0$ oder $\deg(r) < \deg(x-a) = 1$, d.h. es gilt $r \in K$; Wegen $0 = f(a) = r(a)$ also $r = 0$. Somit $f = q(x-a)$. Da f irreduzibel ist muss $\deg(q) = 0$ gelten. Damit $\deg(f) = \deg(x-a) = 1$. □

(3) Jedes Polynom über K vom Grad 2 oder vom Grad 3 ist genau dann irreduzibel, wenn es keine Nullstelle in K hat.

Beweis. Sei $f \in K[x]$ ein Polynom von Grad 2 oder 3. Ist f irreduzibel, so folgt aus der vorherigen Bemerkung, dass f keine Nullstelle in K hat. Die Rückrichtung zeigen wir per Kontraposition. Sei f also reduzibel. Dann finden wir $g, h \in K[x]$ von Grad mindestens 1 mit $f = gh$. Nach Satz 2.1(ii) gilt

$$\deg(f) = \deg(fg) = \deg(g) + \deg(h).$$

Es folgt $\deg(g) = 1$ oder $\deg(h) = 1$ (ggf. Fallunterscheidung durchführen, ob $\deg(f) = 2$ oder $\deg(f) = 3$). Also hat g oder h, und damit auch f eine Nullstelle in K. □

In Beispiel 5.12 aus der Vorlesung wird behauptet, dass

$$f = x^2 + 1 = (x+i)(x-i)$$

irreduzibel über $\mathbb{R}$ sei. Dies folgt aus Bemerkung 4.2(3) oder alternativ aus der eindeutigen Zerlegung in Primpolynome (Satz 5.15) angewandt auf $\mathbb{C}[x]$.

5. Beweise aus dem Skript

Kurz zu **Proposition 1.4** etwas sagen (Assoziativität).

Satz 5.1. *(Skript: Satz 2.1) Seien $f, g \in K[x]$ und $f, g \neq 0$. Es gelten*

(i) $fg \neq 0$.
(ii) $\deg(fg) = \deg f + \deg g$
(iii) *fg ist normiert, falls f und g normiert sind.*
(iv) *fg ist skalar $\Leftrightarrow$ f und g sind sklar.*
(v) *Falls $f + g \neq 0$, so gilt* $\deg(f + g) \leq \max(\deg f, \deg g)$.

Beweis. Setze $\deg f := m$ und $\deg g := n$. Dann können wir f und g in der Form $f = \sum_{i=0}^{m} f_i x^i$ und $g = \sum_{j=0}^{n} g_j x^j$ schreiben. Es gilt also $f_m \neq 0$ und $f_k = 0$ für alle $k > m$ und entsprechend $g_n \neq 0$ und $g_k = 0$ für alle $k > n$.

Nach Definition des Produkts fg erhalten wir für jedes $l \in \mathbb{N}_0$, dass

$$(fg)_l = \sum_{r=0}^{l} f_r g_{l-r}.$$

Wir behaupten, dass

(1) $(fg)_{m+n} = f_m g_n$
(2) $(fg)_{m+n+k} = 0$ für $k > 0$.

Sei also $k \geq 0$. Dann gilt

$$(fg)_{m+n+k} = \sum_{r=0}^{m+n+k} f_r g_{m+n+k-r}.$$

Wir untersuchen nun, welche Beiträge ungleich Null sind.

- $f_r g_{m+n+k-r} \neq 0 \Rightarrow r \leq m$ und $m + n + k - r \leq n$, da $\deg(f) = m$ und $\deg g = n$. Die zweite Ungleichung vereinfacht sich zu $m + k \leq r$. Somit erhalten wir $m + k \leq r \leq m$.
- $f_r g_{m+n+k-r} \neq 0$ impliziert also $k = 0$ und $r = m$.
- Dies beweist sofort (2).
- Für (1) erhalten wir

$$(fg)_{m+n} = \sum_{r=0}^{m+n} f_r g_{m+n-r} = f_m g_n$$

  und wegen $f_m \neq 0$ und $g_n \neq 0$ ist auch $f_m g_n \neq 0$.

Nun zu den einzelnen Aussagen aus der Behauptung:

- $fg \neq 0$ ist klar, da $(fg)_{m+n} \neq 0$.
- $(fg)_{m+n} \neq 0$ und $(fg)_{m+n+k} = 0$ für alle $k > 0$. Folglich $\deg(fg) = m+n = \deg(f) + \deg(g)$.
- f, g normiert bedeutet $f_m = g_n = 1$. Dann aber auch $(fg)_{m+n} = f_m g_n = 1$.
- fg skalar $\Leftrightarrow \deg(fg) = 0 \Leftrightarrow \deg(f)+\deg(g) = 0 \Leftrightarrow \deg(f) = 0$ und $\deg(g) = 0$, da es keine negativen Grade gibt.

□

Zu Satz 3.0: Sei K ein Körper, $V := K[x]_{\leq n}$, seien $t_0, \ldots, t_n \in K$ paarweise verschieden und sei

$$P_i := \prod_{j \neq i} \frac{x - t_j}{t_i - t_j}$$

das **i-te Lagrange Polynom**.

Im Beweis von Satz 3.0 wird behauptet, dass für alle $f \in V$ gilt:

$$f = \sum_{i=0}^{n} f(t_i)P_i.$$

Dieses Resultat kann über die beiden folgenden Aussagen hergeleitet werden:

(1) **Übungsaufgabe:** $P_i(t_j) = \delta_{ij}$, d.h.

$$P_i(t_j) = \begin{cases} 1, & \text{falls } i = j \\ 0, & \text{sonst} \end{cases}$$

(2) **Fakt:** Sei $0 \neq f \in K[x]$. Dann hat f höchstens $\deg(f)$ viele Nullstellen in K.

(3) Diesen Fakt können wir aus dem Divsionsalgorithmus (Satz 3.4) ableiten, in dem wir nach und nach alle Nullstellen $a \in K$ als Linearfaktoren $(x - a)$ herausteilen. Tatsächlich begehen wir hierbei keinen Zirkelschluss.

Wir erhalten hieraus nämlich

$$f(t_j) = \sum_{i=0}^{n} f(t_i)P_i(t_j) \quad (j \in \{0, \dots, n\})$$

d.h. $f - \sum_{i=0}^{n} f(t_i)P_i$ hat $n + 1$ verschiedene Nullstellen in K, nämlich $t_0, \dots, t_n$. Da dieses Polynom aber von Grad höchstens n ist, muss $f - \sum_{i=0}^{n} f(t_i)P_i = 0$, also $f = \sum_{i=0}^{n} f(t_i)P_i$ gelten.

Satz 5.2. *(Skript: Satz 3.2) Sei K unendlich. Die Abbildung*

$$K[x] \mapsto K[x]^{\sim}, \, f \mapsto \tilde{f}$$

ist eine K-Algebren-Isomorphie.

Proof. Bis auf die Injektivität ist alles klar. Wir zeigen nun, dass der Kern der Abbildung nur die 0 enthält.

Sei also $\tilde{f} = 0$, d.h. $f(\alpha) = 0$ für alle $\alpha \in K$. Wir zeigen, dass bereits $f = 0$ gilt. Angenommen $f \neq 0$. Da $\deg(f)$ endlich und K unendlich ist, folgt hieraus bereits das $f = 0$ gelten muss (analog zu oben; wäre $f \neq 0$, so hätte es zu viele Nullstellen). □

Satz 5.3. *(Skript Satz 3.4 (Divisionsalgorithmus))*
Seien $0 \neq f, d \in K[x]$ mit $d \neq 0$. Es existieren $q, r \in K[x]$, so dass

(i) $f = dq + r$.
(ii) $r = 0$ *oder* $\deg r < \deg d$.

Ferner sind q und r mit (i) und (ii) eindeutig.

Beweis: **Eindeutigkeit:** Sei $f = dq_1 + r_1 = dq + r$ mit $r = 0$ oder $\deg r < \deg d$ und $r_1 = 0$ oder $\deg r < \deg_d$. Aus $dq_1 + r_1 = dq + r$ folgt $d(q - q_1) = (r_1 - r)$.

Angenommen $q \neq q_1$. Dann auch $r \neq r_1$. Es gilt $d(q - q_1) \neq 0$ und

$$\deg(r_1 - r) = \deg(d(q - q_1)) = \deg(d) + \deg(q - q_1) \geq \deg(d)$$

(Satz 2.1). Der selbe Satz und der Divisionsalgorithmus implizieren

$$\deg(r_1 - r) \leq \max(\deg r_1, \deg r) < \deg(d),$$

ein Widerspruch. Also $q = q_1$ und damit auch $r = r_1$. □

Satz 5.4. *(Skript Satz 4.5 (Taylor's Formel))*
Seien $Char(K) = 0$, $n \in \mathbb{N}_0, a \in K, p \in K[x]$ und $\deg p \leq n$. Es gilt

$$p = \sum_{i=0}^{n} p^{(i)}(a) \frac{(x - a)^i}{i!}.$$

Beweis. (Analog zum Beweis der Lagrange Interpolation, siehe Satz 3.3).

Sei $V = K[x]_{\leq n}$. Für alle $i = 0, \dots, n$ definiere $l_i \colon V \to K$ durch $l_i(p) := p^{(i)}(a)$. Definiere ferner $p_i := \frac{1}{i!}(x-a)^i$ für $i = 0, \dots, n$. Zeige (ÜB 3)

(1) $l_j(p_i) = \delta_{ij}$
(2) $\{p_0, \dots, p_n\}$ ist eine Basis von V.

Mit Satz 3.1 erhalten wir, dass $\{l_0, \dots, l_n\}$ eine Basis von V^* ist und das

$$p = \sum_{i=0}^{n} l_i(p)p_i = \sum_{i=0}^{n} p^{(i)}(a)\frac{(x-a)^i}{i!}$$

gilt. □

Satz 5.5. *(Skript Satz 4.8) Sei Char$(K) = 0$, sei $0 \neq f \in K[x]_{\leq n}$ und sei $c \in K$ eine Nullstelle von f. Es gilt: c hat die Vielfachheit μ genau dann wenn $f^{(k)}(c) = 0$ für alle $0 \leq k \leq \mu - 1$ und $f^{(\mu)}(c) \neq 0$.*

Beweis. $\Rightarrow$: Habe c die Vielfachheit μ für ein $\mu \in \mathbb{N}$. Nach Definition ist $(x-c)^\mu$ ein Teiler von f und $(x-c)^{\mu+1}$ teilt f nicht. Es gibt also ein $0 \neq g \in K[x]$ mit $f = (x-c)^\mu g$.

Es gilt $\deg g \leq \deg f - \mu \leq n - \mu$ nach Satz 2.1 aus dem Skript. Außerdem ist $g(c) \neq 0$; andernfalls könnten wir nach Korollar 4.1 aus dem Skript g schreiben als $(x-c)h$ für ein $h \in K[x]$. Nun würde aus $f = (x-c)^\mu g$ folgen, dass $(x-c)^{\mu+1}$ ein Teiler von f wäre, ein Widerspruch.

Wir wenden zunächst die Taylorformel auf g an:

$$f = (x-c)^\mu g = (x-c)^\mu \left(\sum_{i=0}^{n-\mu} g^{(m)}(c)\frac{(x-c)^m}{m!} \right)$$

Hieraus folgt

$$f = \sum_{m=0}^{n-\mu} g^{(m)}(c)\frac{(x-c)^{\mu+m}}{m!}.$$

Wir können aber auch die Taylorformel auf f selber anwenden:

$$f = \sum_{k=0}^{n} f^{(k)}(c)\frac{(x-c)^k}{k!}.$$

Gleichsetzen liefert:

$$\sum_{m=0}^{n-\mu} g^{(m)}(c)\frac{(x-c)^{\mu+m}}{m!} = \sum_{k=0}^{n} f^{(k)}(c)\frac{(x-c)^k}{k!}.$$

Da $1, (x-c), \dots, (x-c)^n$ linear unabhängig sind (Skript, Bemerkung 4.6(1)), sind deren Koeffizienten eindeutig bestimmt. Wir führen einen **Koeffizientenvergleich** durch und erhalten

$$\frac{f^{(k)}(c)}{k!} = 0 \text{ für } 0 \leq k \leq \mu - 1$$

und

$$\frac{f^{(k)}(c)}{k!} = \frac{g^{(k-\mu)}(c)}{(k-\mu)!} \text{ für } \mu \leq k \leq n.$$

Ersteres liefert $f^{(k)}(c) = 0$ für $0 \leq k \leq \mu - 1$, zweiteres $f^{(\mu)}(c) = k! \cdot g(c) \neq 0$ (setze $k = \mu$).

$\Leftarrow$: Gemäß der Voraussetzung und der Taylorformel können wir schreiben:

$$f = \sum_{k=\mu}^{n} f^{(k)}(c)\frac{(x-c)^k}{k!} = (x-c)^\mu \left(\sum_{k=\mu}^{n} f^{(k)}(c)\frac{(x-c)^{k-\mu}}{k!}\right).$$

Definiere $g := \sum\limits_{k=\mu}^{n} f^{(k)}(c)\frac{(x-c)^{k-\mu}}{k!}$. Dann ist $f = (x-c)^\mu g$ mit $g(c) = \frac{f^{(\mu)}(c)}{\mu!} \neq 0$, da $f^{(\mu)}(c) \neq 0$.

Wir zeigen nun per Widerspruchsbeweis, dass $(x-c)^{\mu+1}$ kein Teiler von f ist. Ansonsten fänden wir ein $h \in K[x]$ mit

$$(x-c)^{\mu+1}h = f = (x-c)^\mu g.$$

Da g ein Integritätsbereich ist, dürfen wir kürzen. Es gilt also $(x-c)h = g$, ein Widerspruch zu $g(c) \neq 0$. Somit ist $(x-c)^{\mu+1}$ kein Teiler von f, wohingegen $(x-c)^\mu$ für alle $1 \leq \mu \leq k$ ein Teiler von f ist. Somit hat c die Vielfachheit μ. $\square$