

§ 4. Nullstellen von Polynomen

Sei $(R, +, \cdot)$ ein kommutativer Ring mit $1_R \neq 0_R$. Dann ist die Menge $R[T]$ aller Polynome in einer Unbestimmten T wieder ein kommutativer Ring, der sog. **Polynomring in einer Unbestimmten über R** . Ein Polynom $0 \neq f \in R[T]$ läßt sich in der Form

$$f = \sum_{\mu=0}^m a_\mu T^\mu$$

mit eindeutig bestimmten Koeffizienten $a_\mu \in R$ darstellen. Daher läßt sich ein **Koeffizientenvergleich** anstellen, um die Gleichheit zweier Polynome festzustellen. Die Summe zweier Polynome wird koeffizientenweise vorgenommen und das Produkt wird als **Cauchy-Produkt** gebildet, d.h.

$$f = \sum_{\mu=0}^m a_\mu T^\mu \quad \text{und} \quad g = \sum_{\nu=0}^n a_\nu T^\nu \quad \implies \quad f \cdot g := \sum_{\kappa=0}^{m+n} c_\kappa T^\kappa \quad \text{mit} \quad c_\kappa := \sum_{\mu+\nu=\kappa} a_\mu + b_\nu$$

Als **Grad** eines Polynoms $\neq 0$ ist der größte Index eines Koeffizienten $\neq 0$ definiert, so daß sich ein Polynom f vom Grade $m \in \mathbb{N}_0$ in der Form

$$f = \sum_{\mu=0}^m a_\mu T^\mu \quad \text{mit} \quad a_m \neq 0$$

darstellen läßt. Es gilt

$$(4.1a) \quad \text{grad}(f + g) \leq \max(\text{grad}(f), \text{grad}(g)) \quad \forall f, g \in R[T] \setminus \{0\}, \text{ falls } f + g \neq 0$$

$$(4.1b) \quad \text{grad}(f \cdot g) \leq \text{grad}(f) + \text{grad}(g) \quad \forall f, g \in R[T] \setminus \{0\}, \text{ falls } f \cdot g \neq 0$$

$$(4.1c) \quad \text{Ist } R \text{ ein IB, so gilt sogar}$$

$$\text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g) \quad \forall f, g \in R[T] \setminus \{0\},$$

so daß $R[T]$ selbst wieder ein IB ist.

Unter bestimmten Voraussetzungen läßt sich die **Division mit Rest** in einem Polynomring ausführen:

(4.2) SATZ: R sei ein kommutativer Ring mit $1_R \neq 0_R$ und $g \in R[T]$ sei ein Polynom, dessen Leitkoeffizient eine Einheit (d.h. invertierbar bzgl. der Multiplikation) in R ist. Dann gibt es zu jedem Polynom $f \in R[T]$ eindeutig bestimmte Polynome $q, r \in R[T]$, so daß gilt:

$$f = qg + r \quad \text{mit} \quad r = 0 \quad \text{oder} \quad \text{grad}(r) < \text{grad}(g).$$

BEM: Ist K ein Körper, so ist jedes Element $\neq 0$ eine Einheit. Folglich läßt sich in $K[T]$ Division mit Rest durch jedes Polynom $\neq 0$ durchführen. Dies hat insbesondere zur Konsequenz, daß ein Polynomring über einem Körper ein Hauptidealbereich ist, d.h. ein IB, in dem jedes Ideal ein Hauptideal ist.

(4.3) DEF: Seien $R \neq 0$ ein Ring, S ein Oberring von R und $c \in S$.

a) Ist $f = \sum_{\mu=0}^m a_\mu T^\mu \in R[T]$ ein Polynom, so ist der **Wert $f(c)$ von f an der Stelle c** definiert durch

$$f(c) := \sum_{\mu=0}^m a_\mu c^\mu \in S$$

b) $c \in S$ heißt **Nullstelle von f** , wenn $f(c) = 0_S$ gilt.

c) Die Abbildung $E_c : R[T] \longrightarrow S$ sei definiert durch $E_c(f) := f(c)$.

(4.4) LEMMA: Seien $R \neq 0$ ein Ring, S ein Oberring von R und $c \in S$. Dann ist die Abbildung $E_c : R[T] \longrightarrow S$ ein Ringhomomorphismus mit $E_c(a) = a$ ($\forall a \in R$) und $E_c(T) = c$. E_c heißt **Einsetzungshomomorphismus**.

(4.5) LEMMA: Seien $R \neq 0$ ein Ring, S ein Oberring von R und $c \in S$. Für $f \in R[T]$ ist $f(c)$ der Rest bei Division von f durch das Polynom $T - c$.

(4.6) KOROLLAR: a) Ein Element $c \in S$ ist genau dann eine Nullstelle von $f \in R[T]$, wenn es ein Polynom $q \in S[T]$ gibt mit $f = q \cdot (T - c)$.

b) Ist $c \in S$ Nullstelle von $f \in K[T]$, so gibt es ein Polynom $q \in S[T]$ und ein $m \in \mathbb{N}$ mit

$$f = q \cdot (T - c)^m \quad \text{und} \quad q(c) \neq 0$$

m heißt die **Vielfachheit der Nullstelle c von f** , in Zeichen: $m =: \mu(f, c)$.

(4.7) SATZ: Sei R ein IB. Dann besitzt jedes Polynom $f \in R[T]$ vom Grade $n \geq 0$ höchstens n Nullstellen in R .

BEM: Für die Gültigkeit der Aussage von (4.7) ist die Nullteilerfreiheit entscheidend: Das Polynom $f = T^2 - 1 \in \mathbb{Z}_8$ hat 4 Nullstellen in $\mathbb{Z}_8$, $\mathbb{Z}_8$ ist nicht nullteilerfrei.

Damit wissen wir etwas über die Anzahl der Nullstellen eines Polynoms. Schwieriger läßt sich die Frage nach der Existenz von Nullstellen eines Polynoms beantworten.

BEISPIEL: Das Polynom $f = T^2 + 1 \in \mathbb{R}[T]$ besitzt **keine** Nullstellen in $\mathbb{R}$ besitzt jedoch in dem $\mathbb{R}$ umfassenden Körper $\mathbb{C}$ zwei Nullstellen, nämlich i und $-i$.

(4.8) DEF: R sei ein IB. Sind $a, b \in R$, so heißt a **assoziert zu b** (in Zeichen: $a \sim b$), wenn es eine Einheit $e \in R^\star$ gibt mit der Eigenschaft $a = be$.

(4.9) BEM: a) Es gilt $a \sim b \iff (a) = (b)$.

b) $\sim$ ist eine Äquivalenzrelation auf R .

c) $[1_R]_\sim = R^\star$ (Menge der Einheiten in R).

(4.10) DEF: R sei ein IB. Ein Polynom $f \in R[T]$ heißt **irreduzibel (über R)**, wenn gilt:

- i) $f \neq 0$ und f ist keine Einheit in $R[T]$.
- ii) Für jedes Polynom $g \in R[T]$ mit $g \mid f$ folgt $g \sim 1$ oder $g \sim f$.

Ein Polynom, das nicht irreduzibel (über) R ist, heißt **reduzibel (über R)**.

(4.11) BEM: a) $p \in \mathbb{P} \implies p \in \mathbb{Z}[T]$ irreduzibel

- b) $f = 2T + 2 \in \mathbb{Z}[T]$ ist reduzibel über $\mathbb{Z}$.
- c) $2T + 3$, $T - 7$ sind irreduzibel über $\mathbb{Z}$.
- d) Ist R ein IB, so kann ein irreduzibles Polynom vom Grade ≥ 2 keine Nullstelle in R besitzen.
- e) Ist K ein Körper, so ist ein Polynom $f \in K[T]$ genau dann irreduzibel, wenn gilt:
 - i) $\text{grad}(f) \geq 1$ und ii) $\forall g \in K[T] : g \mid f \implies \text{grad}(g) = 0$ oder $\text{grad}(g) = \text{grad}(f)$.
- f) $2T + 2$ ist irreduzibel über $\mathbb{Q}$. Jedes lineare Polynom über einem Körper ist irreduzibel.
- g) $f = T^2 - 3T + 2 \in \mathbb{R}[T]$ ist reduzibel, da $f(1) = 0$.
- h) $f = 2T^3 + 3T^2 + 6T + 9 \in \mathbb{R}[T]$ ist reduzibel, da $\text{grad}(f) = 3$ ungerade.
- i) Über $\mathbb{C}$ ist jedes Polynom vom Grade ≥ 2 reduzibel.
- j) $T^2 + 1$ ist irreduzibel über $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$, jedoch reduzibel über $\mathbb{C}$.

(4.12) SATZ: Sei K ein Körper. Dann läßt sich jedes Polynom $f \in K[T]$ vom Grade ≥ 1 als Produkt von (endlich vielen) irreduziblen Polynomen darstellen. Diese Darstellung ist eindeutig bis auf die Reihenfolge und Multiplikation mit Einheiten.

(4.13) SATZ: Satz von Kronecker

K sei ein Körper und $f \in K[T]$ ein Polynom vom Grade ≥ 1 . Dann gibt es einen K umfassenden Körper L , in dem f eine Nullstelle besitzt.

(4.14) KOROLLAR: K sei ein Körper und $f \in K[T]$ ein Polynom vom Grade ≥ 1 . Dann gilt:

- a) Es gibt einen K umfassenden Körper L , über dem f in Linearfaktoren zerfällt.
- b) Es gibt einen kleinsten K umfassenden Unterkörper Z von L , über dem f in Linearfaktoren zerfällt. Z heißt **Zerfällungskörper von f über K** .

Es kann auch der Fall eintreten, daß über einem Körper K jedes Polynom vom Grade ≥ 1 in Linearfaktoren zerfällt.

(4.15) LEMMA: Für einen Körper K sind folgende Aussagen äquivalent:

- a) Jedes nichtkonstante Polynom aus $K[T]$ besitzt eine Nullstelle in K
- b) Jedes nichtkonstante Polynom aus $K[T]$ zerfällt über K in Linearfaktoren.
- c) Jedes über K irreduzible Polynom hat den Grad 1 (ist linear).

(4.16) DEF: Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom aus $K[T]$ eine Nullstelle in K besitzt.

(4.17) BEM: a) $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra)

b) Man kann zeigen, daß sich jeder Körper K in einen algebraisch abgeschlossenen Körper einbetten läßt (**algebraischer Abschluß von K**).