

Einschub D: Polynome

Ein "formaler Ausdruck" der Form

$$p = \sum_{i=0}^n a_i T^i = a_0 + a_1 T + a_2 T^2 + \dots + a_{n-1} T^{n-1} + a_n T^n,$$

wobei T eine "Unbestimmte" und die Koeffizienten a_i Elemente aus einem Körper K sind, heißt ein **Polynom in der Unbestimmten T über K** . Mit der Unbestimmten T kann man fast genauso rechnen wie mit Elementen aus K , allerdings darf T **nicht** invertiert werden. Zwei solche Polynome sind gleich, wenn Sie bei entsprechenden T -Potenzen dieselben Koeffizienten haben (man darf einen **Koeffizientenvergleich** vornehmen!). Polynome lassen sich addieren (koeffizientenweise) und multiplizieren (Cauchy-Produkt, ganz "normales" Ausmultiplizieren unter Berücksichtigung des Distributiv-Gesetzes).

Sind $p = \sum_{i=0}^n a_i T^i$ und $q = \sum_{j=0}^m b_j T^j$ zwei Polynome über K , so definiert man

$$p + q := \sum_{k=0}^r (a_k + b_k) T^k \quad \text{mit } r = \max(m, n)$$

$$p \cdot q := \sum_{k=0}^{m+n} c_k T^k \quad \text{mit } c_k = \sum_{i+j=k} a_i b_j \quad (k = 0, 1, \dots, m+n)$$

Bezüglich dieser Rechenoperationen bildet die Menge $K[T]$ aller Polynome in einer Unbestimmten über dem Körper K einen **kommutativen Ring**. Auf $K[T]$ läßt sich eine Skalarmultiplikation mit Elementen aus K definieren ($ap := \sum_{i=0}^n (aa_i) T^i \quad \forall a \in K, \forall p \in K[T]$), so daß $K[T]$ auch zu einem K -Vektorraum wird. Dieser Vektorraum ist unendlichdimensional, die Menge $\{1_K, T, T^2, T^3, \dots\}$ der Potenzen von T (es ist $T^0 := 1_K$) bildet eine K -Basis von $K[T]$.

Ist in einem Polynom $p = \sum_{i=0}^n a_i T^i$ der Koeffizient $a_n \neq 0_K$, so heißt dieser der **Leitkoeffizient** von p , und p hat dann den **Grad** n (in Zeichen: $\text{grad}(p) = n$). Dem **Nullpolynom**, bei dem alle Koeffizienten Null sind, wird kein Grad zugewiesen. Ein Polynom, dessen Leitkoeffizient gleich 1_K ist, heißt **normiert**, Polynome vom Grade 0 heißen **konstante Polynome**, Polynome vom Grade 1 **lineare Polynome**, Polynome vom Grade 2 **quadratische Polynome**.

Für Polynome $p, q \in K[T] \setminus \{0\}$ gilt

$$\text{grad}(p + q) \leq \max(\text{grad}(p), \text{grad}(q)) \quad (\text{falls } p + q \neq 0) \quad \text{und} \quad \text{grad}(p \cdot q) = \text{grad}(p) + \text{grad}(q)$$

In ein Polynom $p = \sum_{i=0}^n a_i T^i$ kann man Elemente aus einem K umfassenden Ring L einsetzen:

Für $\alpha \in L$ ist $p(\alpha) := \sum_{i=0}^n a_i \alpha^i \in L$ der **Wert von p an der Stelle α** . Insbesondere heißt α eine **Nullstelle von p** , wenn $p(\alpha) = 0$ gilt. Das Einsetzen in eine Summe geschieht summandenweise und das Einsetzen in ein Produkt faktorenweise, d.h.

$$(p + q)(\alpha) = p(\alpha) + q(\alpha) \quad , \quad (p \cdot q)(\alpha) = p(\alpha) \cdot q(\alpha)$$

In dem Polynomring $K[T]$ über einem Körper K läßt sich (entsprechend wie in \mathbb{Z}) **Division mit Rest** ausführen, genauer:

(D.1) SATZ: Zu zwei Polynomen $p, q \in K[T]$ mit $q \neq 0$ existieren eindeutig bestimmte Polynome $r, s \in K[T]$ mit $p = sq + r$, wobei entweder $r = 0$ ist oder $\text{grad}(r) < \text{grad}(q)$ gilt.

(D.2) FOLG: Der Polynomring in einer Unbestimmten über einem Körper K ist ein HIB.

(D.3) LEMMA: Seien $p \in K[T]$ und $\alpha \in K$. Dann sind äquivalent:

- a) α ist eine Nullstelle von p .
- b) Es existiert ein Polynom $q \in K[T]$ mit $p = (T - \alpha) \cdot q$.
(Man sagt hier: "Eine Nullstelle spaltet einen Linearfaktor von p ab")

(D.4) DEF: Sei $p \in K[T]$. Ein Element $\alpha \in K$ heißt eine k -**fache Nullstelle von p** , wenn es ein Polynom $q \in K[T]$ gibt mit

$$p = (T - \alpha)^k \cdot q \quad \text{und} \quad q(\alpha) \neq 0.$$

Die Zahl k heißt dann die **Vielfachheit der Nullstelle α** .

Bezeichnung: $k =: \mu(p, \alpha)$.

(D.5) SATZ: Ein Polynom $p \in K[T]$ vom Grade $n \geq 0$ hat höchstens n Nullstellen in K .

(D.6) SATZ: Fundamentalsatz der Algebra (Gauß, 1799)

Sei \mathbb{C} der Körper der komplexen Zahlen. Dann gilt:

- a) Ein Polynom $p \in \mathbb{C}[T]$ vom Grade ≥ 1 hat mindestens eine Nullstelle in \mathbb{C} .
- b) Ist $n = \text{grad}(p) \geq 1$ und sind $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ ($r \leq n$) die paarweise verschiedenen Nullstellen von p , so gilt:

$$(*) \quad p = a \cdot (T - \alpha_1)^{\mu(p, \alpha_1)} \cdot (T - \alpha_2)^{\mu(p, \alpha_2)} \cdot \dots \cdot (T - \alpha_r)^{\mu(p, \alpha_r)}$$

mit $\sum_{j=1}^r \mu(p, \alpha_j) = n = \text{grad}(p)$ (a ist der Leitkoeffizient von p).

Die Formel (*) besagt gerade, daß das Polynom p in **Linearfaktoren zerfällt**.

BEM: Natürlich gibt es eine im mathematischen Sinne exakte Einführung von Polynomen, bei der insbesondere die Unbestimmte T genau definiert wird. Dies geschieht in einer weiterführenden Algebra-Vorlesung.