Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Anhang 1

Der Polynomring über einem Körper

DEFINITION 1.1. Der *Polynomring* über einem Körper K besteht aus allen Polynomen

$$P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

mit $a_i \in K$, $n \in \mathbb{N}$, und mit komponentenweiser Addition und einer Multiplikation, die durch distributive Fortsetzung der Regel

$$X^n \cdot X^m := X^{n+m}$$

definiert ist.

Ein Polynom $P = \sum_{i=0}^{n} a_iX^i = a_0 + a_1X + \ldots + a_nX^n$ ist formal gesehen nichts anderes als das Tupel $(a_0, a_1, \ldots, a_n)$, die die *Koeffizienten* des Polynoms heißen. Der Körper K heißt in diesem Zusammenhang der *Grundkörper* des Polynomrings. Aufgrund der komponentenweisen Definition der Addition liegt unmittelbar eine Gruppe vor, mit dem *Nullpolynom* (bei dem alle Koeffizienten null sind) als neutralem Element. Zwei Polynome sind genau dann gleich, wenn sie in allen ihren Koeffizienten übereinstimmen. Die Polynome mit $a_i = 0$ für alle $i \geq 1$ heißen *konstante Polynome*, man schreibt sie einfach als a_0.

Die für ein einfaches Tupel zunächst ungewöhnliche Schreibweise deutet in suggestiver Weise an, wie die Multiplikation aussehen soll, das Produkt $X^n \cdot X^m$ ist nämlich durch die Addition der Exponenten gegeben. Dabei nennt man X die *Variable* des Polynomrings. Für beliebige Polynome ergibt sich die Multiplikation aus dieser einfachen Multiplikationsbedingung durch distributive Fortsetzung gemäß der Vorschrift, „alles mit allem“ zu multiplizieren. Die Multiplikation ist also explizit durch folgende Regel gegeben:

$$\sum_{i=0}^{n} a_iX^i \cdot \sum_{j=0}^{m} b_jX^j = \sum_{k=0}^{n+m} c_kX^k \text{ mit } c_k = \sum_{r=0}^{k} a_rb_{k-r}\,.$$

In ein Polynom $P \in K[X]$ kann man ein Element $a \in K$ *einsetzen*, indem man die Variable X an jeder Stelle durch a ersetzt. Dies führt zu einer Abbildung

$$K \longrightarrow K,\ a \longmapsto P(a),$$

die die durch das Polynom definierte *Polynomfunktion* heißt.

DEFINITION 1.2. Der *Grad* eines von null verschiedenen Polynoms

$$P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

mit $a_n \neq 0$ ist n.

Das Nullpolynom bekommt keinen Grad. Der Koeffizient a_n, der zum Grad n des Polynoms gehört, heißt *Leitkoeffizient* des Polynoms.

SATZ 1.3. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $P, T \in K[X]$ zwei Polynome mit $T \neq 0$. Dann gibt es eindeutig bestimmte Polynome $Q, R \in K[X]$ mit*

$$P = TQ + R \text{ und mit } \operatorname{grad}(R) < \operatorname{grad}(T) \text{ oder } R = 0\,.$$

Beweis. Wir beweisen die Existenzaussage durch Induktion über den Grad von P. Wenn der Grad von T größer als der Grad von P ist, so ist $Q = 0$ und $R = P$ die Lösung, so dass wir dies nicht weiter betrachten müssen. Bei $\operatorname{grad}(P) = 0$ ist nach der Vorbemerkung auch $\operatorname{grad}(T) = 0$ und damit ist (da $T \neq 0$ und K ein Körper ist) $Q = P/T$ und $R = 0$ die Lösung. Sei nun $\operatorname{grad}(P) = n$ und die Aussage für kleineren Grad schon bewiesen. Wir schreiben $P = a_nX^n + \ldots + a_1X + a_0$ und $T = b_kX^k + \ldots + b_1X + b_0$ mit $a_n, b_k \neq 0$, $k \leq n$. Dann gilt mit $H = \frac{a_n}{b_k}X^{n-k}$ die Beziehung

$$\begin{aligned} P' = P - TH = 0X^n + (a_{n-1} - \frac{a_n}{b_k}b_{k-1})X^{n-1} + \ldots \\ + (a_{n-k} - \frac{a_n}{b_k}b_0)X^{n-k} + a_{n-k-1}X^{n-k-1} + \ldots + a_0. \end{aligned}$$

Dieses Polynom P' hat einen Grad kleiner als n und darauf können wir die Induktionsvoraussetzung anwenden, d.h. es gibt Q' und R' mit

$$P' = TQ' + R' \text{ mit } \operatorname{grad}(R') < \operatorname{grad}(T) \text{ oder } R' = 0\,.$$

Daraus ergibt sich insgesamt

$$P \;=\; P' + TH \;=\; TQ' + TH + R' \;=\; T(Q' + H) + R',$$

so dass also $Q = Q' + H$ und $R = R'$ die Lösung ist. Zur Eindeutigkeit sei $P = TQ + R = TQ' + R'$ mit den angegebenen Bedingungen. Dann ist $T(Q - Q') = R' - R$. Da die Differenz $R' - R$ einen Grad kleiner als $\operatorname{grad}(T)$ besitzt, und der Polynomring nullteilerfrei ist, ist diese Gleichung nur bei $R = R'$ und somit $Q = Q'$ lösbar. □

LEMMA 1.4. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X - a$ ist.*

Beweis. Wenn P ein Vielfaches von $X - a$ ist, so kann man

$$P = (X - a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a) = (a-a)Q(a) = 0\,.$$

Im Allgemeinen gibt es aufgrund der Division mit Rest eine Darstellung

$$P = (X-a)Q + R\,,$$

wobei $R = 0$ oder aber den Grad null besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a) = R\,.$$

Wenn also $P(a) = 0$ ist, so muss der Rest $R = 0$ sein, und das bedeutet, dass $P = (X-a)Q$ ist. Also ist $X - a$ ein Linearfaktor von P. □

KOROLLAR 1.5. *Es sei K ein Körper und $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom (ungleich null) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d = 0, 1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P = Q(X-a)$ nach Lemma Anhang 1.4 und Q hat den Grad $d-1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d-1$ Nullstellen. Für $b \in K$ gilt $P(b) = Q(b)(b-a)$. Dies kann nur dann null sein, wenn einer der Faktoren null ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

KOROLLAR 1.6. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann besitzt jedes $P \in K[X]$, $P \neq 0$, eine Produktzerlegung*

$$P = (X-\lambda_1)^{\mu_1} \cdots (X-\lambda_k)^{\mu_k} \cdot Q$$

mit $\mu_j \geq 1$ und einem nullstellenfreien Polynom Q. Dabei sind die auftretenden verschiedenen Zahlen $\lambda_1, \ldots, \lambda_k$ und die zugehörigen Exponenten $\mu_1, \ldots, \mu_k$ (bis auf die Reihenfolge) eindeutig bestimmt.

Beweis. Siehe Aufgabe 17.7 (Mathematik (Osnabrück 2009-2011)/Teil I). □

Es gilt allgemeiner, dass die Zerlegung eines Polynoms in irreduzible Faktoren im Wesentlichen eindeutig ist. Der Polynomring $K[X]$ ist ein kommutativer Ring, aber kein Körper.