

§9 Der Zerfällungskörper eines Polynoms

(9.1) DEF: $L : K$ sei eine Körpererweiterung und $f \in K[T]$ sei ein Polynom vom Grade ≥ 1 . L heißt **Zerfällungskörper (ZFK) von f über K** , wenn gilt:

- a) f zerfällt über L in Linearfaktoren.
- b) Ist E ein beliebiger Zwischenkörper von $L : K$, über dem f in Linearfaktoren zerfällt, so folgt $E = L$.

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

- a) f besitzt einen Zerfällungskörper Z über K .
- b) $Z : K$ ist eine endliche Körpererweiterung.

Nachdem nun die Existenz eines Zerfällungskörpers gesichert ist, wenden uns der Frage nach seiner Eindeutigkeit zu. Dazu sind einige Vorbereitungen erforderlich. In Aufgabe 20 hatten wir gesehen, daß jeder Körperisomorphismus $\sigma : K \longrightarrow K'$ einen Ringisomorphismus $\bar{\sigma} : K[T] \longrightarrow K'[T]$ mit $\bar{\sigma}(a) = \sigma(a)$ ($\forall a \in K$) und $\bar{\sigma}(T) = T$ definiert.

(9.3) LEMMA: $L : K$ und $L' : K'$ seien Körpererweiterungen, $\sigma : K \longrightarrow K'$ sei ein Körperisomorphismus, $f \in K[T]$ sei ein irreduzibles Polynom, $\alpha \in L$ sei eine Nullstelle von f und $\beta \in L'$ sei eine Nullstelle von $\bar{\sigma}(f) \in K'[T]$. Dann existiert genau ein Körperisomorphismus

$$\rho : K(\alpha) \xrightarrow{\cong} K'(\beta)$$

mit $\rho(a) = \sigma(a)$ ($\forall a \in K$) und $\rho(\alpha) = \beta$.

(9.4) DEF: $L : K$ sei eine Körpererweiterung und $f \in K[T]$. Dann bezeichne

$$\text{Null}_L(f)$$

die Menge aller Nullstellen von f , die in L gelegen sind.

(9.5) SATZ: K und K' seien Körper, $\sigma : K \longrightarrow K'$ sei ein Körperisomorphismus und $f \in K[T]$ sei ein Polynom vom Grade ≥ 1 . Ist dann Z ein Zerfällungskörper von f über K und ist Z' ein Zerfällungskörper von $\bar{\sigma}(f)$ über K' , so gibt es einen Körperisomorphismus

$$\rho : Z \xrightarrow{\cong} Z'$$

mit **i)** $\rho(a) = \sigma(a)$ ($\forall a \in K$) und **ii)** $\rho(\text{Null}_Z(f)) = \text{Null}_{Z'}(\bar{\sigma}(f))$.

(9.6) KOROLLAR: Sind $Z : K$ und $Z' : K$ zwei Zerfällungskörper eines Polynoms $f \in K[T]$ vom Grade ≥ 1 , so gibt es einen Körperisomorphismus

$$\rho : Z \xrightarrow{\cong} Z'$$

mit $\rho(a) = a \quad (\forall a \in K) \quad \text{und} \quad \rho(\text{Null}_Z(f)) = \text{Null}_{Z'}(f).$

Fazit: Zu jedem Polynom $f \in K[T]$ vom Grade ≥ 1 gibt es einen Zerfällungskörper Z (9.2), der bis auf Isomorphie eindeutig bestimmt ist (9.6). Wir sprechen daher von dem Zerfällungskörper von f und benutzen die Bezeichnung

$$Z = \text{ZFK}_K(f).$$

Es gilt $\text{ZFK}_K(f) = K(\text{Null}_Z(f)).$

Wir wollen die gefundenen Ergebnisse auf **endliche Körper** anwenden.

(9.7) SATZ: Sind K und L **endliche Körper**, so gilt:

$$|K| = |L| \implies K \cong L.$$

Bew: Es wird gezeigt, daß K Zerfällungskörper des Polynoms $T^{|K|} - T \in P(K)[T]$ ist.

Um die Existenz endlicher Körper nachzuweisen, benötigen wir den Begriff der formalen Ableitung.

(9.8) DEF: Sei K ein Körper. Die Abbildung $D : K[T] \longrightarrow K[T]$, definiert durch

$$D\left(\sum_{\nu=0}^n a_\nu T^\nu\right) := \sum_{\nu=1}^n \nu a_\nu T^{\nu-1}$$

heißt **formale Ableitung in $K[T]$** . Man benutzt auch die Bezeichnung $D(f) =: f'$ für $f \in K[T]$.

(9.9) LEMMA: K sei ein Körper. Dann hat die formale Ableitung $D : K[T] \longrightarrow K[T]$ die folgenden Eigenschaften:

- a) D ist K -linear.
- b) Für alle $f, g \in K[T]$ gilt $D(fg) = fD(g) + D(f)g$.
- c) $\text{grad}(f) = n \geq 1 \implies \text{grad}(D(f)) \leq n - 1$ (falls $D(f) \neq 0$).
- d) $f \in K \implies D(f) = 0$.

(9.10) LEMMA: $\alpha \in L$ sei eine Nullstelle eines Polynoms $f \in K[T]$ in einem Erweiterungskörper L von K . Genau dann ist α eine einfache Nullstelle von f , wenn $f'(\alpha) \neq 0$ gilt.

(9.11) SATZ: Seien $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Dann existiert ein Körper K mit

$$|K| = p^n.$$

Bew: K wird als Zerfällungskörper des Polynoms $T^{p^n} - T \in \mathbb{Z}_p[T]$ konstruiert.

Fazit: Zu jeder Primzahl p und zu jeder natürlichen Zahl n gibt es einen endlichen Körper K mit p^n Elementen, und K ist bis auf Isomorphie eindeutig bestimmt. Nach (3.8) sind dies alle endlichen Körper.