Zerfällungskörper

Im Folgenden sei wieder $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ ein Körper.

Definition 73

Sei $\mathcal{F} = (f_i)_{i \in I}$ eine Familie von Polynomen $f_i \in K[X]$. Dann nennen wir

$$L := K(\{\alpha \in \mathbb{C} \mid f_i(\alpha) = 0 \text{ für ein } i \in I\})$$

(L = kleinster Körper, der sowohl K als auch $\{\alpha \in \mathbb{C} \mid f_i(\alpha) = 0 \text{ für ein } i \in I\}$ enthält)

den Zerfällungskörper von $\mathcal{F}$. Wir schreiben $L = ZFK(\mathcal{F})$.
Falls $\mathcal{F} = (f)$ nur aus einem Polynom besteht, schreiben $L = ZFK(f)$.

Beispiel $f = X^2 - 2 \in \mathbb{Q}[X]$. Die Nullstellen von f sind $\sqrt{2}$, $-\sqrt{2}$.
$\leadsto ZFK(f) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

Definition 74

Der algebraische Abschluss $\overline{K}$ von K ist

$$\overline{K} := ZFK(K[X] \setminus \{0\})$$

Bemerkung: $\overline{K} \subseteq \mathbb{C}$, da $\mathbb{C}$ selbst algebraisch abgeschlossen.

(Dabei heißt ein Körper L algebraisch abgeschlossen, falls jedes Polynom mit Koeff. in L bereits eine Nullstelle in L hat).

Definition 75

(1) Seien K und L Körper. Eine Abbildung $\sigma: K \to L$ heißt Körperhomomorphismus, falls:

(1) $\forall x, y \in K: \quad \sigma(x+y) = \sigma(x) + \sigma(y)$

(2) $\forall x, y \in K: \quad \sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$.

(3) $\sigma(1) = 1$.

(2) Seien K, L, L' Körper mit $K \subseteq L$, $K \subseteq L'$. Wir nennen $\sigma: L \to L'$ einen K-Homomorphismus, falls σ ein Körperhomomorphismus ist und für alle $x \in K$ gilt: $\sigma(x) = x$.

Wir schreiben:
$$\mathrm{Hom}(K, L) = \{\text{Körperhomomorphismen } \sigma: K \to L\}$$
$$\mathrm{Hom}_K(L, L') = \{K\text{-Homomorphismen } \sigma: L \to L'\}$$

Definition 76

Seien K, L Körper und sei $K \subseteq K'$ eine Körpererweiterung. Sei $\sigma \in \mathrm{Hom}(K, L)$. Wir nennen $\sigma' \in \mathrm{Hom}(K', L)$ eine Fortsetzung von σ, falls $\sigma'|_K = \sigma$.

Lemma 77

Sei $K' = K(\alpha)$ eine algebraische Körpererweiterung von K. Sei $f \in K[X]$ das Minimalpolynom von α, $f(X) = \sum_{i=0}^{d} a_i X^i$. Sei außerdem $\sigma \in \mathrm{Hom}(K, L)$, wobei L ein weiterer Körper ist.

(1) Falls $\sigma' \in \mathrm{Hom}(K', L)$ eine Fortsetzung von σ ist, so ist $\sigma'(\alpha)$ eine Nullstelle $f^\sigma := \sum_{i=0}^{d} \sigma(a_i) X^i$.

(2) Zu jeder Nullstelle $\beta \in L$ von f^σ gibt es genau eine Fortsetzung $\sigma' \in \mathrm{Hom}(K', L)$ von σ, so dass $\beta = \sigma'(\alpha)$.

Insbesondere ist die Anzahl der Fortsetzungen σ' gleich der Anzahl der Nullstellen von f^σ in L.

Beweis

(1) Es gilt:
$$f^\sigma(\sigma'(\alpha)) = \sum_{i=0}^{d} \sigma(a_i) \cdot \sigma'(\alpha)^i$$
$$= \sum_{i=0}^{d} \sigma'(a_i) \cdot \sigma'(\alpha^i)$$
$$= \sum_{i=0}^{d} \sigma'(a_i \cdot \alpha^i)$$
$$= \sigma'\Big(\sum_{i=0}^{d} a_i \alpha^i\Big) = \sigma'(0) = 0.$$

(2) Eindeutigkeit: Da $K' = K(\alpha) = \{ g(\alpha) \mid g \in K[X],\ \deg(g) < d \}$, folgt, dass σ' eindeutig durch Angabe von $\sigma'(\alpha)$ definiert ist.

Existenz: Sei $g(\alpha) \in K'$, $g \in K[X]$, $\deg(g) < d$, so dass $g(x) = \sum_{i=0}^{k} c_i \cdot x^i$.

Dann definieren eine Abbildung $\sigma' : K' \longrightarrow L$ durch:
$$\sigma'(g(\alpha)) := \sum_{i=0}^{k} \sigma(c_i) \cdot \beta^i \in L.$$
Per Definition gilt: $\sigma'|_K = \sigma$ und $\sigma' \in \mathrm{Hom}(K', L)$. $\square$

Korollar 78

Sei L ein algebraisch abgeschlossener Körper und $\sigma \in Hom(K, L)$.
Sei $K' := K(z_1, \ldots, z_m)$, wobei die z_i algebraisch über K sind ($K \subseteq K'$ ist eine endliche algebraische Körpererweiterung). Dann exististiert eine Fortsetzung $\sigma' \in Hom(K', L)$ von σ.

Beweis

Sei $K_i = K(z_1, \ldots, z_i)$. Dann ist $K_i = K_{i-1}(z_i)$. Für $\sigma_i \in Hom(K_{i-1}, L)$ finden wir eine Fortsetzung $\sigma_{i+1} \in Hom(K_i, L)$ (wegen Lemma 77 und weil L algebraisch abgeschlossen ist). Dann ist $\sigma_m = \sigma'$. $\square$

<u>Erinnerung</u> $Hom_K(K', L) = \{ \sigma \in Hom(K', L) \mid \forall x \in K: \sigma(x) = x \}$
$= \{ \sigma \in Hom(K', L) \mid \sigma \text{ setzt } id_K \text{ fort} \}$.
sind die K-Homomorphismen $K' \to L$.

Satz 79

Sei $L = K(z_1, \ldots, z_m)$ eine endliche algebraische Körpererweiterung und sei $\bar{L}$ der algebraische Abschluss von L. Dann sind die folgenden drei Punkte äquivalent:

(1) Jeder K-Homomorphismus $\sigma: L \to \bar{L}$ beschränkt sich auf einen K-Homomorphismus $\sigma: L \to L$. D.h. $Hom_K(L, \bar{L}) = Hom_K(L, L)$.

(2) L ist ein Zerfällungskörper einer Familie von Polynomen in $K[x]$.

(3) Jedes Polynom $f \in K[x]$, welches in L eine Nullstelle hat, hat alle Nullstellen in L.

Beweis

(1) ⇒ (3): Sei also $f \in K[X]$ und $a \in L$ eine Nullstelle von f. Sei $b \in \overline{L}$ eine weitere Nullstelle von f. Mit Lemma 77 finden wir einen Körperhomomorphismus $\sigma: K(a) \to \overline{L}$, der die Identität auf K fortsetzt und so dass $\sigma(a) = b$. D.h. $\sigma \in Hom_K(K(a), \overline{L})$. Wir finden mit Korollar 78 eine Fortsetzung $\sigma' \in Hom_K(L, \overline{L})$ von σ. Nach Annahme gilt: $\sigma' \in Hom_K(L, L)$.

$\Rightarrow b = \sigma(a) = \sigma'(a) \in L$.

(3) ⇒ (2): Sei $f_i \in K[X]$ das Minimalpolynom von z_i. Nach Annahme sind alle Nullstellen von f_i in L enthalten.

$\Rightarrow L = ZFK((f_1, \ldots, f_m))$.

(2) ⇒ (1): Sei $L = ZFK(\mathcal{F})$, mit $\mathcal{F} = (f_i)_{i \in I}$. Und sei $\sigma \in Hom_K(L, \overline{L})$. Da $f_i \in K[X]$, ist $f_i^\sigma = f_i \in K[X]$. $\Rightarrow \sigma(L)$ ist auch Zerfällungskörper der Familie $\mathcal{F}$ $\Rightarrow L = \sigma(L)$. $\Rightarrow \sigma \in Hom_K(L, L)$. □

Satz 80

Sei $L = K(z_1, \ldots, z_m)$ eine endliche algebraische Körpererweiterung von K. Dann gilt:

$$[L : K] = \# Hom_K(L, \overline{K}).$$

Bemerkung Da $\overline{K} = \overline{L}$, ergibt sich für einen Zerfällungskörper L:

$[L : K] = \# Hom_K(L, L)$.

Beweis von Satz 80

Sei $K_i := K(z_1, \dots z_i)$, so dass $K_i = K_{i-1}(z_i)$. Sei $f_i \in K_{i-1}[x]$ das Minimalpolynom von z_i über K_{i-1}. Dann gilt:

- $[K_i : K_{i-1}] = \deg(f_i)$
- Nach Lemma 77 (2): $\# \mathrm{Hom}_{K_{i-1}}(K_i, \overline{K}) = \deg(f_i)$.

$\Rightarrow [K_i : K_{i-1}] = \# \mathrm{Hom}_{K_{i-1}}(K_i, \overline{K})$.

Andererseits: $[L : K] = [K_m : K_{m-1}] \cdot [K_{m-1} : K_{m-2}] \cdot \dots [K_1 : K]$.

$$= \# \mathrm{Hom}_{K_{m-1}}(K_m, \overline{K}) \cdot \dots \cdot \# \mathrm{Hom}_K(K_1, \overline{K}) =: (*)$$

Wir müssen jetzt zeigen, dass $(*) = \# \mathrm{Hom}_K(L, \overline{K})$.

Dazu genügt es das folgende Hilfslemma zu beweisen:

Hilfslemma:

Sei $K \subseteq L \subseteq M$ eine Kette von endlichen algebraischen Körpererweiterungen.

Dann gilt: $\# \mathrm{Hom}_K(M, \overline{K}) = \# \mathrm{Hom}_L(M, \overline{K}) \cdot \# \mathrm{Hom}_K(L, \overline{K})$.

Beweis

Sei $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i \mid i \in I\}$, $\mathrm{Hom}_L(M, \overline{K}) = \{\tau_j \mid j \in J\}$.

Mit Korollar 78 kann ich die σ_i fortsetzen zu $\sigma_i' : M \to \overline{K}$.

Zu zeigen: (1) Die $\sigma_i' \circ \tau_j$ für $i \in I$, $j \in J$ sind paarweise verschieden.

(2) $\mathrm{Hom}_K(M, \overline{K}) = \{\sigma_i' \circ \tau_j \mid i \in I, j \in J\}$

Zu (1): Sei $\sigma_i' \circ \tau_j = \sigma_k' \circ \tau_\ell$. Da τ_j und τ_ℓ auf L die Identität sind, gilt: $\sigma_i' = \sigma_k'$ und damit gilt auch $\tau_j = \tau_\ell$.

$\Rightarrow i = k$ und $j = \ell$.

Zu (2): Sei $\pi \in \mathrm{Hom}_K(M, \overline{K})$. Dann ist die Einschränkung

$\pi|_L \in \mathrm{Hom}_K(L, \overline{K}) \Rightarrow \exists\, i \in I : \pi|_L = \sigma_i'$.

$\Rightarrow (\sigma_i')^{-1} \circ \pi \in \mathrm{Hom}_L(M, \overline{K}) \Rightarrow \exists\, j \in J : (\sigma_i')^{-1} \circ \pi = \tau_j$

$\Rightarrow \pi = \sigma_i' \circ \tau_j$. $\square$

<u>Bemerkung</u> Die meisten Resultate in dieser Vorlesung wurden für endliche Körpererweiterungen bewiesen. Die meisten davon lassen sich auch für unendliche Körpererweiterungen verallgemeinern.