

6 Struktur von Körpererweiterungen

Körpertheorie ist das Studium von Körpererweiterungen, insbesondere ihre Konstruktion, Klassifikation, und das Lösen von Gleichungen darin.



Erinnerung:

Betrachte eine Körpererweiterung L/K und ein Element $a \in L$.

3.2.1 Definition: Der Grad von L/K ist $[L/K] := \dim_K(L)$. Ist dieser endlich, so heisst L/K endlich.

3.3.1 Definition: Existiert ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$, so heisst a algebraisch über K , andernfalls transzendent über K .

3.3.8 Proposition: Für a algebraisch über K existiert genau ein normiertes Polynom $m_a = m_{a,K} \in K[X]$ mit den äquivalenten Eigenschaften:

- m_a ist das eindeutige normierte Polynom $f \in K[X]$ von minimalem Grad mit $f(a) = 0$.
- m_a ist das eindeutige normierte irreduzible Polynom $f \in K[X]$ mit $f(a) = 0$.
- Wir haben einen Isomorphismus der Form $K[X]/(m_a) \xrightarrow{\sim} K(a)$, $f + (m_a) \mapsto f(a)$.

Für dieses gilt weiter $\deg(m_a) = [K(a)/K]$.

3.3.9 Definition: Das Polynom $m_a = m_{a,K}$ heisst das Minimalpolynom von a über K .

Sein Grad heisst auch der Grad von a über K .

3.4.1 Definition: L/K heisst *algebraisch*, wenn jedes $a \in L$ algebraisch über K ist; sonst *transzendent*.

3.4.3-5 Proposition: Es sind äquivalent:

- L/K ist endlich.
- L/K ist endlich erzeugt und algebraisch.
- L/K ist von endlich vielen über K algebraischen Elementen erzeugt.

$K(a_1, \dots, a_n) \subset L$
|
endlich
|
 K

Nun betrachte einen Körperturm $M/L/K$.

3.2.4 Proposition: Es gilt $[M/K] = [M/L] \cdot [L/K]$.

Insbesondere ist M/K endlich genau dann, wenn M/L und L/K endlich sind.

3.4.10 Proposition: Es ist M/K algebraisch genau dann, wenn M/L und L/K algebraisch sind.

3.1.5 Proposition: Jeder Körperhomomorphismus $K \rightarrow L$ ist injektiv.

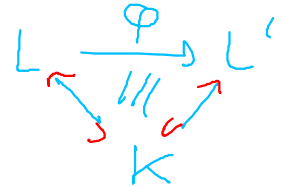
3.1.6 Bemerkung: Durch einen Körperhomomorphismus $K \hookrightarrow L$ kann man K mit einem Unterkörper von L identifizieren. Dies sollte man aber nur dann tun, wenn man nur einen einzigen Homomorphismus betrachtet und ihn später nicht mehr abändert.

6.1 Transzendente Körpererweiterungen

eventuell später

6.2 Homomorphismen zwischen Körpererweiterungen

Betrachte zwei Körpererweiterungen L/K und L'/K .



6.2.1 Definition: Ein Körperhomomorphismus $L \rightarrow L'$, der auf K die Identität ist, heisst ein **Homomorphismus über K** . Die Menge aller Homomorphismen $L \rightarrow L'$ über K bezeichnen wir mit $\text{Hom}_K(L, L')$. Ein Homomorphismus über K , der ein Isomorphismus ist, heisst ein **Isomorphismus über K** .

6.2.2 Beispiel: Die komplexe Konjugation $\mathbb{C} \rightarrow \mathbb{C}$ ist ein Isomorphismus über \mathbb{R} .

6.2.3 Beispiel: Die Abbildung $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ mit $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ für alle $a, b \in \mathbb{Q}$ ist ein Isomorphismus über \mathbb{Q} .

6.2.4 Proposition: Ist $[L/K] = [L'/K] < \infty$, so ist jeder Homomorphismus $L \rightarrow L'$ über K ein Isomorphismus.

Beweis: φ ist K -Vektraumhomom., injektiv,
 $\dim_K(L) = \dim_K(L')$

gesd.

6.2.5 Proposition: Für jedes $\varphi \in \text{Hom}_K(L, L')$ gilt: Ein Element $a \in L$ ist algebraisch über K genau dann, wenn $\varphi(a)$ algebraisch über K ist. In diesem Fall haben a und $\varphi(a)$ dasselbe Minimalpolynom und denselben Grad über K .

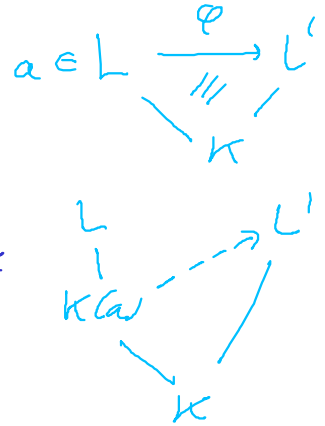
Bem.: Für jedes $f \in K[X] \setminus \{0\}$ gilt $f(a) = 0 \Leftrightarrow \varphi(f(a)) = 0$
 \Leftrightarrow algebraisch über K \Leftrightarrow $f(\varphi(a)) = 0$ ged.

6.2.6 Proposition: Für jedes $a \in L$ haben wir eine natürliche Bijektion

$$\text{Hom}_K(K(a), L') \xrightarrow{\sim} \{a' \in L' \mid m_{a,K}(a') = 0\}, \quad \varphi \mapsto \varphi(a).$$

Bem.: Wohldef. Abb. wegen $(*)$. Umgekehrt; Sei ψ

$$\begin{array}{ccc} K(a) \cong K[X]/(m_{a,K}) & \xrightarrow{\exists!} & L' \\ \psi \uparrow & \nearrow \psi & \\ a \cong [X] & \xrightarrow{f \mapsto f(a')} & a' \end{array} \quad \begin{array}{l} \text{Richtigkeit} \\ \text{ged.} \end{array}$$



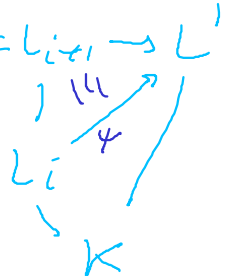
6.2.7 Proposition: Ist L/K endlich, so gilt $|\text{Hom}_K(L, L')| \leq [L/K]$.

Bem.: Schreibe $L = K(a_1, \dots, a_n)$; Sei $L_i := K(a_1, \dots, a_i)$ $L_i(a_{i+1}) = L_{i+1} \rightarrow L'$
 $\Rightarrow L_0 = K, |\text{Hom}_K(L_0, L')| = 1 = [L_0/K]$

Ist $|\text{Hom}_K(L_i, L')| \leq [L_i/K]$ für $i < n$, so folgt:

Jedes $\varphi \in \text{Hom}_K(L_{i+1}, L')$ induziert $\varphi|_{L_i} \in \text{Hom}_K(L_i, L')$

Für jedes $\psi \in \text{Hom}_K(L_i, L')$ forme L' als Erweiterung von L_i auf
 dann folgt aus 6.2.6: $|\{\varphi \in \text{Hom}_K(L_{i+1}, L') : \varphi|_{L_i} = \psi\}| \leq [L_{i+1}/L_i]$.



$$\Rightarrow |\text{Hom}_K(L_i, L')| \leq |\text{Hom}_K(L_i, L)| \cdot [L_i/L] \leq [L_i/K] \cdot [L_i/L] = [L_i/L]^2$$

6.2.8 Satz: Ist L/K algebraisch und L' algebraisch abgeschlossen, so ist $\text{Hom}_K(L, L') \neq \emptyset$.

Früher mit Zählweise gel.

6.2.9 Definition: Ein Körperautomorphismus von L , der auf K die Identität ist, heisst ein Automorphismus über K . Die Menge aller Automorphismen von L über K bezeichnen wir mit $\text{Aut}_K(L)$.

Beweis: Sei $S := \{(\pi, \varphi) \mid K \subset \pi \subset L \text{ Zwischenkörper}, \varphi \in \text{Hom}_K(\pi, L')\}$

Setze $(\pi, \varphi) \preceq (\pi', \varphi') \Leftrightarrow \pi \subset \pi'$ und $\varphi = \varphi'|_{\pi}$.

Partialordnung auf S . Wegen $(K, id) \in S$ ist $S \neq \emptyset$.

Sei $T \subset S$ eine Kette. Setze $\tilde{\pi} := \bigcup_{(\pi, \varphi) \in T} \pi \stackrel{\tilde{\varphi}}{\rightarrow} L'$
 $\Rightarrow (\tilde{\pi}, \tilde{\varphi}) \in S$ ist obere Schranke von T .

Zum $\Rightarrow S$ besitzt ein maximales Element (π, φ) .

Wäre $\pi \neq L$, wähle $a \in L \setminus \pi \Rightarrow a$ algebraisch über π .

Sei $f \in \pi[x]$ sein Min.Pol. über $\pi \Rightarrow \varphi(f) \in L'[x]$ univert
 von Grad > 0

$$\Rightarrow \exists a' \in L' : \varphi(f)(a') = 0$$

6.2.6. $\Rightarrow \exists \varphi' \in \text{Hom}_K(\pi(a), L')$ mit $\varphi'|_{\pi} = \varphi$ und $\varphi'(a) = a'$.
 also bildet $\pi = L$ gel. K $\Rightarrow (\pi(a), \varphi') \in S$ echt größer als $(\pi, \varphi) \Rightarrow \text{ggl.}$



6.2.10 Proposition: Ist L/K algebraisch, so ist $\text{Hom}_K(L, L) = \text{Aut}_K(L)$.

Beweis: Zu zeigen: Jeder $\varphi \in \text{Hom}_K(L, L)$ ist surjektiv.

Sei $a \in L$ mit Minimal $f \in K[X]$ über K .

Sei $S := \{a' \in L \mid f(a') = 0\}$.

$\Rightarrow \varphi$ induziert $S \rightarrow S, a' \mapsto \varphi(a')$.

die ist injektiv. } \Rightarrow surjektiv,
 S endlich

Jeder $a \in S$ ist im Bild. qed.

6.2.11 Beispiel: Die Abbildung $K(X) \rightarrow K(X), f(X) \mapsto f(X^2)$ ist ein Homomorphismus über K , aber kein Automorphismus.

6.3 Konstruktion von Körpererweiterungen

6.3.1 Definition: Sei $f \in K[X]$ irreduzibel. Ein Oberkörper von K der Form $K(a)$ mit $f(a) = 0$ heisst ein Stammkörper von f über K .

6.3.2 Beispiel: Für jede Körpererweiterung L/K und jedes über K algebraische Element $a \in L$ ist $K(a)$ ein Stammkörper des Minimalpolynoms $m_{a,K}$ über K .

6.3.3 Proposition: Jedes irreduzible Polynom $f \in K[X]$ besitzt einen Stammkörper L über K . Dabei ist das Paar (L, a) bis auf eindeutige Isomorphie über K bestimmt.

Bem. $L := K[X]/(f) = \text{Körper.}$ $\Rightarrow f(a) = f(x) + (f) = (f) = 0$.
 ψ
 $a := x + (f)$ und $L = K(a)$.

Sei (L', a') ein weiteres Paar wie oben. Objekt f variiert.

$\Rightarrow L = K[X]/(f) \xrightarrow{\exists! \psi} L'$
 ψ
 $a = x + (f) \mapsto a'$

qed.

6.3.4 Definition: Sei $f \in K[X] \setminus \{0\}$. Ein Oberkörper von K der Form $L = K(a_1, \dots, a_n)$ mit

$$f(X) = \alpha \prod_{i=1}^n (X - a_i) \quad \text{in} \quad L[X]$$

für ein $\alpha \in L^\times$ heisst ein Zerfällungskörper von f über K .

6.3.5 Proposition: Jedes Polynom $f \in K[X] \setminus \{0\}$ besitzt einen Zerfällungskörper über K . Dieser ist bis auf Isomorphie über K bestimmt; der Isomorphismus ist aber im allgemeinen nicht eindeutig.

Beweis: Zuelement über $\deg(f)$. $\deg(f) = 0 \Rightarrow K$ tut's.

$\deg(f) > 0 \Rightarrow$ wähle irgnd. Faktor g

wähle Stammkörper $K(a_1)$ von g über K .

Schreibe $f(X) = (X - a_1) \cdot h(X)$ für $h \in K(a_1)[X] \setminus \{0\}$.

Sei L ein Zerfällungskörper von h über $K(a_1)$.

$$L = K(a_1)(a_2, \dots, a_n) \quad \text{mit} \quad h(X) = \alpha \cdot \prod_{i=2}^n (X - a_i)$$

$$\Rightarrow L = K(a_1, \dots, a_n) \quad \text{mit} \quad f(X) = \alpha \cdot \prod_{i=1}^n (X - a_i) \quad \Rightarrow \text{Existenz.}$$

Sei $L' = K(a'_1, \dots, a'_n)$ ein weiterer Zerfällungskörper von f über K :

Dann $\exists i: a'_i$ Nullstelle von g

6.2.6 $\Rightarrow \exists \varphi \in \text{Hom}_K(K(a_1), L')$ mit $\varphi(a_1) = a'_i$. Betrachte L' als Erweiterung von $K(a_1)$ via φ .

Zurück in L, L' zerf. Körper von h über $K(a_1) \Rightarrow \varphi$ besitzt eine Fortsetzung zu $L \xrightarrow{\sim} L'$. qed.

