

Algebraische Körpererweiterungen

Definition 59

Seien K, L Körper mit $K \subseteq L$. Dann nennen wir L eine Körpererweiterung von K .

Definition 60

Sei K ein Körper und $f(x) = \sum_{i=0}^d a_i \cdot x^i$ mit $a_i \in K$, ein Polynom mit Koeffizienten in K .

$$(1) \quad K[x] = \left\{ \sum_{i=0}^d a_i x^i \mid d \geq 0, a_i \in K \right\}$$

(2) Sei $f = \sum_{i=0}^d a_i x^i \in K[x]$ mit $a_d \neq 0$, dann nennen wir $d := \deg(f)$ den Grad von f .

(3) $f \in K[x]$ heißt irreduzibel, falls:

$$\text{" } f(x) = g(x) \cdot h(x) \Rightarrow g(x) \in K \text{ oder } f(x) \in K \\ (\text{d.h. } \deg(g) = 0 \text{ oder } \deg(f) = 0)$$

Im Folgenden wollen wir die Theorie der alg. Körpererweiterungen von \mathbb{Q} behandeln.

(Der allgemeine Fall lässt auch endliche Körper \mathbb{F}_p zu)

Lemma 61

Sei K ein Körper mit $K \subseteq \mathbb{Q}$. Dann ist $\mathbb{Q} \subseteq K$.

Beweis

Da K ein Körper ist, ist $1 \in K$. $\Rightarrow \mathbb{Z} \subseteq K \Rightarrow \mathbb{Q} \subseteq K$. \square

In Folgenden: K ist ein Körper mit $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$.

Definition 62

Sei $f(x) \in K[x]$, $f(x) = \sum_{i=0}^d \alpha_i x^i$.

- (1) $z \in \mathbb{C}$ heißt Nullstelle von f , falls $f(z) = \sum_{i=0}^d \alpha_i z^i = 0$.
- (2) $z \in \mathbb{C}$ heißt algebraisch über K , falls $f \in K[x]$ existiert mit $f(z) = 0$.

Definition 63

Sei $K \subseteq L$ eine Körpererweiterung. Wir nennen diese eine algebraische Körpererweiterung, wenn alle $z \in L$ algebraisch über K sind.

Beobachtung Sei $K \subseteq L$ eine Körpererweiterung. Dann ist L ein K -Vektorraum.

Definition 64

- (1) $[L : K] := \dim_K(L)$ heißt der Erweiterungsgrad von L über K .
- (2) Wir nennen $K \subseteq L$ eine endliche Körpererweiterung, falls $[L : K] < \infty$.

Satz 65

Jede endliche Körpererweiterung von K ist algebraisch über K .

Beweis

Sei $K \subseteq L$ mit $[L:K] =: n < \infty$. Sei $z \in L$.

Die Elemente $1, z^1, z^2, \dots, z^n$ sind nicht linear unabhängig über K . D.h. es existieren $a_0, \dots, a_n \in K$ mit

$$a_0 \cdot 1 + a_1 \cdot z^1 + \dots + a_n \cdot z^n = 0$$

$\Rightarrow z$ ist algebraisch über L .

Satz 66

Seien $K \subseteq L \subseteq M$ eine Reihe von Körpererweiterungen. Dann gilt:

$$[M:K] = [M:L] \cdot [L:K]$$

Beweis

Zunächst: Annahme $n := [M:L], m := [L:K] < \infty$.

Seien x_1, \dots, x_m eine K -Basis von L und y_1, \dots, y_n eine L -Basis von M .

Behauptung: $x_i \cdot y_j \quad i=1, \dots, m, j=1, \dots, n$ sind eine K -Basis von M

Lineare Unabh.: Sei $\sum_{i,j} c_{ij} \cdot x_i \cdot y_j = 0$

$$\Rightarrow \sum_j \underbrace{\left(\sum_i c_{ij} x_i \right)}_{\in L} y_j = 0 \Rightarrow \sum_i c_{ij} x_i = 0 \quad \downarrow \in K$$

$$\Rightarrow c_{ij} = 0 \text{ für alle } i, j$$

Erzeugendensystem: Sei $z \in M$. Dann ist $z = \sum_{j=1}^n z_j \cdot y_j$ für geeignete $z_j \in L$

Wir finden $c_{ij} \in K$ s.d. $z_j = \sum_{i=1}^m c_{ij} x_i$.

$$\Rightarrow z = \sum_{j=1}^n \left(\sum_{i=1}^m c_{ij} x_i \right) y_j = \sum_{i,j} c_{ij} x_i y_j$$

Falls $[L:K]$ oder $[M:L]$ unendlich ist, dann zeigt der obige Beweis, dass M unendlich viele linear unabhängige Elemente enthält. $\Rightarrow [M:K] = \infty$. □

Definition 67

Sei $K \subseteq L$ eine alg. Körpererweiterung und $z \in L$.

Ein Minimalpolynom von z ist ein Polynom $f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i \in K[x]$, so dass $f(z) = 0$ und so dass f den geringsten Grad $d = \deg(f)$ mit dieser Eigenschaft. Wir nennen f Minimalpolynom von z über K .

Lemma 68

Sei $K \subseteq L$ eine alg. Körpererweiterung und $z \in L$.

Das Minimalpolynom von $z \in L$ ist eindeutig und irreduzibel.

Beweis

Eindeutigkeit Seien $f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$ und $g(x) = x^d + \sum_{i=0}^{d-1} b_i x^i$.

Dann gilt: $f(z) - g(z) = \sum_{i=0}^{d-1} (a_i - b_i) z^i = 0$.

Da $\deg(\sum_{i=0}^{d-1} (a_i - b_i) x^i) \leq d-1$, muss $\sum_{i=0}^{d-1} (a_i - b_i) x^i = 0 \Rightarrow f(x) = g(x)$.

Irreduzibilität Sei $f(x) \in K[x]$ das Minimalpolynom von z und $f(x) = g(x) \cdot h(x)$.

$\Rightarrow f(z) = g(z) \cdot h(z) = 0 \Rightarrow \text{ObdA } g(z) = 0$.

Falls $0 < \deg(g), \deg(h) < \deg(f) \Rightarrow \deg(g) < \deg(f) \Leftarrow$ Widerspruch dazu, dass f das Minimalpolynom ist.

$\Rightarrow \deg(g) = \deg(f) \Rightarrow f$ ist irreduzibel. \square

Definition 69

Sei K ein Körper und $z_1, \dots, z_m \in \mathbb{C}$ algebraisch über K .

Wir definieren: $K(z_1, \dots, z_m) := \bigcap_{\substack{L \text{ Körper} \\ L \supset K \cup \{z_1, \dots, z_m\}}} L$

Satz 70

Sei $z \in \mathbb{C}$ mit Minimalpolynom $f(x) \in K[x]$ über K .

Dann gilt: $[K(z) : K] = \deg(f)$.

Beweis

Sei $f(x) = \sum_{i=0}^d a_i x^i \in K[x]$ das Minimalpolynom von z über K mit $d = \deg(f)$. Dann definier:

$$L := \left\{ \sum_{i=0}^{d-1} c_i z^i \mid c_i \in K \right\} = \{ g(z) \mid g \in K[x], \deg(g) \leq d-1 \}$$

Per Definition ist L ein K -VR von Dimension $\dim_K(L) \leq d$.

Ang. $\{1, z^1, \dots, z^{d-1}\}$ sind nicht L.u., dann finden wir ein Polynom $g(x) \in K[x]$ mit $\deg(g) < d$, und $g(z) = 0$. \rightarrow Widerspruch.
 $\Rightarrow \dim_K(L) = d$.

Behauptung: $L = K(z)$.

Per Definition gilt $L \subseteq K(z)$. Es genügt zu zeigen, dass L ein Körper ist.

1. L ist eine abelsche Gruppe bzgl "+"

2. $L \setminus \{0\}$ ist eine abelsche Gruppe bzgl. "·".

\rightsquigarrow z.z.: für $a, b \in L \setminus \{0\}$ gilt: $\frac{a}{b} \in L \setminus \{0\}$.

Wir werden zeigen: (1) $a \cdot b \in L \setminus \{0\}$

$$(2) \frac{1}{b} \in L \setminus \{0\}$$

Zu (1): Sei $a = g(z)$, $b = h(z)$, mit $g, h \in K[x]$, $\deg(g) \leq d-1$
Dann gilt: $\deg(h) \leq d-1$.

$$\deg(g \cdot h) \leq 2(d-1).$$

Anwendung des euklid'schen Algorithmus liefert:

$$g(x) \cdot h(x) = q(x) \cdot f(x) + r(x),$$

wobei: $q(x) \in K[x]$, $r(x) \in K[x]$, $\deg(r) < \deg(f) = d$.

$$\Rightarrow a \cdot b = g(z) \cdot h(z) = q(z) \cdot f(z) + r(z) = r(z)$$

$$\Rightarrow a \cdot b \in L \setminus \{0\}. \quad \text{mit } \dim_K(L) = d$$

Zu (2): L ist ein K -VR mit einer Multiplikation $\cdot : L \times L \rightarrow L$.
($\rightsquigarrow L$ ist eine K -Algebra)

Sei $b \in L$. Dann sind: $1, b, b^2, \dots, b^d \in L$

\rightsquigarrow es existieren $z_0, \dots, z_d \in K$: $\sum_{i=0}^k z_i b^i = 0$, mit $1 \leq k \leq d$.

$$\text{OBdA: } z_0 \neq 0. \Rightarrow z_0 = - \sum_{i=1}^k z_i b^i = b \left(\sum_{i=1}^k z_i b^{i-1} \right)$$

$$\Rightarrow b \cdot \underbrace{\left(\frac{1}{z_0} \cdot \sum_{i=1}^k z_i b^{i-1} \right)}_{\in L, \text{ weil es eine Linearkombination aus Elementen in } L \text{ ist.}} = 1$$

Bemerkung Der Beweis des Satzes liefert insbesondere:

Sei $f(x) = \sum_{i=0}^d a_i x^i \in K[x]$ das Minimalpolynom von $z \in \mathbb{C}$ über K mit $d = \deg(f)$. Dann gilt:

$$K(z) = \left\{ \sum_{i=0}^{d-1} c_i z^i \mid c_i \in K \right\} = \{ g(z) \mid g \in K[x], \deg(g) \leq d-1 \}$$

Satz 71

Seien $z_1, \dots, z_k \in \mathbb{C}$ algebraisch über K . Dann ist
 $K(z_1, \dots, z_k)$ eine algebraische Körpererweiterung von K .

Beweis

Für $1 \leq i \leq k$ definieren wir $K_i := K(z_1, \dots, z_i)$. Dann gilt:

$$K_{i+1} = K_i(z_{i+1})$$

Nach Satz 70 ist $[K_{i+1} : K_i] < \infty$.

Nach Satz 66 gilt: $[K_K : K] = \underbrace{[K_K : K_{k-1}]}_{<\infty} \cdot \underbrace{[K_{k-1} : K_{k-2}]}_{<\infty} \cdots \underbrace{[K_1 : K]}_{<\infty}$
 $\Rightarrow [K(z_1, \dots, z_k) : K] < \infty$

Da endliche Körpererweiterungen algebraisch sind, ist also
 $K(z_1, \dots, z_k)$ eine algebraische Körpererweiterung von K \square

Satz 72

Sei $K \subseteq L$ eine algebraische Körpererweiterung und sei $z \in \mathbb{C}$ algebraisch über L . Dann ist z auch algebraisch über K .

Beweis

Sei $f(x) \in L[x]$ mit $f(z) = 0$. Wir schreiben $f(x) = \sum_{i=0}^d c_i x^i$ mit $c_i \in L$. Dann gilt: z ist algebraisch über $K(c_0, \dots, c_d)$.

Nach Annahme sind die c_0, \dots, c_d algebraisch über K .

$\Rightarrow [K(c_0, \dots, c_d) : K] < \infty$. Und es gilt: $[K(z, c_0, \dots, c_d) : K(c_0, \dots, c_d)] < \infty$

\swarrow folgt aus dem Beweis von Satz 71 \searrow Satz 65

Aus Satz 66 folgt: $[K(z, c_0, \dots, c_d) : K] < \infty \Rightarrow z$ algebraisch über K . \square