Der Grad einer Körpererweiterung

Definition (15.5)

Ist $L|K$ eine Körpererweiterung, dann definieren die beiden Abbildungen

$$+ : L \times L \to L\ ,\ (\alpha, \beta) \mapsto \alpha + \beta \quad \text{und} \quad \cdot : K \times L \to L\ ,\ (a, \alpha) \mapsto a\alpha$$

eine K-Vektorraumstruktur auf L. Dabei bezeichnet man $[L : K] = \dim_K L$ als den Grad der Körpererweiterung. Ist $[L : K]$ endlich, dann nennt man $L|K$ eine endliche Körpererweiterung.

Algebraische und transzendente Elemente

Definition (15.7)

Sei $L|K$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt algebraisch über K, wenn ein Polynom $f \neq 0$ in $K[x]$ mit der Eigenschaft existiert, dass α eine Nullstelle von f ist. Gibt es ein solches Polynom nicht, dann nennt man α transzendent über K.

Definition (15.8)

Sei $L|K$ eine Körpererweiterung, und sei $\alpha \in L$ algebraisch über K. Dann gibt es ein eindeutig bestimmtes, normiertes Polynom $f \in K[x]$, $f \neq 0$ minimalen Grades mit $f(\alpha) = 0$. Man nennt f das Minimalpolynom von α über K. Wir bezeichnen es mit $\mu_{\alpha,K}$.

Die Struktur einfacher algebraischer Erweiterungen

Satz (15.10)

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K, $f = \mu_{\alpha,K}$ und $n = \mathrm{grad}(f)$. Dann bilden die Elemente

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

eine Basis von $K(\alpha)$ als K-Vektorraum. Insbesondere gilt $[K(\alpha) : K] = n$.

Anwendungsbeispiel zu Satz 10.

Rechnen in einem Körper mit 9 Elementen

Achtung: $\mathbb{Z}/9\mathbb{Z}$ ist kein solcher Körper

Sei $L|\mathbb{F}_3$ eine Körpererweiterung und $\alpha \in L$ mit $\alpha^2 = -\bar{1} = \bar{2}$. Beh.: $|\mathbb{F}_3(\alpha)| = 9$

Zeige zunächst das Minimalpolynom $\mu_{\alpha,\mathbb{F}_3}$:

$\alpha^2 - \bar{1} = \bar{0} \Rightarrow \alpha^2 + \bar{1} = \bar{0} \Rightarrow \alpha$ ist Nullstelle von $f = x^2 + \bar{1} \in \mathbb{F}_3[x]$. f ist normiert, hat außerdem in $\mathbb{F}_3$ keine Nullstelle ($f(\bar{0}) = \bar{1} \neq \bar{0}$, $f(\bar{1}) = \bar{2} \neq \bar{0}$, $f(\bar{2}) = \bar{5} = \bar{2} \neq \bar{0}$), wegen $\operatorname{grad}(f) = 2$ also irreduzibel in $\mathbb{F}_3[x]$.

$\alpha^2 - \bar{1} = \bar{0} \Rightarrow \alpha^2 + \bar{1} = \bar{0} \Rightarrow \alpha$ ist Nullstelle von $f =$
$x^2 + \bar{1} \in \mathbb{F}_3[x]$ f ist normiert, hat außerdem in $\mathbb{F}_3$

insgesamt: $\mu_{\alpha, \mathbb{F}_3} = f \overset{\text{Satz 15.10}}{\Longrightarrow} [\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \text{grad}(f) = 2$
und jedes Element hat eine eindeutige Darstellung der Form
$a + b\alpha$ mit $a, b \in \mathbb{F}_3 \rightarrow |\mathbb{F}_3(\alpha)| =$ Anzahl der Möglichkeiten
für das Koeff. paar $(a, b) \in \mathbb{F}_3 \times \mathbb{F}_3 = 3 \cdot 3 = 9$

- wichtiges Prinzip: Die Gleichung $\alpha^2 = \bar{2}$ kann verwendet werden, um jedes Element der Form $g(\alpha)$ mit $g \in \mathbb{F}_3[x]$ in der Form $a + b\alpha$ mit $a, b \in \mathbb{F}_3$ darzustellen.

$(\bar{2}\alpha + \bar{1}) \cdot (\bar{2}\alpha + \bar{2}) = \bar{2} + \bar{6}\alpha + \bar{4}\alpha^2 = \bar{2} + \alpha^2 = \bar{2} + \bar{2} =$
$\bar{4} = \bar{1}$ (Daraus folgt auch $(\bar{2}\alpha + \bar{1})^{-1} = \bar{2}\alpha + \bar{2}$.)

- Vorgehensweise bei der Kehrwertberechnung:
Ziel: Berechnung von β^{-1} für ein Element der Form $\beta = g(\alpha)$

in $\mathbb{F}_3(\alpha)^*$ mit $g \in \mathbb{F}_3[x]$. Aus $\beta \neq \bar{0}$ folgt

$\mathrm{ggT}(f, g) = \bar{1}$. Lemma von Bézout $\Rightarrow$

$\exists\, u, v \in \mathbb{F}_3[x]$ mit $u \cdot f + v \cdot g = \bar{1}$

Es gilt dann $\beta^{-1} = v(\alpha)$.

Anwendung hier: Bestimme $(1 + \bar{\alpha})^{-1}$.

Setze $g = x + \bar{1}$ ($\Rightarrow \bar{1} + \alpha = g(\alpha)$)

Die Gleichung $u \cdot \underbrace{(x^2 + \bar{1})}_{= f} + v \cdot \underbrace{(x + \bar{1})}_{= g} = \bar{1}$

wird gelöst durch $v = x + \bar{2}$, $u = \bar{2}$

$\Rightarrow (\alpha + \bar{1})^{-1} = v(\alpha) = \bar{2} + \alpha$

Satz (15.11)

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K und $f = \mu_{\alpha,K}$. Dann gibt es einen Isomorphismus

$$\bar{\phi} : K[x]/(f) \longrightarrow K(\alpha) \quad \text{mit} \quad \phi(g+(f)) = g(\alpha) \text{ für alle } g \in K[x].$$

Dabei bezeichnet $K(\alpha)$ den von α erzeugten Zwischenkörper der Erweiterung $L|K$.

Beweis von Satz 15.11:

geg.: Körpererweiterung $L|K$, $\alpha \in L$ algebraisch über K, $f = \mu_{\alpha,K} \in K[x]$

z.zg.: $K[x]/(f) \cong K(\alpha)$ $(*)$

Wir wenden den Homomorphiesatz für Ringe an auf den Einsetzungshom $\phi : K[x] \to L$, $\alpha \mapsto g(\alpha)$. Damit der Hom. den Isom. $(*)$ liefert, müssen wir überprüfen

(1) ϕ definiert eine surj. Abb. $K[x] \to K(\alpha)$

(2) $\ker(\phi) = (f)$

<u>zu (1)</u> klar: Für jedes $g \in K[x]$ gilt $\phi(g) = g(\alpha) \in K(\alpha)$ $\Rightarrow$ ϕ definiert einen Hom. $K[x] \to K(\alpha)$

bekannt aus Satz 15.10: Jedes $\beta \in K(\alpha)$ hat die Form $\beta = g(\alpha) = \phi(g)$ für ein $g \in K[x]$. ($\Rightarrow$ Surjektivität)

<u>zu (2)</u> Sei $g \in K[x]$. zzg: $g \in \ker(\phi) \Leftrightarrow g \in (f)$

„$\Leftarrow$" $g \in (f) \Rightarrow \exists\, h \in K[x]$ mit $g = hf$

$\Rightarrow \phi(g) = g(\alpha) = h(\alpha) \cdot f(\alpha) = h(\alpha) \cdot 0_K = 0_K$

$\Rightarrow g \in \ker(\phi)$

„$\Rightarrow$" $g \in \ker(\phi) \Rightarrow g(\alpha) = \phi(g) = 0_K \xRightarrow{\text{Eig des Min-pol.}}$

$f \mid g \Rightarrow \exists\, h \in K[x] : g = hf \Rightarrow g \in (f)$ $\square$

Existenz algebraischer Erweiterungen

Satz (15.12)

Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann gibt es eine Körpererweiterung $L|K$ und ein Element $\alpha \in L$ mit $f(\alpha) = 0$.

Beweis von Satz 15.12

geg: K Körper, $f \in K[x]$ irreduzibles Pol.

<u>Beh.</u> Es gibt einen Erweiterungskörper $L|K$ und ein Element $\alpha \in L$ mit $f(\alpha) = 0_K$.

Setze $\tilde{L} = K[x]/(f)$. $f \in K[x]$ irreduzibel, $K[x]$ Hauptidealring $\overset{\text{Ringth.}}{\Longrightarrow}$ (f) ist maximales Ideal in $K[x]$ $\overset{\text{Ringth.}}{\Longrightarrow}$ $\tilde{L} = K[x]/(f)$ ist Körper.

Betrachte nun den Ringhom. $\phi: K \to \tilde{L}$, $a \mapsto a + (f)$. <u>Beh.:</u> ϕ ist injektiv

zzg: $\ker(\phi) \subseteq \{0_K\}$ Sei $a \in \ker(\phi) \Rightarrow$

$\phi(a) = 0_{\tilde{L}} \Rightarrow a + (f) = 0_K + (f) \Rightarrow a \in (f) \Rightarrow$

$\exists\, h \in K[x] : a = hf \xRightarrow[\operatorname{grad}(a) = 0]{\operatorname{grad}(f) \geq 1} h = 0_K,\ a = 0_K$ ($\Rightarrow$ Beh.)

Die Anwendung von Prop. 11.16 auf den Ringmonomorphismus ϕ liefert einen Erweiterungsring $L \supseteq K$ und einen Ringisom. $\hat{\phi} : L \to \tilde{L}$ mit $\hat{\phi}|_K = \phi$. $\tilde{L}$ Körper, $\hat{\phi}$ Isom. $\Rightarrow$ L ist Körper

Setze $\alpha = \hat{\phi}^{-1}(x + (f))$. <u>Beh</u> $f(\alpha) = 0_K$

Schreibe $f = \sum_{k=0}^{n} a_k x^k$ mit $n = \operatorname{grad}(f)$, $a_0, \dots, a_n \in K$.

$$\hat{\phi}(f(\alpha)) = \hat{\phi}\left(\sum_{k=0}^{n} a_k \alpha^k\right) \overset{\hat{\phi}\text{ Ringhom}}{=} \sum_{k=0}^{n} \hat{\phi}(a_k)\, \hat{\phi}(\alpha)^k =$$

$$\sum_{k=0}^{n} \phi(a_k)(x+(f)) = \sum_{k=0}^{n} (a_k+(f))(x+(f)) = \sum_{k=0}^{n} (a_k x+(f))$$

$$= \sum_{k=0}^{n} a_k x^k + (f) = f+(f) \overset{f\in(f)}{=} 0_K + (f) = 0_{\tilde{L}} = \hat{\phi}(0_L)$$

$$= \hat{\phi}(0_K) \overset{\hat{\phi} \text{ injektiv}}{\Longrightarrow} f(x) = 0_K. \qquad \square$$

Algebraische Körpererweiterungen

Definition (15.13)

Eine Körpererweiterung $L|K$ wird algebraisch genannt, wenn jedes Element $\alpha \in L$ algebraisch über K ist.

Proposition (15.14)

Sei $L|K$ eine Körpererweiterung.

(i) Ist $L|K$ endlich, dann auch algebraisch.

(ii) Sind $\alpha_1, ..., \alpha_n \in L$ algebraisch über K und gilt $L = K(\alpha_1, ..., \alpha_n)$, dann ist die Erweiterung $L|K$ endlich (also insbesondere algebraisch).

Es gibt aber unendliche algebraisch Erweiterungen, zum Beispiel

$$\mathbb{Q}(S)|\mathbb{Q} \qquad \text{mit} \quad S = \{\sqrt[n]{2} \mid n \in \mathbb{N}\}.$$

α_{n+1} ist alg. über K $\Rightarrow$ $\exists f \in K[x]$ mit $f(\alpha_{n+1}) = 0$

Beweis von Prop. 15.14

<u>zu (i)</u> geg. endliche Erweiterung $L|K$, z.zg: $L|K$ alg.

Angenommen, $L|K$ ist <u>nicht</u> algebraisch. Dann gibt es ein $\alpha \in L$, das nicht algebraisch über K ist. Betrachte für jedes $n \in \mathbb{N}$ die Menge $S_n = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$. Diese Menge ist linear unabhängig im K-Vektorraum L, und $|S_n| = n+1$.

Denn ang., dies ist nicht der Fall $\Rightarrow \exists a_0, a_1, \ldots, a_n \in K$, nicht alle gleich 0_K, mit $\sum_{k=0}^{n} a_k \alpha^k = 0_K$. Setze $g = \sum_{k=0}^{n} a_k x^k$. Dann gilt $g \neq 0_K$ und $g(\alpha) = 0_K$. $\Rightarrow$

α ist algebraisch über K ↯ Der K-Vektorraum L enthält also endliche Mengen beliebig großer Mächtigkeit. Also kann L nicht endl.-dim sein ↯ zur $L|K$ endlich

zu (ii) Sei $L|K$ eine beliebige Körpererweiterung.

Zeige durch vollst. Ind. über $n \in \mathbb{N}_0$: Sind $\alpha_1, \dots, \alpha_n \in L$ algebraisch über K, dann ist $K(\alpha_1, \dots, \alpha_n)|K$ eine endliche Erweiterung. Für $n = 0$ ist dies offensichtlich, wegen $[K:K] = 1$. Sei nun $n \in \mathbb{N}_0$, setze die Aussage für n voraus. Seien $\alpha_1, \dots, \alpha_{n+1}$ algebraisch über K. Ind-V. $\Rightarrow$ $M|K$ mit $M = K(\alpha_1, \dots, \alpha_n)$ ist eine endliche Erweiterung

α_{n+1} ist alg. über $K \Rightarrow \exists f \in K[x]$ mit $f(\alpha_{n+1}) = 0 \overset{M \supseteq K}{\Longrightarrow}$

$\exists\, g \in M[x]$ mit $g(\alpha) = 0_K \Rightarrow \alpha_{n+1}$ ist algebraisch über $M \Rightarrow [M(\alpha_{n+1}) : M] =$ grad $\mu_{\alpha, M}$, insb. ist $M(\alpha_{n+1}) \mid M$ endlich.

Offenbar ist $M(\alpha_{n+1}) = K(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$.

Gradformel $\Rightarrow$ Mit $M(\alpha) \mid M$ und $M \mid K$ ist auch $M(\alpha) \mid K$ endlich, d.h. die Erweiterung $K(\alpha_1, \dots, \alpha_n, \alpha_{n+1}) \mid K$ ist endlich.

$\square$

Eigenschaften algebraischer Erweiterungen

Satz (15.15)

(i) Sei $L|K$ eine Körpererweiterung und $T \subseteq L$ die Teilmenge bestehend aus den Elementen, die algebraisch über K sind. Dann ist T ein Teilkörper von L.

(ii) Seien $L|K$ und $M|L$ Körpererweiterungen. Genau dann ist die Erweiterung $M|K$ algebraisch, wenn die Erweiterungen $L|K$ und $M|L$ beide algebraisch sind.

Folgerung (15.16)

Ist $L|K$ eine Körpererweiterung und $S \subseteq L$ eine Teilmenge mit der Eigenschaft, dass jedes $\alpha \in S$ algebraisch über K ist, dann ist $K(S)|K$ eine algebraische Erweiterung.

Beweis von Satz 15.15:

geg.: Körpererweiterung $L|K$ und

$T = \{\alpha \in L \mid \alpha$ ist algebraisch über $K\}$.

z.zg.: T ist Zwischenkörper von $L|K$

Seien $\alpha, \beta \in T$. Um zu zeigen, dass T ein Teilkörper von L ist, müssen wir überprüfen: $1_K \in T$, $\alpha - \beta, \alpha\beta \in T$, im Fall $\alpha \neq 0_K$ auch $\alpha^{-1} \in T$. Betrachte den Zwischenkörper $M = K(\alpha, \beta)$. α, β alg. über $K \Rightarrow$ $M|K$ ist endlich, damit auch algebraisch

$\Rightarrow$ Jedes $\gamma \in M$ ist algebraisch über K.

insb. die Elemente $1_K \in T$, $\alpha - \beta$, $\alpha\beta$, im Fall $\alpha \neq 0_K$ auch α^{-1}

Jedes $a \in K$ ist algebraisch über K $\Rightarrow K \subseteq T$

Insgesamt ist T also ein Zwischenkörp. von $L|K$.

zu (ii) $L|K$, $M|L$ seien Körpererw.

z.zg.: $L|K$, $M|L$ beide alg. $\Longleftrightarrow$ $M|K$ ist alg.

„$\Leftarrow$" leicht (siehe Skript)

„$\Rightarrow$" Sei $\alpha \in M$. z.zg.: α ist algebraisch über K

$M|L$ ist alg., $\alpha \in M$ $\Rightarrow$ α ist algebraisch über L

$\Rightarrow \exists f \in L[x]$, $f \neq 0$ mit $f(\alpha) = 0$. Schreibe

$f = \sum_{k=0}^{n} a_k x^k$ mit $a_0, \ldots, a_n \in L$, $n \in \mathbb{N}$

Dann liegt f in $L_0[x]$ mit $L_0 = K(a_0, \dots, a_n)$

Nach Prop. 15.14 ist $L_0 | K$ eine endliche Erweiterung, ebenso ist $L_0(\alpha) | L_0$ endlich. Damit ist auch $L_0(\alpha) | K$ eine endl. Erweiterung (Gradformel) $\Rightarrow$ $L_0(\alpha) | K$ ist algebraisch $\square$

Daraus folgt, dass α algebraisch über K ist.