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.

Satz (15.6)

Seien $L|K$ und $M|L$ endliche Körpererweiterungen. Dann ist auch die Körpererweiterung $M|K$ endlich, und es gilt

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

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 $\mu_{\alpha,K}$.

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 $[K(\alpha) : K] = n$.

letztes Mal bereits gezeigt:

Die Menge der Linearkombinationen von $B = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, also

$$U = \left\{ \sum_{k=0}^{n-1} a_k \alpha^k \;\middle|\; a_0, ..., a_{n-1} \in K \right\} = \{g(\alpha) \mid g \in K[x], g = 0 \vee \mathrm{grad}(g) < n\}$$

ist ein Teilring von L.

$g - x$ vom grad $\leq n-1$ und

Beweis von Satz 15.10

geg: Körpererw. $L|K$, $\alpha \in L$ alg. über K, $f = \mu_{\alpha,K}$,
$n = \text{grad}(f)$

bereits gezeigt: $U = \{ \sum_{k=0}^{n-1} a_k \alpha^k \mid a_k \in K$ für $0 \leq k < n \}$
$= \{ g(\alpha) \mid g \in K[x], g = 0$ oder $\text{grad}(g)$
$\leq n-1 \}$ ist ein Teilring von L. Für die Teilkörper-Eigenschaft muss noch gezeigt werden: $\beta^{-1} \in U$ für alle $\beta \in U$ mit $\beta \neq 0_K$. Sei also β ein solches Element.

$\Rightarrow \exists g \in K[x], g \neq 0, \text{grad}(g) \leq n-1$ mit $\beta = g(\alpha)$.

f irred., $\text{ggT}(g, f) \mid f \Rightarrow \text{ggT}(g, f) = 1_K$ oder

$ggT(g,f) = f$ Die zweite Möglichkeit kann nicht eintreten, da $ggT(g,f) \mid g \Rightarrow grad(ggT(g,f)) \leq n-1 < grad(f)$

also: $ggT(g,f) = 1_K$ Lemma von Bézout $\Rightarrow \exists u, v \in K[x]$ mit

$ug + vf = 1_K \Rightarrow u(\alpha)\cdot g(\alpha) + v(\alpha)\cdot f(\alpha) = 1_K \rightarrow$

$u(\alpha)\cdot\beta + v(\alpha)\cdot 0_K = 1_K \Rightarrow u(\alpha) = \beta^{-1}$ Division mit Rest

$\Rightarrow \exists q, r \in K[x]$ mit $u = qf + r$, wobei $r = 0$ oder $grad(r) \leq$

$n-1 \Rightarrow \beta^{-1} = u(\alpha) = q(\alpha)\cdot \underbrace{f(\alpha)}_{=0} + r(\alpha) = r(\alpha) \Rightarrow \beta^{-1} \in U$

<u>also</u>: U ist ein Teilkörper von L

Jedes $a \in K^*$ kann als Pol vom Grad $0 \leq n-1$ angesehen werden.

$\rightarrow a = a(\alpha) \in U \ \forall a \in K^*$, ebenso $0_K \in U$, insg. $K \leq U$

$\Rightarrow U$ ist <u>Zwischenkörper</u> von $L|K$

<u>Beh.</u>: $\alpha \in U$ 1. <u>Fall</u>: $n \geq 2$ Dann ist $g = x$ vom Grad $\leq n-1$ und

Somit $\alpha = g(\alpha) \in U$.

2. Fall: $n = 1 \Rightarrow \alpha \in K \overset{\text{s.o.}}{\underset{K \subseteq U}{\Longrightarrow}} \alpha \in U$

($\Rightarrow$ Beh.) also: U ist Zwischenkörp. von $L|K$, $\alpha \in U \Rightarrow K(\alpha) \subseteq U$

Umgekehrt ist $g(\alpha)$ für jedes Pol. $g \in K[x]$ mit $g = 0_K$ oder $\operatorname{grad}(g) \leq n-1$ offenbar in $K(\alpha)$ enthalten $\Rightarrow U \subseteq K(\alpha)$.

insgesamt $U = K(\alpha)$

damit gezeigt: Die Elemente $1, \alpha, \dots, \alpha^{n-1}$ bilden ein Erzeugendensystem von $K(\alpha)$ als K-Vektorraum. noch z.zg.: lineare Unabhängigkeit

Ang.: die Elemente sind linear abhängig. $\Rightarrow \exists$ Koeffizienten $a_0, \dots, a_{n-1} \in K$, nicht alle gleich 0_K, mit $\sum_{k=0}^{n-1} a_k \alpha^k = 0_K$

Sei $g = \sum_{k=0}^{n-1} a_k x^k \in K[x]$. $\Rightarrow g(\alpha) = 0$

Sei $\tilde{g}$ die Normierung von g $\Rightarrow \tilde{g}(\alpha) = 0$

aber: $\operatorname{grad}(\tilde{g}) \leq n-1 < \operatorname{grad}(f)$ ↯ zur Eigenschaft des Minimalpolynoms f

$\square$

β

β

$\mathbb{F}_{3}$

Sa

add

wed

$\beta_{\cdot} =$

Multi

d.h.

wobe

Kehrwe

nome u

mit Rest

Anwendungsbeispiel zu Satz 15.10: kein Körper

ein Körper mit neun Elementen (nicht $\mathbb{Z}/9\mathbb{Z}$)

Sei $L \mid \mathbb{F}_3$ eine Körpererweiterung und $\alpha \in L$ mit $\alpha^2 + \bar{1} = \bar{0}$. Beh.: $\mu_{\alpha, \mathbb{F}_3} = x^2 + \bar{1} \in \mathbb{F}_3[x]$

klar: α ist Nullstelle des Polynoms, $x^2 + \bar{1}$ ist normiert.

Außerdem ist $x^2 + \bar{1}$ in $\mathbb{F}_3[x]$ irreduzibel, denn es ist vom Grad 2, und es besitzt in $\mathbb{F}_3$ keine Nullstelle, wegen $\bar{0}^2 + \bar{1} = \bar{1} \neq \bar{0}$, $\bar{1}^2 + \bar{1} = \bar{2} \neq \bar{0}$, $\bar{2}^2 + \bar{1} = \bar{5} = \bar{2} \neq \bar{0}$ ($\Rightarrow$ Beh.)

Satz 15.10 $\Rightarrow$ $\mathbb{F}_3(\alpha)$ ist 3-dim. $\mathbb{F}_3$-Vektorraum, mit $\bar{1}, \alpha$ als Basis $\Rightarrow$ Jedes

$\beta \in \mathbb{F}_3(\alpha)$ hat eine eindeutige Darstellung der Form

$\beta = a + b\alpha$ mit $a, b \in \mathbb{F}_3$ $\rightarrow$

$\mathbb{F}_3(\alpha) = \{\bar{0}, \bar{1}, \bar{2}, \alpha, \alpha + \bar{1}, \alpha + \bar{2}, \bar{2}\alpha, \bar{2}\alpha + \bar{1}, \bar{2}\alpha + \bar{2}\}$

Satz 15.10 gibt an, wie die Elemente von $\mathbb{F}_3(\alpha)$ addiert, multipliziert und wie Kehrwerte gebildet werden können. Seien $\beta, \gamma \in \mathbb{F}_3(\alpha)$ mit $\beta = g(\alpha)$, $\gamma = h(\alpha)$, $g, h \in \mathbb{F}_3[x]$.

Multiplikation: Teile gh durch $x^2 + \bar{1}$ mit Rest, d.h. bestimme $q, r \in \mathbb{F}_3[x]$ mit $gh = q(x^2 + \bar{1}) + r$, wobei $r = \bar{0}$ oder $\operatorname{grad}(r) \leq 1$. $\Rightarrow \beta\gamma = r(\alpha)$

Kehrwertbildung: Setze $\beta \neq 0$ voraus. Bestimme Polynome $u, v \in \mathbb{F}_3[x]$ mit $ug + vf = \bar{1}$. Teile u durch $x^2 + \bar{1}$ mit Rest, d.h. finde $q, r \in \mathbb{F}_3[x]$ mit

$u = q \cdot (x^2 + \bar{1}) + r$, $r = \bar{0}$ oder $\mathrm{grad}(r) \leq 1$. Dann ist $\beta^{-1} = r(\alpha)$

<u>Beispiel:</u> $\beta = \alpha + \bar{1}$, $\gamma = \alpha + \bar{2} \Rightarrow \beta = g(\alpha)$, $\gamma = h(\alpha)$

mit $g = x + \bar{1}$, $h = x + \bar{2} \Rightarrow gh = (x + \bar{1})(x + \bar{2}) = x^2 + \bar{2}$

Division mit Rest $\Rightarrow x^2 + \bar{2} = \bar{1} \cdot (x^2 + \bar{1}) + \underline{\underline{\bar{1}}}$

$\Rightarrow$ Ergebnis: $\beta\gamma = \bar{1}$, $\gamma = \beta^{-1}$

einfachere Durchführung der Multiplikation:

$\alpha^2 + \bar{1} = \bar{0} \Rightarrow \alpha^2 = -\bar{1} = \bar{2} \Rightarrow \beta\gamma = (\alpha + \bar{1}) \cdot (\alpha + \bar{2})$

$= \alpha^2 + \bar{3}\alpha + \bar{2} = \alpha^2 + \bar{2} = \bar{2} + \bar{2} = \bar{4} = \bar{1}$

Beispiel für eine Kehrwertbestimmung:

ges.: α^{-1} Es gilt $\alpha = g(\alpha)$ mit $g = x$.

Die Gleichung $u \cdot x + v \cdot (x^2 + \bar{1}) = \bar{1}$ wird gelöst von

$u = -x$, $v = \bar{1}$ $\Rightarrow$ $\alpha^{-1} = u(\alpha) = -\alpha = \bar{2}\alpha$

(Probe: $\alpha \cdot \bar{2}\alpha = \bar{2}\alpha^2 = \bar{2} \cdot \bar{2} = \bar{1}$)

Algebraische Erweiterungen als Faktorring

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: Körpererw. $L|K$, $\alpha \in L$ alg. über K, $f = \mu_{\alpha,K}$

Sei $\phi : K[x] \to L$ der Auswertungshom. an der Stelle α,
geg. durch $g \mapsto g(\alpha)$. Nach Satz 15.10 besteht
$K(\alpha)$ aus Elementen der Form $g(\alpha)$ mit $g \in K[x]$.
Daraus folgt, dass durch ϕ ein surjektiver Hom.
$K[x] \to K(\alpha)$ von Ringen geg. ist.

<u>Bch</u>: $\ker(\phi) = (f)$ „$\supseteq$" $f(\alpha) = 0 \Rightarrow \phi(f) = 0 \Rightarrow f \in \ker(\phi) \xRightarrow[\text{Ideal von } K[x]]{\ker(\phi) \text{ ist}} (f) \subseteq \ker(\phi)$

„$\subseteq$" $g \in \ker(\phi) \Rightarrow g(\alpha) = 0 \Rightarrow g$ ist Vielfaches des Min.pol. von α über K, also von $f \Rightarrow \exists h \in K[x]$ mit $g = hf$ $\Rightarrow g \in (f)$ ($\Rightarrow$ Beh.)

Insgesamt sind also die Voraussetzung des Hom.-satzes für Ringe erfüllt. Demnach existiert ein Isomorphismus $\bar{\phi}: K[x]/(f) \to K(\alpha)$ von Ringen mit $\bar{\phi}(g+(f)) = \phi(g) = g(\alpha)\ \forall g \in K[x]$.

$\square$

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: Körper K, $f \in K[x]$ irreduzibel

Beh: Es gibt einen Erweiterungskörper L von K und ein $\alpha \in L$ mit $f(\alpha) = 0_K$.

Betrachte die Abb. $\varphi: K \to K[x]/(f)$ geg. durch $\varphi(a) = a + (f)$ $\forall a \in K$.

Beh: φ ist Monomorphismus von Ringen

Als Komposition der Einbettungsabb. $K \to K[x]$, $a \mapsto a$ und des kan. Epimorphismus $K[x] \to K[x]/(f)$ ist φ ein Ringhom.

Für die Injektivität reicht es, $\ker(\phi) \subseteq \{0_K\}$ zu überprüfen. Sei $a \in \ker(\phi) \Rightarrow \phi(a) = 0_{K[x]/(f)}$

$\Rightarrow a + (f) = (f) \Rightarrow a \in (f) \Rightarrow f \mid a$

$\overset{\text{grad}(f) \geq 1}{\underset{a \in K}{\Longrightarrow}} \quad a = 0_K \quad (\Rightarrow \text{Beh.})$

Auf Grund der Beh. existiert lt. Ringtheorie ein Erweiterungsring $R \supseteq K$ und ein Ring-isomorphismus $\hat{\varphi} : R \to K[x]/(f)$ mit $\hat{\varphi}|_K = \varphi$.

Der Faktorring $K[x]/(f)$ ist ein Körper, denn: $K[x]$ ist Hauptidealring (als Pol-ring über einem Körper), $f \in K[x]$ irreduzibles Element $\Rightarrow$ (f) <u>maximales</u> Ideal $\Rightarrow K[x]/(f)$ ist Körper

D

da

kö

$\Rightarrow$

Sch

Dann

$\sum_{k=0}^{n} a$

$\sum_{k=0}^{n} (a$

$(\sum_{k=0}^{n} a$

$0_K]$

$K[x]/(f)$

a

orze

zung-

d

er denn:

über einem

nt $\Rightarrow$

ist Körper

Da R isomorph zu $K[x]/(f)$ ist, ist auch R damit ein Körper. Setze $L = R$ (Erweiterungskörper von K). Setze $\alpha = \hat{\varphi}^{-1}(x+(f))$.

$\Rightarrow \alpha \in L$. Beh. $f(\alpha) = 0_K$

Schreibe $f = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}$, $a_0, \dots, a_n \in K$.

Dann gilt $\hat{\varphi}(f(\alpha)) = \hat{\varphi}\left(\sum_{k=0}^{n} a_k \alpha^k\right) =$

$$\sum_{k=0}^{n} \hat{\varphi}(a_k)\hat{\varphi}(\alpha)^k \underset{[\hat{\varphi}|_K = \varphi]}{=} \sum_{k=0}^{n} \varphi(a_k)(x+(f))^k$$

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

$$\left(\sum_{k=0}^{n} a_k x^k\right) + (f) = f + (f) = 0_{K[x]/(f)} = \hat{\varphi}(0_K)$$

Aus der Injektivität von $\hat{\varphi}$ folgt $f(x) = 0_K$. $\square$

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

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

Beweis von Prop. 15.14:

zu (i) Sei $L|K$ eine endl. Körpererweiterung

(d.h. L ist ein endlich-dim. K-Vektorraum)

Ang. $L|K$ ist nicht algebraisch $\Rightarrow \exists\, \alpha \in L$ transzendent über K

Beh.: Für jedes $n \in \mathbb{N}$ ist $1, \alpha, \ldots, \alpha^{n-1}$ eine n-elementige linear unabhängige Teilmenge von L ($\Rightarrow \dim_K L \geq n \;\forall n \in \mathbb{N}$ $\lightning$ zur Endlichkeit)

Ang., die Elemente sind linear abhängig $\Rightarrow$ $\exists\, a_0, \ldots, a_{n-1} \in K$, nicht alle null, mit $\sum_{k=0}^{n-1} a_k \alpha^k = 0_K$

Setze $g = \sum_{k=0}^{n-1} a_k x^k \Rightarrow g \neq 0$, $g(\alpha) = 0_K \Rightarrow$

α ist algebraisch über K $\lightning$ zur Vor.