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

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

Beweis von Satz 15.6 (Gradformel)

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

geg.: endliche Körperweiterungen $L|K$ und $M|L$

Sei $r = [L:K]$ und $s = [M:L]$

z.zg.: $[M:K] = rs$

Nach Voraussetzung gibt es eine r-elementige Basis $\{\alpha_1, \ldots, \alpha_r\}$ von L als K-Vektorraum, und eine s-elementige Basis $\{\beta_1, \ldots, \beta_s\}$ von M als L-Vektorraum

<u>Beh.</u>: $\mathcal{B} = \{\alpha_i \beta_j \mid 1 \le i \le r, 1 \le j \le s\}$ ist eine rs-elementige Basis von M als K-Vektorraum

Lem: $\mathcal{B} = \{\alpha_i\beta_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s\}$ ist eine rs-elementige Basis von M als K-Vektorraum

z.zg: (1) $\underline{\mathcal{B}}$ ist Erz.-system von M als K-Vektorraum

(2) $\underline{\mathcal{B}}$ ist im K-Vektorraum M linear unabhängig.

Und es gilt $|\underline{\mathcal{B}}| = rs$

<u>zu (1)</u> Sei $\gamma \in M$. Basiseig. von $\mathcal{B}_2 = \{\beta_1, \ldots, \beta_s\} \Rightarrow$ $\exists\, \rho_1, \ldots, \rho_s \in L$ mit $\gamma = \sum_{j=1}^{s} \rho_j \beta_j$ Basis-Eig. von $\mathcal{B}_1 = \{\alpha_1, \ldots, \alpha_r\} \Rightarrow$ Für $1 \leq j \leq s$ gibt es jeweils Koeff. $a_{ij} \in K$ $(1 \leq i \leq r)$ mit $\rho_j = \sum_{i=1}^{r} a_{ij}\alpha_i$. einsetzen $\Rightarrow$ $\gamma = \sum_{i=1}^{r}\sum_{j=1}^{s} a_{ij}\alpha_i\beta_j$, d.h. γ ist eine K-Linearkomb. von $\mathcal{B}$

<u>zu (2)</u> Seien $a_{ij} \in K$ $(1 \leq i \leq r,\ 1 \leq j \leq s)$ mit $\sum_{i=1}^{r}\sum_{j=1}^{s} a_{ij}\alpha_i\beta_j = 0_K$

z.zg: $a_{ij} = 0$ für $1 \leq i \leq r,\ 1 \leq j \leq s$

$$\sum_{j=1}^{s}\left(\sum_{i=1}^{r} a_{ij}\alpha_i\right)\beta_j = 0_K$$ lineare Unabh.

von $B_2 \Rightarrow \sum_{i=1}^{r} a_{ij}\alpha_i = 0_K$ für $1 \leq j \leq s$

lineare Unabh. von $B_1 \Rightarrow a_{ij} = 0_K \ \forall i,j$. $\square$

<u>Anwendung</u>: Die Erweiterung $\mathbb{C} | \mathbb{R}$ hat keinen echten Zwischenkörper.

Ang. K ist ein solcher Zwischenkörp., d.h. $\mathbb{R} \subsetneq K \subsetneq \mathbb{C}$. Gradformel $\Rightarrow [\mathbb{C}:K]\cdot[K:\mathbb{R}] = [\mathbb{C}:\mathbb{R}] = 2 \Rightarrow [\mathbb{C}:K] = 1$ oder $[K:\mathbb{R}] = 1$

$\Rightarrow \mathbb{C} = K$ oder $K = \mathbb{R}$ ↯

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 $\mu_{\alpha,K}$.

Beispiele für algebraische bzw. transzendente Elemente in Körpererweiterungen

- Ist K ein Körper, dann ist jedes $a \in K$ algebraisch über K, da a Nullstelle des Polynoms $f = x - a \in K[x]$ ist.
- Das Element $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, da $\sqrt{2}$ Nullstelle von $x^2 - 2 \in \mathbb{Q}[x]$ ist.
- Jedes $z = a + ib \in \mathbb{C}$ mit $a, b \in \mathbb{R}$ ist algebraisch über $\mathbb{R}$, da z Nullstelle des Polynoms $(x - z)(x - \overline{z}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$ ist.
- Man kann zeigen, dass e (Eulersche Zahl) und π transzendent über $\mathbb{Q}$ sind. (= nicht algebraisch)

Beweis der Eindeutigkeit und Existenz des Minimalpolynoms

Sei $L|K$ eine Körpererw. und $\alpha \in L$ algebraisch über K.

<u>Existenz</u>: In der nichtleeren Menge der Polynome $g \in K[x]$ mit $g(\alpha) = 0$ gibt es eines mit minimalem Grad. Bezeichne dies mit $\tilde{g}$ und den Leitkoeff. mit c. Dann ist $g_0 = c^{-1}\tilde{g}$ normiert, $g_0(\alpha) = 0$, und g_0 hat minimalen Grad unter den Polynomen mit dieser Eigenschaft.

ge

al-

des

über

ist

al-

s Poly-

$a^2+b^2)$

) und π

ebraisch)

<u>Eindeutigkeit</u>: Ang. $h \in K[x]$ sei ein weiteres normiertes Polynom mit $h(\alpha) = 0$ und demselben minimalen Grad.

Ang. $h \neq g_0$. Sei $d \in K^\times$ der Leitkoeff. von $h - g_0$.

Setze $r = d^{-1}(h - g_0) \Rightarrow r(\alpha) = d^{-1}(h(\alpha) - g_0(\alpha)) =$
$d^{-1}(0 - 0) = 0$, und $\mathrm{grad}(r) < \mathrm{grad}(g_0)$

↯ zur Minimalität von $\mathrm{grad}(g_0)$ $\square$

Eigenschaften des Minimalpolynoms

Proposition (15.9)

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

(i) Das Polynom f ist irreduzibel.

(ii) Ist $g \in K[x]$ mit $g(\alpha) = 0$, dann folgt $f \mid g$.

(iii) Ist $g \in K[x]$ ebenfalls normiert, irreduzibel, mit $g(\alpha) = 0_K$, dann folgt $f = g$.

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

Beweis von Satz 15.10

geg: Körpererweiterung $L|K$, $\alpha \in L$ algebraisch über K
$f = \mu_{\alpha,K} \in K[x]$, $n = \mathrm{grad}(f)$

Beh: $\underline{B} = \{1, \alpha, \dots, \alpha^{n-1}\}$ ist n-elementige Basis
von $K(\alpha)$ als K-Vektorraum (klar: $\underline{B} \subseteq K(\alpha)$)

zu zeigen: (1) $\underline{B}$ ist linear unabh. und $|\underline{B}| = n$
(2) $\underline{B}$ ist Erzeugendensystem von K als K-Vektorraum

zu (1) Ang. die Aussage ist falsch. Dann gibt es Koeff.
$a_0, \dots, a_{n-1} \in K$ nicht alle null, mit $\sum_{i=0}^{n-1} a_i \alpha^i = 0_K$.
Setze $g = \sum_{i=0}^{n-1} a_i x^i \in K[x]$. $\Rightarrow g \neq 0_K$ und $g(\alpha) = 0_K$

(2) B ist Erzeugendensystem von K als K-Vektorraum

Sei $c \in K^\times$ der Leitkoeff. von g. Dann ist $c^{-1}g$ normiert mit α als Nullst. und kleinerem Grad als f. ↯ zur Definition des Minimalpolynoms.

<u>zu (2)</u> Sei $U = \{ \sum_{i=0}^{n-1} a_i \alpha^i \mid a_0, \ldots, a_{n-1} \in K \} = \{ g(\alpha) \mid g \in K[x]$ mit $\mathrm{grad}(g) < n$ oder $g = 0_K \}$. Beh: $U = K(\alpha)$

Wir überprüfen, dass U die definierenden Eigenschaften von $K(\alpha)$ besitzt, im Einzelnen

(2.1) U ist Zwischenkörper von $L|K$

(2.2) $\alpha \in U$

(2.3) Ist M ein bel. Zwischenkörper von $L|K$ mit $\alpha \in M$, dann folgt $M \supseteq U$.

<u>zu (2.1)</u> Für die Teilkörpereig. von U muss gezeigt werden: Es gilt $1_K \in U$, und für alle $\beta, \gamma \in U$ gilt $\beta - \gamma, \beta\gamma \in U$, im Fall $\beta \neq 0_K$ gilt auch $\beta^{-1} \in U$.

Setze $u = 1_K \in K[x]$. Dann gilt $\operatorname{grad}(u) < n$ und $u(\alpha) = 1_K \Rightarrow 1_K \in U$.

Seien nun $\beta, \gamma \in U \Rightarrow \exists g, h \in K[x]$ mit $\beta = g(\alpha)$, $\gamma = h(\alpha)$, wobei $\operatorname{grad}(g) < n$ oder $g = 0_K$ und dasselbe auch für h gilt.

- Subtraktion: Für $g-h$ gilt $g-h = 0_K$ oder $\operatorname{grad}(g-h) < n$, und $\beta - \gamma = (g-h)(\alpha) \Rightarrow \beta - \gamma \in U$

$u($

Dir

$v =$

Wie (

$r(\alpha)$

$v(\alpha)$

Offen

$a \in K$

Dann

U dan

0_K und dasselbe auch für h gilt.

- Multiplikation: Division mit Rest $\Rightarrow$ $\exists\, q, r \in K[x]$ mit $gh = qf + r$, wobei $r = 0_K$ oder $\operatorname{grad}(r) < n$ $\Rightarrow$ $r(\alpha) \in U$, außerdem: $r(\alpha) = (gh - qf)(\alpha) = g(\alpha)h(\alpha) - q(\alpha)f(\alpha)$ $= \beta\gamma - q(\alpha)\, 0_K = \beta\gamma \Rightarrow \beta\gamma \in U$
- Kehrwertbildung: Setze nun $\beta \neq 0$ voraus. Dann folgt $g \neq 0_K$. Sei $d = \operatorname{ggT}(f, g)$. Weil $d \mid g$, also $\operatorname{grad}(d) \leq \operatorname{grad}(g) < n$ gilt, andererseits auch $d \mid f$ und f irreduzibel ist, muss d eine Einheit in $K[x]$ sein, d.h. $d \in K^*$, o.B.d.A. $d = 1_K$. Lemma von Bézout $\Rightarrow$

$\exists\, u, v \in K[x]$ mit $uf + vg = d = 1_K$.

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

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

Division mit Rest $\Rightarrow \exists\, q, r \in K[x]$ mit $v = qf + r$, wobei $r = 0_K$ oder $\operatorname{grad}(r) < n$.

Wie bei der Multiplikation überprüft man $v(\alpha) = r(\alpha)$. Insgesamt gilt damit $\beta^{-1} = v(\alpha) = r(\alpha)$, und $r(\alpha)$ ist in U enthalten.

Offenbar gilt $K \subseteq U$. (Für bel. vorgeg. $a \in K$ setze $a_0 = a$, $a_i = 0_K$ für $1 \leq i \leq n-1$. Dann gilt $a = \sum_{i=0}^{n-1} a_i \alpha^i$.) Insgesamt ist U damit ein Zwischenkörper von $L|K$.

$a \in K$ setze $a_0 = a$, $a_i = 0_K$ für $1 \leq i \leq n-1$.

<u>zu (2.2)</u> Ist $n > 1$, dann können wir $g = x$ setzen und erhalten $\alpha = g(\alpha) \in U$. Ist $n = 1$, dann folgt $f = x - \alpha$. $f \in K[x] \Rightarrow \alpha \in K \xrightarrow[\text{von } L|K]{U \text{ Zwi-} \atop \text{schenkörp.}} \alpha \in U$.

<u>zu (2.3)</u> Sei M ein bel. Zwischenkörper von $L|K$ mit $\alpha \in M$. z.zg.: $U \subseteq M$

Sei also $\beta \in U$ z.zg. $\beta \in M$

Wegen $\beta \in U$ gibt es $a_0, \ldots, a_{n-1} \in K$ mit $\beta = \sum_{i=0}^{n-1} a_i \alpha^i$. $K \cup \{\alpha\} \subseteq M$, M Teilkörp. von L

$\Rightarrow a_i \alpha^i \in M$ für $0 \leq i < n \Rightarrow \sum_{i=0}^{n-1} a_i \alpha^i \in M$

$\Rightarrow \beta \in M$. $\square$