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

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

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.

Anhang: Quadratische Erweiterungen von $\mathbb{Q}$

Proposition (15.17)

Sei K ein Körper mit $\mathrm{char}(K) \neq 2$ und $L|K$ eine Erweiterung mit $[L : K] = 2$. Dann existiert ein $\gamma \in L$ mit $L = K(\gamma)$ und $\gamma^2 \in K$. (Man sagt dazu auch, dass L aus K durch Adjunktion einer Quadratwurzel entsteht.)

Folgerung (15.18)

Sei $K|\mathbb{Q}$ eine Erweiterung mit $[K : \mathbb{Q}] = 2$. Dann gibt es eine quadratfreie Zahl $m \in \mathbb{Z} \setminus \{0, 1\}$ mit $K = \mathbb{Q}(\sqrt{m})$.

Satz (15.19)

Seien $m, n \in \mathbb{Z} \setminus \{0, 1\}$ zwei verschiedene quadratfreie Zahlen. Dann gilt $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$, $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$, also insbesondere

$$\mathbb{Q}(\sqrt{m}) \neq \mathbb{Q}(\sqrt{n}).$$

Beweis von Proposition 15.17

geg. Körpererw. $L|K$ mit $[L:K]=2$, $\mathrm{char}(K) \neq 2$

Beh: $\exists\, \gamma \in L$ mit $L = K(\gamma)$ und $\gamma^2 \in K$

$[L:K] > 1 \Rightarrow \exists\, \alpha \in L \setminus K$ $\quad K(\alpha)$ ist Zwischenkörp. von $L|K$. Gradformel $\Rightarrow 2 = [L:K] = [L:K(\alpha)] \cdot [K(\alpha):K]$

$\Rightarrow [K(\alpha):K] \in \{1,2\}$ Ang. $[K(\alpha):K] = 1 \Rightarrow K(\alpha) = K$

$\Rightarrow \alpha \in K$ ↯ also $[K(\alpha):K] = 2$, $[L:K(\alpha)] = 1$.

somit $L = K(\alpha)$

Sei $f = \mu_{\alpha,K} \in K[x] \Rightarrow \mathrm{grad}(f) = [K(\alpha):K] = 2$

... Ang $[K(\alpha):K] = 1 \Rightarrow K(\alpha) = K$

$\Rightarrow \alpha \in K$ ↯ also $[K(\alpha):K] = 2$, $[L:K(\alpha)] = 1$.

$\Rightarrow \exists\, p, q \in K$ mit $f = x^2 + px + q$ $\quad f(\alpha) = 0_K \Rightarrow$

$\alpha^2 + p\alpha + q = 0 \xrightarrow[\operatorname{char}(K) \neq 2]{} \alpha^2 + p\alpha + \frac{1}{4}p^2 = \frac{1}{4}p^2 - q \Rightarrow$

$(\alpha + \frac{1}{2}p)^2 = \frac{1}{4}p^2 - q$ Setze $\gamma := \alpha + \frac{1}{2}p$. Dann gilt

$\gamma^2 = \frac{1}{4}p^2 - q \Rightarrow \gamma^2 \in K$ __Beh:__ $L = K(\gamma)$

gleichbedeutend: $K(\alpha) = K(\gamma)$ Überprüfe dafür

(1) $\gamma \in K(\alpha)$ (2) $\alpha \in K(\gamma)$

__zu (1)__ $\alpha \in K(\alpha)$, $\frac{1}{2}p \in K \Rightarrow \gamma = \alpha + \frac{1}{2}p \in K(\alpha)$

__zu (2)__ $\gamma \in K(\gamma)$, $-\frac{1}{2}p \in K \Rightarrow \alpha = \gamma + (-\frac{1}{2}p) \in K(\gamma)$

$\square$

Beweis von Satz 15.19

geg: quadratfreie Zahlen $m, n \in \mathbb{Z} \setminus \{0, 1\}$
mit $m \neq n$

zeige: $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$ (Bew. von $\sqrt{m} \in \mathbb{Q}(\sqrt{n})$
läuft analog)

Zeige zunächst, dass $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$ ist.
Sei $f = x^2 - m \in \mathbb{Q}[x]$. f ist normiert, $f(\sqrt{m})$
$= 0$. Angenommen, f ist reduzibel in $\mathbb{Q}[x]$.
$\overset{\text{grad}(f)=2}{\Longrightarrow}$ Die Nullstellen $\pm\sqrt{m}$ sind in $\mathbb{Q}$ ent-
halten. $\Rightarrow \exists\, r \in \mathbb{Z}, s \in \mathbb{N}$ mit $\sqrt{m} = \frac{r}{s}$ und

$\mathrm{ggT}(r,s) = 1 \Rightarrow m = \frac{r^2}{s^2} \Rightarrow ms^2 = r^2$ Da m quadratfrei ist, folgt $r^2 = 1 \Rightarrow ms^2 = 1$

$\overset{m,s\in\mathbb{Z}}{\Longrightarrow} s^2 = 1 \Rightarrow m = 1$ ↯

Aus $[\mathbb{Q}(\sqrt{m}):\mathbb{Q}] = 2$ folgt, dass $\{1, \sqrt{m}\}$ eine zweielementige Basis von $\mathbb{Q}(\sqrt{m})$ als $\mathbb{Q}$-Vektorraum ist.

Ang. $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$. Dann gibt es (eind. best.) $r,s \in \mathbb{Q}$ mit $\sqrt{n} = r + s\sqrt{m} \Rightarrow n = (r + s\sqrt{m})^2$

$= r^2 + 2rs\sqrt{m} + s^2 m \Rightarrow n \cdot 1 + 0\sqrt{m} = (r^2 + s^2 m)\cdot 1 + 2rs\sqrt{m} \xrightarrow[\text{Basis}]{\{1,\sqrt{m}\}} n = r^2 + s^2 m$ und $2rs = 0 \Rightarrow r = 0$ oder $s = 0$

<u>1. Fall</u>: $r = 0$. Dann gilt $n = s^2 m$.

Schreibe $s = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\operatorname{ggT}(a,b) = 1$

$\Rightarrow n = \left(\frac{a}{b}\right)^2 m \Longrightarrow n b^2 = m a^2$. Da n quadratfrei ist, gilt $a^2 = 1$. Da m quadratfrei ist, gilt $b^2 = 1$. $\Longrightarrow n = m$ ↯

<u>2. Fall</u>: $s = 0$. Dann gilt $n = r^2$. Schreibe $r = \frac{c}{d}$ mit $c \in \mathbb{Z}$, $d \in \mathbb{N}$, $\operatorname{ggT}(c,d) = 1$. $\Rightarrow$

$n = \left(\frac{c}{d}\right)^2 \Longrightarrow n d^2 = c^2$. Da n quadratfrei ist, gilt

$c = 1 \Longrightarrow n d^2 = 1 \overset{n,\, d^2 \in \mathbb{N}}{\Longrightarrow} n = 1$ ↯. $\square$

oder

Notation:

(i) Sind L und M Körper, dann bezeichnen wir mit $\mathrm{Hom}(L, M)$ die Menge der Körperhomomorphismen $L \to M$.

(ii) Ist K ein gemeinsamer Teilkörper von L und M, dann bezeichnet $\mathrm{Hom}_K(L, M)$ die Menge der Körperhomomorphismen $\phi : L \to M$ mit $\phi(a) = a$ für alle $a \in K$. Solche Körperhomomorphismen werden auch K-Homomorphismen genannt.

Weitere Grundbegriffe

(iii) Für jeden Körper L sei $\mathrm{Aut}(L)$ die Menge der Automorphismen von L.

(iv) Ist K ein Teilkörper L, dann bezeichnet $\mathrm{Aut}_K(L)$ die Teilmenge von $\mathrm{Aut}(L)$ bestehend aus den Automorphismen von L, die zugleich K-Homomorphismen sind. Man spricht in diesem Zusammenhang von K-Automorphismen. Offenbar handelt es sich bei $\mathrm{Aut}_K(L)$ um eine Untergruppe von $\mathrm{Aut}(L)$.

(v) Sei $L|K$ eine Körpererweiterung und $\phi : K \to \tilde{K}$ ein Homomorphismus von K in einen weiteren Körper $\tilde{K}$. Ein Homomorphismus $\psi : L \to \tilde{K}$ wird Fortsetzung von ϕ genannt, wenn $\psi|_K = \phi$ erfüllt ist.

Eindeutigkeit der Fortsetzungen

Satz (16.1)

Sei $L|K$ eine Körpererweiterung, $S \subseteq L$ eine Teilmenge mit $L = K(S)$ und $\phi : K \to \tilde{K}$ ein Homomorphismus in einen weiteren Körper $\tilde{K}$. Sind dann $\psi_1, \psi_2 : L \to \tilde{K}$ zwei Fortsetzungen von ϕ mit $\psi_1|_S = \psi_2|_S$, dann gilt $\psi_1 = \psi_2$.

wichtiger Spezialfall:

Gilt $L = K(\alpha)$ für ein $\alpha \in L$ und ist $\beta \in \tilde{K}$, dann gibt es für jeden Homomorphismus $\phi : K \to \tilde{K}$ und jedes $\beta \in \tilde{K}$ höchstens eine Fortsetzung $\psi_\beta : K(\alpha) \to \tilde{K}$ von ϕ mit der Eigenschaft $\psi_\beta(\alpha) = \beta$.

Beweis von Satz 16.1

geg: Körpererw. $L|K$, $S \subseteq L$ mit $L = K(S)$

$\tilde{K}$ weiterer Körper, $\phi : K \to \tilde{K}$ Körperhom.

$\psi_1, \psi_2 : L \to \tilde{K}$ Fortsetzungen von ϕ (d.h. $\psi_1|_K = \psi_2|_K = \phi$) mit $\psi_1|_S = \psi_2|_S$ <u>Beh</u>: $\psi_1 = \psi_2$

Betrachte in L die Teilmenge $M = \{\alpha \in L \mid \psi_1(\alpha) = \psi_2(\alpha)\}$

Zu zeigen ist $M = L$ (wobei $M \subseteq L$ offensichtlich ist).

Für alle $a \in K$ gilt $\psi_1(a) = \phi(a) = \psi_2(a)$. $\Rightarrow K \subseteq M$

<u>Beh</u>: M ist ein Teilkörper von L

$= \varphi)$ mit $\psi_1|_S = \psi_2|_S$ **Beh.:** $\psi_1 = \psi_2$

Betrachte in L die Teilmenge $M = \{\alpha \in L \mid \psi_1(\alpha) = \psi_2(\alpha)\}$

zu überprüfen: $1_L \in M$, $\forall \alpha, \beta \in M$: $\alpha - \beta, \alpha\beta \in M$, im Fall $\alpha \neq 0_L$ auch $\alpha^{-1} \in M$

K Teilkörper von $L \Rightarrow 1_L = 1_K \in K \xRightarrow{K \subseteq M} 1_L \in M$

Seien nun $\alpha, \beta \in M \Rightarrow \psi_1(\alpha) = \psi_2(\alpha), \psi_1(\beta) = \psi_2(\beta) \Rightarrow$

$\psi_1(\alpha - \beta) = \psi_1(\alpha) - \psi_1(\beta) = \psi_2(\alpha) - \psi_2(\beta) = \psi_2(\alpha - \beta) \Rightarrow \alpha - \beta \in M$

$\psi_1(\alpha\beta) = \psi_1(\alpha)\psi_1(\beta) = \psi_2(\alpha)\psi_2(\beta) = \psi_2(\alpha\beta) \Rightarrow \alpha\beta \in M$

$\psi_1(\alpha^{-1}) = \psi_1(\alpha)^{-1} = \psi_2(\alpha)^{-1} = \psi_2(\alpha^{-1}) \Rightarrow \alpha^{-1} \in M$ ($\Rightarrow$ Beh.)

Also ist M insgesamt ein Zwischenkörper von $L|K$. Aus $\psi_1|_S = \psi_2|_S$ folgt $S \subseteq M$. Da $K(S)$ der kleinste Zwischenkörper von $L|K$ mit $K(S) \supseteq S$ ist, folgt $K(S) \subseteq M$. $\Rightarrow L \subseteq M \Rightarrow L = M$

$\square$

Der Fortsetzungssatz

Satz (16.2)

- Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern.
- Seien $L|K$ und $\tilde{L}|\tilde{K}$ Körpererweiterungen.
- Sei $\alpha \in L$ ein über K algebraisches Element und f das Minimalpolynom von α über K.
- Sei $\tilde{\alpha} \in \tilde{L}$ eine Nullstelle von $\tilde{f} = \phi(f) \in \tilde{K}[x]$.

Dann gibt es eine eindeutig bestimmte Fortsetzung ψ von ϕ auf $K(\alpha)$ mit $\psi(\alpha) = \tilde{\alpha}$. Dieser Homomorphismus ψ definiert einen Isomorphismus zwischen den beiden Körpern $K(\alpha)$ und $\tilde{K}(\tilde{\alpha})$.

phis-
nen
rch

ullst.")
$K[x]$.
$L \to \tilde{L}$
e Null-

Beweis des Fortsetzungssatzes 16.2:

geg.: $L|K$, $\tilde{L}|\tilde{K}$ Körpererw., $\alpha \in L$ alg. über K,
$\phi: K \to \tilde{K}$ Isom., $f = \mu_{\alpha,K}$, $\tilde{f} = \phi(f)$

$\tilde{\alpha} \in \tilde{L}$ Nullstelle von $\tilde{f}$

$$\begin{tikzcd}
L \arrow[d, dash] & \tilde{L} \arrow[d, dash] \\
K(\alpha) \arrow[r, dashed, "\sim"', "\psi"] \arrow[d, dash] & \tilde{K}(\tilde{\alpha}) \arrow[d, dash] \\
K \arrow[r, "\sim", "\phi"'] & \tilde{K}
\end{tikzcd}$$

z.zg.:
(1) $\exists!$ Fortsetzung $\psi: K(\alpha) \to \tilde{L}$ von ϕ mit $\psi(\alpha) = \tilde{\alpha}$
(2) $\psi|_{K(\alpha)}$ definiert einen Isom. $K(\alpha) \cong \tilde{K}(\tilde{\alpha})$

bereits bekannt aus §15: Es gibt einen Isom. $\sigma: K[x]/(f) \to K(\alpha)$ mit $\sigma(g + (f)) = g(\alpha)$ für alle $g \in K[x]$.

Mit f ist auch $\tilde{f} = \phi(f)$ irreduzibel und normiert, und es gilt $\tilde{f}(\tilde{\alpha}) = 0_{\tilde{L}} \Rightarrow \tilde{f} = \mu_{\tilde{\alpha},\tilde{K}} \Rightarrow$

Es gibt einen Isom. $\tilde{\sigma} : \tilde{K}[x]/(\tilde{f}) \to \tilde{K}(\tilde{\alpha})$ mit $\tilde{\sigma}(\tilde{g} + (\tilde{f})) = \tilde{g}(\tilde{\alpha})$ $\forall \tilde{g} \in \tilde{K}[x]$.

$$K(\alpha) \xrightarrow{\sigma^{-1}} K[x]/(f) \xrightarrow{\bar{\Phi}} \tilde{K}[x]/(\tilde{f}) \xrightarrow{\tilde{\sigma}} \tilde{K}(\tilde{\alpha})$$

Betrachten den Ringhom $\hat{\phi} : K[x] \to \tilde{K}[x]/(\tilde{f})$ geg. durch $\hat{\phi}|_K = \phi$ und $\hat{\phi}(x) = x + (\tilde{f})$

Überprüfe: (1) $\hat{\phi}$ ist surjektiv (klar, da ϕ surjektiv)

(2) $\ker(\hat{\phi}) = (f)$ (siehe Skript)

Der Homomorphiesatz für Ringe liefert somit einen Isom. $\overline{\Phi} : K[x]/(f) \to \tilde{K}[x]/(\tilde{f})$.

Durch $\psi := \tilde{\partial} \circ \overline{\Phi} \circ \partial^{-1}$ erhalten wir einen Isom. $K(\alpha) \to \tilde{K}(\tilde{\alpha})$, und somit auch einen Hom. $K(\alpha) \to L$. Wie man leicht überprüft, gilt $\psi|_K = \phi$ und $\psi(\alpha) = \tilde{\alpha}$.

Die Eindeutigkeit der Fortsetzung folgt aus Satz 16.1.

$\square$

„Nullstellen auf Nullstellen“

Satz (16.3)

Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern. Seien außerdem $L|K$ und $\tilde{L}|\tilde{K}$ Körpererweiterungen, $\alpha \in L$ und $f \in K[x]$ ein Polynom mit $f(\alpha) = 0$. Ist dann $\psi : K(\alpha) \to \tilde{L}$ ein Körperhomomorphismus mit $\psi|_K = \phi$, dann ist $\tilde{\alpha} = \psi(\alpha)$ eine Nullstelle von $\tilde{f} = \phi(f)$.

Bem.: Ist $\phi : K \to \tilde{K}$ ein Körperisomorphismus, dann erhält man (offensichtlich) einen Ringisomorphismus $K[x] \to \tilde{K}[x]$ durch

$$\sum_{k=0}^{n} a_k x^k \longmapsto \sum_{k=0}^{n} \phi(a_k) x^k .$$

Beweis von Satz 16.3 („Nullstellen auf Nullst.")

geg.: Körperisom. $\phi : K \to \tilde{K}$, $f \in K[x]$, $L|K$, $\tilde{L}|\tilde{K}$ Körpererweiterungen, $\psi : L \to \tilde{L}$ Fortsetzung von ϕ. Sei $\alpha \in L$ eine Nullstelle von f.

Beh: $\tilde{\alpha} = \psi(\alpha)$ ist eine Nullst. von $\tilde{f} = \phi(f)$

Schreibe $f = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}_0$, $a_0, \ldots, a_n \in K$.

Dann gilt $\tilde{f}(\tilde{\alpha}) = \sum_{k=0}^{n} \phi(a_k)\tilde{\alpha}^k = \sum_{k=0}^{n} \phi(a_k)\psi(\alpha)^k$

$= \sum_{k=0}^{n} \psi(a_k)\psi(\alpha^k) = \sum_{k=0}^{n} \psi(a_k \alpha^k) =$

$\psi|_K = \phi$

$\psi\left(\sum_{k=0}^{n} a_k \alpha^k\right) = \psi(f(\alpha)) = \psi(0_L) = 0_{\tilde{L}}$.

wichtiger Spezialfall: Ist ψ ein K-Hom. (also eine Fortsetzung von $\phi = \mathrm{id}_K$), dann wird somit jede Nullstelle $\alpha \in L$ eines Polynom $f \in K[x]$ durch ψ auf eine Nullstelle desselben Pol. abgebildet, d.h. $f(\psi(\alpha)) = 0_L$.