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.

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 (ii)

geg: Körpererweiterung $L|K$, $n \in \mathbb{N}_0$, $\alpha_1, \dots, \alpha_n \in L$
algebraisch über K mit $L = K(\alpha_1, \dots, \alpha_n)$

<u>Beh.</u>: $L|K$ ist eine end<u>liche</u> Erweiterung

Beweis durch vollst. Ind.

<u>Ind.-Anf.</u> $n = 0$ (Der Körper L entsteht aus K durch Adjunktion von null Elementen.) $\Rightarrow L = K \Rightarrow [L:K] = 1$, insb. ist die Erweiterung endlich

<u>Ind.-Schritt</u> $n \mapsto n+1$ Sei $n \in \mathbb{N}_0$, setze die Aussage für n voraus. Seien $\alpha_1, \dots, \alpha_{n+1} \in L$, algebraisch über K, mit $L = K(\alpha_1, \dots, \alpha_{n+1})$ Ind.-V. $\Rightarrow K(\alpha_1, \dots, \alpha_n) | K$ ist

endliche Erweiterung. Setze $L_0 = K(\alpha_1, \dots, \alpha_n)$, betrachte das Min-pol. von α_{n+1} über L_0 $\Rightarrow [L : L_0] = [L_0(\alpha_{n+1}) : L_0]$ $= \mathrm{grad}(\mu_{\alpha_{n+1}, L_0}) \in \mathbb{N}$. Auf Grund der Gradformel ist mit $L | L_0$ und $L_0 | K$ auch $L | K$ eine endliche Erweiterung (und $[L : K] = [L : L_0] \cdot [L_0 : K]$) $\square$

Ind.-V. $\Rightarrow K(\alpha_1, \dots, \alpha_n) | K$ ist

mit $L = K(\alpha_1, \dots, \alpha_{n+1})$

Sei $S = \{\sqrt[n]{2} \mid n \in \mathbb{N}\}$.

Beh. $\mathbb{Q}(S)|\mathbb{Q}$ ist eine unendl. Erw.

Ang. $[\mathbb{Q}(S):\mathbb{Q}]$ ist endlich. Sei $n \in \mathbb{N}$.

$\sqrt[n]{2} \in S \Rightarrow \sqrt[n]{2} \in \mathbb{Q}(S) \Rightarrow$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{Q}(S)$. d.h. $\mathbb{Q}(\sqrt[n]{2})$ ist ein Zwischenkörper von $\mathbb{Q}(S)|\mathbb{Q}$.

Gradformel $\Rightarrow$

(*) $[\mathbb{Q}(S):\mathbb{Q}] = [\mathbb{Q}(S):\mathbb{Q}(\sqrt[n]{2})]\,[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]$

Das Element $\sqrt[n]{2}$ ist Nullstelle von $f_n = x^n - 2 \in \mathbb{Q}[x]$, außerdem f_n ist normiert und nach dem Eisenstein-Kriterium (angew. auf die Primzahl 2) irreduzibel $\Rightarrow$

$f_n = \mu_{\sqrt[n]{2},\mathbb{Q}} \Rightarrow [\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = \mathrm{grad}(f_n) = n$

Aus (*) folgt somit $n \mid [\mathbb{Q}(S):\mathbb{Q}]$.

also: $n \mid [\mathbb{Q}(S):\mathbb{Q}] \ \forall n \in \mathbb{N} \Rightarrow$

$[\mathbb{Q}(S):\mathbb{Q}]$ kann nicht endlich sein $\lightning$.

E

α-

die

zu li

der

„$\Rightarrow$

K,

Sei

mit

$\Rightarrow \alpha$

über

„$\Leftarrow$"

1,

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.

$\in \mathbb{N}$.

) ist

$\Sigma):\mathbb{Q}]$

n

normiert

Beweis von Satz 15.15

<u>zu (i)</u> geg.: Körpererweiterung $L|K$,

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

z.zg.: T ist Teilkörper von L, dafür zu überprüfen:

(1) $1_L \in T$ (2) $\forall \alpha, \beta \in T: \alpha - \beta, \alpha\beta \in T$

(3) $\forall \alpha \in T \setminus \{0_L\}: \alpha^{-1} \in T$

<u>zu (1)</u> Da $L|K$ eine Körpererw. ist, gilt $1_L = 1_K \in K$.

Daraus folgt, dass 1_L algebraisch über K ist

<u>zu (2), (3)</u> Seien $\alpha, \beta \in T$. Sei $L_0 = K(\alpha, \beta)$.

Da α, β algebraisch über K sind, ist $L_0|K$ nach Prop. 15.14 (ii) eine endliche Erweiterung, nach Prop. 15.14 (i) somit auch algebraisch. $\Rightarrow$ <u>Jedes</u>

Element aus L_0 ist algebraisch über K, insb. auch $\alpha - \beta$, $\alpha\beta$, im Fall $\alpha \neq 0_L$ auch α^{-1}. Also liegen all diese Elemente in L_0.

zu (ii) geg: Körpererweiterung $M|K$, L Zwischenkörper der Erweiterung. z.zg. $M|K$ ist alg $\iff$ $M|L$ und $L|K$ sind algebraisch

„$\Rightarrow$" $M|K$ algebraisch $\Rightarrow$ Jedes $\alpha \in M$ ist algebraisch über K, insb. (wegen $L \subseteq M$) auch jedes $\alpha \in L$. $\Rightarrow L|K$ ist alg

Sei $\alpha \in M$. $M|K$ alg. $\Rightarrow \alpha$ ist alg. über $K \Rightarrow \exists f \in K[x] \setminus \{0_K\}$ mit $f(\alpha) = 0_K$. Wegen $L \supseteq K$ gilt auch $f \in L[x] \setminus \{0_K\}$

$\Rightarrow \alpha$ ist algebraisch über L. also: Jedes $\alpha \in M$ ist algebraisch über $L \Rightarrow M|L$ ist algebraisch.

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

$M|L$ ist alg. $\Rightarrow \alpha$ ist alg. über $L \Rightarrow \exists\, f \in L[x] \setminus \{0_K\}$
mit $f(\alpha) = 0_K$. Schreibe $f = a_n x^n + \dots + a_1 x + a_0$ mit $n \in \mathbb{N}$,
$a_0, \dots, a_n \in L$, setze $L_0 = K(a_0, \dots, a_n)$ $\Rightarrow f \in L_0[x]$
$L|K$ algebraisch $\Rightarrow a_0, \dots, a_n$ sind alg. über $K \overset{\text{Prop. 15.14 (ii)}}{\Longrightarrow}$
$L_0|K$ ist endl. Erw. $\quad f \in L_0[x] \setminus \{0_K\}$, $f(\alpha) = 0_K \Rightarrow$
α ist alg. über $L_0 \overset{15.14\,(ii)}{\Longrightarrow} L_0(\alpha)|L_0$ ist endl. Erw.
$L_0|K$ endlich, $L_0(\alpha)|L_0$ endlich $\overset{\text{Gradformel}}{\Longrightarrow} L_0(\alpha)|K$ ist endl.
$\Rightarrow L_0(\alpha)|K$ ist algebraisch $\Rightarrow \alpha$ ist algebraisch über K.

$\square$

Beweis von Folgerung 15.16

geg.: Körpererweiterung $L|K$, $S \subseteq L$ Teilmenge bestehend aus Elementen, die alle algebraisch über K sind

<u>Beh.</u>: $K(S)|K$ ist algebraische Erweiterung

Sei $T = \{\alpha \in L \mid \alpha \text{ ist algebraisch über } K\}$. Satz 15.15 (i)

$\Longrightarrow$ T ist Teilkörper von L, darüber hinaus ein Zwischenkörper von $L|K$ (da jedes $a \in K$ alg. über K ist)

T Zwischenkörp. von $L|K$ und $S \subseteq T$ (nach Vor.) $\Rightarrow K(S) \subseteq T$

$\Longrightarrow$ Jedes $\alpha \in K(S)$ ist alg. über K. $\Rightarrow K(S)|K$ ist algebraisch. $\square$

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 Prop. 15.17:

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

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

$[L:K]=2 \Rightarrow L \supsetneq K$. Sei $\alpha \in L \setminus K$ und $f = \mu_{\alpha,K}$.

Gradformel $\Rightarrow 2 = [L:K] = [L:K(\alpha)]\,[K(\alpha):K]$ $(*)$

$\alpha \notin K \Rightarrow K(\alpha) \supsetneq K \Rightarrow [K(\alpha):K] > 1$. Aus $(*)$ folgt

somit $[K(\alpha):K] = 2$, $[L:K(\alpha)] = 1$, also $L = K(\alpha)$

$\Rightarrow \mathrm{grad}(f) = [K(\alpha):K] = 2 \Rightarrow \exists\, a,b \in K: f = x^2 + ax + b$

$f(\alpha) = 0_K \Rightarrow \alpha^2 + a\alpha + b = 0_K \Rightarrow \alpha^2 + a\alpha = -b \Rightarrow$

$\alpha^2 + a\alpha + \frac{1}{4}a^2 = \frac{1}{4}(a^2 - 4b)$ (beachte: $\mathrm{char}(K) \neq 2 \Rightarrow 2$ und $4 = 2\cdot 2$ sind in K invertierbar)

$\Rightarrow (\alpha + \frac{1}{2}a)^2 = \frac{1}{4}(a^2 - 4b)$ Setzen wir $\gamma = \alpha + \frac{1}{2}a$, dann gilt $\gamma^2 = \frac{1}{4}(a^2 - 4b) \in K$. noch zu überprüfen: $L = K(\gamma)$

genügt: $K(\alpha) = K(\gamma)$ „$\subseteq$" $\alpha = \gamma - \frac{1}{2}a \in K(\gamma)$

„$\supseteq$" $\gamma = \alpha + \frac{1}{2}a \in K(\alpha)$ $\square$

Beweis von Satz 15.19:

geg.: $m, n \in \mathbb{Z} \setminus \{0, 1\}$, $\underbrace{}_{}$verschieden, beide quadratfrei

(d.h. es gibt keinen quadratischen Primteiler)

Aus Symmetriegründen reicht es zu zeigen, dass $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$ gilt. bekannt:

(*) $\{1, \sqrt{m}\}$ ist Basis von $\mathbb{Q}(\sqrt{m})$ als $\mathbb{Q}$-Vektorraum. Ang.: $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$.

$\Rightarrow \exists\, r, s \in \mathbb{Q}: \sqrt{n} = r + s\sqrt{m}$

$\Rightarrow n = (r + s\sqrt{m})^2 = r^2 + ms^2 + 2rs\sqrt{m}$

$\Rightarrow n \cdot 1 + 0 \cdot \sqrt{m} = (r^2 + ms^2) \cdot 1 + 2rs\sqrt{m}$

$\Rightarrow n = r^2 + ms^2,\ 2rs = 0$

$2rs = 0 \Rightarrow r = 0$ oder $s = 0$

<u>1. Fall</u>: $r = 0 \Rightarrow n = ms^2$ Schreibe $s = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $\operatorname{ggT}(a,b) = 1 \Rightarrow n = m\left(\frac{a}{b}\right)^2$

$\Rightarrow b^2 n = a^2 m$ Sei p Primteiler von a

$\Rightarrow p^2 \mid b^2 n \xRightarrow{\operatorname{ggT}(a,b)=1} p^2 \mid n$ ↯ zu n quadratfrei

Sei p ein Primteiler von b. Dann folgt genau $p^2 \mid m$ ↯ zu n quadratfrei $\Rightarrow a, b \in \{\pm 1\}$

$\Rightarrow m = n$ ↯ zu $m \neq n$

<u>2. Fall</u>: $s = 0$ ähnlich zum 1. Fall, siehe Skript. $\square$

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.

(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 $\psi_\beta(\alpha) = \beta$.

...t frei
...nteiler)
...ugen,
...t:
$\mathbb{Q}$-
...)
...rs $\sqrt{m}$
...rs $\sqrt{m}$

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 mit

$\psi_1|_S \overset{(*)}{=} \psi_2|_S$ Beh.: $\psi_1 = \psi_2$

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

Wegen $(*)$ gilt $S \subseteq M$. zeige noch:

M ist Zwischenkörper von $L|K$. zu überprüfen:

(1) $K \subseteq M$ (2) $\forall \alpha, \beta \in M : \alpha - \beta, \alpha\beta \in M$

(3) $\forall \alpha \in M \setminus \{0_K\} : \alpha^{-1} \in M$

$= \frac{a}{v}$

dratfrei

genau

$\in k \pm 17$

Skript.

$\square$

zu (1) Sei $a \in K$. $\psi_1(a) = \phi(a) = \psi_2(a)$

$\uparrow$ ψ_1 Fortsetzung von ϕ

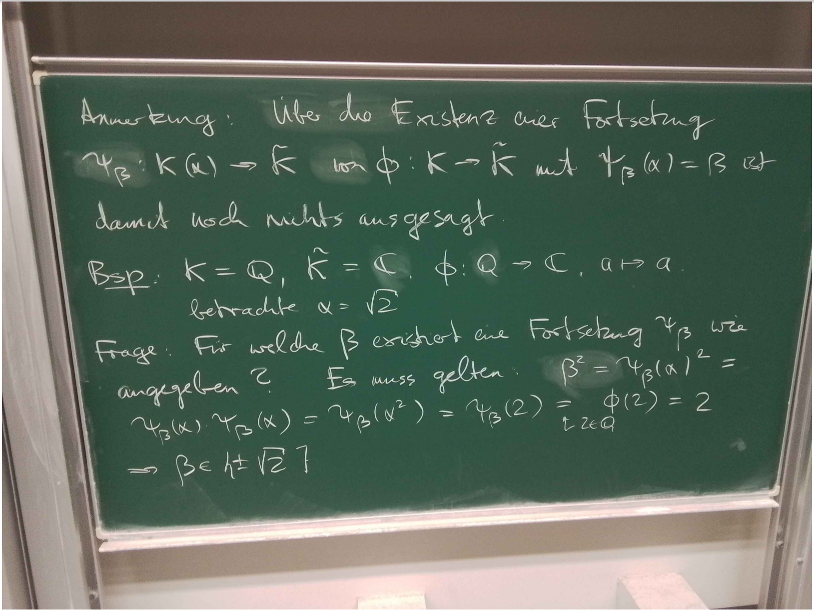
$\Rightarrow a \in M$

zu (2) Seien $\alpha, \beta \in M$. $\Rightarrow \psi_1(\alpha) = \psi_2(\alpha)$, $\psi_1(\beta) = \psi_2(\beta)$

$\Rightarrow \psi_1(\alpha - \beta) = \psi_1(\alpha) - \psi_1(\beta) = \psi_2(\alpha) - \psi_2(\beta) =$
$\psi_2(\alpha - \beta) \Rightarrow \alpha - \beta \in M$ Genauso erhält man $\alpha\beta \in M$.

zu (3) Sei $\alpha \in M \setminus \{0_K\}$. $\Rightarrow \psi_1(\alpha) = \psi_2(\alpha) \Rightarrow$
$\psi_1(\alpha^{-1}) = \psi_1(\alpha)^{-1} = \psi_2(\alpha)^{-1} = \psi_2(\alpha^{-1})$
$\Rightarrow \alpha^{-1} \in M$.

damit insgesamt: M ist Zwischenkörper von $L|K$
mit $M \supseteq S \Rightarrow M \supseteq K(S) \Rightarrow M \supseteq L$
$\Rightarrow \psi_1(\alpha) = \psi_2(\alpha)\ \forall \alpha \in L \Rightarrow \psi_1 = \psi_2$. $\square$



Wir werden sehen, dass für die Werte $\beta = \sqrt{2}$ und $\beta = -\sqrt{2}$ tatsächlich jeweils eine Fortsetzung ψ_β von ϕ existiert.