Körpertheorie

Def. Seien K und L Körper.

(i) K ist Teilkörper von $L \iff 1_L \in K$
und $\forall \alpha, \beta \in L : \alpha, \beta \in K \Rightarrow \alpha - \beta, \alpha\beta \in K$
sowie $\forall \alpha \in L : \alpha \in K^\times \Rightarrow \alpha^{-1} \in K$

(ii) L ist Erweiterungskörper von $K \iff$
K ist Teilkörper von L

Das Paar (K, L) wird dann Körpererweiterung genannt. (Notation: $L|K$)

Wichtige Beispiele für Körpererweiterungen:

(1) Zahlbereiche: $\mathbb{R} | \mathbb{Q}$, $\mathbb{C} | \mathbb{R}$, $\mathbb{C} | \mathbb{Q}$

(2) $\mathbb{Q}(\sqrt{2}) | \mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{4+\sqrt{5}}) | \mathbb{Q}$

(3) $\mathbb{F}_{p^r} | \mathbb{F}_p$ falls p Primzahl, $r \in \mathbb{N}$
(allgemeiner: $\mathbb{F}_{p^s} | \mathbb{F}_{p^r}$ falls $r | s$)
aber: $\mathbb{F}_8 | \mathbb{F}_4$ ist keine Körpererweiterung
(Achtung: $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_8 \neq \mathbb{Z}/8\mathbb{Z}$)

(4) $K^{alg} | K$, wobei K bel. Körper, K^{alg} ein algebraischer Abschluss von K

(5) $K(t)|K$, wobei K einen bel. Körper und $K(t)$ den rationalen Funktionenkörper über K bezeichnet (Dies ist der Quotientenkörper des Polynomrings $K[t]$, d.h. $K(t) = \{ \frac{f}{g} \mid f, g \in K[t], g \neq 0 \}$.)

Notation: Sei $L|K$ eine Körpererweiterung und $S \subseteq L$. Dann bezeichnet $K(S)$ den kleinsten Erweiterungskörper von L, der S enthält.

wichtige Regel: Sei T eine weitere Teilmenge von L. Dann gilt: $K(S) = K(T) \Leftrightarrow T \subseteq K(S)$ und $S \subseteq K(T)$

Def. Sei $f \in K[x] \setminus K$ und L ein Erweiterungskörper von K, über dem f in Linearfaktoren zerfällt (häufig: $K = \mathbb{Q}$, $L = \mathbb{C}$). Sei $\{\alpha_1, \dots, \alpha_m\}$ die Menge der verschiedenen Nullstellen von f in L. Dann wird $K(\alpha_1, \dots, \alpha_m)$ der Zerfällungskörper von f über K in L genannt.

Bsp.: Sei $f = x^5 - 7 \in \mathbb{Q}[x]$, $\zeta = e^{2\pi i/5}$ und $\alpha = \sqrt[5]{7}$. Dann ist $L = \mathbb{Q}(\alpha, \zeta)$ der Zerfällungskörper von f über $\mathbb{Q}$ in L. denn:

Beh.: Die Menge $N = \{\zeta^k \alpha \mid 0 \leq k < 5\}$ ist die Menge der komplexen Nullstellen von f.

Jedes der Elemente ist eine Nullstelle von f, denn für $0 \leq k < 5$ gilt $f(\zeta^k \alpha) = (\zeta^k \alpha)^5 - 7$

$= (\zeta^5)^k \alpha^5 - 7 = 1^k \cdot 7 - 7 = 0$.

Weil ζ eine primitive 5-te Einheitswurzel (also ein Element der Ordnung 5 in $\mathbb{C}^\times$) ist, sind ζ^k mit $0 \leq k < 5$ fünf verschiedene komplexe Zahlen und wg. $\alpha \neq 0$ sind damit auch $\zeta^k \alpha$ mit $0 \leq k < 5$ verschieden. $\Rightarrow |N| = 5$ Als Polynom vom Grad 5 kann f nicht mehr als fünf Nullstellen in

$\mathbb{C}$ haben. Also hat f außerhalb von N keine weiteren Nullstellen. ($\Rightarrow$ Beh.)

zu überprüfen also: $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(N)$

genügt: i) $N \subseteq \mathbb{Q}(\alpha, \beta)$ ii) $\{\alpha, \beta\} \subseteq \mathbb{Q}(N)$

zu i) Sei $\beta \in N$, d.h. $\beta = \beta^k \alpha$ mit $k \in \{0, \dots, 4\}$.
$\alpha, \beta \in \mathbb{Q}(\alpha, \beta)$; $\mathbb{Q}(\alpha, \beta)$ ist als Teilkörp. von $\mathbb{C}$ abgeschlossen unter Multiplikation $\Rightarrow \beta = \beta^k \alpha \in \mathbb{Q}(\alpha, \beta)$

zu ii) $\alpha \in N \Rightarrow \alpha \in \mathbb{Q}(N)$

$\alpha, \beta\alpha \in N$. $\mathbb{Q}(N)$ ist abg. unter Kehrwert-bildung und Mult. ($\forall \alpha \neq 0$) $\Rightarrow \beta = (\beta\alpha) \cdot \alpha^{-1}$ liegt in $\mathbb{Q}(N)$

□

Erinnerung: Sei $L|K$ eine Körpererweiterung. Dann besitzt L die Struktur eines K-Vektorraums. (1)
(Vektoraddition $L \times L \to L$, $(\alpha, \beta) \mapsto \alpha + \beta$
skalare Multiplikation $K \times L \to L$, $(a, \alpha) \mapsto a\alpha$)

Def. Sei $L|K$ eine Körpererweiterung. Dann wird die Dimension des K-Vektorraums L als der Grad $[L:K]$ der Erweiterung bezeichnet. Ist dieser endlich, dann nennt man $L|K$ eine endliche Körpererweiterung. (2)

Bsp.: $[\mathbb{C}:\mathbb{R}] = 2$ (denn $\{1, i\}$ ist eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum)

Hilfsmittel zur Bestimmung von Erw.-graden

(1) Ist $L|K$ eine Körpererw., $\alpha \in L$ algebraisch über K und f das Minimalpolynom von α über K (siehe unten), dann gilt $[K(\alpha):K] = \operatorname{grad}(f)$.
(Ist α nicht algebraisch über L, dann gilt $[K(\alpha):K] = \infty$.)

(2) Gradformel: Ist M ein Zwischenkörper von $L|K$ ist (d.h. $K \subseteq M \subseteq L$, und $M|K$, $L|M$ sind Körpererweiterungen), dann gilt $[L:K] = [L:M] \cdot [M:K]$.

Def. Sei $L|K$ eine Körpererweiterung.

(i) Ein Element $\alpha \in L$ heißt <u>algebraisch</u> über K, wenn ein $f \in K[x] \setminus \{0\}$ mit $f(\alpha) = 0$ existiert.

(ii) Das eind. best. normierte Pol. minimalen Grades mit dieser Eig. ist das <u>Minimalpol.</u> $\mu_{\alpha,K}$ von α über dem Körper K.

(iii) Die Erweiterung $L|K$ heißt algebraisch, wenn jedes $\alpha \in L$ algebraisch über K ist.

Bem.: (ii) wichtige Eigenschaften des Min.-pol.:

(1) $f \in K[x]$ normiert, irred., $f(\alpha) = 0$

$\longrightarrow f = \mu_{\alpha,K}$

(2) Ist $g \in K[x]$ mit $g(\alpha) = 0$, dann ist $M_{\alpha, K}$ ein Teiler von g.

(iii) Jede endliche Körpererweiterung ist algebraisch, aber die Umkehrung ist im Allgemeinen falsch.

Beispiele für unendliche algebraische Erweiterungen:

(1) $\mathbb{Q}^{alg} \mid \mathbb{Q}$ (2) $\mathbb{F}_p^{alg} \mid \mathbb{F}_p$ (p Primzahl)

(3) $\mathbb{Q}(S) \mid \mathbb{Q}$, wobei $S = \{\sqrt[n]{2} \mid n \in \mathbb{N}\}$

F26T2A5 (a) Sei $f = x^5 - 7$ und K der Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$. Bestimmen Sie den Erweiterungsgrad $[K:\mathbb{Q}]$.

bereits gezeigt: $K = \mathbb{Q}(\alpha, \zeta)$, wobei $\alpha = \sqrt[5]{7}$, $\zeta = e^{2\pi i/5}$

Beh.: (1) $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$ (2) $[\mathbb{Q}(\zeta):\mathbb{Q}] = 4$

zu (1) Das Polynom f ist normiert, erfüllt $f(\alpha) = 0$ und ist irreduzibel auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 7). $\rightarrow f = M_{\alpha,\mathbb{Q}}$

$\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = \text{grad}(f) = 5$

$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = \operatorname{grad}(f) = 5$

zu (2) Aus der Vorlesung ist bekannt, dass das n-te Kreisteilungspol Φ_n für alle $n \in \mathbb{N}$ jeweils das Minimalpolynom von $\zeta_n = e^{2\pi i/n}$ über $\mathbb{Q}$ ist, und dass $\operatorname{grad} \Phi_n = \varphi(n)$ gilt. $\Rightarrow [\mathbb{Q}(\zeta) : \mathbb{Q}] = \operatorname{grad} \Phi_5 = \varphi(5) = 4$

$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot 5$

$\Rightarrow$ 5 ist Teiler von $[K : \mathbb{Q}]$

$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)] \cdot 4$

$\Rightarrow$ 4 ist Teiler von $[K : \mathbb{Q}]$

insgesamt: $\operatorname{kgV}(4,5) = 20$ ist Teiler von $[K : \mathbb{Q}]$

$\Rightarrow [K : \mathbb{Q}] \geq 20$

s.o. $\Rightarrow [K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)] \cdot 5$, außerdem

$[K:\mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\sqrt{5}):\mathbb{Q}(\alpha)] = \operatorname{grad} \mu_{\sqrt{5},\mathbb{Q}(\alpha)}$

Es gilt $\Phi_5 \in \mathbb{Q}(\alpha)[x]$ und $\Phi_5(\sqrt{5}) = 0$

Daraus folgt $\mu_{\sqrt{5},\mathbb{Q}(\alpha)} \mid \Phi_5$ in $\mathbb{Q}(\alpha)[x]$

$\Rightarrow \operatorname{grad} \mu_{\sqrt{5},\mathbb{Q}(\alpha)} \leq \operatorname{grad} \Phi_5 = 4$

$\Rightarrow [K:\mathbb{Q}(\alpha)] \leq 4 \Rightarrow [K:\mathbb{Q}] \leq 4 \cdot 5$

$= 20$. Insgesamt gilt also $[K:\mathbb{Q}] = 20$

□

Übung: Bestimmen Sie den Erweiterungsgrad von $\mathbb{Q}(\sqrt[5]{2}, \sqrt[6]{7}, i) \mid \mathbb{Q}$.

F26T1A2 Sei $f = x^4 - 6x^2 - 3 \in \mathbb{Q}[x]$

(a) Zeigen Sie, dass f über $\mathbb{Q}$ irreduzibel ist, und bestimmen Sie die Nullstellen von f in $\mathbb{C}$.

[Lösung, Ergebnis: Die Nullstellenmenge ist gegeben durch $N = \{\pm\alpha, \pm\beta\}$ mit $\alpha = \sqrt{3+2\sqrt{3}}$, $\beta = \sqrt{3-2\sqrt{3}}$.]

(b) Zeigen Sie: $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ und

$\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3})$