

Körpertheorie

Def Körpererweiterung = Paar (K, L) ,
wobei K ein Teilkörper von L ist

Bsp. für Körpererweiterungen

(i) $\mathbb{R} \subset \mathbb{C}$, $\mathbb{C} \subset \mathbb{C}$

(ii) $\mathbb{F}_{q^m} \mid \mathbb{F}_q$, wobei q Primzahlpotenz > 1
und $m \in \mathbb{N}$ ist.

(iii) $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$, $\mathbb{Q}(\zeta) \mid \mathbb{Q}$
wobei $\zeta = e^{2\pi i/m}$ ($m \in \mathbb{N}$)

und $m \in \mathbb{N}$ ist

(iv) $K^{\text{alg}} | K$, wobei K^{alg} algebraischer Abschluss von K ist

(v) $K(t) | K$, wobei $K(t)$ den rationalen Funktionenkörper über K bezeichnet

$$K(t) = \left\{ \frac{p}{q} \mid p, q \in K[t], q \neq 0 \right\}$$

Erinnerung Sei $\tilde{K} | K$ eine beliebige Körpererweiterung und $S \subseteq \tilde{K}$. Dann bezeichnet $K(S)$ den kleinsten Teilkörper von $\tilde{K}$ mit $K(S) \supseteq K \cup S$ (d.h. für jeden Teilkörper L von $\tilde{K}$ mit $L \supseteq K \cup S$ gilt jeweils $L \supseteq K(S)$.)

wichtige Klasse von Beispielen:

Ist $\tilde{K}|K$ eine Körpererweiterung, $f \in K[x]$, K ein Polynom, das über $\tilde{K}$ in Linearfaktoren zerfällt und $N = \{\alpha \in \tilde{K} \mid f(\alpha) = 0\}$, dann wird $K(N)$ der Zerfällungskörper von f über K in $\tilde{K}$ bezeichnet.

Bsp.: Sei $f = x^n - a \in \mathbb{Q}[x]$ (mit $n \in \mathbb{N}$, $a \in \mathbb{Q}$, $a \neq 0$).

Dann ist $\mathbb{Q}(\alpha, \beta)$ mit $\alpha = \sqrt[n]{a}$ und $\beta = e^{2\pi i/n}$ der Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$.

(Beweis: Übung)

wichtige Regel: Ist $\tilde{K}|K$ eine Körpererweiterung

Körper von f über $\mathbb{Q}$ in $\mathbb{C}$.

(Beweis: Übung)

und sind $S, T \subseteq \tilde{K}$, dann folgt aus $S \subseteq K(T)$ und $T \subseteq K(S)$ bereits $K(S) = K(T)$.

Def. Sei $L|K$ eine Körpererweiterung

i) $x \in L$ ist algebraisch über $K \iff \exists f \in K[x] \setminus \{0\}$
mit $f(x) = 0$

ii) Ist $x \in L$ algebraisch über K , dann wird das eindeutig bestimmte normierte Polynom minimalen Grades über K mit x als Nullstelle als Minimalpolynom $m_{x,K}$ von x über K bezeichnet.

iii) Die Erweiterung $L|K$ wird algebraisch genannt, wenn jedes $x \in L$ algebraisch über K ist.

wichtiges Kriterium: Ist $f \in K[x]$ ein normiertes irreduzibles Polynom mit $f(\alpha) = 0$, dann folgt $f = \mu_{\alpha, K}$.

H21T2A4 Sei $\alpha = \sqrt{1+\sqrt{2}} \in \mathbb{R}$ und $\beta = i\sqrt{\sqrt{2}-1} \in \mathbb{C}$.

(a) Bestimmen Sie die Minimalpolynome von α und β über $\mathbb{Q}$.

$$\alpha = \sqrt{1+\sqrt{2}} \Rightarrow \alpha^2 = 1+\sqrt{2} \Rightarrow \alpha^2 - 1 = \sqrt{2}$$

$$\Rightarrow (\alpha^2 - 1)^2 = 2 \Rightarrow \alpha^4 - 2\alpha^2 + 1 = 2$$

$$\Rightarrow \alpha^4 - 2\alpha^2 - 1 = 0 \Rightarrow \alpha \text{ ist Nullstelle}$$

$$\text{des Polynoms } f = x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$$

Offenbar ist f normiert, und $f(x) \neq 0$

noch z.zg: f ist irreduzibel über $\mathbb{Q}$

Es reicht z.zg., dass f irreduzibel in $\mathbb{Z}[x]$ ist. Seien also $g, h \in \mathbb{Z}[x]$ mit $f =$

gh . z.zg. Eines der Polynome g, h liegt in $(\mathbb{Z}[x])^\times = \mathbb{Z}^\times = \{\pm 1\}$. f ist normiert $\Rightarrow$

d.B.d.A. sind g, h beide normiert

Da das Produkt der konstanten Terme von g und h gleich 1 sein muss, können wir davon ausgehen, dass der konstante Term von g gleich 1 und der konstante Term von h gleich -1 ist.

Im Grad $g = 0$ oder Grad $h = 0$, dann folgt bereits $g = 1$ oder $h = 1$, also $g \in \{\pm 1\}$ oder $h \in \{\pm 1\}$.

Ist $\text{grad}(g) = 1$ oder $\text{grad}(h) = 1$ ist, dann hat f in $\mathbb{Q}$ eine Nullstelle. Da f in $\mathbb{Z}[x]$ liegt und normiert ist, muss die Nullstelle in $\mathbb{Z}$ liegen und den konstanten Term -1 von f teilen. $\Rightarrow$ nur ± 1 als Nullstellen möglich aber: $f(1) = -2 \neq 0$, $f(-1) = -2 \neq 0$ $\Downarrow$

einzig verbleibende Möglichkeit:
 $\text{grad}(g) = \text{grad}(h) = 2$

$$\Rightarrow \exists a, b \in \mathbb{Z} : g = x^2 + ax + 1,$$

$$h = x^2 + bx - 1 \Rightarrow x^4 - 2x^2 - 1 =$$

$$f = gh = (x^2 + ax + 1)(x^2 + bx - 1) =$$

$$x^4 + (a+b)x^3 + abx^2 + (b-a)x - 1$$

$$\Rightarrow b-a=0, ab=-2 \Rightarrow a=b, a^2=-2 \Downarrow$$

$$f(-1) = -2 \neq 0 \quad \wedge$$

da -2 kein Quadrat in $\mathbb{Z}$ ist.

Insgesamt ist damit $M_{\mathbb{Q}} = f$ nachgewiesen.

$$\beta = i\sqrt{\sqrt{2}-1} \Rightarrow \beta^2 = (-1)(\sqrt{2}-1) = 1-\sqrt{2}$$

$$\Rightarrow \beta^2 - 1 = -\sqrt{2} \Rightarrow (\beta^2 - 1)^2 = 2$$

$$\Rightarrow \beta^4 - 2\beta^2 + 1 = 2 \Rightarrow \beta^4 - 2\beta^2 - 1 = 0 \Rightarrow$$

Auch β ist Nullstelle von $f = x^4 - 2x^2 - 1$.

Da f normiert und irreduzibel ist, folgt

$$M_{\mathbb{Q}} = f.$$

Erweiterung: Ist $L|K$ eine Körpererweiterung, dann bezeichnet man die Dimension von L als K -Vektorraum als Grad $[L:K]$ der Erweiterung.

folgt
oder $f \in \mathbb{Z}[x]$

wichtige Hilfsmittel zur Bestimmung
von Erweiterungsgraden

(i) Gradformel: Ist $M|K$ eine Körper-
erweiterung und L ein Zwischenkörper von
 $M|K$ mit der Eigenschaft, dass $[M:L]$
und $[L:K]$ endlich sind, dann gilt

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

(ii) Ist $L|K$ eine Körpererw. und $\alpha \in L$ alg.
über K , dann gilt $[K(\alpha):K] = \text{grad } \mu_{\alpha,K}$.

H21T2A4 (B)

Bestimmen Sie die Erweiterungsgrade $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ und $[\mathbb{Q}(\beta) : \mathbb{Q}]$ und von $[\mathbb{Q}(\alpha, i) : \mathbb{Q}]$.

Aufgrund des Ergebnisses von Teil (a) gilt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad } M_{\alpha, \mathbb{Q}} = \text{grad } f = 4.$$

Ebenso erhält man $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$.

Bestimme nun zunächst $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)]$. Die Zahl i ist eine Nullstelle von $g = x^2 + 1 \in \mathbb{Q}(\alpha)[x]$.

Beh.: $g = M_{i, Q(x)}$ Offenbar ist g normiert. Ang. g ist reduzibel $\xrightarrow{\text{grad}(g)=2}$ Die Nullstellen $\pm i$ von g sind in $Q(x)$ enthalten $\nleftrightarrow$ da $Q(x) \subseteq \mathbb{R}$ (wg $x \in \mathbb{R}$) und $\pm i \in \mathbb{C} \setminus \mathbb{R}$. Also ist g in $Q(x)[x]$ irred. ($\Rightarrow$ Beh.)

$$\Rightarrow [Q(x, i) : Q(x)] = \text{grad}(g) = 2$$

$$\text{Gradformel} \Rightarrow [Q(x, i) : Q] = [Q(x, i) : Q(x)] \cdot [Q(x) : Q] \\ = 2 \cdot 4 = 8.$$

Frage: Gilt $Q(x) = Q(\beta)$? Antwort: Nein, denn wegen $x \in \mathbb{R}$ gilt $Q(x) \subseteq \mathbb{R}$, aber wegen $\beta \notin \mathbb{R}$ gilt $Q(\beta) \not\subseteq \mathbb{R}$. $\square$

Übung: H17T3A4(a), F17T1A2

Übung: H17T3A4 (a), F17T1A2

H25T2A3 (a) Sei $f = x^4 + 1 \in \mathbb{Q}[x]$ und L der Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$.

Zeigen Sie: $L = \mathbb{Q}(i, \sqrt{2})$.

Sei $\alpha \in \mathbb{C}$ mit $f(\alpha) = 0 \Rightarrow \alpha^4 + 1 = 0 \Rightarrow \alpha^4 = -1$
 $\Rightarrow \alpha^8 = 1 \Rightarrow \alpha$ ist achte Einheitswurzel

Betrachte $\zeta = e^{2\pi i/8} = e^{\pi i/4}$ $f(\zeta) = \zeta^4 + 1 =$
 $(e^{\pi i/4})^4 + 1 = e^{\pi i} + 1 = -1 + 1 = 0 \Rightarrow \zeta \in L$

Eulersche Formel $\Rightarrow \zeta = e^{\pi i/4} = \cos(\frac{\pi}{4}) + i \sin(\frac{\pi}{4}) =$

$\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ $|\zeta| = 1 \Rightarrow \zeta \bar{\zeta} = |\zeta|^2 = 1 \Rightarrow \zeta^{-1} = \bar{\zeta} = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$

$$\gamma, \gamma^{-1} \in \mathbb{Q}(\gamma) \rightarrow \gamma + \gamma^{-1} = \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\right) + \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right) = \frac{2}{\sqrt{2}} = \sqrt{2} \in \mathbb{Q}(\gamma)$$

$$\gamma, \sqrt{2} \in \mathbb{Q}(\gamma) \rightarrow \gamma - \frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}} \in \mathbb{Q}(\gamma) \\ \Rightarrow \frac{1}{\sqrt{2}} \cdot \sqrt{2} = 1 \in \mathbb{Q}(\gamma) \quad \text{Insgesamt gilt}$$

also $\{\sqrt{2}, 1\} \subseteq \mathbb{Q}(\gamma) \subseteq L$, somit

$$\mathbb{Q}(\sqrt{2}, 1) \subseteq L, \quad \text{noch z.zg. } L \subseteq \mathbb{Q}(\sqrt{2}, 1)$$

Sei $N \subseteq \mathbb{C}$ die Menge der komplexen Nullstellen von f . Wegen $L = \mathbb{Q}(N)$ genügt es, $N \subseteq \mathbb{Q}(\sqrt{2}, 1)$ zu überprüfen. Sei $K = \mathbb{Q}(\sqrt{2}, 1)$.

$\sqrt{2}, 1 \in K \Rightarrow \gamma = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \in K$. Wie oben gezeigt, besteht N aus acht Einheitswurzeln.

Das Element ζ ist eine primitive 8-te Einheitswurzel, und lt. VL ist die Menge aller achten Einheitswurzeln geg. durch

$$M = \{\zeta^k \mid 0 \leq k \leq 7\} \quad \text{Aus } \zeta \in K \text{ folgt}$$

$$M \subseteq K \Rightarrow N \in M \subseteq K$$



(i)
stellen
 $\zeta \in$
(VL ii).
Die oben
swurzeln.