

Erinnerung: Sei $L|K$ eine Körpererweiterung und $\alpha \in L$.

(i) Die Erweiterung $L|K$ heißt normal, wenn jedes in $K[x]$ irreduzible Polynom, das in L eine Nullstelle hat, über L in Linearfaktoren zerfällt.

(ii) Man nennt ein irreduzibles Polynom separabel, wenn es in jeder Erweiterung von K nur einfache Nullstellen besitzt (Dies sind genau die irreduziblen Pol. $f \in K[x]$ mit $\text{ggT}(f, f') = 1$.)

(iii) Das Element α ist separabel über K , wenn es algebraisch über K ist und $M_{\alpha, K}$ separabel ist.

Körpererwei-

normal,
le Polynom,
bes L in

mon separabel,
 K nur ein-
sind genau die
($T(f, f') = 1$.)
ver K , wenn
da K separabel ist.

(iv) Die Erweiterung L/K heißt
separabel, wenn jedes $y \in L$
separabel über K ist, und
galois'sch, wenn L/K normal
und separabel ist.

Anmerkungen / Beispiele:

zu (i) Eine endliche Erweiterung L/K
ist genau dann normal, wenn ein
 $f \in K[x] \setminus K$ existiert, so dass L Zer-
fällungskörper von f über K ist.

- Jede Erweiterung vom Grad 2 ist normal.
- Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht
normal, (Grund: Das Polynom $f = x^3 - 2$

ist in $\mathbb{Q}$
hat in $\mathbb{Q}$
aber f zer-
in Linear
von $\sqrt[3]{2}$ re-
len liegen

zu (iv) Ist
dann ist jed
von K sepa-

- Für jede
 $f_p(t) \mid f_p$
bel), wobei
Körper über

heißt
s. $\gamma \in L$
st, und
K normal

Erweiterung L/K
normal, wenn ein
so dass L zer-
fällt über K ist.

Grad 2 ist normal.
 $(\mathbb{Z})/\mathbb{Q}$ ist nicht
s. Polynom $f = x^3 - 2$

ist in $\mathbb{Q}[x]$ irreduzibel (Eisenstein),
hat in $\mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle ($x = \sqrt[3]{2}$),
aber f zerfällt aber nicht in $\mathbb{Q}(\sqrt[3]{2})[x]$
in Linearfaktoren, denn die Wurzeln
von $\sqrt[3]{2}$ verschiedenen komplexen Nullstel-
len liegen in $\mathbb{C} \setminus \mathbb{R}$, also nicht in $\mathbb{Q}(\sqrt[3]{2})$.

zu (iv) Ist $\text{char}(K) = 0$ oder K endlich,
dann ist jede algebraische Erweiterung
von K separabel.

- Für jede Primzahl p ist die Erweiterung
 $\mathbb{F}_p(t) / \mathbb{F}_p(t^p)$ inseparabel (= nicht separa-
bel), wobei $\mathbb{F}_p(t)$ den rationalen Funktionen-
körper über $\mathbb{F}_p$ bezeichnet.

• Satz

Für

L/K

mit

H25

(a) Bas

- stell

Für $f \in$

$f(x) =$

$x^4 - 4x^2$

$(x^2 - 2)^2$

$-2 + \sqrt{2}$

• Satz vom primitiven Element:

Für jede endliche separable Erweiterung $L|K$ gibt es jeweils ein $\alpha \in L$ mit $L = K(\alpha)$.

H25T1A4 Sei $f = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$

(a) Bestimmen Sie alle komplexen Nullstellen von f .

Für jedes $\alpha \in \mathbb{C}$ gilt die Äquivalenz

$$f(\alpha) = 0 \Leftrightarrow \alpha^4 - 4\alpha^2 + 2 = 0 \Leftrightarrow$$

$$\alpha^4 - 4\alpha^2 + 4 = 2 \Leftrightarrow (\alpha^2 - 2)^2 = 2 \Leftrightarrow$$

$$(\alpha^2 - 2)^2 - (\sqrt{2})^2 = 0 \Leftrightarrow (\alpha^2 - 2 - \sqrt{2}) \cdot (\alpha^2 - 2 + \sqrt{2}) = 0 \Leftrightarrow \alpha^2 \in \{2 \pm \sqrt{2}\} \Leftrightarrow$$

$$\alpha \in \{\pm\sqrt{2 \pm \sqrt{2}}\}$$

$$\alpha \in \mathbb{C}$$

von f in

$$\beta = \sqrt{\alpha}$$

(Hinweis

Für α ,

nicht $\sqrt{\alpha}$

$$\sqrt{\alpha\beta} \in \mathbb{C}$$

für α, β

(b) Sei

f über

und be

Erweiterung
 $\alpha \in L$

$x^2 + 2 \in \mathbb{Q}[x]$
 komplexen Null-
 äquivalenz

$0 \Leftrightarrow$
 $(\sqrt{2})^2 = 2 \Leftrightarrow$
 $(\sqrt{2} - \sqrt{2}) \cdot (\sqrt{2} + \sqrt{2})$
 $\pm \sqrt{2} \Leftrightarrow$

$\alpha \in \{\pm \sqrt{2 \pm \sqrt{2}}\}$. Die Nullstellen
 von f in $\mathbb{C}$ sind also $\pm \beta, \pm \gamma$ mit
 $\beta = \sqrt{2 + \sqrt{2}}, \gamma = \sqrt{2 - \sqrt{2}}$

(Hinweis zum Rechnen mit Wurzeln:

Für $\alpha, \beta \in \mathbb{C}$ gilt im Allgemeinen
 nicht $\sqrt{\alpha \beta} \stackrel{(*)}{=} \sqrt{\alpha} \cdot \sqrt{\beta}$, sondern nur
 $\sqrt{\alpha \beta} \in \{\pm \sqrt{\alpha} \cdot \sqrt{\beta}\}$. Gilt es ist (*)
 für $\alpha, \beta \in \mathbb{R}_+$.)

(b) Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von
 f über $\mathbb{Q}$. Zeigen Sie: $L = \mathbb{Q}(\gamma)$,
 und bestimmen Sie $[L : \mathbb{Q}]$

Nach
 $L = \mathbb{Q}$
 z.zg.
 (1) γ
zu (1)
zu (2)
 $\beta \gamma =$
 $= \sqrt{4 -}$
 $\gamma \in \mathbb{Q}(\gamma)$
 $\gamma^2, 2 \in$
 $\sqrt{2}, \gamma \in$

Nach Def. des Zerkörperkörpers gilt
 $L = \mathbb{Q}(N)$ mit $N = 1 \pm \beta, \pm \gamma$.

z.zg. $\mathbb{Q}(N) = \mathbb{Q}(\gamma)$, es genügt z.zg.:

$$(1) \gamma \in \mathbb{Q}(N) \quad (2) N \in \mathbb{Q}(\gamma)$$

zu (1) klar, da $\gamma \in N$

zu (2) Es gilt $2 \pm \sqrt{2} \in \mathbb{R}_+$ und somit

$$\begin{aligned} \beta \gamma &= \sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} \\ &= \sqrt{4-2} = \sqrt{2} \Rightarrow \beta = \frac{\sqrt{2}}{\gamma} \Rightarrow \text{gilt.} \end{aligned}$$

$$\gamma \in \mathbb{Q}(\gamma) \Rightarrow \gamma^2 = 2 - \sqrt{2} \in \mathbb{Q}(\gamma)$$

$$\gamma^2, 2 \in \mathbb{Q}(\gamma) \Rightarrow \sqrt{2} \in \mathbb{Q}(\gamma)$$

$$\sqrt{2}, \gamma \in \mathbb{Q}(\gamma) \Rightarrow \beta = \frac{\sqrt{2}}{\gamma} \in \mathbb{Q}(\gamma)$$

$$\beta, \gamma \in \mathbb{Q}(\gamma) \Rightarrow -\beta, -\gamma \in \mathbb{Q}(\gamma)$$

$$\text{insgesamt: } N = \{\pm\beta, \pm\gamma\} \subseteq \mathbb{Q}(\gamma)$$

Bestimmung von $[\mathbb{L}:\mathbb{Q}] = [\mathbb{Q}(\gamma):\mathbb{Q}]$:

Das Pol. $f \in \mathbb{Q}[x]$ ist normiert und erfüllt $f(\gamma) = 0$, außerdem ist f nach dem Eisenstein-Kriterium (mit der Primzahl 2) irreduzibel über $\mathbb{Q}$.

$$\Rightarrow M_{\gamma, \mathbb{Q}} = f \Rightarrow [\mathbb{Q}(\gamma):\mathbb{Q}] = \deg(f) = 4.$$

(c) Zeigen Sie, dass $\mathbb{L}|\mathbb{Q}$ galois'sch ist

Da $\mathbb{L}$ Zerfällungskörper eines Polynoms über $\mathbb{Q}$ ist, ist die Erweiterung $\mathbb{L}|\mathbb{Q}$ normal, somit auch algebraisch. Wegen $\text{char}(\mathbb{Q}) = 0$ ist jede alg. Erw. von $\mathbb{Q}$ separabel, also auch $\mathbb{L}|\mathbb{Q}$. Insgesamt ist $\mathbb{L}|\mathbb{Q}$ damit galois'sch.

ist $g(\beta) = 0$,
 ommen, g ist
 $\text{grad}(g) = 2$
 β von g dann
 dann auf jeden
 mit ist $\mathbb{Q}(\beta)$

$\mathbb{Q}(x) \mid \mathbb{Q}$.
 $\mathbb{Q}(\beta) : \mathbb{Q}$
 Polynom g ist über
 mit Primz. 3). Zu-
 $g \in \mathbb{Q}[x]$ in $\mathbb{Q}$ -
 $\mathbb{Q}(\beta) : \mathbb{Q} = \text{grad}(g) = 2$
 5 $\nmid$ da $2 \nmid 3$.

H25T3 A4 Sei $K = \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3})$ und
 $\varepsilon = e^{2\pi i/3}$, außerdem $L = K(\varepsilon)$.

(a) Bestimmen Sie den Erweiterungs-
 $\text{grad}[K : \mathbb{Q}]$. (Wir bestimmen außer-
 dem $[L : \mathbb{Q}]$.)

Sei $\alpha = \sqrt[3]{3}$, $\beta = \sqrt{3}$. Das Polynom
 $f = x^3 - 3$ ist normiert, erfüllt $f(\alpha) = 0$
 und ist irreduzibel nach dem Eisenstein-
 Kriterium (für die Primz. 3). $\Rightarrow M_{\mathbb{Q}, \mathbb{Q}} = f$
 $\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad}(f) = 3$.

Es gilt $K = \mathbb{Q}(\alpha)(\beta)$, bestimme zu-
 nächst $[K : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)]$.

B. x
 insges

Bestimm

Das Pol

$f(x) =$

Kriterium

$\Rightarrow M_{\mathbb{Q}, \mathbb{Q}}$

(c) Zeig

Da L zu

ist, ist d

auch algeb

alg Erw

Insgesamt

Sei $g = x^2 - 3 \in \mathbb{Q}(\alpha)[x]$. Es ist $g(\beta) = 0$,
 und g ist normiert ^(*). Angenommen, g ist
 in $\mathbb{Q}(\alpha)$ reduzibel. Wegen $\text{grad}(g) = 2$
 liegen die Nullstellen $\pm \beta$ von g dann
 beide in $\mathbb{Q}(\alpha)$. Es gilt dann auf jeden
 Fall $\beta \in \mathbb{Q}(\alpha)$, und damit ist $\mathbb{Q}(\beta)$
 ein Zwischenkörper von $\mathbb{Q}(\alpha) \mid \mathbb{Q}$.

Gradformel $\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \mid [\mathbb{Q}(\beta) : \mathbb{Q}]$
 $= [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Das Polynom g ist über
 $\mathbb{Q}$ irreduzibel (Eisensteinkrit. mit Primz. 3). Zu-
 sammen mit (*) folgt wegen $g \in \mathbb{Q}[x]$ mit-
 gesamt $M_{\beta, \mathbb{Q}} = g$ und $[\mathbb{Q}(\beta) : \mathbb{Q}] = \text{grad}(g) = 2$
 $\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot 2 = 3 \nmid$ da $2 \nmid 3$.

H25T3A

$$\varepsilon = e^{2\pi i}$$

(a) Bestim-
 grad $[K$
 dem $[L:$

Sei $\alpha = \sqrt[3]{f}$

$$f = x^3 - 3$$

und ist un-
 krit. (Krit. (

$$\Rightarrow [\mathbb{Q}(\alpha) :$$

Es gilt K
 nächst $[K:$

$\mathbb{R}$, es

$\varepsilon =$

$\in (\frac{2\pi}{3})$

$(\frac{2\pi}{3}) \neq 0$

$\mathbb{K}[x]$, wsg.

$\neq [\mathbb{K}(\varepsilon) : \mathbb{K}]$

normal $\Rightarrow$

$2 \cdot 6 = 12$

nicht galoissch

(x) ist über $\mathbb{Q}$

also: g ist irreduzibel über $\mathbb{Q}(\kappa)$

$\Rightarrow \mu_{\mathbb{B}, \mathbb{Q}(\kappa)} = g \Rightarrow [\mathbb{K} : \mathbb{Q}(\kappa)] =$

$\text{grad}(g) = 2$ Gradformel $\Rightarrow$

$[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\kappa)] [\mathbb{Q}(\kappa) : \mathbb{Q}] =$

$2 \cdot 3 = 6$

Bestimmung von $L|\mathbb{Q}$:

Das Element ε ist eine primitive dritte Einheitswurzel, und somit ist $\mu_{\varepsilon, \mathbb{Q}}$ das dritte Kreisteilungspolynom $\Phi_3 = x^2 + x + 1$.

Insb. liegt Φ_3 auch in $\mathbb{K}[x]$, ist normiert und erfüllt $\Phi_3(\varepsilon) = 0$. Ang. Φ_3 ist in $\mathbb{K}[x]$ reduzibel.

Wegen $\text{grad } \Phi_3 = 2$ müsste dann ε in $\mathbb{K}$ liegen.

Sei

und

in $\mathbb{Q}$

lies

beid

Fall

ein $\mathbb{Z}$

Gradf

$= [\mathbb{Q}$

$\mathbb{Q}$ in

Summe

gesamt

$\Rightarrow [\mathbb{Q}$

stelle,
n, dann
ste f
llen. Jede
also in
 $\mathbb{E}$ gilt

$e^{2\pi i/3} - 3$
o $x' \in K$ gelten.
ano $x' \in \mathbb{R}$
 $e^{2\pi i/3} + i \sin(\frac{2\pi}{3})$
aber nicht reell. $\downarrow$

Wegen $\alpha, \beta \in \mathbb{R}$ gilt $K \subseteq \mathbb{R}$, es
wäre also $\varepsilon \in \mathbb{R}$, aber: $\varepsilon =$
 $e^{2\pi i/3} = \cos(\frac{2\pi}{3}) + i \sin(\frac{2\pi}{3})$
 $\Rightarrow \varepsilon \notin \mathbb{R}$ wegen $\sin(\frac{2\pi}{3}) \neq 0$.
(Es ist $\varepsilon = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.)

also: Φ_3 ist irreduzibel in $K[x]$, insg.

$$M_{\varepsilon, K} = \Phi_3 \Rightarrow [L:K] = [K(\varepsilon):K]$$

$$= \text{grad } \Phi_3 = 2 \quad \text{Gradformel} \Rightarrow$$

$$[L:\mathbb{Q}] = [L:K] \cdot [K:\mathbb{Q}] = 2 \cdot 6 = 12$$

(b) zeige: (1) $K|\mathbb{Q}$ ist nicht galois'sch

(2) $L|\mathbb{Q}$ ist galois'sch

bereits gezeigt: $f \in \mathbb{Q}(x)$ ist über $\mathbb{Q}$

also: g

$\Rightarrow M$

grad (g

$[K:\mathbb{Q}]$

$2 \cdot 3$

Bestimmen

Das Element

Einheitswurzel

dritte Kre

Insb. liegt

erfüllt Φ_3

Wegen grad

irreduzibel und hat in K eine Nullstelle, nämlich α . Wäre $K|\mathbb{Q}$ galoissch, dann auch normal, und folglich müsste f über K in Linearfaktoren zerfallen. Jede komplexe Nullstelle von f müsste also in K liegen. aber: Sei $\alpha' = \varepsilon\alpha$. Es gilt

$$f(\alpha') = (\varepsilon\alpha)^3 - 3 = \varepsilon^3\alpha^3 - 3 = e^{2\pi i} \cdot 3 - 3 = 1 \cdot 3 - 3 = 0 \quad \text{Es müsste also } \alpha' \in K \text{ gelten.}$$

aber: $\alpha, \beta \in \mathbb{R} \Rightarrow K \subseteq \mathbb{R}$, also wäre $\alpha' \in \mathbb{R}$

$$\text{Wegen } \alpha' = \alpha\varepsilon = \alpha \cdot e^{2\pi i/3} = \alpha \cdot \cos\left(\frac{2\pi}{3}\right) + i\alpha \sin\left(\frac{2\pi}{3}\right)$$

und $\operatorname{Im}(\alpha') = \alpha \sin\left(\frac{2\pi}{3}\right) \neq 0$ ist α' aber nicht reell. $\downarrow$

zu (2) z.z.g.: $L|\mathbb{Q}$ ist normal und separabel

- Die Elemente $\alpha, \beta, \varepsilon$ sind algebraisch über $\mathbb{Q}$ (als Nullstellen der Pol. f, g bzw. Φ_3 in $\mathbb{Q}[x]$). Wegen $L = \mathbb{Q}(\alpha, \beta, \varepsilon)$ ist $L|\mathbb{Q}$ also algebraisch. Wegen $\text{char}(\mathbb{Q}) = 0$ ist $L|\mathbb{Q}$ damit auch separabel.

Übung

- Um zu zeigen, dass $L|\mathbb{Q}$ normal ist, genügt es zu überprüfen, dass L Zerfällungskörper des Polynoms $h = fg$ über $\mathbb{Q}$ ist. Überprüfe: Die Nullstellenmenge von h in $\mathbb{C}$ ist $N = \{\alpha, \varepsilon\alpha, \beta, -\beta\}$. Der Zerf.körper ist also $\mathbb{Q}(N)$. Für den Nachweis, dass $\mathbb{Q}$ und $L = \mathbb{Q}(\alpha, \beta, \varepsilon)$ gleich sind, reicht es zu überprüfen: i) $N \subseteq L$ ii) $\{\alpha, \beta, \varepsilon\} \subseteq \mathbb{Q}(N)$

zu (1) $\alpha, \beta, \varepsilon \in L \Rightarrow \varepsilon\alpha, \varepsilon\alpha^2, -\beta \in L$, insge-
samt gilt also $N \subseteq L$

zu (2) $\alpha, \varepsilon\alpha, \beta \in N \Rightarrow \alpha, \varepsilon\alpha, \beta \in \mathbb{Q}(N)$

$\Rightarrow \varepsilon = \frac{\varepsilon\alpha}{\alpha} \in \mathbb{Q}(N)$, insg. $\{\alpha, \beta, \varepsilon\} \subseteq \mathbb{Q}(N)$