

F13T2A4 geg: $\alpha \in \mathbb{F}_5^{\text{alg}}$ mit $\alpha^4 = \bar{3}$

bereits gezeigt: $K \mid \mathbb{F}_5$ mit $K = \mathbb{F}_5(\alpha)$ ist eine
Galois-Erweiterung

noch zu erledigen:

- i) Bestimmung der Zwischenkörper
von $K \mid \mathbb{F}_5$ einschließlich Inklusionen
- ii) Anzahl der Elemente $\beta \in K$ mit $K = \mathbb{F}_5(\beta)$

zu i) Beh. $f = x^4 - \bar{3}$ ist das Minimal-
polynom von α über $\mathbb{F}_5$

klar: f ist normiert, $f(\alpha) = 0$

noch z. zgg: f ist irreduzibel in $\mathbb{F}_5[x]$

$f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{3}$, $f(\bar{2}) = \bar{3}$, $f(\bar{3}) = \bar{3}$, $f(\bar{4}) = \bar{3} \Rightarrow f$ hat in $\mathbb{F}_5$ keine Nullstelle. Allg. f ist dennoch reduzibel.

$\text{grad}(f) = 4 \nmid$ Zerlegung $f = gh$, wobei $g, h \in \mathbb{F}_5[x]$ normiert, irred. vom Grad 2 $f(x) = \bar{0} \Rightarrow g(x) = \bar{0}$ oder $h(x) = \bar{0}$, o. Bd A. $g(x) = \bar{0}$
 $g = \mu_{\alpha, \mathbb{F}_5}$ (da $g \in \mathbb{F}_5[x]$ normiert, irred. und $g(x) = \bar{0}$) $\Rightarrow (\mathbb{F}_5(\alpha) : \mathbb{F}_5) = \text{grad}(g) = 2$
 $\Rightarrow \mathbb{F}_5(\alpha) = \mathbb{F}_{25} \rightarrow \alpha \in \mathbb{F}_{25} \quad \alpha \notin \mathbb{F}_5$
 (da g irred., $\text{grad}(g) > 1$) $\Rightarrow \alpha \neq \bar{0} \Rightarrow \alpha \in \mathbb{F}_{25}^\times$

$\Rightarrow \text{ord}(\alpha) \mid 24$ (da $|\mathbb{F}_{25}^\times| = 24$)

aber: $\alpha^4 = \bar{3} \Rightarrow \alpha^8 = \bar{3}^2 = \bar{4} \neq \bar{1}$, $\alpha^{16} = \bar{4}^2 = \bar{1}$

$\Rightarrow \text{ord}(\alpha) = 16$ Lagrange $\Rightarrow 16 \mid 24$ $\nLeftarrow$ ($\Rightarrow$ Beh.)

Aus der Beh. folgt $[K : \mathbb{F}_5] = \text{grad}(f) = 4 \Rightarrow$

$K = \mathbb{F}_{5^4}$ Laut VL sind die Zwischenkörper von $\mathbb{F}_{5^4} / \mathbb{F}_5$ geg. durch $\mathbb{F}_{5^d}$ wobei $d \in \mathbb{N}$ die Teiler von 4 durchläuft, d.h. $d \in \{1, 2, 4\} \Rightarrow$ einzige Zwischenkorp. von $K / \mathbb{F}_5$ sind

$$\mathbb{F}_{5^1} = \mathbb{F}_5, \mathbb{F}_{5^2} = \mathbb{F}_{25}, \mathbb{F}_{5^4} = K$$

Lt. VL gilt für alle $m, n \in \mathbb{N}$ die Äquivalenz

$$m \mid n \Leftrightarrow \mathbb{F}_{5^m} \subseteq \mathbb{F}_{5^n} \quad \text{Es gilt also } \mathbb{F}_{5^1} \subseteq \mathbb{F}_{5^2}, \mathbb{F}_{5^2} \subseteq \mathbb{F}_{5^4}$$

$$F_{S1} = F_S, F_S = F_{S2}, F_{S4} = K$$

Lt. VI. gilt für alle $m, n \in \mathbb{N}$ die Äquivalenz

und $F_{S1} \subseteq F_{S4}$ und keine weiteren Inklusionen.

zu II) Die Anzahl beträgt 600 (Nachweis: Übung). $\square$

Def. Ist $L|K$ eine Galois-Erweiterung (also eine normale und separable Erweiterung), dann wird

$$\text{Gal}(L|K) = \text{Aut}_K(L) = \{ \sigma \in \text{Aut}(L) \mid \sigma(a) = a \text{ für alle } a \in K \}$$

die Galoisgruppe von $L|K$ genannt.
wichtige Eigenschaften der Galoisgruppe:

- Ist $L|K$ eine endliche Galois-Erweiterung, dann gilt $|\text{Gal}(L|K)| = [L:K]$.
- Fortsetzungssatz (für Galoisgruppen):

Ist L/K eine endl. Galoiserw.
 $f \in K[x]$ irreduzibel und sind $\alpha, \beta \in L$
mit $f(\alpha) = f(\beta) = 0$, dann existiert ein
 $\sigma \in \text{Gal}(L/K)$ mit $\sigma(\alpha) = \beta$

• Ist S ein Erzeugendensystem von L/K
(d.h. $L = K(S)$), dann ist jedes $\sigma \in \text{Gal}(L/K)$
durch $\sigma|_S$ bereits eindeutig festgelegt)

Bsp: $S = \{\sqrt{2}, \sqrt{3}\} \Rightarrow$ Jedes $\sigma \in \text{Gal}(L/K)$ ist
durch $\sigma(\sqrt{2}), \sigma(\sqrt{3})$ eindeutig bestimmt.

• Ist $g \in K[x]$, $\alpha \in L$ eine Nullstelle von g und
 $\sigma \in \text{Gal}(L/K)$, dann ist auch $\sigma(\alpha)$ eine Null-
stelle von g . (Bsp. Anwendung auf $g = x^2 - 2$
 $\rightarrow$ nur $\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}$ für $\sigma \in \text{Gal}(L/K)$ möglich)

F26T3A4 geg. $\zeta = e^{2\pi i/5}$

in (a) bereits gezeigt: $\alpha = \zeta + \zeta^4 \Rightarrow \text{Min. Pol.} = x^2 + x - 1$

(b) Begründen Sie, dass $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta)$ gilt, und
geben Sie die Elemente der Galoisgruppe von
 $\mathbb{Q}(\zeta) | \mathbb{Q}(\sqrt{5})$ an.

zu erledigen:

(1) Nachweis $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta)$

(2) Nachweis: $\mathbb{Q}(\zeta) | \mathbb{Q}(\sqrt{5})$ ist gal.

(3) Elemente von $\text{Gal}(\mathbb{Q}(\zeta) | \mathbb{Q}(\sqrt{5}))$

zu (1) Es gilt $\alpha = \zeta + \zeta^4 \in \mathbb{Q}(\zeta)$, somit

$\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$, außerdem: α Nullstelle von

$x^2 + x - 1 \xrightarrow{\text{p-q-Formel}} \alpha \in \left\{ -\frac{1}{2} \pm \frac{1}{2}\sqrt{5} \right\} \Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{5})$

Aus $\sqrt{5} \in \{ \pm(1+2\alpha) \}$ (wg. $\alpha = -\frac{1}{2} + \frac{1}{2}\sqrt{5}$ ~~und~~
 $\alpha + \frac{1}{2} = \frac{1}{2}\sqrt{5} \Rightarrow 2\alpha + 1 = \sqrt{5}$ und $\alpha = -\frac{1}{2} - \frac{1}{2}\sqrt{5} \Rightarrow$
 $\alpha + \frac{1}{2} = -\frac{1}{2}\sqrt{5} \Rightarrow -1 - 2\alpha = \sqrt{5}$) folgt andererseits
 $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\alpha)$, insgesamt $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(S)$

zu (2) Als Kreisteilungskörper ist $\mathbb{Q}(S) | \mathbb{Q}$ galois'sch,
 und weil $\mathbb{Q}(\sqrt{5})$ ein Zwischenkörper des Erzw. ist, ist
 auch $\mathbb{Q}(S) | \mathbb{Q}(\sqrt{5})$ galois'sch. (Achtung: L/K
 galois'sch, M Zwischenkörper $\nRightarrow$ M/K galois'sch
 im Allg.
 Nur L/M ist unter dieser Voraussetzung immer ga-
 lois'sch.)

zu (3) Lant VI gilt für jedes $n \in \mathbb{N}$ mit $n \geq 2$
 und $\zeta_n = e^{2\pi i/n}$ stets $[\mathbb{Q}(S) : \mathbb{Q}] = \varphi(n)$. $\Rightarrow$
 hier $[\mathbb{Q}(S) : \mathbb{Q}] = \varphi(5) = 4$ weil $5 \in \mathbb{Z} \setminus \{0, 1, 7\}$ und

quadratfrei ist, gilt $[Q(\sqrt{5}) : Q] = 2$

quadratisch $\Rightarrow 4 = [Q(S) : Q] = [Q(S) : Q(\sqrt{5})] \cdot [Q(\sqrt{5}) : Q] = [Q(S) : Q(\sqrt{5})] \cdot 2 \Rightarrow [Q(S) : Q(\sqrt{5})] = 2$

Also ist auch die Ordnung von $G = \text{Gal}(Q(S) | Q(\sqrt{5}))$ gleich 2. Eines der beiden Elemente von G ist $\text{id}_{Q(S)}$.

Weil das 5-te Kreisteilungspolynom Φ_5 irreduzibel und S, S^4 beides Nullstellen von Φ_5 sind, existiert auf Grund des Fortsetzungssatzes ein $\sigma \in \text{Gal}(Q(S) | Q)$ mit $\sigma(S) = S^4 \Rightarrow \sigma(S^4) = \sigma(S)^4 = (S^4)^4 = S^{16} = (S^5)^3 \cdot S = 1 \cdot S = S \Rightarrow \sigma(\alpha) = \sigma(S + S^4)$

$= \sigma(5) + \sigma(5^4) = 5^4 + 5 = \alpha \Rightarrow \sigma \in \text{Gal}(\mathbb{Q}(5) | \mathbb{Q}(\alpha))$
 $\Rightarrow \sigma \in \text{Gal}(\mathbb{Q}(5) | \mathbb{Q}(\sqrt{5}))$ Wegen $\sigma(5) \neq 5$ ist σ das
 zweite, von $\text{id}_{\mathbb{Q}(5)}$ verschiedene Element von G . Es
 gilt also $G = \{ \text{id}_{\mathbb{Q}(5)}, \sigma \}$ □

F26T1 A2 geg: $f = x^4 - 6x^2 - 3 \in \mathbb{Q}[x]$

in (a) gezeigt: Die komplexen Nullst. von f sind $\pm \alpha, \pm \beta$
 mit $\alpha = \sqrt{3+2\sqrt{3}}$ und $\beta = \sqrt{3-2\sqrt{3}}$, und f ist über $\mathbb{Q}$
 irreduzibel

in (b) gezeigt: $\alpha \in \mathbb{R}, \beta \notin \mathbb{R}, \mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$
 und $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3})$

(c) Zeigen Sie, dass $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}(\sqrt{3})$ galois'sch ist,
und bestimmen Sie die Struktur der Galoisgruppe.

Nach Teil (a) ist $N = \{\pm\alpha, \pm\beta\}$ die Menge der komplexen Nullstellen von f und $\mathbb{Q}(N)$ somit Zerfällungskörper von f über $\mathbb{Q}$. Offenbar gilt $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \beta)$ („ $\supseteq$ “ wegen $\{\alpha, \beta\} \subseteq N$, „ $\supseteq$ “ da mit $\alpha, \beta \in \mathbb{Q}(\alpha, \beta)$ auch $-\alpha, -\beta \in \mathbb{Q}(\alpha, \beta)$ gilt). Als Zerf. körp. von f über $\mathbb{Q}$ ist $\mathbb{Q}(\alpha, \beta)$ normal über $\mathbb{Q}$, damit n. b. algebraisch, wegen $\text{char}(\mathbb{Q}) = 0$ auch separabel, insgesamt also galois'sch. Weil $\mathbb{Q}(\sqrt{3})$ wegen $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$ ein Zwischenkörper von $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}$ ist, ist auch $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}(\sqrt{3})$ eine Galois-Erweiterung.

Bestimmung des Struktur von $G = \text{Gal}(\mathbb{Q}(\alpha, \beta) | \mathbb{Q}(\sqrt{3}))$:

$$\text{Gradformel} \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})]$$

Aus Teil (a) ist bekannt, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ und $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Gradformel $\Rightarrow 4 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] \cdot 2$

$$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = \frac{4}{2} = 2 \quad \text{Wegen } \sqrt{3} \in \mathbb{Q}(\alpha)$$

liegt das Polynom $h = x^2 - (3 - 2\sqrt{3})$ in $\mathbb{Q}(\alpha)[x]$ und $h(\beta) = \beta^2 - (3 - 2\sqrt{3}) = (3 - 2\sqrt{3}) - (3 - 2\sqrt{3}) = 0$

$$\Rightarrow M_{\beta, \mathbb{Q}(\alpha)} \text{ teilt } h \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] =$$

$$\text{grad } \mu_{\beta, \mathbb{Q}(x)} \leq \text{grad}(h) = 2 \Rightarrow$$

$$[\mathbb{Q}(x, \beta) : \mathbb{Q}(x)] \in \{1, 2\} \quad \text{Ang. } [\mathbb{Q}(x, \beta) : \mathbb{Q}(x)] = 1 \Rightarrow \mathbb{Q}(x, \beta) = \mathbb{Q}(x) \Rightarrow \beta \in \mathbb{Q}(x)$$

$$\mathbb{Q}(x) \subseteq \mathbb{R} \Rightarrow \beta \in \mathbb{R} \quad \downarrow$$

$$\Rightarrow [\mathbb{Q}(x, \beta) : \mathbb{Q}(\sqrt{\beta})] = 2 \cdot 2 = 4$$

$\Rightarrow G$ hat Ordnung 4 Als Gruppe von Primzahl quadrat ordn. ist G abelsch, als endliche abelsche Gruppe außerdem isomorph zu einem Prod zyklische Gruppen $\Rightarrow$

$$G \cong \mathbb{Z}/4\mathbb{Z} \text{ oder } G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$