H24 T3 A5 Sei $\zeta_{16} = e^{\frac{2\pi i}{16}} = e^{\frac{\pi i}{8}}$.

In (a) gezeigt: Die Erweiterung $\mathbb{Q}(\zeta_{16}) \mid \mathbb{Q}(i)$ ist galois'sch vom Grad 4.

(b) Bestimmen Sie das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$.

Es gilt $\zeta_{16}^4 = (e^{\pi i/8})^4 = e^{\pi i/2} = i$.

$\Rightarrow \zeta_{16}$ ist Nullstelle von $f = x^4 - i$, und $f \in \mathbb{Q}(i)[x]$. $\Rightarrow \mu_{\zeta_{16}, \mathbb{Q}(i)}$ teilt f

Aus dem Ergebnis von Teil (a) folgt

Aus dem Ergebnis von Teil (a) folgt

grad $M_{\zeta_{16}, \mathbb{Q}(i)} = [\mathbb{Q}(i)(\zeta_{16}) : \mathbb{Q}(i)] = [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] = 4 = \text{grad}(f)$. Da $M_{\zeta_{16}, \mathbb{Q}(i)}$ und f beide normiert sind und $M_{\zeta_{16}, \mathbb{Q}(i)} \mid f$ gilt, folgt daraus $M_{\zeta_{16}, \mathbb{Q}(i)} = f = x^4 - i$.

$\zeta_{16}^4 = i$

(c) Entscheiden Sie, ob $G = \text{Gal}(\mathbb{Q}(\zeta_{16}) \mid \mathbb{Q}(i))$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $(\mathbb{Z}/2\mathbb{Z})^2$ ist (mit Begründung).

Sei $\tilde{G} = \text{Gal}(\mathbb{Q}(\zeta_{16}) \mid \mathbb{Q})$. Laut Vorlesung existiert ein Isom. $\phi : (\mathbb{Z}/16\mathbb{Z})^\times \to \tilde{G}$

$\mathbb{Q}(i)$

geg durch $a+16\mathbb{Z} \mapsto \sigma_a$ für alle $a \in \mathbb{Z}$ mit $ggT(a,16)=1$, wobei das Element $\sigma_a \in \tilde{G}$ jeweils durch $\sigma_a(\zeta_{16}) = \zeta_{16}^a$ gegeben ist. $\left(\Rightarrow \tilde{G} = \{\sigma_1 = id_{\mathbb{Q}(\zeta_{16})}, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}\}\right)$

Die Gruppe G ist nach Def. die Untergruppe von $\tilde{G}$ definiert durch $\{\sigma \in \tilde{G} \mid \sigma(\alpha) = \alpha \ \forall \alpha \in \mathbb{Q}(i)\}$. Für jedes $a \in \mathbb{Z}$ mit $ggT(a,16)=1$ gilt die Äquivalenz $\sigma_a \in G \Leftrightarrow \sigma_a(\alpha) = \alpha$ für alle $\alpha \in \mathbb{Q}(i)$

$\Leftrightarrow \sigma_a(i) = i \Leftrightarrow \sigma_a(\zeta_{16}^4) = \zeta_{16}^4 \Leftrightarrow \sigma_a(\zeta_{16})^4 = \zeta_{16}^4$

($\Leftarrow$ da $\mathbb{Q}(i)$ über $\mathbb{Q}$ durch i erzeugt ist)

$\Leftrightarrow (\zeta_{16}^a)^4 = \zeta_{16}^4 \Leftrightarrow \zeta_{16}^{4a} = \zeta_{16}^4 \Leftrightarrow \zeta_{16}^{4a-4} = 1$ ($\Leftarrow$ $ord(\zeta_{16}) = 16$ in $\mathbb{C}^\times$)

$16 \mid 4a-4 \Leftrightarrow 4 \mid (a-1) \Leftrightarrow a \equiv 1 \bmod 4$

$\Leftrightarrow (\zeta_{16}^9)^4 = \zeta_{16}^4$ durch ζ_{16}^4 erzeugt ist $\Leftrightarrow \zeta_{16}^{4a} = \zeta_{16}^4 \Leftrightarrow \zeta_{16}^{4a-4} = 1 \Leftrightarrow$ $\operatorname{ord}(\zeta_{16}) = 16$ in $\mathbb{C}^\times$

$16 \mid 4a-4 \Leftrightarrow 4 \mid (a-1) \Leftrightarrow a \equiv 1 \bmod 4$

Daraus folgt $G = \{\sigma_1, \sigma_5, \sigma_9, \sigma_{13}\}$. Unter dem Isom. ϕ entspricht das der Untergr. $U = \{\bar{1}, \bar{5}, \bar{9}, \overline{13}\}$ von $(\mathbb{Z}/16\mathbb{Z})^\times$.
Es gilt $\bar{5}^2 = \overline{25} = \bar{9} \neq \bar{1}$. Wegen $|U| = 4$ gilt andererseits $\bar{5}^4 = \bar{1}$, $\bar{5}^2 \neq \bar{1}$, $\bar{5}^4 = \bar{1} \Rightarrow \operatorname{ord}(\bar{5}) = 4$. Wegen $|U| = 4$ und $\bar{5} \in U$, $\operatorname{ord}(\bar{5}) = 4$ ist U eine zyklische Gruppe der Ordnung 4, also $U \cong \mathbb{Z}/4\mathbb{Z}$.
Es folgt $G = \phi(U) \cong U \cong \mathbb{Z}/4\mathbb{Z}$. □

Übung: (a) Zeigen Sie, dass $\mathbb{Q}(\sqrt{2})$ ein Zwischenkörper von $\mathbb{Q}(\zeta_{16}) | \mathbb{Q}$ ist. (Hinweis: $\zeta_{16}^2 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$)

(b) Entscheiden Sie, ob $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}) | \mathbb{Q}(\sqrt{2}))$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $(\mathbb{Z}/2\mathbb{Z})^2$ ist.

F23T3A4 Sei $\zeta \in \mathbb{C}$ eine primitive 7-te Einheitswurzel, außerdem $a = \zeta + \zeta^{-1}$ und $b = \zeta + \zeta^2 + \zeta^4$.

(a)* Geben Sie einen konkreten Isomorphismus $(\mathbb{Z}/7\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$, und ebenso einen Isom. $\mathbb{Z}/6\mathbb{Z} \to \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$

Laut Vl existiert für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,7) = 1$ ein eindeutig bestimmtes Element σ_a der Gruppe $G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ mit $\sigma_a(\zeta) = \zeta^a$. Daher gilt $\sigma_a = \sigma_b$ für $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,7) = \mathrm{ggT}(b,7) = 1$

genau dann, wenn $a \equiv b \bmod 7$ gilt.

Daraus folgt $G = \{\sigma_1 = \mathrm{id}_{\mathbb{Q}(\zeta)}, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$. Desweiteren existiert ein Isom. ϕ: $(\mathbb{Z}/7\mathbb{Z})^\times \to G$ mit $\phi(a+7\mathbb{Z}) = \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,7) = 1$. Insb. gilt also $\phi_a(a+7\mathbb{Z}) = \sigma_a$ für $1 \le a \le 6$.

In $(\mathbb{Z}/7\mathbb{Z})^\times$ gilt $\mathrm{ord}(\bar{3}) = 6$ wegen $\bar{3}^3 = \bar{27} = \bar{6} \neq \bar{1}$, $\bar{3}^2 = \bar{9} = \bar{2} \neq \bar{1}$ und $|(\mathbb{Z}/7\mathbb{Z})^\times| = \varphi(7) = 6$. Aus $\mathrm{ord}(\bar{3}) = 6 = |(\mathbb{Z}/7\mathbb{Z})^\times|$ folgt, dass $\alpha : \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^\times$, $k+6\mathbb{Z} \mapsto \bar{3}^k$ ein Isom. gegeben ist. Es gilt $\alpha(\bar{0}) = \bar{3}^0 = \bar{1}$, $\alpha(\bar{1}) = \bar{3}^1 = \bar{3}$, $\alpha(\bar{2}) = \bar{3}^2 = \bar{9} = \bar{2}$, und ebenso erhält man $\alpha(\bar{3}) = \bar{6}$, $\alpha(\bar{4}) = \bar{4}$, $\alpha(\bar{5}) = \bar{5}$

(und $\alpha(\bar{6}) = \bar{1}$). Es ist dann $\phi \circ \alpha$ ein Isom. $\mathbb{Z}/6\mathbb{Z} \to G$, gegeben durch $\bar{0} \mapsto \mathrm{id}_{\mathbb{Q}(\zeta)|\mathbb{Q}}$ $= \sigma_1$, $\bar{1} \mapsto \sigma_3$, $\bar{2} \mapsto \sigma_2$, $\bar{3} \mapsto \sigma_6$, $\bar{4} \mapsto \sigma_4$, $\bar{5} \mapsto \sigma_5$

(b) Zeigen Sie, dass $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galois-Erweiterungen sind, und bestimmen Sie die Galoisgruppen bis auf Isomorphie.

Wegen $G \cong \mathbb{Z}/6\mathbb{Z}$ ist G zyklisch, damit auch abelsch. Jede Untergruppe von G ist somit ein Normalteiler von G, insb. auch die Untergruppen $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(a))$ und $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(b))$ von G. Laut Galoistheorie folgt daraus, dass die Erweiterungen $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galoissch sind.

imitive

$= \zeta + \zeta^{-1}$

Isomorphis-

$\mathbb{Q})$, und

$(\mathbb{Q}(\zeta)|\mathbb{Q})$

$a \in \mathbb{Z}$ mit

bestimmtes

$(\mathbb{Q}(\zeta)|\mathbb{Q})$

$\sigma_a = \sigma_b$

$= ggT(6,7) = 1$

Laut Galoistheorie erhält man durch $\Psi : Gal(\mathbb{Q}(\zeta)|\mathbb{Q}) \to Gal(\mathbb{Q}(a)|\mathbb{Q})$, $\sigma \mapsto \sigma|_{\mathbb{Q}(a)}$ einen surjektiven Hom. (mit $Gal(\mathbb{Q}(\zeta)|\mathbb{Q}(a))$ als Kern, so dass $G/Gal(\mathbb{Q}(\zeta)|\mathbb{Q}(a)) \cong Gal(\mathbb{Q}(a)|\mathbb{Q})$ lt. Homomorphiesatz gilt).

Da nach Teil (a) $(\mathbb{Z}/7\mathbb{Z})^\times = \langle \bar{3} \rangle$ gilt, ist $\phi(\bar{3}) = \sigma_3$ ein Erzeuger von G, und auf Grund der Surjektivität von Ψ somit $\Psi(\sigma_3) = \sigma_3|_{\mathbb{Q}(a)}$ somit ein Erzeuger von $Gal(\mathbb{Q}(a)|\mathbb{Q})$; insb. ist die Gruppe zyklisch.

Es gilt $\sigma_3(a) = \sigma_3(\zeta + \zeta^{-1}) = \sigma_3(\zeta) + \sigma_3(\zeta)^{-1} = \zeta^3 + (\zeta^3)^{-1} = \zeta^3 + \zeta^4$ und $\sigma_3^2(a) = \sigma_3(\zeta^3 + \zeta^4) = \sigma_3(\zeta)^3 + \sigma_3(\zeta)^4$

$(\zeta^3)^3 + (\zeta^3)^4 = \zeta^9 + \zeta^{12} = \zeta^2 + \zeta^5$

$\sigma_3^3(a) = \sigma_3(\sigma_3^2(a)) = \sigma_3(\zeta^2+\zeta^5) = \sigma_3(\zeta)^2 + \sigma_3(\zeta)^5$

$= (\zeta^3)^2 + (\zeta^3)^5 = \zeta^6 + \zeta^{15} = \zeta^{-1} + \zeta = a$ Aus $\sigma_3^3(a) = a$

$\zeta^7 = 1$

folgt $\sigma_3^3|_{\mathbb{Q}(a)} = id_{\mathbb{Q}(a)} \Rightarrow ord(\sigma_3|_{\mathbb{Q}(a)}) \mid 3 \Rightarrow$

$ord(\sigma_3|_{\mathbb{Q}(a)}) \in \{1,3\}$ Ang. $ord(\sigma_3|_{\mathbb{Q}(a)}) = 1 \Rightarrow \sigma_3|_{\mathbb{Q}(a)}$

$= id_{\mathbb{Q}(a)} \Rightarrow \sigma_3(a) = a \overset{s.o.}{\Rightarrow} \zeta^3 + \zeta^4 = \zeta + \zeta^{-1}$ aber:

Wegen $[\mathbb{Q}(\zeta):\mathbb{Q}] = 6$ ist $1, \zeta, \ldots, \zeta^5$ eine Basis von $\mathbb{Q}(\zeta)$ als $\mathbb{Q}$-Vektorraum, d.h. jedes Element hat eine eind. Darstellung als Linearkomb. dieser Elemente über $\mathbb{Q}$. $\Phi_7(\zeta) = 0 \Rightarrow$

$\zeta^6 + \ldots + \zeta + 1 = 0 \Rightarrow \zeta^6 = -1 - \zeta \ldots - \zeta^5 \Rightarrow$

$\zeta + \zeta^{-1} = \zeta + \zeta^6 = \zeta + (-1 - \zeta \dots - \zeta^5) =$

$-1 - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5 \neq \zeta^3 + \zeta^4$ also:

$\operatorname{ord}(\sigma_3 | \mathbb{Q}(a)) = 3 \Rightarrow \operatorname{Gal}(\mathbb{Q}(a) | \mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

zum Isomorphietyp von $\operatorname{Gal}(\mathbb{Q}(G) | \mathbb{Q})$:

$\sigma_3(G) = \sigma_3(\zeta + \zeta^2 + \zeta^4) = \sigma_3(\zeta) + \sigma_3(\zeta)^2 + \sigma_3(\zeta)^4 =$

$\zeta^3 + (\zeta^3)^2 + (\zeta^3)^4 = \zeta^3 + \zeta^6 + \zeta^{12} = \zeta^3 + \zeta^5 + \zeta^6$

$\sigma_3^2(G) = \sigma_3(\sigma_3(G)) = \sigma_3(\zeta^3 + \zeta^5 + \zeta^6) =$ ($\zeta^7 = 1$)

$\sigma_3(\zeta)^3 + \sigma_3(\zeta)^5 + \sigma_3(\zeta)^6 = (\zeta^3)^3 + (\zeta^3)^5 + (\zeta^3)^6$

$= \zeta^9 + \zeta^{15} + \zeta^{18} = \zeta^2 + \zeta + \zeta^4 = G$ Wie oben folgt

daraus $\operatorname{ord}(\sigma_3 | \mathbb{Q}(G)) \in \{1, 2\}$ Um Ordnung 1 auszuschlie-

Bem. überprüfen wir $\sigma_3(b) \neq b$, also $\zeta^3+\zeta^5+\zeta^6 \neq \zeta+\zeta^2+\zeta^4$ ist. Es ist $\zeta^3+\zeta^5+\zeta^6 = \zeta^3+\zeta^5+(-1-\zeta-\zeta^2-\zeta^3-\zeta^4) = -1-\zeta-\zeta^2-\zeta^4 \neq \zeta+\zeta^2+\zeta^4$, wiederum auf Grund der Eindeutigkeit der Darst. als Linearkombination.
also: $\operatorname{ord}(\sigma_3|_{\mathbb{Q}(b)}) = 2$. Wie beim Körper $\mathbb{Q}(a)$ folgt daraus $\mathrm{Gal}(\mathbb{Q}(b)|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

(c) Bestimmen Sie das Minimalpolynom von b über $\mathbb{Q}$.

Da $\mathbb{Q}(b)|\mathbb{Q}$ eine Galois-Erweiterung ist, gilt $\operatorname{grad} \mu_{b,\mathbb{Q}} = [\mathbb{Q}(b):\mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(b)|\mathbb{Q})| = |\mathbb{Z}/2\mathbb{Z}| = 2 \Rightarrow \exists u,v \in \mathbb{Q}$ mit $\mu_{b,\mathbb{Q}} = x^2+ux+v$

$M_{b,Q}(b) = 0 \Rightarrow b^2 + ub + v = 0 \rightarrow$

$(\zeta + \zeta^2 + \zeta^4)^2 + u \cdot (\zeta + \zeta^2 + \zeta^4) + v = 0 \Rightarrow$

$\zeta^2 + \zeta^4 + \zeta^8 + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 =$

$-u(\zeta + \zeta^2 + \zeta^4) - v = (-v) + (-u)\zeta + (-u)\zeta^2 + (-u)\zeta^4$

Die linke Seite der Gleichung ist gleich

$\zeta^2 + \zeta^4 + \zeta + 2\zeta^3 + 2\zeta^5 + 2(-1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5)$

$= -2 - \zeta - \zeta^2 - \zeta^4$ Die Eindeutigkeit der Darst. als Linearkombination liefert $-v = -2$, $-u = -1 \Rightarrow$

$u = 1$, $v = 2 \Rightarrow M_{b,Q} = x^2 + x + 2$