H21T1A5 Übung: F21T2A4

Sei K ein Teilkörper von $\mathbb{C}$ derart, dass $K|\mathbb{Q}$ galois'sch vom Grad 2021 ist.

(a) Zeigen Sie, dass Zwischenkörper L_1, L_2 von $K|\mathbb{Q}$ mit $[L_1 : \mathbb{Q}] = 43$ und $[L_2 : \mathbb{Q}] = 47$ existieren, die beide galois'sch über $\mathbb{Q}$ sind.

Sei $G = \mathrm{Gal}(K|\mathbb{Q})$. Da $K|\mathbb{Q}$ galois'sch ist, gilt $|G| = [K : \mathbb{Q}] = 2021 = 43 \cdot 47$.

Für jede Primzahl p sei ν_p die Anzahl der

p-Sylowgp. von G. 3. Sylowsatz $\Rightarrow \nu_{47} \mid \frac{2021}{47}$

$\Rightarrow \nu_{47} \mid 43$ (43 Primz) $\Rightarrow \nu_{47} \in \{1, 43\}$, außerdem

$\nu_{47} \equiv 1 \bmod 47$ $\quad 43 \not\equiv 1 \bmod 47 \Rightarrow \nu_{47} = 1$

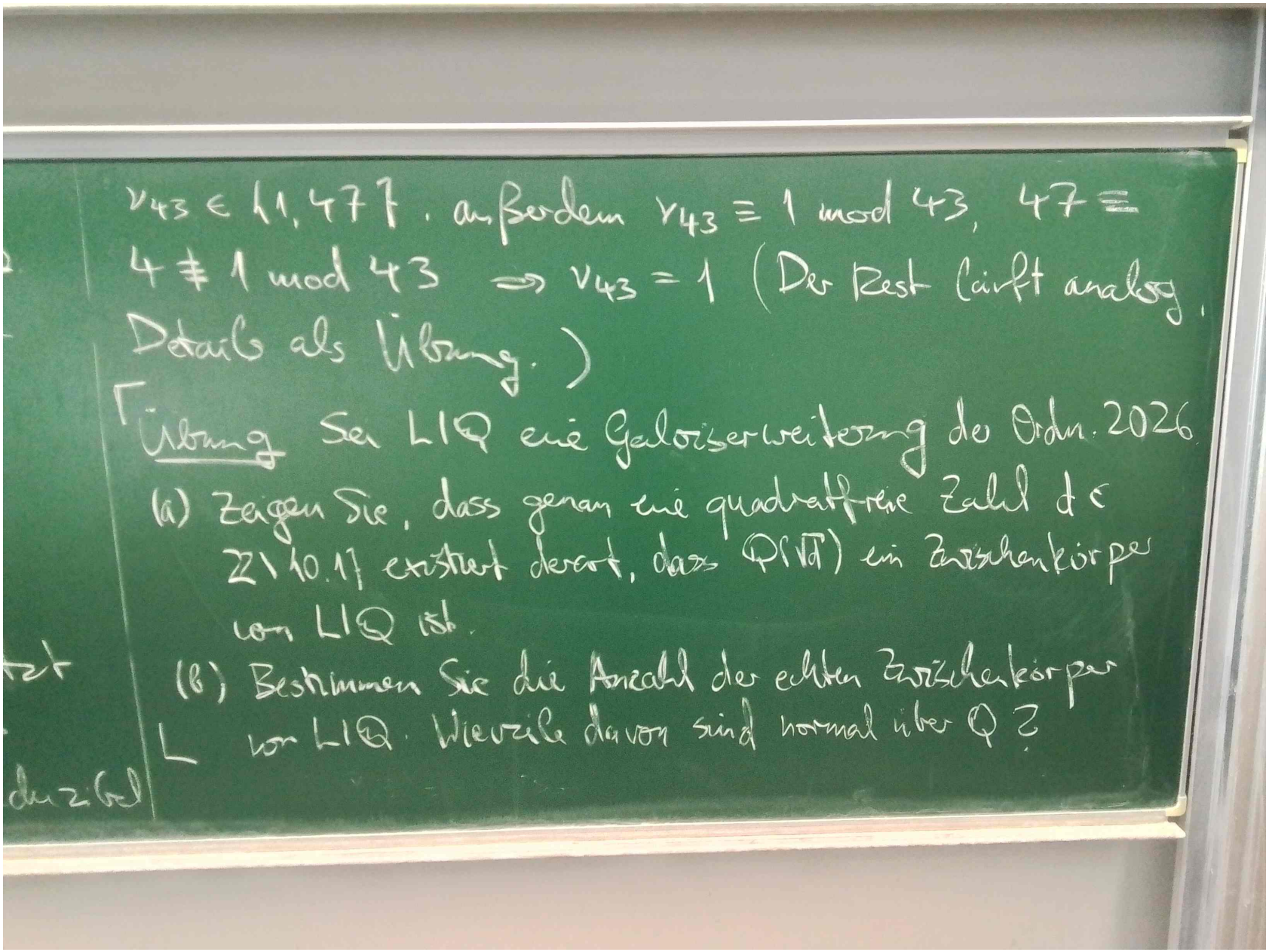
Sei N_1 die einzige 47-Sylowgruppe. 2. Sylowsatz,

$\nu_{47} = 1 \Rightarrow N_1 \trianglelefteq G$ $\quad$ Sei $L_1 = K^{N_1}$.

Laut Galoistheorie folgt aus $N_1 \trianglelefteq G$, dass $L_1 | \mathbb{Q}$ galois'sch ist. Außerdem gilt H. Galoistheorie

$[L_1 : \mathbb{Q}] = (G : N_1) = \frac{2021}{47} = 43$.

Für $p = 43$ liefert der 3. Sylowsatz $\nu_{43} \mid 47 \Rightarrow$ (47 Primzahl)



Korrekturhinweis auf der nächsten Seite

Statt „Galois-Erweiterung der Ordnung 2026“ muss es „Galois-Erweiterung vom Grad 2026“ oder „Galois-Erweiterung mit einer Galoisgruppe der Ordnung 2026“ heißen. Teil (b) ist keine gut gestellte Aufgabe, weil das Ergebnis vom Isomorphietyp der Galoisgruppe abhängt.

Es gilt $2026 = 2 \cdot 1013$, und 1013 ist eine Primzahl. In der Vorlesung wurde mit Hilfe der Sylowsätze gezeigt, dass jede Gruppe der Ordnung $2p$ mit einer ungeraden Primzahl p entweder isomorph zur zyklischen Gruppe $\mathbb{Z}/2p\mathbb{Z}$ oder zur Diedergruppe D_p ist.

Ist nun $G = \mathrm{Gal}(L|\mathbb{Q})$ und $G \cong \mathbb{Z}/2026\mathbb{Z}$, dann hat G genau vier Untergruppen, von Ordnung 1, 2, 1013 und 2026. Mit der Galoistheorie kann man daraus schließen, dass es in $L|\mathbb{Q}$ zwei echte Zwischenkörper gibt, die beide normal über $\mathbb{Q}$ sind (weil jede Untergruppe einer abelschen Gruppe ein Normalteiler ist).

Im Fall $G \cong D_{1013}$ gibt es genau eine Untergruppe der Ordnung 1013 (diese entspricht der Untergruppe der „Drehungen“ in D_{1013}) und 1013 Untergruppen der Ordnung 2 (entsprechend den 1013 Spiegelungen in D_{1013}). Die Untergruppe der Ordnung 1013 ist als Untergruppe vom Index 2 ein Normalteiler von G.

Die Untergruppen der Ordnung 2 sind genau die 2-Sylowgruppen von G, und weil es mehr als eine gibt, kann keine von ihnen ein Normalteiler von G sein. Mit der Galoistheorie erhält man das Ergebnis, dass $L|\mathbb{Q}$ genau 1014 echte Zwischenkörper besitzt, von denen nur einer normal über $\mathbb{Q}$ ist, nämlich der einzige Zwischenkörper vom Grad 2 über $\mathbb{Q}$.

(b) Sei $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$ und $f = \mu_{\alpha,\mathbb{Q}}$.
Zeigen Sie, dass f über $\mathbb{R}$ in Linearfaktoren zerfällt.

Wegen $f = \text{grad } \mu_{\alpha,\mathbb{Q}}$ gilt $\text{grad } f = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 2021$.

Weil der Grad von f ungerade ist, besitzt f (mindestens) eine reelle Nullstelle β.

Weil $K|\mathbb{Q}$ normal und f über $\mathbb{Q}$ irreduzibel

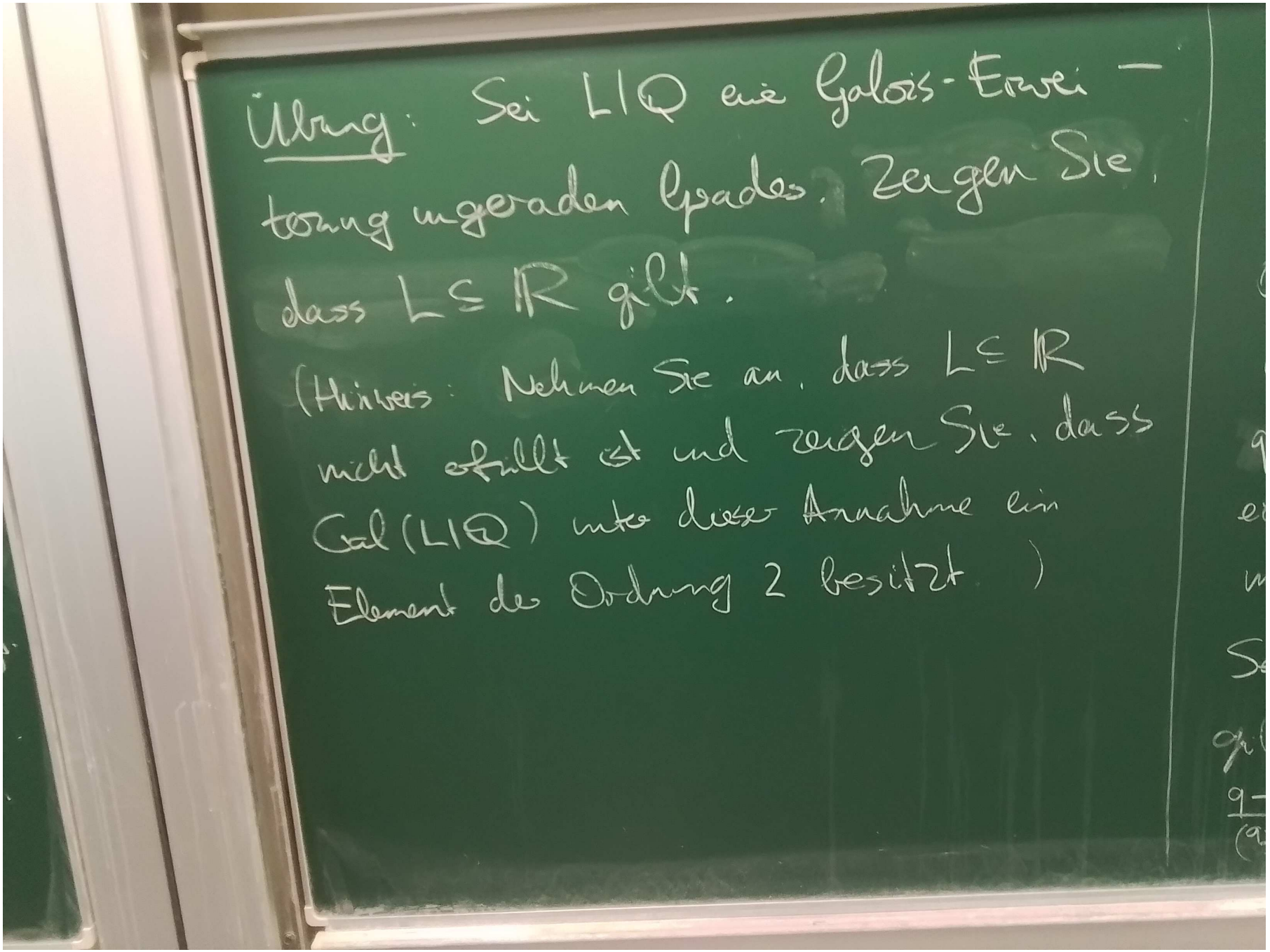
ist und f in K eine Nullstelle besitzt, zerfällt f über $\mathbb{Q}(\alpha)$ in Linearfaktoren.

$\longrightarrow \beta \in \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\beta)$ ist Zwischenkörper von $\mathbb{Q}(\alpha)|\mathbb{Q}$ Da β Nullstelle von f und f irreduzibel über $\mathbb{Q}$ ist, gilt $\mu_{\beta,\mathbb{Q}} = f$ und somit $[\mathbb{Q}(\beta):\mathbb{Q}] = \operatorname{grad}(f)$ $= 2021$ Gradformel $\Rightarrow 2021 =$

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

$[\mathbb{Q}(\alpha):\mathbb{Q}(\beta)] \cdot 2021 \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}(\beta)] =$

$1 \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) \Rightarrow f$ zerfällt über $\mathbb{Q}(\beta)$ in Linearfaktoren, wegen $\mathbb{Q}(\beta) \subseteq \mathbb{R}$ somit erst recht über $\mathbb{R}$. □


Übung: Sei L|Q eine Galois-Erweiterung ungeraden Grades. Zeigen Sie, dass L ⊆ ℝ gilt.
(Hinweis: Nehmen Sie an, dass L ⊆ ℝ nicht erfüllt ist und zeigen Sie, dass Gal(L|Q) unter dieser Annahme ein Element der Ordnung 2 besitzt.)

esitzt,
en.
hem-
telle
gilt
grad(f)
=
Q] =
Q(β)] =
über Q(β)
omit erst
□

F25T2A2

bereits erledigt: Ist p eine Primzahl und q ein Primteiler von $2^p - 1$, dann folgt $q \equiv 1 \bmod p$.

(b) Zeigen Sie, dass für jede Primzahl p eine Galois-Erweiterung $K_p | \mathbb{Q}$ mit $\mathrm{Gal}(K_p|\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$ existiert.

(Hinweis: Betrachten Sie Zwischenkörper geeigneter Kreisteilungserweiterungen.)

Sei p eine Primzahl und q ein Primteiler von $2^p - 1$. s.o. $\rightarrow q \equiv 1 \bmod p \Rightarrow p | (q-1)$

Sei $\zeta_q = e^{2\pi i/q}$, laut Vorlesung ist $\mathbb{Q}(\zeta_q)|\mathbb{Q}$

galois'sch mit $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ isomorph zu $(\mathbb{Z}/q\mathbb{Z})^\times$.
Da q eine Primzahl ist, ist $(\mathbb{Z}/q\mathbb{Z})^\times$ und damit auch
$\mathrm{Gal}(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ isomorph zu $\mathbb{Z}/(q-1)\mathbb{Z}$, d.h. zyklisch von
Ordnung $q-1$. Da die Galoisgruppe zyklisch
ist, besitzt sie zu jedem Teiler $d \in \mathbb{N}$ von
$q-1$ eine Untergruppe der Ordn. d. Insb.
existiert eine Untergr. $U \leq \mathrm{Gal}(\mathbb{Q}(\zeta_q)|\mathbb{Q})$
mit $|U| = \frac{p-1}{q}$ $\left(q|(p-1) \Rightarrow \frac{p-1}{q} \in \mathbb{N}\right)$
Sei $K_p = \mathbb{Q}(\zeta_q)^U$. Laut Galoistheorie
gilt $[K_p : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\zeta_q)|\mathbb{Q}) : U| =$
$\frac{q-1}{\left(\frac{q-1}{p}\right)} = p$. Da $(\mathbb{Z}/q\mathbb{Z})^\times$ und $\mathrm{Gal}(\mathbb{Q}(\zeta_q)|\mathbb{Q})$

abelsch sind, ist H Normalteiler von $\mathrm{Gal}(\mathbb{Q}(\zeta_q)|\mathbb{Q})$.
Daraus folgt, dass $K_p|\mathbb{Q}$ galoisch ist. $\Rightarrow$
$|\mathrm{Gal}(K_p|\mathbb{Q})| = [K_p : \mathbb{Q}] = p$. Weil p eine Primzahl ist, folgt $\mathrm{Gal}(K_p|\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$. □

F1ST3A5 Sei p eine Primzahl, $n \in \mathbb{N}$ und
$E|K$ eine Galois-Erweiterung vom Grad p^n mit zykl. Galoisgr.
Sei F ein Zwischenkörper von $E|K$ mit $[F:K] = p^{n-1}$.
Zeigen Sie, dass $E = K(\alpha)$ für jedes $\alpha \in E \setminus F$ gilt.

Sei $G = \mathrm{Gal}(E|K)$. $E|K$ galoisch $\Rightarrow$
$|G| = [E:K] = p^n$, d.h. G ist zyklisch von

Ordnung p^n. Sei $U = \mathrm{Gal}(E|F)$. Dies ist eine Untergruppe von G. Galoistheorie $\Rightarrow$

$(G:U) = [F:K] = p^{n-1} \Rightarrow |U| = \frac{|G|}{(G:U)} = \frac{p^n}{p^{n-1}} = p$.

Sei $\alpha \in E \setminus F$ und $V = \mathrm{Gal}(E|K(\alpha))$. $\alpha \notin F$

$\Rightarrow K(\alpha) \nsubseteq F$ Weil die Zuordnung von Untergr. zu Zwischenkörpern antiton ist, folgt daraus $V \neq U$.

Es genügt zu zeigen, dass $\boxed{V = \{\mathrm{id}_E\}}$ gilt, denn daraus folgt $E^V = E^{\{\mathrm{id}_E\}} = E$, und weil die Zuordnungen $M \mapsto \mathrm{Gal}(E|M)$, $U_1 \mapsto E^{U_1}$ zwischen

Umkehrfkt. von G und Zwischenkörpern von $E|K$ zueinander invers sind, gilt $EV = K(\alpha)$, d.h. wir erhalten dann $K(\alpha) = E$.

Weil G zyklisch von Ordnung n ist, gibt es für jedes $m \in \{0, \dots, n\}$ eine eind. bestimmte Untergr. U_m von Ordnung p^m, und keine weiteren. Außerdem gilt für alle $l, m \in \{0, \dots, n\}$ die Äquivalenz $U_l \subseteq U_m \Leftrightarrow l \leq m$.

$|U| = p \Rightarrow U = U_1$ Sei $m \in \{0, \dots, n\}$ mit $V = U_m$. $U_m = V \neq U = U_1 \Rightarrow \neg(m \geq 1)$

$\Rightarrow m = 0 \Rightarrow V = V_0 = \ker \mathrm{id}_E = 7$ □

Übung: H12T2A4

H24T3A5 Sei $\zeta_{16} = e^{2\pi i/16}$

(a) Zeigen Sie, dass $\mathbb{Q}(\zeta_{16}) | \mathbb{Q}(i)$ galoissch vom Grad 4 ist.

Laut Vl. ist $\mathbb{Q}(\zeta_{16}) | \mathbb{Q}$ galoissch, mit

$|\mathrm{Gal}(\mathbb{Q}(\zeta_{16}) | \mathbb{Q})| = |(\mathbb{Z}/16\mathbb{Z})^\times| = \varphi(16) = 8$

$i = \sqrt{-1}$, $-1 \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei $\Rightarrow$

$[\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}] = 2$

Gradformel $\Rightarrow \delta = [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] =$

$[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] \cdot 2$

$\Rightarrow [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)] = \frac{\delta}{2} = 4$

(b) Bestimmen Sie das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$. [Das Min-pol. ist $x^4 - i$. Nachweis als Übung]

(c) Entscheiden Sie begründet, ob $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{16}) | \mathbb{Q}(i))$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist. Laut Vl. existiert ein Isomorphismus $\phi : (\mathbb{Z}/16\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_{16}) | \mathbb{Q})$, der für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, 16) = 1$ (bzw. $2 \nmid a$) die Restkl. $a + 16\mathbb{Z} \in (\mathbb{Z}/16\mathbb{Z})^\times$ auf das Element

$\sigma_a \in Gal(\mathbb{Q}(\zeta_{16})|\mathbb{Q})$ gegeben durch $\sigma_a(\zeta) = \zeta^a$ abbildet wobei $\zeta = \zeta_{16}$.

$(\mathbb{Z}/16\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\}$

$\rightarrow Gal(\mathbb{Q}(\zeta_{16})|\mathbb{Q}) = \{\sigma_1 = id, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}\}$

$\sigma_3(i) = \sigma_3(\zeta^4) = \sigma_3(\zeta)^4 = (\zeta^3)^4 =$

$\uparrow i = \zeta^4$

$(\zeta^4)^3 = i^3 = -i \neq i \Rightarrow \sigma_3 \notin Gal(\mathbb{Q}(\zeta)|\mathbb{Q}(i))$

$\sigma_5(i) = \sigma_5(\zeta^4) = \sigma_5(\zeta)^4 = (\zeta^5)^4 =$

$(\zeta^4)^5 = i^5 = i \Rightarrow \sigma_5 \in Gal(\mathbb{Q}(\zeta)|\mathbb{Q}(i))$

Das Element $\overline{5} \in (\mathbb{Z}/16\mathbb{Z})^\times$ hat wegen $\overline{5}^2 = \overline{25}$

$= \overline{9} \neq \overline{1}$ und $\overline{5}^4 = \overline{9}^2 = \overline{81} = \overline{1}$ in $(\mathbb{Z}/16\mathbb{Z})^\times$

die Ordnung 4. Auf Grund des Isom. ist σ_5 ein Element der Ordn. 4 in $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q})$, und damit auch in $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q}(i))$. Die Gruppe besitzt also ein Element von Ordnung 4 und ist selbst von Ordn. $[\mathbb{Q}(\zeta_5):\mathbb{Q}(i)]$ $=4$. Also ist $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q}(i))$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$. □