

H17T2A4 Sei $f = x^{12} - 729 \in \mathbb{Q}[x]$ und

$L \subseteq \mathbb{C}$ der Zerf. körp. von f über $\mathbb{Q}$. Sei $\zeta \in \mathbb{C}^*$ die primitive 12-te Einheitswurzel $\zeta = e^{\pi i/6} = \frac{1}{2}(\sqrt{3} + i)$. ($729 = 9 \cdot 81 = 3^6$)

(a) Zeigen Sie: $\sqrt{3} \in \mathbb{Q}(\zeta)$ und $L = \mathbb{Q}(\zeta)$

Da ζ eine 12-te Einheitswurzel ist, gilt $\bar{\zeta} = \zeta^{-1}$

Aus $\zeta, \zeta^{-1} \in \mathbb{Q}(\zeta)$ folgt $\zeta + \zeta^{-1} = \zeta + \bar{\zeta} = \frac{1}{2}(\sqrt{3} + i) + \frac{1}{2}(\sqrt{3} - i) = \sqrt{3} \in \mathbb{Q}(\zeta)$.

Beh. $N = \{ \zeta^k \sqrt[12]{729} \mid 0 \leq k < 12 \}$ ist die Menge der

Aus $S, S^{-1} \in \mathbb{Q}(S)$ folgt $S + S^{-1} = \eta + \bar{\eta} =$

komplexen Nullstellen von f in $\mathbb{C}$.

$$\begin{aligned}\text{Für } 0 \leq k < 12 \text{ gilt } f(S^k \sqrt[12]{729}) &= (S^k \sqrt[12]{729})^{12} - 729 \\ &= (S^{12})^k (\sqrt[12]{729})^{12} - 729 = 1^k \cdot 729 - 729 = 0\end{aligned}$$

Weil S eine prim. 12-te Einheitswurzel ist, sind die Elemente S^k mit $0 \leq k < 12$ alle verschieden. Wegen $\sqrt[12]{729} \neq 0$ besteht die Menge N aus 12 verschiedenen Elementen. Da f wegen $\deg(f) = 12$ höchstens 12 Nullstellen besitzt, muss N also die gesamte Nullstellenmenge sein. ($\rightarrow$ Beh.)

Aus der Beh. folgt $L = \mathbb{Q}(N)$ zu zeigen bleibt also $\mathbb{Q}(N) = \mathbb{Q}(S)$ zu überprüfen also:

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

...eben dieses Erzeugendensystem ein primitives Element.

(Hilfsmittel: $\mathbb{Q}(\sqrt[12]{729}) \supset \mathbb{Q}(\sqrt[6]{729}) \supset \mathbb{Q}(\sqrt[3]{729}) \supset \mathbb{Q}(\sqrt{729})$)

$$\text{Es gilt } \sqrt[12]{729} = \sqrt[12]{3^6} = 3^{6/12} = 3^{1/2} = \sqrt{3}$$

$$\text{zu (1)} \quad \sqrt{3} = \sqrt[12]{729} \in N \quad \sqrt[12]{729}, \sqrt[12]{729}^5 \in \mathbb{Q}(N)$$

$$\Rightarrow S = \frac{\sqrt[12]{729}^5}{\sqrt[12]{729}} \in \mathbb{Q}(N)$$

$$\text{zu (2)} \quad \text{s.o.} \Rightarrow \sqrt{3} \in \mathbb{Q}(S) \Rightarrow \sqrt[12]{729} \in \mathbb{Q}(S)$$

$$\Rightarrow S^k \sqrt[12]{729} \in \mathbb{Q}(S) \Rightarrow N \subseteq \mathbb{Q}(S)$$

(b) Zeigen Sie, dass $\text{Gal}(L/\mathbb{Q})$ eine abelsche Gruppe der Ordnung 4 ist, mit drei Elementen der Ordnung 2. [Skizze: (1) Zeige: $L/\mathbb{Q}$ ist Galois-erw. (2) Bestimme den Erzeugend. entweder mit Hilfe der Gleichung $L = \mathbb{Q}(\sqrt{3}, i)$, oder mit Hilfe der

Beh.)

Formel $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ für den Grad von Kreisteilungseren, folgere $|\text{Gal}(L|\mathbb{Q})| = 4$ (3) 4 ist Primzahlquadrat $\Rightarrow \text{Gal}(L|\mathbb{Q})$ ist abelsch (4) Leite aus der Existenz der beiden Zwischenkörper $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$ ab, dass $\text{Gal}(L|\mathbb{Q})$ nicht zyklisch ist. Folgere daraus, dass es zwei Fkt. der Ordnung 2 gibt.]

Details: Übung

(d) Geben Sie alle echten Zwischenkörper von $L|\mathbb{Q}$ an, und für jeden dieser Zwischenkörper ein primitives Element.

(Übung; die Körper sind $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{3})$)

weitere Übungen: F22T2A5, H22T1A3,
H24T2A5

F22T3A4 Sei K ein Teilkörper von $\mathbb{Q}$ mit der Eigenschaft, dass $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 4 ist, mit zyklischer Galoisgruppe G . Zeigen Sie, dass i nicht in K liegt.

(Hinweis: Setzen Sie $i \in K$ voraus und betrachten Sie $K|\mathbb{Q}(i)$.)

Angenommen, es gilt $i \in K$. Dann ist $\mathbb{Q}(i)$ ein Zwischenkörper von $K|\mathbb{Q}$.

Wir betrachten in G die Untergruppe $H = \text{Gal}(K|\mathbb{Q}(i))$. Da $K|\mathbb{Q}$ galois'sch ist, gilt $|G| = |\text{Gal}(K|\mathbb{Q})| = [K:\mathbb{Q}] = 4$.

die
über

K Zef

$\Rightarrow K$

separabel

Sei G

$|G| = [$

zahlen

Sei $\forall p$

gruppen

$\forall 43|47$

$47 \equiv 4 \equiv$

einzigste 4

Weil -1 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, gilt lt. Vorlesung $[\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}] = 2$. Laut Galoistheorie folgt daraus $(G : U) = 2$, und der Satz von Lagrange liefert $|U| = \frac{|G|}{(G : U)} = \frac{4}{2} = 2$.

Weil G zyklisch ist, ist U die einzige Untergruppe der Ordnung 2.

Betrachte die Abb. $\sigma : K \rightarrow \mathbb{C}$, $\alpha \mapsto \bar{\alpha}$ geg. durch komplexe Konjugation. Für diese Abb. gilt $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$, $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ $\forall \alpha, \beta \in K$ und $\sigma(a) = a \forall a \in \mathbb{Q}$, es handelt sich also um ein Element von $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Weil $K/\mathbb{Q}$ normal ist, gilt $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \text{Aut}_{\mathbb{Q}}(K)$.

$\Rightarrow$

$\Rightarrow$

Für α

$= \alpha$

aber

Da U

folgt

$\Rightarrow \sigma$

HZIT1

Sei K

über $\mathbb{Q}$

(a) Zeig

$K/\mathbb{Q}$ mit

17

$\Rightarrow \sigma$ ist ein Element von $\text{Aut}_{\mathbb{Q}}(K) = \text{Gal}(K|\mathbb{Q})$.

$\Rightarrow V = \langle \sigma \rangle$ ist eine Untergr. von $\text{Gal}(K|\mathbb{Q})$

Für alle $\alpha \in K$ gilt $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\bar{\alpha}) = \overline{\bar{\alpha}} = \alpha$.

$\Rightarrow \sigma^2 = \text{id}_K$ Wegen $\sigma(i) = -i \neq i$ gilt

aber $\sigma \neq \text{id}_K$, $\Rightarrow |V| = |\langle \sigma \rangle| = \text{ord}(\sigma) = 2$

Da U die einzige Untergr. der Ordnung 2 in $\text{Gal}(K|\mathbb{Q})$ ist,

folgt $U = V$. $\sigma \in V \Rightarrow \sigma \in U \Rightarrow \sigma \in \text{Gal}(K|\mathbb{Q}(i))$

$\Rightarrow \sigma(\alpha) = \alpha \forall \alpha \in \mathbb{Q}(i) \Rightarrow \sigma(i) = i \downarrow$

□

H21T1A5 (ähnlich: F17T2A5)

Sei K der Zerfällungskörper eines Polynoms $f \in \mathbb{Q}[x]$

über $\mathbb{Q}$ in $\mathbb{C}$, mit $[K:\mathbb{Q}] = 2021$

(a) Zeigen Sie, dass es Zwischenkörper L_1, L_2 von

$K|\mathbb{Q}$ mit $[L_1:\mathbb{Q}] = 43$ und $[L_2:\mathbb{Q}] = 47$ gibt,

die ebenfalls Zerfällungskörper von Polynomen über $\mathbb{Q}$ sind.

K Zerf.körper eines Pol $f \in \mathbb{Q}[x]$ über $\mathbb{Q} \Rightarrow K|\mathbb{Q}$ ist normal
 $\Rightarrow K|\mathbb{Q}$ ist algebraisch. $K|\mathbb{Q}$ alg., $\text{char}(\mathbb{Q})=0 \Rightarrow K|\mathbb{Q}$ ist
separabel. Insgesamt ist $K|\mathbb{Q}$ also eine Galois-erw.

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

Sei v_p für $p \in \{43, 47\}$ die Anzahl der p -Sylow-
gruppen von G . 3. Sylowsatz $\Rightarrow v_{43} \mid \frac{2021}{43} \rightarrow$
 $v_{43} \mid 47 \Rightarrow v_{43} \in \{1, 47\}$, außerdem $v_{43} \equiv 1 \pmod{43}$,
 $47 \equiv 4 \not\equiv 1 \pmod{43} \Rightarrow v_{43} = 1$. Sei P die
einzige 43-Sylowgruppe von G .

$$\text{ebenso: } n_{47} \mid \frac{2043}{47} \Rightarrow n_{47} \mid 43 \Rightarrow n_{47} \in \{1, 43\}$$

$$n_{47} \equiv 1 \pmod{47}, 43 \not\equiv 1 \pmod{47} \Rightarrow n_{47} = 1$$

Sei Q die einzige 47-Sylowsg. von G .

$$|G| = 43' \cdot 47' \Rightarrow |P| = 43, |Q| = 47$$

Sei $L_1 = K^Q$ und $L_2 = K^P$ (Fixkörper von P

bzw. Q). Laut Galois-Theorie gilt $[L_1: Q] =$

$$(G:Q) = \frac{|G|}{|Q|} = \frac{2021}{47} = 43 \text{ und } [L_2: Q] =$$

$$(G:P) = \frac{|G|}{|P|} = \frac{2021}{43} = 47.$$

Aus $n_{43} = 1$ und dem 2. Sylowsatz folgt $P \trianglelefteq G$.

Sei $L_1 = K^Q$ und $L_2 = K^P$ (Fixkörper von P
bzw. Q). Laut Galois-Theorie gilt $[L_1: Q] =$

Laut Galois-Theorie folgt daraus, dass die Erweiterung L_2/K normal ist. Daraus wiederum folgt, dass L_2 Zerfällungskörper eines Polynoms aus $K[x]$ über K ist. Genauso folgt aus $V_{L_1} = 1$, dass L_1 Zerf.-korp. eines Pol. aus $K[x]$ über K ist.

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

Es gilt $\deg(f) = \deg M_{\alpha, Q} = [Q(\alpha): Q]$
 $= [K: Q] = 2021$. Als Polynom ungeraden Grades besitzt f zumindest eine reelle Null-

stelle α_1 . Da $K|Q$ als Galois-Erweiterung normal ist, außerdem f als Min. pol. (irreduzibel) ist und f mit α in $Q(\alpha)$ eine Nullstelle besitzt, zerfällt f über $Q(\alpha)$ in Linearfaktoren. Aus $f(\alpha_1) = 0$ folgt somit $\alpha_1 \in Q(\alpha)$.

$$\Rightarrow Q(\alpha_1) \subseteq Q(\alpha) \xrightarrow{\text{grad } f} [Q(\alpha):Q] = [Q(\alpha):Q(\alpha_1)] \cdot [Q(\alpha_1):Q]$$

Da f normiert und irred. ist, folgt aus $f(\alpha_1) = 0$ die Gleichung

$$f = \mu_{\alpha_1, K} \Rightarrow [Q(\alpha_1):Q] = \text{grad}(f) = 2021 = [Q(\alpha):Q] \Rightarrow$$

$$[Q(\alpha):Q(\alpha_1)] = 1 \Rightarrow Q(\alpha) = Q(\alpha_1) \quad \text{Daraus folgt, dass } f \text{ auch über } Q(\alpha_1) \text{ in Linearfaktoren zerfällt.}$$

Wz. $\alpha_1 \in \mathbb{R}$ gilt $Q(\alpha_1) \subseteq \mathbb{R}$. Also zerfällt f auch

$$\Rightarrow \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha) \xrightarrow{\text{grad.}} [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$$

Da f normiert und irred. ist, folgt aus $f(\alpha_1) = 0$ die Gleichung

über $\mathbb{R}$ in Linearfaktoren.