Aufgaben zur Körpertheorie

Gibt es einen Körper K, so dass ...

(1) $K|\mathbb{Q}$ algebraisch vom Grad 100 ist?

Ja. Ein Körper K ist algebraisch über $\mathbb{Q}$ wenn jd. Element aus K eine Nullstelle eines Polynoms mit Elementen aus $\mathbb{Q}$ ist. Um einen Körper K zu konstruieren, der algebraisch vom Grad 100 über $\mathbb{Q}$ ist, betrachte $P(x) = (x^2-2)(x^2-3)(x^2-5)\cdots(x^2-101)$. Dieses Polynom hat Grad 100, und keine rationalen Nullstellen. Wir definieren dann K als den Zerfällungskörper von $P(x)$ über $\mathbb{Q}$.

(2) $K|\mathbb{Q}$ galoissch vom Grad 100 ist?

Ja. Eine Galoiserweiterung ist eine Körpererweiterung, bei der der Grad der Erweiterung gleich der Anzahl der Automorphismen des Erweiterungskörpers über den Grundkörper ist. Wähle den Zerfällungskörper aus (1), dann ist $K|\mathbb{Q}$ eine KE vom Grad 100. Da $\operatorname{char}(\mathbb{Q}) = 0$, ist die Körpererweiterung separabel und da K Zerfällungskörper von $P(x)$ ist, ist die Erweiterung auch normal, also galoissch.

(3) $K|\mathbb{Q}$ abelsch vom Grad 100 ist?

Ja. Eine Körpererweiterung $K|\mathbb{Q}$ heißt abelsch, wenn für jd. $\alpha \in K$ der Körper $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ für alle Nullstellen β des Minimalpolynoms von α über $\mathbb{Q}$ gilt. Betrachte $P(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_{100})$. Da $P(x)$ ein separables Polynom ist, falls $\alpha_i \neq \alpha_j$ für alle $i,j \in \{1,\dots,100\}$ und $i \neq j$, ist $K|\mathbb{Q}$ ebenfalls separabel mit $K = \mathbb{Q}(\alpha_1,\dots,\alpha_{100})$ und damit abelsch.

(4) $K|\mathbb{Q}$ zyklisch vom Grad 100 ist?

Ja. Eine Körpererweiterung $K|\mathbb{Q}$ heißt zyklisch, wenn es ein $\alpha \in K$ gibt, so dass $K = \mathbb{Q}(\alpha)$ und das Minimalpolynom von α über $\mathbb{Q}$ ein zyklisches Polynom ist. Um einen solchen Körper zu konstruieren, können wir das Polynom $P(x) = (x^{100}-2)$ betrachten. Dieses hat keine rationalen Nullstellen, ist also irreduzibel über $\mathbb{Q}$ vom Grad 100. Sei K der Zerfällungskörper von $P(x)$, dann ist K eine zyklische KE.

Ein zyklisches Polynom vom Grad n hat die Form $P(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ wobei $a_0, a_1, \dots, a_n$ in einer zyklischen Permutation angeordnet sind

Berechne das zwölfte Kreisteilungspolynom $\phi_{12}(x)$.

$\phi_1 = X - 1$

$X^2 - 1 = \prod_{d|2} \phi_d(x) = \phi_2 \phi_1 \Rightarrow \phi_2 = \frac{X^2-1}{\phi_1} = X+1$

$X^3 - 1 = \prod_{d|3} \phi_d(x) = \phi_3 \phi_1 \Rightarrow \phi_3 = \frac{X^3-1}{\phi_1} = X^2+X+1$

$\Rightarrow X^4 - 1 = \prod_{d|4} \phi_d \Rightarrow \phi_4 = \frac{X^4-1}{\prod_{\substack{d|4\\d\neq 4}} \phi_d}$

Teiler von 12 sind $\{1,2,3,4,6,12\}$.

$\Rightarrow \phi_{12} = \frac{X^{12}-1}{\prod_{\substack{d|12\\d\neq 12}} \phi_d} = \frac{X^{12}-1}{\phi_1\phi_2\phi_3\phi_4\phi_6} = \frac{X^{12}-1}{(X^6-1)(X^2+1)} = \frac{X^6-1}{X^2+1} = X^4 - X^2 + 1$

Was ist $\phi_{p^2}(1)$ für eine Primzahl p?

Allgemein ist $\phi_{p^n} = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \ldots + x^{(p-1)p^{n-1}} = \sum_{i=0}^{p-1} x^{ip^{n-1}}$

$\Rightarrow \phi_{p^2}(1) = 1 + 1^{2^1} = 2$

Welche Kreisteilungskörper haben Grad 4 über $\mathbb{Q}$?

Sei $K = \mathbb{Q}(\sqrt{6})$

(1) Schreibe $\frac{1+2\sqrt{6}}{3+4\sqrt{6}}$ als $\mathbb{Q}$ Linearkombination von $1, \sqrt{6}$.

$$\frac{1+2\sqrt{6}}{3+4\sqrt{6}} \cdot \frac{3-4\sqrt{6}}{3-4\sqrt{6}} = \frac{3-4\sqrt{6}+6\sqrt{6}-48}{9-96} = -\frac{3}{87} - \frac{2\sqrt{6}}{87} + \frac{48}{87} = \frac{45}{87} - \frac{2\sqrt{6}}{87}$$

(2) Berechne für $x,y \in \mathbb{Q}$ die Spur $Sp_{K|\mathbb{Q}}(x+y\sqrt{6})$ und die Norm $N_{K|\mathbb{Q}}(x+y\sqrt{6})$.

$$x+y\sqrt{6} \cdot \begin{pmatrix} 1 \\ \sqrt{6} \end{pmatrix} = \begin{pmatrix} x+\sqrt{6} \\ \sqrt{6}x+6y \end{pmatrix} = \begin{pmatrix} x & 1 \\ 6y & x \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{6} \end{pmatrix} = A(x+y\sqrt{6})$$

$\Rightarrow Sp_{K|\mathbb{Q}}(x+y\sqrt{6}) = 2x$

$\Rightarrow N_{K|\mathbb{Q}}(x+y\sqrt{6}) = \det\begin{pmatrix} x & 1 \\ 6y & x \end{pmatrix} = x^2 - 6y$

Sei $f = x^6+6x+6 \in \mathbb{Q}[x]$ und α das Bild von x in $\mathbb{Q}[x]/(f)$.

(1) Zeige, dass K ein Körper ist.

$K = \mathbb{Q}[x]/(f)$ ist ein Körper, wenn (f) ein maximales Ideal ist.

Da $\mathbb{Q}$ ein Hauptidealring ist, ist (f) maximal, wenn f irreduzibel über $\mathbb{Q}$ ist.

$x^6+6x+6 = 6 \cdot \left(\frac{1}{6}x^6 + x + 1\right)$

Die Nullstelle müsste also Teiler von 1 sein, also ± 1.

Es ist $f(1) = 6 \cdot \left(\frac{1}{6} \cdot 1^6 + 1 + 1\right) = 1+6+6 = 13 \neq 0$

$f(-1) = 6 \cdot \left(\frac{1}{6} \cdot (-1)^6 - 1 + 1\right) = 1 \neq 0$

$\Rightarrow f(x)$ hat über $\mathbb{Q}$ keine Nullstelle

$\Rightarrow f$ ist irreduzibel

$\Rightarrow (f)$ ist ein maximales Ideal

$\Rightarrow \mathbb{Q}[x]/(f)$ ist ein Körper.

(2) Gib eine $\mathbb{Q}$-Basis von K an.

Da f irreduzibel und (f) somit maximal ist, ist K eine Körpererweiterung von $\mathbb{Q}$, und hat damit Grad 6 über $\mathbb{Q}$. Jede $\mathbb{Q}$-Basis von K hat also 6 Elemente. Eine mögliche Basis ist $\{1, x, x^2, x^3, x^4, x^5\}$. Diese Basis besteht aus den Restklassen der Potenzen von x mod f. Eine Nullstelle von f in $\mathbb{Q}[x]/(f)$ ist $x+(f)$.

(3) Schreibe $\frac{1}{\alpha}$ als $\mathbb{Q}$-Linearkombination der $\mathbb{Q}$-Basis aus (2)

Sei $g = x$. Es folgt $f = (x^5+6)g + 6$ und damit $1 = \frac{1}{6}f - \frac{1}{6}(x^5+6)g$. Einsetzen von $x = \alpha$ und Nutzung von $f(\alpha) = 0$ liefert $1 = -\left(\frac{1}{6}\alpha^5 + 1\right)\alpha$, also $\frac{1}{\alpha} = -\left(\frac{1}{6}\alpha^5+1\right)$ $= -\frac{1}{6}\alpha^5 - 1$.

Sei K ein Körper und $\pi: K \to K$ mit $\pi(x) = x^3$. Wahr oder Falsch?

(1) Ist $\mathrm{char}(K)=3$, so ist π ein Körperhomomorphismus.

Wahr. Ist $\mathrm{char}(K)=3$, so ist $K \cong \mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Dann ist $\pi(\bar{0}\cdot\bar{1}+\bar{1}\cdot\bar{2}) = \pi(\bar{0})\cdot\pi(\bar{1})+\pi(\bar{1})\cdot\pi(\bar{2}) = \bar{0}^3\cdot\bar{1}^3+\bar{1}^3\cdot\bar{2}^3$

$= \bar{0}+\bar{8} = \bar{2} = \bar{2}^3 = \pi(\bar{2})$.

π ist in K der Frobenius-Homomorphismus.

(2) Ist π ein Körperhomomorphismus, so ist $\mathrm{char}(K)=3$.

Falsch. Sei $K=\mathbb{F}_2$. Dann ist π die Identität auf $\mathbb{F}_2$ aber $\mathrm{char}(\mathbb{F}_2)=2\neq 3$.

Sei $f = x^3-9x-9 \in \mathbb{Q}[x]$ und $\alpha \in \bar{\mathbb{Q}}$ eine Nullstelle von f. Weiter sei $K=\mathbb{Q}(\alpha)$ und $\beta = 6+\alpha-\alpha^2$.

(1) Zeige, dass f irreduzibel ist.

Nach dem Satz über rationale Nullstellen muss die Nullstelle Teiler des konstanten Glieds sein, also $\pm1, \pm3, \pm9$. Aber es ist:

$f(1) = 1^3-9-9 = -17$, $\quad f(9) = 729-81-9 = 639$

$f(-1) = -1+9-9 = -1$, $\quad f(-9) = -729+81-9 = -657$

$f(3) = 27-27-9 = -9$, $\quad$ Damit ist gezeigt, dass f irreduzibel ist.

$f(-3) = -27+27-9 = -9$.

(2) Zeige, dass $f(\beta)=0$ gilt.

Es ist $f(\alpha) = \alpha^3-9\alpha-9 = 0 \iff \alpha^3 = 9\alpha+9$

$\Rightarrow f(\beta) = f(6+\alpha-\alpha^2) = (6+\alpha-\alpha^2)^3 - 9\cdot(6+\alpha-\alpha^2)-9$

$= (6+\alpha-\alpha^2)(36+6\alpha-6\alpha^2+6\alpha+\alpha^2-\alpha^3-6\alpha^2-\alpha^3+\alpha^4)-9\cdot(6+\alpha-\alpha^2)-9$

$= (6+\alpha-\alpha^2)(36+12\alpha-11\alpha^2-2\alpha^3+\alpha^4)-9\cdot(6+\alpha-\alpha^2)-9$

$= (6+\alpha-\alpha^2)(27+12\alpha-11\alpha^2-2\alpha^3+\alpha^4)-9$

$= (6+\alpha-\alpha^2)(27+12\alpha-11\alpha^2-2(9\alpha+9)+\alpha(9\alpha+9))-9$

$= (6+\alpha-\alpha^2)(27+12\alpha-11\alpha^2-18\alpha-18+9\alpha^2+9\alpha)-9$

$= (6+\alpha-\alpha^2)(9+3\alpha-2\alpha^2)-9$

$= (54+18\alpha-12\alpha^2+9\alpha+3\alpha^2-2\alpha^3-9\alpha^2-3\alpha^3+2\alpha^4)-9$

$= 54+27\alpha-18\alpha^2-5\alpha^3+2\alpha^4-9$

$= 54+27\alpha-18\alpha^2-5(9\alpha+9)+2\alpha(9\alpha+9)-9$

$= 54+27\alpha-18\alpha^2-45\alpha+45+18\alpha^2+18\alpha-9$

$= 45+27\alpha-18\alpha^2-5\alpha^3+2\alpha^4 = 45+27\alpha-18\alpha^2-5(9+9\alpha)+2\alpha(9+9\alpha)$

$= 45+27\alpha-18\alpha^2-45-45\alpha+18\alpha+18\alpha^2 = 0$

(3) Zeige, dass ein $\gamma \in K\setminus\{\alpha,\beta\}$ existiert mit $f(\gamma)=0$. Schreibe γ als $\mathbb{Q}$-Linearkombination von $1, \alpha, \alpha^2$.

Da f in $\mathbb{Q}(\alpha)$ neben α auch $\beta = 6+\alpha-\alpha^2$ als Nullstelle hat, zerfällt f über $\mathbb{Q}(\alpha)$ in Linearfaktoren und es muss eine weitere Nullstelle geben, die wir γ nennen. Jedes irreduzible Polynom über $\mathbb{Q}$ ist wegen $\mathrm{char}(\mathbb{Q})=0$ separabel, also muss offensichtlich $\gamma\neq\alpha,\beta$ gelten.

Wir erhalten folgende Zerlegung von f:

$x^3-9x-9 = (x-\alpha)(x-\beta)(x-\gamma) = (x^2-(\alpha+\beta)x+\alpha\beta)(x-\gamma)$

$= x^3-\gamma x^2-(\alpha+\beta)x^2+\gamma(\alpha+\beta)x+\alpha\beta x-\alpha\beta\gamma$

$= x^3-(\alpha+\beta+\gamma)x^2+(\alpha\beta+\alpha\gamma+\beta\gamma)x-\alpha\beta\gamma$

Koeffizientenvergleich ergibt $\alpha+\beta+\gamma=0$, $\alpha\beta+\alpha\gamma+\beta\gamma=-9$ und $\alpha\beta\gamma=9$. Es folgt $\gamma = -\alpha-\beta = -\alpha-(6+\alpha-\alpha^2) = -6-2\alpha+\alpha^2$.

Warum ist $K|\mathbb{Q}$ eine Galoisgruppe? Bestimme den Isomorphietyp.

Da wir β, γ als $\mathbb{Q}$-Linearkombination der Basis $1, \alpha, \alpha^2$ schreiben können, gilt $\beta,\gamma \in K = \mathbb{Q}(\alpha)$. Also ist $\mathbb{Q}(\alpha)$ Zerfällungskörper von f und damit normal, da f über $\mathbb{Q}$ nicht in Linearfaktoren zerfällt. Da $\mathrm{char}(\mathbb{Q})=0$ gilt ist die Erweiterung separabel und somit galoissch. Es ist $\mathrm{Gal}(K|\mathbb{Q}) = \mathrm{Aut}(K|\mathbb{Q})$. Da f irreduzibel über $\mathbb{Q}$ ist, stehen die $\mathbb{Q}$-Automorphismen in Bijektion zu den Nullstellen von f. Wir erhalten drei Automorphismen $\sigma_1: \alpha\mapsto\alpha$, $\sigma_2: \alpha\mapsto\beta$, $\sigma_3: \alpha\mapsto\gamma$.

Also ist $|\mathrm{Gal}(K|\mathbb{Q})| = 3$ und somit $\mathrm{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_3$.

Sei $K = \mathbb{Q}(\sqrt[5]{3}, \sqrt{7})$

(1) Zeige, dass $K = \mathbb{Q}(\alpha)$ gilt mit $\alpha = \sqrt[5]{3} \cdot \sqrt{7}$

Es ist $\alpha \in \mathbb{Q}(\sqrt[5]{3}, \sqrt{7})$, also ist $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt[5]{3}, \sqrt{7})$.

Es ist $\alpha^5 = 3 \cdot (\sqrt{7})^4 \cdot \sqrt{7} = 3 \cdot 49 \cdot \sqrt{7} = 147\sqrt{7}$ also $\sqrt{7} = \frac{1}{147} \alpha^5 \in \mathbb{Q}(\alpha)$

Es ist $\alpha^6 = 3 \cdot \sqrt[5]{3} \cdot \sqrt{7}^6 = 3 \cdot 7^3 \cdot \sqrt[5]{3} = 1029 \cdot \sqrt[5]{3}$, also $\sqrt[5]{3} = \frac{1}{1029} \alpha^6 \in \mathbb{Q}(\alpha)$

Es folgt $\mathbb{Q}(\sqrt[5]{3}, \sqrt{7}) \subseteq \mathbb{Q}(\alpha)$ und damit $K = \mathbb{Q}(\alpha)$.

(2) Bestimme $[K:\mathbb{Q}]$

Da $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{7}, \sqrt[5]{3})$, betrachten wir

$[\mathbb{Q}(\sqrt{7}, \sqrt[5]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}(\sqrt[5]{3})] \cdot [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}]$

$= 2 \cdot 5 = 10$

nach dem Gradsatz, denn es gilt

$ggT([\mathbb{Q}(\alpha):\mathbb{Q}], [\mathbb{Q}(\beta):\mathbb{Q}]) = 1 \Rightarrow [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] \cdot [\mathbb{Q}(\beta):\mathbb{Q}]$

(3) Bestimme das Minimalpolynom von α über $\mathbb{Q}$.

$\alpha = \sqrt[5]{3}\sqrt{7} \Rightarrow \alpha^{10} = 9 \cdot 7^5 = 9 \cdot 16807 = 151263$

$\Rightarrow \alpha^{10} - 151263 = 0$

$\Rightarrow x^{10} - 151263$ ist das Minimalpolynom von α.

Sei $L|K$ eine Körpererweiterung. Wahr oder Falsch?

(1) Ist $L|K$ algebraisch, so ist $L|K$ endlich.

Falsch. Die Erweiterung $\overline{\mathbb{Q}}|\mathbb{Q}$ ist per Definition algebraisch, aber nicht endlich über $\mathbb{Q}$. Betrachte dafür $\prod_{i=1}^{n}(x-\alpha_i)+1$ mit $\alpha_i \in \overline{\mathbb{Q}} = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Dann hat das Polynom in $\overline{\mathbb{Q}}$ keine Nullstelle. Folglich wäre $\overline{\mathbb{Q}}$ nicht der algebraische Abschluss. Also kann $\overline{\mathbb{Q}}$ nicht endlich sein.

(2) Ist $L|K$ endlich, so ist $L|K$ algebraisch.

Wahr. Jede endliche Körpererweiterung ist algebraisch. Sei $L|K$ vom Grad $n<\infty$ und $\alpha \in L$. Die $n+1$ Elemente $1, \alpha, \dots, \alpha^n$ sind dann linear abhängig über K, d.h. es gibt $c_0, \dots, c_n \in K$ nicht alle 0 mit $c_0 + c_1\alpha + \dots + c_n\alpha^n = 0$. Nach Definition ist somit α algebraisch über K.

(3) Gibt es ein $\alpha \in L$ mit $L = K(\alpha)$, so ist $L|K$ algebraisch.

Falsch. Die primitive Erweiterung $\mathbb{Q}(\pi)|\mathbb{Q}$ ist nicht algebraisch, denn π ist transzendent über $\mathbb{Q}$.

(4) Ist $L|K$ endlich, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.

Falsch. $\mathbb{F}_p(x,y)$ ist endlich über $\mathbb{F}_p(x^p, y^p)$. Es gibt aber kein $\alpha \in \mathbb{F}_p(x,y)$ mit $\mathbb{F}_p(x,y) = \mathbb{F}_p(x^p, y^p)(\alpha)$.

Seien $\alpha, \beta \in \mathbb{C}$ algebraisch über $\mathbb{Q}$ mit $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$. Gilt dann $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] \cdot [\mathbb{Q}(\beta):\mathbb{Q}]$?

Falsch. Seien $\alpha = \sqrt[3]{2}$, $\zeta = \zeta_3 = \frac{-1+i\sqrt{3}}{2}$ und $\beta = \zeta\alpha$. Dann ist $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6$, aber $[\mathbb{Q}(\alpha):\mathbb{Q}] \cdot [\mathbb{Q}(\beta):\mathbb{Q}] = 3 \cdot 3 = 9$

Warum ist ein endlicher Körper K nicht algebraisch abgeschlossen?

Jeder endliche Körper ist von der Form $\mathbb{F}_{p^n}$ für p prim und $n \in \mathbb{N}$. Wäre $\mathbb{F}_{p^n}$ algebraisch abgeschlossen, so würde jedes nicht konstante Polynom über $\mathbb{F}_{p^n}$ vollständig in Linearfaktoren zerfallen. Aber $\prod_{\alpha \in \mathbb{F}_{p^n}}(x-\alpha)+1$ hat keine Nullstellen in $\mathbb{F}_{p^n}$. Also kann $\mathbb{F}_{p^n}$ nicht algebraisch abgeschlossen sein.

Wahr oder falsch? Beweisen oder widerlegen Sie.

(1) Der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ ist eine algebraische Erweiterung von $\mathbb{Q}$.

Per Definition ist der algebraische Abschluss $\overline{\mathbb{Q}}$ algebraisch über $\mathbb{Q}$.

(2) Der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ ist eine endliche Körpererweiterung von $\mathbb{Q}$.

Falsch. Sei f ein irreduzibles Polynom n-ten Grades über $\mathbb{Q}$ mit n verschiedenen Nullstellen. Dann faktorisiert f über $\overline{\mathbb{Q}}$ in $f = (x-\alpha_1) \cdots (x-\alpha_n)$. Dann ist $g = f+1$ ein Polynom ohne Nullstelle in $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Per Induktion sehen wir, dass $\overline{\mathbb{Q}}$ nicht endlich sein kann.

(3) $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{Q}$.

Falsch. Denn $\mathbb{C}$ enthält über $\mathbb{Q}$ transzendente Elemente wie π und e.

Sei K ein Unterkörper von $\mathbb{C}$. Wahr oder falsch?

(1) Die komplexe Konjugation ist ein Element von $\mathrm{Aut}(K|\mathbb{Q})$.

Die komplexe Konjugation bildet für $\alpha = \sqrt[3]{2}$, $\zeta = \zeta_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ und $K = \mathbb{Q}(\alpha, \zeta)$

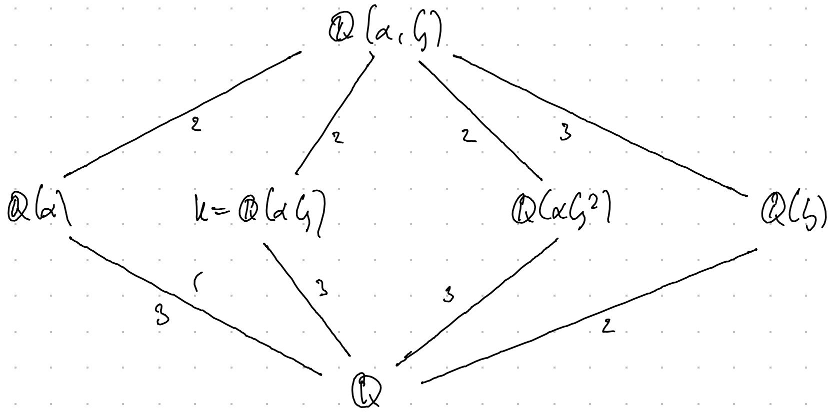
$\alpha\zeta$ auf $\overline{\alpha\zeta} = \bar{\alpha}\bar{\zeta} = \alpha\bar{\zeta} = \alpha\zeta^2$ ab. Sie ist also kein Element von $\mathrm{Aut}(K|\mathbb{Q})$.

(2) Gilt $K \not\subseteq \mathbb{R}$, so ist K über $K \cap \mathbb{R}$ algebraisch vom Grad 2.

Sei $K = \mathbb{Q}(\alpha\zeta)$. Wegen $[K:\mathbb{Q}] = 3$ hat K über $\mathbb{Q}$ keine echten Zwischenkörper. Es folgt $K \cap \mathbb{R} = \mathbb{Q}$

und damit $[K : K \cap \mathbb{R}] = 3 \neq 2$.

Wir erhalten folgendes Unterkörperdiagramm:



Sei $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$.

(1) Bestimme $[K:\mathbb{Q}]$.

Das Minimalpolynom von $\sqrt[3]{2}$ ist $x^3 - 2 = f \implies \deg(f) = 3$

Das Minimalpolynom von $\sqrt{3}$ ist $x^2 - 3 = g \implies \deg(g) = 2$

Das Minimalpolynom von i ist $x^2 + 1 = h \implies \deg(h) = 2$

$\mathrm{ggT}(f, g) = \mathrm{ggT}(f, h) = \mathrm{ggT}(g, h) = 1$

Damit folgt nach dem Gradsatz

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \cdot [\mathbb{Q}(i) : \mathbb{Q}]$$
$$= 3 \cdot 2 \cdot 2 = 12$$

(2) Ist K eine normale Körpererweiterung?

Seien $\alpha = \sqrt[3]{2}$, $\zeta = \zeta_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ und sei L ein Zerfällungskörper der über $\mathbb{Q}$ irreduziblen

Polynome $x^3 - 2$, $x^2 - 3$ und $x + 1$. Es gilt

$$L = \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2, \sqrt{3}, -\sqrt{3}, i, -i) = \mathbb{Q}(\alpha, \sqrt{3}, i) = K$$

denn $\zeta \in \mathbb{Q}(\sqrt{3}, i)$. Also ist $K|\mathbb{Q}$ normal.

Wahr oder Falsch? Beweise oder widerlege.

(1) In Charakteristik 0 ist jedes Polynom separabel.

Falsch. Das Polynom $x^2 = f \in \mathbb{Q}[x]$ hat die doppelte Nullstelle 0, ist also nicht separabel über $\mathbb{Q}$. Für irreduzible Polynome stimmt die Aussage, denn wegen $\operatorname{char}(\mathbb{Q}) = 0$ ist $\mathbb{Q}$ ein vollkommener Körper.

(2) In Charakteristik p ist jedes Polynom f vom Grad ≥ 1 mit $f' = 0$ inseparabel.

Wahr. Sei K ein Körper mit Charakteristik p. Für Polynome $f \in K[x]$ mit $\operatorname{grad}(f) \geq 1$ gilt die Äquivalenz: f ist separabel über $K \Longleftrightarrow \operatorname{ggT}(f, f') = 1$. Ist $\operatorname{grad}(f) \geq 1$ und $f' = 0$, so folgt $\operatorname{ggT}(f, f') = \operatorname{ggT}(f, 0) = f$. Also ist f inseparabel über $\mathbb{Q}$.

(3) In Charakteristik p ist jedes Polynom f vom Grad p inseparabel.

Falsch. Sei K ein Körper mit Charakteristik p. Insbesondere gilt $\mathbb{F}_p \subseteq K$. Nach dem kleinen Satz von Fermat gilt $x^p = x$ für alle $x \in \mathbb{F}_p$. Somit hat das Polynom $f = x^p - x$ $\in K[x]$ nur einfache Nullstellen, ist also separabel über K.

(4) Ist p eine Primzahl und $\alpha \in \mathbb{F}_p$ mit $\alpha^p + 1 = 0$, so ist $\mathbb{F}_p(\alpha)$ eine separable Körpererweiterung von $\mathbb{F}_p$.

In $\mathbb{F}_p$ gilt $\alpha^p = \alpha$, nach dem kleinen Satz von Fermat. Damit ist

$\alpha^p + 1 = \alpha + 1 = 0$, also hat $\alpha^p + 1$ nur eine einfache Nullstelle, ist also separabel.

$\mathbb{F}_p(\alpha)$ ist also eine separable Körpererweiterung von $\mathbb{F}_p$.

Es ist $\alpha = p - 1$ und damit $\mathbb{F}_p(\alpha) = \mathbb{F}_p$. Da endliche Körper vollkommen sind, ist die triviale Körpererweiterung separabel.

Ist $\mathbb{Q}(\sqrt[4]{2})$ galoisch über $\mathbb{Q}$?

Da $\operatorname{char}(\mathbb{Q}) = 0$ ist jedes Polynom über $\mathbb{Q}$ separabel.

Das Minimalpolynom von $\sqrt[4]{2}$ ist $f(x) = x^4 - 2$ mit Nullstellen $\{\pm\sqrt{2}, \pm i\sqrt{2}\}$.

$\Rightarrow f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2})$

aber $\pm i\sqrt{2} \notin \mathbb{Q}$. Also ist $\mathbb{Q}(\sqrt[4]{2})$ nicht normal und somit nicht galoisch.

Sei $L|\mathbb{Q}$ galoisch und K ein Zwischenkörper, d.h. $\mathbb{Q} \subseteq K \subseteq L$. Wahr oder falsch? Beweisen oder widerlegen sie.

(1) $K|\mathbb{Q}$ ist galoisch.

Falsch. Seien $L = \mathbb{Q}(\sqrt[4]{2}, i)$ und $K = \mathbb{Q}(\sqrt[4]{2})$. Die Erweiterung $L|\mathbb{Q}$ ist galoisch, denn L ist Zerfällungskörper des Polynoms $f = x^4 - 2 \in \mathbb{Q}[x]$ über dem vollkommenen Körper $\mathbb{Q}$. Aber $K|\mathbb{Q}$ ist nicht galoisch.

(2) $L|K$ ist galoisch.

Wahr. Als Galoiserweiterung ist $L|\mathbb{Q}$ algebraisch, normal und separabel. Somit ist L der Zerfällungskörper einer Familie $(f_i)_{i \in I}$ von Polynomen $f_i \in \mathbb{Q}[x]$. Wegen $\mathbb{Q}[x] \subseteq K[x]$ ist L natürlich ebenfalls der Zerfällungskörper dieser Polynome über $K[x]$. Also ist L normal über K. Da $\mathbb{Q}$ und danach auch K und L vollkommen sind, folgt aus der Separabilität von $L|\mathbb{Q}$ sofort die von $L|K$.

Sei $f = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$ und $\alpha_1 = \sqrt{1+\sqrt{3}}, \alpha_2 = \sqrt{1-\sqrt{3}}, \alpha_3 = -\alpha_1, \alpha_4 = -\alpha_2$.

(1) Zeige, dass $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ die komplexe Nullstelle von f sind.

$f(\alpha_1) = (\sqrt{1+\sqrt{3}})^4 - 2(\sqrt{1+\sqrt{3}})^2 - 2$

$= (1+\sqrt{3})^2 - 2 - 2\sqrt{3} - 2$

$= 1 + 2\sqrt{3} + 3 - 2 - 2\sqrt{3} - 2 = 0$

$\Rightarrow f(\alpha_3) = f(-\alpha_1) = f(\alpha_1) = 0$

$f(\alpha_2) = (\sqrt{1-\sqrt{3}})^4 - 2(\sqrt{1-\sqrt{3}})^2 - 2$

$= (1-\sqrt{3})^2 - 2 + 2\sqrt{3} - 2$

$= 1 - 2\sqrt{3} + 3 - 2 + 2\sqrt{3} - 2 = 0$

$\Rightarrow f(\alpha_2) = f(-\alpha_2) = f(\alpha_4) = 0$

$\Rightarrow \alpha_1, \alpha_2, \alpha_3, \alpha_4$ sind die komplexen Nullstellen von f.

(2) Zeige, dass $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$ gilt.

Es ist $\alpha_1 \in \mathbb{R}$ und $\alpha_2 \notin \mathbb{R}$ mit $\alpha_2 \in \mathbb{C}$.

Damit ist $\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$ aber $\mathbb{Q}(\alpha_2) \not\subseteq \mathbb{R}$, also $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$.

(3) Zeige dass $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$ gilt.

$\sqrt{3} = \alpha_1^2 - 1 \Rightarrow \sqrt{3} \in \mathbb{Q}(\alpha_1)$

$\sqrt{3} = 1 - \alpha_2^2 \Rightarrow \sqrt{3} \in \mathbb{Q}(\alpha_2)$

$\Rightarrow \sqrt{3} \in \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$

$\Rightarrow \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$

Das Minimalpolynom von $\sqrt{3}$ ist $x^2 - 3$, also ist $\mathbb{Q}(\sqrt{3})$ eine KE vom Grad 2. Nun ist $\alpha = \sqrt{1+\sqrt{3}}$ und das Minimalpolynom von α ist $\alpha^4 - 2\alpha - 2$, denn dieses ist 2-Eisensteinsch über $\mathbb{Q}$ und damit irreduzibel. Dies ist allerdings auch das Minimalpolynom von β. Also ist $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}] \in \{1, 2, 4\}$. Wäre der Grad 4, so würde gelten $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ ↯. Wäre $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}] = 1$ würde gelten $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, aber $\sqrt{3} \in \mathbb{Q}(\alpha) \wedge \sqrt{3} \in \mathbb{Q}(\beta) \wedge \sqrt{3} \notin \mathbb{Q}$ ↯. Also muss gelten $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Damit folgt $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$.

(4) Zeige, dass die Erweiterung $\mathbb{Q}(\alpha_1) | \mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\alpha_2) | \mathbb{Q}(\sqrt{3})$ galoissch sind.

Da $\operatorname{char}(\mathbb{Q}) = 0$, gilt $\operatorname{char}(\mathbb{Q}(\sqrt{3})) = 0$, also sind alle Polynome über $\mathbb{Q}(\sqrt{3})$ separabel. Das Minimalpolynom von α_1 ist $x^4 - 2\alpha - 2$ und somit 2-eisensteinsch, also irreduzibel über $\mathbb{Q}$. Die Nullstellen von $x^4 - 2\alpha - 2$ sind $\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{1-\sqrt{3}}$ und da $\pm\sqrt{1-\sqrt{3}} \notin \mathbb{Q}(\sqrt{3})$ ist, zerfällt $x^4 - 2\alpha - 2$ nicht über $\mathbb{Q}(\sqrt{3})$. Aber es zerfällt vollständig in Linearfaktoren über $\mathbb{Q}(\alpha_1)$ und über $\mathbb{Q}(\alpha_2)$ also sind diese beiden Körpererweiterungen normal und somit galoissch.

(5) Sei K der Zerfällungskörper von f über $\mathbb{Q}$. Zeige, dass $K | \mathbb{Q}(\sqrt{3})$ galoissch ist und bestimme den Isomorphietyp der Galoisgruppe.

Nach (4) ist $\mathbb{Q}(\sqrt{1+\sqrt{3}})$ der Zerfällungskörper von f und damit galoissch.
Über $\mathbb{Q}(\sqrt{3})$ zerfällt f in die zwei irreduziblen Polynome

$$f = (x^2 - 1 - \sqrt{3})(x^2 - 1 + \sqrt{3}) = (x^2 - \alpha_1^2)(x^2 - \alpha_2^2)$$

Damit sind die $\mathbb{Q}(\sqrt{3})$-Automorphismen von K durch die Werte auf α_1 und α_2 eindeutig bestimmt und sie müssen jeweils die Nullstellen der beiden Polynome $x^2 - 1 - \sqrt{3}$ und $x^2 - 1 + \sqrt{3}$ permutieren. Wir erhalten diese Möglichkeiten:

$\sigma_1 : \alpha_1 \mapsto \alpha_1, \ \alpha_2 \mapsto \alpha_2$

$\sigma_2 : \alpha_1 \mapsto \alpha_1, \ \alpha_2 \mapsto -\alpha_2$

$\sigma_3 : \alpha_1 \mapsto -\alpha_1, \ \alpha_2 \mapsto \alpha_2$

$\sigma_4 : \alpha_1 \mapsto -\alpha_1, \ \alpha_2 \mapsto -\alpha$

Der $\mathbb{Q}(\sqrt{3})$-Automorphismus σ_1 ist gleich der Identität auf K, alle weiteren $\mathbb{Q}(\sqrt{3})$-Automorphismen $\sigma_4, \sigma_2, \sigma_3$ besitzen die Ordnung 2. Es folgt $\operatorname{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(1) Warum ist K galoissch über $\mathbb{Q}$. Bestimme $\mathrm{Gal}(K|\mathbb{Q})$.

Zunächst ist jd. Polynom über $\mathbb{Q}$ separabel, da $\mathrm{char}(\mathbb{Q}) = 0$. Also ist $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ eine separable Körpererweiterung. Das Minimalpolynom von $\sqrt{2}$ ist $x^2 - 2$ und das Minimalpolynom von $\sqrt{3}$ ist $x^2 - 3$. Damit ist K Zerfällungskörper dieser beiden Polynome und somit normal. Also ist K galoissch.

(2) Zeige $K = \mathbb{Q}(2\sqrt{2} + 3\sqrt{3})$.

$2\sqrt{2} + 3\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow \mathbb{Q}(2\sqrt{2} + 3\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

Wir bestimmen das Minimalpolynom von $2\sqrt{2} + 3\sqrt{3}$:

$x = 2\sqrt{2} + 3\sqrt{3}$

$\Leftrightarrow x^2 = 8 + 12\sqrt{6} + 27$

$\Leftrightarrow x^2 - 35 = 12\sqrt{6}$

$\Leftrightarrow (x^2 - 35)^2 = 864$

$\Leftrightarrow x^4 - 70x^2 + 1225 = 864$

$\Leftrightarrow x^4 - 70x^2 + 361 = 0$

Damit ist das Polynom normiert und irreduzibel und somit das Minimalpolynom. Irreduzibilität zeigt man indem man prüft, dass $\{\pm 1, \pm 19, \pm 361\}$ keine Nullstellen sind. Es ist $\deg(f) = \deg(x^4 - 70x^2 + 361) = 4$.

Außerdem gilt $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$.

Also muss gelten $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(2\sqrt{2} + 2\sqrt{3})$.

Sei $\alpha = \sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}$.

(1) Zeige, dass α algebraisch über $\mathbb{Q}$ ist.

Die Zahlen $\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5}$ haben Minimalpolynome x^2-2, x^3-3, x^5-5, welche 2-, 3- und 5-Eisensteinisch sind, also irreduzibel über $\mathbb{Q}$. Damit ist $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5})$ ein Zerfällungskörper von den Polynomen und liegt in $\overline{\mathbb{Q}}$. Da der algebraische Abschluss per Definition algebraisch ist, ist auch $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5})$ algebraisch. Es gilt $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5})$ also ist auch $\mathbb{Q}(\alpha)$ algebraisch.

(2) Gib eine (endliche) Galoiserweiterung von $\mathbb{Q}$ an, die α enthält.

Ein algebraischer Abschluss $\overline{K}$ eines Körpers K ist genau dann galoisch über K, wenn K vollkommen ist. Wegen $\operatorname{char}(\mathbb{Q}) = 0$ ist $\mathbb{Q}$ vollkommen, daher können wir natürlich die (unendliche) Erweiterung $\overline{\mathbb{Q}} | \mathbb{Q}$ wählen.

Alternativ kann bspw. die Galoiserweiterung $L | \mathbb{Q}$ betrachtet werden, wobei L den Zerfällungskörper des Minimalpolynoms von α bezeichnet. Nach Konstruktion ist die Erweiterung $L | \mathbb{Q}$ normal. Als endliche Erweiterung über einen vollkommenen Körper ist sie auch separabel.

Sei $\alpha = \sqrt[3]{2}$, $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\beta = \zeta\alpha$ und $K = \mathbb{Q}(\alpha, \zeta)$.

(1) Zeige, dass $[K:\mathbb{Q}] = 6$ gilt.

Das Minimalpolynom von ζ ist $\phi_3 = x^2 + x + 1$, also $\deg(\phi_3) = 2$. Das Minimalpolynom von α ist $x^3 - 2 = g$ also $\deg(g) = 3$. Ersteres ist als Kreisteilungspolynom irreduzibel, Letzteres ist 2-eisensteinsch. Damit ist nach dem Gradsatz

$$[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta):\mathbb{Q}] = 3 \cdot 2 = 6$$

(2) Zeige, dass $K|\mathbb{Q}$ eine Galoiserweiterung ist.

Über $\mathbb{Q}$ ist jedes Polynom separabel, da $\operatorname{char}(\mathbb{Q}) = 0$. Also ist $\mathbb{Q}(\alpha,\zeta)|\mathbb{Q}$ eine separable Körpererweiterung. $\phi_3 = x^2 + x + 1$ ist Minimalpolynom von ζ und hat ζ und ζ^2 als Nullstelle. Das Minimalpolynom von α ist $x^3 - 2$ mit Nullstelle $\sqrt{2}, \zeta\sqrt{2}, \zeta^2\sqrt{2}$. Damit ist $\mathbb{Q}(\alpha,\zeta)$ der Zerfällungskörper der beiden Polynome und somit normal. Es folgt, dass $\mathbb{Q}(\alpha,\zeta)$ galoisch ist.

Beschreibe $\operatorname{Gal}(K|\mathbb{Q})$ durch Angabe von $\sigma(\alpha)$ und $\sigma(\zeta)$ für alle $\sigma \in \operatorname{Gal}(K|\mathbb{Q})$.

Die Nullstellen der Minimalpolynome sind ζ, ζ^2 und $\sqrt{2}, \zeta\sqrt{2}, \zeta^2\sqrt{2}$.

Die Automorphismengruppe $\operatorname{Aut}(K|\mathbb{Q}) = \operatorname{Gal}(K|\mathbb{Q})$ besteht aus den Automorphismen

$$\sigma_1: \sqrt{2} \longmapsto \sqrt{2}, \quad \zeta \longmapsto \zeta$$
$$\sigma_2: \sqrt{2} \longmapsto \sqrt{2}\zeta, \quad \zeta \longmapsto \zeta$$
$$\sigma_3: \sqrt{2} \longmapsto \sqrt{2}\zeta^2, \quad \zeta \longmapsto \zeta$$
$$\sigma_4: \sqrt{2} \longmapsto \sqrt{2}, \quad \zeta \longmapsto \zeta^2$$
$$\sigma_5: \sqrt{2} \longmapsto \sqrt{2}\zeta, \quad \zeta \longmapsto \zeta^2$$
$$\sigma_6: \sqrt{2} \longmapsto \sqrt{2}\zeta^2, \quad \zeta \longmapsto \zeta^2$$

Damit ist $|\operatorname{Gal}(K|\mathbb{Q})| = 6$ und somit ist $\operatorname{Gal}(K|\mathbb{Q}) \cong S_3$.

$$\begin{tikzcd}
 & & \mathbb{Q}(\alpha,\zeta) \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\mathbb{Q}(\alpha) \arrow[drr, "3"'] & K = \mathbb{Q}(\alpha\zeta) \arrow[dr, "3"] & & \mathbb{Q}(\alpha\zeta^2) \arrow[dl, "3"'] & \mathbb{Q}(\zeta) \arrow[dll, "2"] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

(4) Zeige $\mathbb{Q}(\alpha+\beta) \subsetneq K$ und $\mathbb{Q}(\alpha-\beta) = K$

$K = \mathbb{Q}(\alpha,\zeta)$, $[K:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] \cdot [\mathbb{Q}(\zeta):\mathbb{Q}] = 3 \cdot 2 = 6$

Das Minimalpolynom von $\alpha+\beta$ ist

$\alpha + \beta = \alpha + \zeta\alpha = (1+\zeta)\alpha = -\zeta^2\alpha$

$\Rightarrow (\alpha+\beta)^3 = -\alpha^3 = 2$

$\Rightarrow$ $\alpha+\beta$ ist Nullstelle von $x^3 - 2$, da das Polynom 2-Eisensteinsch ist, ist es irreduzibel.

Damit ist das das Minimalpolynom

$\Rightarrow [\mathbb{Q}(\alpha+\beta):\mathbb{Q}] = 3$

Also gilt $\mathbb{Q}(\alpha+\beta) \subsetneq K$.

$\alpha - \beta = \alpha - \alpha\zeta = \alpha(1-\zeta) \in \mathbb{Q}(\alpha,\zeta) \Rightarrow \mathbb{Q}(\alpha-\beta) \subseteq K$

Das Minimalpolynom von $\alpha-\beta$ ist

$$(\alpha-\beta)^3 = (1-\zeta)^3 \cdot \alpha^3 = (1 - 3\zeta + 3\zeta^2 - 1) \cdot 2 = 6(\zeta^2 - \zeta)$$
$$= 6 \cdot (-1 - 2\zeta) = 6 \cdot \left(-1 - 2 \cdot \frac{-1 + i\sqrt{3}}{2}\right) = 6 \cdot (-1 + 1 - i\sqrt{3})$$
$$= -i \cdot 6\sqrt{3}$$

$\Rightarrow (\alpha-\beta)^6 = -6^2 \cdot 3 = -108 = -2^2 \cdot 3^3$

$\Rightarrow$ $\alpha-\beta$ ist Nullstelle des Polynoms $x^6 + 108$, da $-108 = -2^2 \cdot 3^3$ und somit -108 weder in $\mathbb{Q}^{*2}$ noch in $\mathbb{Q}^{*3}$ liegt, ist $x^6 + 108$ irreduzibel.

$\Rightarrow [\mathbb{Q}(\alpha-\beta):\mathbb{Q}] = 6$

$\Rightarrow \mathbb{Q}(\alpha-\beta) = K$

Irreduzibilitätskriterium: Ist K ein Körper, $n \in \mathbb{N}_{\geq 2}$ und $a \in K^*$, sodass gilt

- $a \notin \{c^p : c \in K\}$ für alle Primzahlen p mit $p|n$
- $a \notin \{-4c^4 : c \in K\}$ falls $4|n$

So ist $x^n - a \in K[x]$ irreduzibel.

Wahr oder Falsch? Beweisen oder widerlegen Sie.

(1) Es gibt eine Galoiserweiterung $K|\mathbb{F}_2$ mit $Gal(K|\mathbb{F}_2) \cong \mathbb{Z}_{100}$.

Wahr. Sei $K = \mathbb{F}_{2^{100}}$. Nach Vorlesung sind die Erweiterungen $\mathbb{F}_{p^n}|\mathbb{F}_p$ zyklisch mit der vom Frobenius-Automorphismus $\pi: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \alpha \mapsto \alpha^p$ erzeugten Galoisgruppe $Gal(K|\mathbb{F}_p) = \langle \pi \rangle \cong \mathbb{Z}_n$.

(2) Es gibt eine Galoiserweiterung $K|\mathbb{Q}$ mit $Gal(K|\mathbb{Q}) \cong \mathbb{Z}_{100}$

Wahr. Sei $K = \mathbb{Q}(\zeta_{101})$. Nach Vorlesung sind die Erweiterungen $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ abelsch mit $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$ und durch

$$(\mathbb{Z}/n\mathbb{Z})^* \to Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}), \quad \bar{a} \mapsto \sigma_a \text{ mit } \sigma_a(\zeta_n) = \zeta_n^a$$

wird ein Gruppenisomorphismus definiert. Für die Primzahl $p = 101$ ist somit $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = 100$ und die Galoisgruppe $Gal(\mathbb{Q}(\zeta_{101})|\mathbb{Q}) = (\mathbb{Z}/101\mathbb{Z})^* \cong \mathbb{Z}_{100}$ ist zyklisch.

(3) Es gibt eine Galoiserweiterung $K|\mathbb{R}$ mit $Gal(K|\mathbb{R}) \cong \mathbb{Z}_{100}$

Falsch. Die Erweiterung $K|\mathbb{R}$ müsste algebraisch mit $[K:\mathbb{R}] = |Gal(K|\mathbb{R})| = 100$ sein. Doch jede algebraische Körpererweiterung von $\mathbb{R}$ ist entweder isomorph zu $\mathbb{R}$ oder zu $\mathbb{C}$. Denn $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$ und daher ist jede algebraische Erweiterung E von $\mathbb{R}$ ein Zwischenkörper $\mathbb{R} \subseteq E \subseteq \mathbb{C}$. Nach dem Gradsatz $[\mathbb{C}:\mathbb{R}] = [\mathbb{C}:E] \cdot [E:\mathbb{R}]$ folgt entweder $[E:\mathbb{R}] = 1$ und $E = \mathbb{R}$, oder $[\mathbb{C}:E] = 1$ und $E = \mathbb{C}$.