Hinweis:

Da ich mein eigenes Tablet am Dienstag nicht dabei hatte, musste ich die Fotos mit einem fremden Gerät machen. Anscheinend wurde nicht alles, was im Display angezeigt wurde, in der Bilddatei abgespeichert. Deshalb sind viele Bilder am rechten Rand abgeschnitten. Ich bitte, das zu entschuldigen.

F24T1A5 geg.: $\alpha = \sqrt{10-5\sqrt{2}}$

in (a) gezeigt: $\mu_{\alpha,\mathbb{Q}} = x^4 - 20x^2 + 50$

(b) Zeigen Sie, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ galoissch ist.

(c) Sei $G = \mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$. Zeigen Sie, dass G z
$(\mathbb{Z}/4\mathbb{Z}, +)$ isomorph ist.

zu (b) Beh.: $\mathbb{Q}(\alpha)$ ist Zerfällungskörper von
$f = \mu_{\alpha,\mathbb{Q}}$ über $\mathbb{Q}$

Für jedes $\gamma \in \mathbb{C}$ gilt die Äquivalenz $f(\gamma) = 0$

$\Leftrightarrow \gamma^4 - 20\gamma^2 + 50 = 0 \Leftrightarrow \gamma^4 - 20\gamma^2 + 100 =$

$\Leftrightarrow (\gamma^2-10)^2 = (5\sqrt{2})^2 \Leftrightarrow (\gamma^2-10)^2-(5$

$\Leftrightarrow (\gamma^2-10-5\sqrt{2})(\gamma^2-10+5\sqrt{2}) = 0$

$\gamma^2 = 10+5\sqrt{2} \vee \gamma^2 = 10-5\sqrt{2} \Leftrightarrow$

$\gamma \in N$, wobei $N = \{\pm\sqrt{10+5\sqrt{2}}, \pm\sqrt{10-$

Also ist N die Menge der komplexen Nullste

Es gilt $\sqrt{10+5\sqrt{2}}\cdot\alpha = \sqrt{10+5\sqrt{2}}\cdot\sqrt{10-5\sqrt{2}}$

$\sqrt{(10+5\sqrt{2})(10-5\sqrt{2})} = \sqrt{100-50} = \sqrt{50} =$

(*) erfüllt, da $\sqrt{\alpha\beta} = \sqrt{\alpha}\cdot\sqrt{\beta}\ \forall \alpha,\beta\in\mathbb{R}_+$, falsch

für bel. $\alpha,\beta\in\mathbb{C}$ ebenfalls im Allg. falsch

Nun gilt $\alpha^2 = 10 - 5\sqrt{2} \in \mathbb{Q}(\alpha) \Rightarrow \sqrt{2} = \frac{1}{5}(10-\alpha^2)$

$\Rightarrow \sqrt{10+5\sqrt{2}} = \frac{5\sqrt{2}}{\alpha} \in \mathbb{Q}(\alpha)$ Damit ist gezei

dass mit $\alpha = \sqrt{10-5\sqrt{2}}$ die Elemente der Menge N,

$\pm\sqrt{10\pm5\sqrt{2}}$, alle in $\mathbb{Q}(\alpha)$ liegen $\Rightarrow$ f zerfällt üb

in Linearfaktoren. Außerdem wird $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ von N e

da α in N enthalten ist. ($\Rightarrow$ Beh.)

Auf Grund der Beh. ist $\mathbb{Q}(\alpha) | \mathbb{Q}$ normal, damit a

algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch

separabel, insgesamt also eine Galois-

Erweiterung.

) = 50

zu (c) Da f über $\mathbb{Q}$ irreduzibel ist und α sow

$\beta = \frac{5\sqrt{2}}{\alpha} = \sqrt{10+5\sqrt{2}}$ Nullstellen von f ~~sind~~,

nach dem Fortsetzungssatz ein $\sigma \in G$ mit $\sigma(\alpha) =$

Beh: $\operatorname{ord}(\sigma) = 4$

Da $\mathbb{Q}(\alpha) | \mathbb{Q}$ galoissch ist, gilt $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

$\operatorname{grad}(f) = 4$. Daraus folgt $\operatorname{ord}(\sigma) \mid 4$, also $\operatorname{ord}($

$\{1, 2, 4\}$. Es genügt somit, $\sigma^2 \neq \mathrm{id}_{\mathbb{Q}(\alpha)}$ zu überprüf

$\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\beta) = \sigma\left(\frac{5\sqrt{2}}{\alpha}\right) \underset{\uparrow \sigma\ \mathbb{Q}\text{-Hom}}{=} \frac{5 \cdot \sigma(\sqrt{2})}{\sigma(\alpha)}$

$\beta < 0$ $\quad \sigma(\sqrt{2}) = \sigma\left(\frac{1}{5}(10-\alpha^2)\right) = \frac{1}{5} \cdot (10 - \sigma(\alpha)^2) =$

$\frac{1}{5}(10-\beta^2) = \frac{1}{5}(10-(10+5\sqrt{2})) = -\sqrt{2}$ einsetzen

$$\sigma^2(\alpha) = \frac{5\cdot(-\sqrt{2})}{\beta} = -\frac{5\sqrt{2}}{\beta} = -\alpha$$

$\llcorner\ \alpha\beta = 5\sqrt{2}$

$\neq \alpha \Rightarrow \sigma^2 \neq \mathrm{id}_{\mathbb{Q}(\alpha)}$ ($\Rightarrow$ Beh.)

Wegen $|G| = 4 = \mathrm{ord}(\sigma)$ ist G zyklisch von Ordnung 4, also isomorph zu $\mathbb{Z}/4\mathbb{Z}$.

$\square$

H24T3A4 geg: $f = x^3 + x^2 - 2x - 1$,

$\alpha \in \mathbb{C}$ Nullstelle von f

in (a) gezeigt: $f \mid f(x^2-2)$

in (b) gezeigt: α, $\alpha^2 - 2$ sind verschiedene Nullstellen von f

D

z

it

A

dam

auch

eine

Wie

irred

und

Da

$|G|$

n

$) = \mathcal{S}_n^a$

$\mathbb{Z})^\times$,

atz der

genau

$\square$

t ist

(c) Zeigen Sie, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ galois…
ist, und dass $G = \mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$ isom…
zu $\mathbb{Z}/3\mathbb{Z}$ ist.

Bew. $\mathbb{Q}(\alpha)$ ist Zerfällungskörper von f üb…

Da α, α^2-2 Nullstellen von f sind, sind $x-$…
und $x-\alpha^2+2$ Teiler von f in $\mathbb{Q}(\alpha)[x]$. Wegen …
α^2-2 sind $x-\alpha$ und $x-\alpha^2+2$ teilerfremd, u…
damit $\mathrm{kgV}(x-\alpha, x-\alpha^2+2) = (x-\alpha)(x-\alpha^2+$…
ebenfalls ein Teiler von f in $\mathbb{Q}(\alpha)[x]$. $\Rightarrow$
$\exists\, h \in \mathbb{Q}(\alpha)[x]$ mit $f = (x-\alpha)(x-\alpha^2+2)\cdot h$,
wobei $\mathrm{grad}(h) = \mathrm{grad}(f) - 2 = 3 - 2 = 1$ ist.

$- \alpha$

$\alpha\beta = 5\sqrt{2}$

$)$

zyklisch

zu $\mathbb{Z}/4\mathbb{Z}$.

$\square$

$-2x-1$,

$)$

verschiedene

Dies zeigt, dass f über $\mathbb{Q}(\alpha)$ in Linearfaktoren zerfällt. Außerdem wird $\mathbb{Q}(\alpha)$ von den Nullstellen von f über $\mathbb{Q}$ erzeugt, da α selbst eine Nullst. ist. ($\Rightarrow$ Beh.)

Aus der Beh. folgt, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal ist, damit auch algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel. Insgesamt ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ damit eine Galois-Erweiterung.

Wie in (b) gezeigt wurde, ist f über $\mathbb{Q}$ irreduzibel. Da f außerdem normiert ist und $f(\alpha) = 0$ gilt, folgt $f = \mu_{\alpha,\mathbb{Q}}$.

Da $\mathbb{Q}(\alpha)|\mathbb{Q}$ galoissch ist, erhalten wir $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(\mu_{\alpha,\mathbb{Q}}) = \mathrm{grad}(f) = 3$

...isch
isomorph

f über $\mathbb{Q}$
d $x-\alpha$
Wegen $\alpha \neq$
...end, und
$)(x-\alpha^2+2)$
$[x]. \implies$
$+2)\cdot h$,
$= 1$ ist.

Als Gruppe von Primzahlordnung ist G zyklisch, also wg. $|G|=3$ isomorph zu $\mathbb{Z}/3\mathbb{Z}$. $\square$

Bem: Mit Hilfe der Galoisgruppe kann man die 3. Nullstelle von f berechnen.
f irred. über $\mathbb{Q}$, α, α^2-2 sind Nullst.
$\to \exists\, \sigma \in G$ mit $\sigma(\alpha) = \alpha^2-2$. Da σ ein $\mathbb{Q}$-Hom. ist, muss auch $\sigma^2(\alpha)$ eine Nullst. von f sein. Dabei ist $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha^2-2)$
$= \sigma(\alpha)^2 - 2 = (\alpha^2-2)^2 - 2 = \alpha^4 - 4\alpha^2 + 4 - 2$
$= -\alpha^3 + 2\alpha^2 + \alpha - 4\alpha^2 + 2 = \alpha^2 - 2\alpha - 1 + 2\alpha^2$
$\hat{=}\ f(\alpha)=0$
$\alpha^3 = -\alpha^2 + 2\alpha + 1$ $\quad + \alpha - 4\alpha^2 + 2 = -\alpha^2 - \alpha + 1$

F24T1A4 Übung: H23T1A

H18T2A5 (schwer

Sei p eine Primzahl mit der Eigenschaft
$p-1$ quadratfrei ist, also in der Primfaktor-
legung keine mehrfachen Teiler vorkommen.

(a) Zeigen Sie: Ist $n \in \mathbb{N}$ und $p-1$ Produ
von n verschiedenen Primzahlen $p_1, \ldots, p_n$
dann besitzt $G = (\mathbb{Z}/p\mathbb{Z})^\times$ genau 2^n Un
gruppen.

(b) Sei $\zeta_p = e^{2\pi i/p}$ mit p wie in Teil (a).
Bestimmen Sie die Anzahl der Zwischenkörper von

$2\pi i/p$

<u>Zu (a)</u> Da p eine Primzahl ist, ist $(\mathbb{Z}/$

zyklische Gruppe der Ordnung $p-1$. Di

Untergruppen von $(\mathbb{Z}/p\mathbb{Z})^\times$ stimmt desh

mit der Anzahl der Teiler von $p-1 = p_1 \cdot \ldots$

Teiler dieser Zahl sind die Zahlen der Fo

$p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \ldots \cdot p_n^{\varepsilon_n}$ mit $\varepsilon_1, \ldots, \varepsilon_n \in \{$

Anzahl ist gleich $|\{0,1\}|^n = 2^n$

<u>zu (b)</u> [Erinnerung: Für jede Zahl $n \in$

die Galoisgruppe von $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ mit

isomorph zu $(\mathbb{Z}/n\mathbb{Z})^\times$. Daher erhält

Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, w

ein $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $a \in \mathbb{Z}$, $\mathrm{ggT}(a,n) = 1$ a

Element $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ abbildet, das durch d

definiert ist.]

Sei $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$. Laut Vorlesung ist G isomorph zu

besitzt also ebenfalls genau 2^n Untergruppen. Nach dem Hau

Galoistheorie besitzt die Erweiterung $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ als

2^n Zwischenkörper.

H24T3A5 Sei $\zeta_{16} = e^{\pi i/8}$.

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

Da $\zeta_{16} = e^{2\pi i/16}$ eine primitive 16-te Einheitswurzel und

A24 ISAS Sei $\zeta_{16} = e$

eine

ahl der

iberein

. Die

], deren

, $n \geq 2$ ist

$\zeta_n = e^{2\pi i/n}$

man einen

somit der 16-te Kreisteilungskörper ist, ist $\mathbb{Q}(\zeta_1$

denn lt. Vl. sind alle Kreisteilungskörper normal.

Ist $L|K$ eine Galois-Erw. und M ein Zwischenkö

dann ist auch $L|M$ galoisch. Wegen $\zeta_{16}^4 = e^{\pi i/2} =$

$= i$ ist i in $\mathbb{Q}(\zeta_{16})$ enthalten, und $\mathbb{Q}(i)$ damit ei

von $\mathbb{Q}(\zeta_{16})|\mathbb{Q}$. Also ist auch $\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i)$ galoisch.

Für jedes $n \in \mathbb{N}$ gilt $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$, falls $\zeta_n =$

$\Rightarrow [\mathbb{Q}(\zeta_{16}):\mathbb{Q}] = \varphi(16) = \varphi(2^4) = 2^3 (2-1) = 8$

$\mathbb{Z}\setminus\{0,1\}$ quadratfrei ist, gilt lt. Vl. $[\mathbb{Q}(i):\mathbb{Q}] = [\mathbb{Q}$

Gradformel $\Rightarrow 8 = [\mathbb{Q}(\zeta_{16}):\mathbb{Q}] = [\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] \cdot [\mathbb{Q}$

$[\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] \cdot 2 \Rightarrow [\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] = \frac{8}{2} = 4$