F22T2A5 (Fortsetzung)

geg.: $K_1 = \mathbb{Q}(\sqrt{3})$, $K_2 = \mathbb{Q}(\sqrt{6})$ als Teil-
körper von $\mathbb{C}$

in (a) gezeigt: $L = K_1 K_2$ stimmt überein mit
dem Teilkörper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

in (b) gezeigt: $K_1 \cap K_2 = \mathbb{Q}$

zu (c) ges.: Erweiterungsgrad $[L : \mathbb{Q}]$

Wegen $\sqrt{2} \in L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist $\mathbb{Q}(\sqrt{2})$ ein
Zwischenkörper von $L|\mathbb{Q}$. Gradformel $\Longrightarrow$

A

da

wz

Als

und

$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$ (*)

Da 2 in $\mathbb{Z}\setminus\{0,1\}$ eine quadratfreie Zahl ist, gilt laut Vorlesung $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$.

Es gilt $L=\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$

<u>Beh.</u>: $\mu_{\sqrt{3},\mathbb{Q}(\sqrt{2})} = x^2-3$

Das Polynom $g=x^2-3\in\mathbb{Q}(\sqrt{2})[x]$ ist normiert und erfüllt $g(\sqrt{3})=0$. Ang., g ist in $\mathbb{Q}(\sqrt{2})[x]$ reduzibel. Wegen $\operatorname{grad}(g)=2$ müsste dann die Nullstelle $\sqrt{3}$ von g in $\mathbb{Q}(\sqrt{2})$ liegen.

Als normale Erweiterung ist $L|\mathbb{Q}$ auch algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch separabel.

Aber dies ist nicht der Fall, denn sind $m, n \in \mathbb{Z} \setminus \{0, 1\}$ zwei verschiedene quadratfreie Zahlen, dann gilt lt. Vl. $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$. Wende dies auf $m = 2$, $n = 3$ an. ($\Rightarrow$ Beh.)

Auf Grund der Beh. gilt $[L : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$ $= \mathrm{grad}(g) = 2$. Einsetzen in (*) liefert dann $[L : \mathbb{Q}] =$ $2 \cdot 2 = 4$.

zu (d) (i) z.zg.: $L|\mathbb{Q}$ ist galois'sch

(ii) Bestimmung von $G = \mathrm{Gal}(L|\mathbb{Q})$ bis auf Isomorphie

(Unter (ii) ist gemeint: Man soll eine „naheliegende" Gruppe $\tilde{G}$ angeben, z.B. eine Untergruppe einer symmetrischen Gruppe oder ein Produkt endl. zyklischer Gruppen, die zu G isomorph ist.)

il- mit) ein el $\Rightarrow$

<u>zu (i)</u> z.zg.: $L|\mathbb{Q}$ ist normal und separabel

Für die Eigenschaft „normal" genügt der Nachweis, dass L Zerfällungskörper eines Polynoms $f \in \mathbb{Q}[x] \setminus \mathbb{Q}$ über $\mathbb{Q}$ ist.

Sei $f = (x^2-2)(x^2-3)$. Die Gleichung $f = (x-\sqrt{2})(x+\sqrt{2})\cdot(x-\sqrt{3})\cdot(x+\sqrt{3})$ zeigt, dass f über L in Linearfaktoren zerfällt, denn die Nullstellen $\pm\sqrt{2}, \pm\sqrt{3}$ liegen alle in L.

Außerdem wird L von $N = \{\pm\sqrt{2}, \pm\sqrt{3}\}$ über $\mathbb{Q}$ erzeugt, da L bereits von der Teilmenge $\{\sqrt{2}, \sqrt{3}\} \subseteq N$ erzeugt wird.

Als normale Erweiterung ist $L|\mathbb{Q}$ auch algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch separabel.

zu (ii) Da $L|\mathbb{Q}$ eine Galois-Erw. vom Grad 4 ist, gilt $|G| = 4$. Als Gruppe von Primzahlquadratordnung ist G abelsch. Aus dem Hauptsatz über endliche abelsche Gruppen folgt $G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G = (\mathbb{Z}/2\mathbb{Z})^2$.

Ang. es ist $G \cong \mathbb{Z}/4\mathbb{Z}$. Dann ist G zyklisch, und wegen $|G| = 4$ stimmt die Anzahl der Untergruppen von G überein mit der Anzahl der Teiler von 4. Es gibt also jeweils genau eine Untergr. der Ordnung 1, 2 und 4. Die eind. best. Unter-

der
El
Dara
Ord
$(\bar{1}, \bar{0}$
$\langle(\bar{1}, \bar{1}$
Also
und L
körpe
$K_1 =$
paarwe
$[\mathbb{Q} : \mathbb{Q}]$

gruppe der Ordn. 1 ist $\{id_L\}$, die eind. best. Untergr. der Ordnung 4 ist G. Es gibt also genau eine Untergr. U mit $\{id_L\} \subsetneq U \subsetneq G$, und es ist $|U| = 2$. Aus dem Hauptsatz der Galoistheorie folgt dann, dass die Erweiterung $L|\mathbb{Q}$ genau einen echten Zwischenkörper besitzt.

Aber in Teil (b) wurde gezeigt, dass K_1 und K_2 zwei verschiedene Zwischenkörper von $L|\mathbb{Q}$ sind. Wegen $1 < [K_1:\mathbb{Q}] = [K_2:\mathbb{Q}] = 2 < [L:\mathbb{Q}]$ sind es darüber hinaus echte Zwischenkörper von $L|\mathbb{Q}$. ↯ Also muss

C

zu (

von

Lan

schen

pen

Anza

Wegen

ist jed

einzige

einzige

Da 2 e

eind.
Es
$\{ id_L \}$
Aus dem
dass die
Zwischen-

ss K_1 und
er von $L|\mathbb{Q}$
$] = 2 <$
s echte
o muss

$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gelten. (**)

<u>zu (e)</u> Bestimmen Sie alle Zwischenkörper von $L|\mathbb{Q}$.

Laut Galoistheorie ist die Anzahl der Zwischenkörper gleich der Anzahl der Untergruppen von G, wegen (**) also auch gleich der Anzahl der Untergruppen von $(\mathbb{Z}/2\mathbb{Z})^2$.

Wegen $|(\mathbb{Z}/2\mathbb{Z})^2| = 4$ und dem Satz von Lagrange ist jede Untergr. von Ordnung 1, 2 oder 4.

einzige Untergr. der Ordn. 1: $\{(\bar{0},\bar{0})\}$

einzige Untergr. der Ordn. 4: $(\mathbb{Z}/2\mathbb{Z})^2$

Da 2 eine Primzahl ist, ist jede Untergruppe

...m
...gruppe
...belsch.
... abelsche
... $(\mathbb{Z}/2\mathbb{Z})^2$.
... ist G
...mmt die
... G überein
...t. Es gibt
... der Ord-
...est. Unter-

der Ordnung 2 zyklisch, wird also durch ein Element $(a,b) \in (\mathbb{Z}/2\mathbb{Z})^2$ der Ordnung 2 erzeugt. Daraus folgt, dass es insgesamt drei Untergruppen der Ordnung 2 gibt, nämlich $\langle(\bar{1},\bar{0})\rangle = \{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}$, $\langle(\bar{0},\bar{1})\rangle = \{(\bar{0},\bar{0}),(\bar{0},\bar{1})\}$ und $\langle(\bar{1},\bar{1})\rangle = \{(\bar{0},\bar{0}),(\bar{1},\bar{1})\}$.

Also hat $(\mathbb{Z}/2\mathbb{Z})^2$ genau fünf Untergruppen und $L|\mathbb{Q}$ damit genau fünf Zwischenkörper. Vier davon sind $\mathbb{Q}$, L, $K_1 = \mathbb{Q}(\sqrt{3})$, $K_2 = \mathbb{Q}(\sqrt{6})$. Diese sind paarweise verschieden wegen $K_1 \neq K_2$ und $[\mathbb{Q}:\mathbb{Q}] = 1 < [K_j:\mathbb{Q}] = 2 < [L:\mathbb{Q}] = 4$

für $j = 1,2$. Ein weiterer Zwischenkörper ist $K_3 = \mathbb{Q}(\sqrt{2})$. Dieser ist verschieden von den vier bereits angegebenen, denn wegen $[K_3 : \mathbb{Q}] = 2$ ist $K_3 \neq \mathbb{Q}, L$, und ebenso ist $K_3 \neq K_1, K_2$, da 2 in $\mathbb{Z} \setminus \{0,1\}$ eine quadratfreie, von 3 und 6 verschiedene Zahl ist. Also sind die Zwischenkörper von $L|\mathbb{Q}$ insgesamt geg. durch

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{6}) \text{ und } L = \mathbb{Q}(\sqrt{2}, \sqrt{3}). \qquad \square$$

F22T3A4 Sei K ein Teilkörper von $\mathbb{C}$ mit der Eigenschaft, dass $K|\mathbb{Q}$ galoissch ist, mit einer zyklischen Galoisgruppe der Ordnung 4. Zeigen Sie, dass $i \notin K$ gilt.

Hinweis: Nehmen Sie $i \in K$ an, und betrachten Sie $K|\mathbb{Q}(i)$.

Angenommen, es gilt $i \in K$. Dann ist $\mathbb{Q}(i)$ ein Zwischenkörper von $K|\mathbb{Q}$, und folglich ist $U = \mathrm{Gal}(K|\mathbb{Q}(i))$ eine Untergruppe von $G = \mathrm{Gal}(K|\mathbb{Q})$. Nach Voraussetzung gilt $G \cong \mathbb{Z}/4\mathbb{Z}$, insb. $|G| = 4$. Daraus folgt,

edene
rper

$\neq \mathrm{id}_K$.
ung 2,
der
für
$= i$.
edene
Fest-
bar
$\square$

Hinweis: Nehmen Sie $i \in K$ an, und betrachten Sie $K|\mathbb{Q}(i)$.

Angenommen, es gilt $i \in K$. Dann ist $\mathbb{Q}(i)$ ein Zwischenkörper von $K|\mathbb{Q}$, und folglich ist $U = \mathrm{Gal}(K|\mathbb{Q}(i))$

dass G genau eine Untergruppe der Ordnung 2 besitzt.

Es ist $[\mathbb{Q}(i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{-1}):\mathbb{Q}] = 2$, denn lt. Vl gilt $[\mathbb{Q}(\sqrt{m}):\mathbb{Q}] = 2$ für jedes quadratfreie $m \in \mathbb{Z} \setminus \{0,1\}$, also insb. für $m = -1$. Laut Galoistheorie folgt daraus $(G:U) = 2$, und damit $|U| = \frac{|G|}{(G:U)} = \frac{4}{2} = 2$. Auf Grund unserer Annahme wäre U also die einzige Untergruppe der Ordnung 2 von G.

Die Einschränkung der komplexen Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ liefert einen $\mathbb{Q}$-Hom. $\iota : K \to \mathbb{C}$, und weil $K|\mathbb{Q}$ normal ist, gilt darüber hinaus $\iota \in \mathrm{Aut}_{\mathbb{Q}}(K)$, also $\iota \in G$. Wegen $\iota^2(\alpha) = \iota(\iota(\alpha)) = \iota(\bar{\alpha}) = \bar{\bar{\alpha}} = \alpha$

Zahl ist. Also sind die Zwischenkörper von $L|\mathbb{Q}$ insgesamt geg. durch

für alle $x \in K$ gilt $\iota^2 = \mathrm{id}_K$, wegen $i \in K$ und $\iota(i) = -i \neq i$ andererseits $\iota \neq \mathrm{id}_K$. Also ist ι in G ein Element der Ordnung 2, und $\langle \iota \rangle$ somit eine Untergruppe von G der Ordnung 2. Dabei gilt $U \neq \langle \iota \rangle$, denn für jedes σ in $U = \mathrm{Gal}(K|\mathbb{Q}(i))$ gilt $\sigma(i) = i$. Die Gruppe G enthält also zwei verschiedene Untergr. der Ordnung 2, im Widerspruch zur Feststellung von oben. Die Annahme $i \in K$ war also falsch. $\square$

F24T1A5 Sei $\alpha = \sqrt{10-5\sqrt{2}} \in \mathbb{R}$.

(a) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}$.

$\alpha = \sqrt{10-5\sqrt{2}} \Rightarrow \alpha^2 = 10-5\sqrt{2} \Rightarrow$
$\alpha^2 - 10 = -5\sqrt{2} \Rightarrow (\alpha^2-10)^2 = (-5\sqrt{2})^2$
$\Rightarrow \alpha^4 - 20\alpha^2 + 100 = 50 \Rightarrow \alpha^4 - 20\alpha^2 + 50 = 0 \Rightarrow$ α ist Nullstelle des Polynoms $f = x^4 - 20x^2 + 50 \in \mathbb{Q}[x]$. Dieses Polynom ist normiert und außerdem irreduzibel nach dem Eisenstein-Kriterium, angewendet auf die Primzahl 2. Daraus folgt insgesamt, dass

$\mu_{\alpha,\mathbb{Q}} = f = x^4 - 20x^2 + 50$ das gesuchte Minimalpolynom ist.

Übung: H15T2A5

$\sqrt{2})^2$

$\alpha^2 + 50$

oms

Polynom

$\mathbb{Q}$ nach

auf die

samt, dass