

H25T2 A3 geg: $f = x^4 + 1 \in \mathbb{Q}[x]$

$L \subseteq \mathbb{C}$ Zerf.-korp. von f über $\mathbb{Q}$

gezeigt in Teil (a): $L = \mathbb{Q}(\sqrt{2}, i)$

(b) Zeigen Sie, dass $L|\mathbb{Q}$ genau drei Teilkörper vom Grad 2 hat, und geben Sie diese explizit an.

Die Erweiterung $L|\mathbb{Q}$ ist galois'sch, denn:

- Weil L Zerfällungskörper eines Polynoms über $\mathbb{Q}$ ist, ist die Erweiterung $L|\mathbb{Q}$ normal.
- Als normale Erweiterung ist $L|\mathbb{Q}$ auch algebraisch und wegen $\text{char}(\mathbb{Q}) = 0$ damit auch separabel.

$\mathbb{Q}[x]$

(1)

rei Teil-
en Sei diese

den:
mons über $\mathbb{Q}$
al.

auch alge-
ramt auch separabel

Sei $G = \text{Gal}(L/\mathbb{Q})$. Da L Zerf.-korp.
eines Polynoms über $\mathbb{Q}$ ist, ist $L/\mathbb{Q}$
endlich und G damit auch eine end-
liche Gruppe, wobei $|G| = [L:\mathbb{Q}]$.

Beh: $[L:\mathbb{Q}] = 4$ (nicht ausgeführt,
Übung)

Also ist $|G| = 4$. Als Gruppe der Ord-
nung 4 ist G isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu
 $(\mathbb{Z}/2\mathbb{Z})^2$. Ang. $G \cong \mathbb{Z}/4\mathbb{Z}$. Dann wäre
 G zyklisch, und zu jedem Teiler $d \in \mathbb{N}$ von 4 gäbe
es genau eine Untergr. der Ordnung d . Insb. gäbe
es genau eine Untergruppe $U \leq G$ der Ordnung 2,

wegen
eine Unt-
Hauptsat-
 L^U der
über $\mathbb{Q}$.
 $= 2$ (ne-
Beh. geze-
wegen $\mathbb{Q}$
 $L/\mathbb{Q}$ mind-
↯ Also
jede Untergr.
in G) ist

$\mathbb{Z}/4\mathbb{Z}$ -Korp.
 ist $L/\mathbb{Q}$
 eine end-
 $= [L:\mathbb{Q}]$
 ausgeführt,
 Gruppe der Ord-
 $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z}$
 $\mathbb{Z}/4\mathbb{Z}$. Dann wäre
 aber die $\mathbb{N}$ von 4 gäbe
 Ordnung d. Insb. gäbe
 $H \leq G$ der Ordnung 2,

wegen $(G:H) = \frac{|G|}{|H|} = \frac{4}{2} = 2$ auch genau
 eine Untergruppe vom Index 2. Nach dem
 Hauptsatz der Galoistheorie wäre dann
 L^H der einzige Zwischenkörper vom Grad 2
 über $\mathbb{Q}$. aber: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(i):\mathbb{Q}]$
 $= 2$ (nehme an, dass das beim Bew. der
 Beh. gezeigt wurde) und $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(i)$
 wegen $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, $i \in \mathbb{Q}(i)$, $i \notin \mathbb{R}$. Also hat
 $L/\mathbb{Q}$ mind. zwei Zwischenkorp. vom Grad 2 über $\mathbb{Q}$.
 $\hookrightarrow$ Also muss $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ gelten.
 Jede Untergr. der Ordnung 2 in $(\mathbb{Z}/2\mathbb{Z})^2$ (und
 in G) ist zyklisch, da 2 Primzahl ist. Sie

wird also
 erzeugt.
 Ordnung
 also:
 $= \text{Anzahl}$
 Die einzige
 $(1, 0)$,
 Ordnung
 gesehen, an
 den Zwischen
 gibt also

nach genau

2. Nach dem

wäre dann

der vom Grad 2

$$] = [Q(i):Q]$$

im Bew. der

$$(\sqrt{2}) \neq Q(i)$$

$i \notin \mathbb{R}$. Also hat

in Grad 2 über Q .

$\mathbb{Z}/2\mathbb{Z}$ gelten.

$(\mathbb{Z}/2\mathbb{Z})^2$ (und
Anzahl ist. Sie

Wird also jeweils durch ein Ekt. der Ordn. 2
erzeugt. Umgekehrt enthält jede Unterg. der
Ordnung 2 genau ein Ekt. der Ordn. 2.

also: Anzahl der Unterg. der Ordn. 2
= Anzahl der Ekt. der Ordn. 2

Die einzigen Ekt. der Ordn. 2 sind $(0,1)$,
 $(1,0)$, $(1,1) \Rightarrow$ 7 genau drei Unterg. der
Ordnung 2 in $(\mathbb{Z}/2\mathbb{Z})^2$ und in G . Wie oben
gesehen, entsprechen die Unterg. der Ordn. 2 bijektiv
den Zwischenkorp. M von $L|Q$ mit $[M:Q] = 2$. Es
gibt also genau drei solche Zw. korp. Zwei davon sind

$$Q(\sqrt{2})$$

Bestim

Sei α

und i

$$[Q(\sqrt{2})$$

Mit i

also $\mathbb{C}$

Beh:

(Daraus

genau die

und der

$\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$.

Bestimmung des dritten Körpers:

Sei $\alpha = i\sqrt{2} = \sqrt{-2}$. $f = x^2 + 2$ ist normiert und irred., erfüllt $f(\alpha) = 0$. $\Rightarrow$

$$[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = \text{grad}(f) = 2.$$

Mit $i, \sqrt{2} \in L$ gilt auch $\alpha = i\sqrt{2} \in L$, also ist auch $\mathbb{Q}(\alpha)$ ein Zw.körp. von $L|\mathbb{Q}$.

Beh.: $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\alpha) \neq \mathbb{Q}(i)$
(Daraus folgt dann, dass $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\alpha)$ genau die Zwischenkörp. von $L|\mathbb{Q}$ vom Grad 2 sind, und deren Anzahl genau 3 ist.)

Die erste Ungl. folgt aus $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$
und $\alpha \in \mathbb{Q}(\alpha)$, $\alpha \notin \mathbb{R}$. Analog, es ist

$$\mathbb{Q}(\alpha) = \mathbb{Q}(i) \Rightarrow \alpha, i \in \mathbb{Q}(i)$$

$$\Rightarrow \sqrt{2} = \frac{\alpha}{i} \in \mathbb{Q}(i), \text{ insg. } \sqrt{2}, i \in$$

$$\subseteq \mathbb{Q}(i) \Rightarrow L = \mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(i)$$

$$\text{Gradformel} \Rightarrow [L: \mathbb{Q}] \text{ teilt } [\mathbb{Q}(i): \mathbb{Q}]$$

$$\swarrow \text{ da } [L: \mathbb{Q}] = 4, [\mathbb{Q}(i): \mathbb{Q}] = 2, 4 \nmid 2$$



F23T1A3

)
primatives Ele-
ment $\mathbb{Q}$

$$\Rightarrow i = \frac{i\sqrt{5}}{\sqrt{5}}$$

$$\mathbb{Q}(N) \Rightarrow$$

$$c) \sqrt{5} + i \in$$

$$\in \mathbb{Q}(\sqrt{5} + i), \text{ wobei}$$

$$i = \frac{1}{6}(\sqrt{5} - 1) \Rightarrow$$

$$i + \frac{1}{2}(\sqrt{5} - 1) = \sqrt{5} \in \mathbb{Q}(i)$$

Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von
 $f = x^4 - 25$ über $\mathbb{Q}$.

(a) Zeigen Sie, dass jedes irreduzible
Faktor von f separabel über $\mathbb{Q}$ ist.

Wegen $\text{char}(\mathbb{Q}) = 0$ ist jedes irreduzible
Polynom in $\mathbb{Q}[x]$ separabel, insb. die ir-
reduziblen Faktoren von f .

(b) Bestimmen Sie ein primitives Element
der Erweiterung $L/\mathbb{Q}$.

$$f = (x^2 - 5)(x^2 + 5) = (x + \sqrt{5})(x - \sqrt{5}) \cdot$$

$$(x - i\sqrt{5})(x + i\sqrt{5}) \Rightarrow L = \mathbb{Q}(N), \text{ wobei}$$

h $\sqrt{5}$, i

von $\mathbb{Q}(X)$ unter

Erweiterung

eine Galois-
Aufgabe

es gilt $\mathbb{Q}(N)$

$\subseteq \mathbb{Q}(N)$ und
nicht ausgeführt.
ist gleich 4

$$N = \{1 \pm \sqrt{5}, \pm i\sqrt{5}\} \text{ ist}$$

$$\text{Beh: } \mathbb{Q}(N) = \mathbb{Q}(\sqrt{5} + i)$$

(d.h. $\alpha = \sqrt{5} + i$ ist ein primitives Ele-
ment der Erweiterung $L | \mathbb{Q}$)

$$\text{"} \supseteq \text{" } \sqrt{5}, i\sqrt{5} \in \mathbb{Q}(N) \Rightarrow i = \frac{i\sqrt{5}}{\sqrt{5}}$$

$$\in \mathbb{Q}(N) \Rightarrow \sqrt{5} + i \in \mathbb{Q}(N) \Rightarrow \\ \mathbb{Q}(\sqrt{5} + i) \subseteq \mathbb{Q}(N)$$

$$\text{"} \subseteq \text{" z.zg.: } N \subseteq \mathbb{Q}(\sqrt{5} + i) \quad \sqrt{5} + i \in$$

$$\mathbb{Q}(\sqrt{5} + i) \Rightarrow (\sqrt{5} + i)^{-1} \in \mathbb{Q}(\sqrt{5} + i), \text{ wobei}$$

$$(\sqrt{5} + i)^{-1} = \frac{\sqrt{5} - i}{(\sqrt{5} + i)(\sqrt{5} - i)} = \frac{1}{6}(\sqrt{5} - i) \Rightarrow$$

$$\sqrt{5} - i \in \mathbb{Q}(X) \Rightarrow \frac{1}{2}(\sqrt{5} + i) + \frac{1}{2}(\sqrt{5} - i) = \sqrt{5} \in \mathbb{Q}(X)$$

F23T

Sei L

$$f = x^4$$

(a) Zer

Fakt

Wegen d

Polynom

reduzible

(b) Bestm
der Er

$$f = (x^2 - 5$$

$$(x - i\sqrt{5})$$

$\Rightarrow (\sqrt{5}+i) - \sqrt{5} = i \in \mathbb{Q}(N)$ Aus $\sqrt{5}, i \in \mathbb{Q}(N)$ folgt $N \subseteq \mathbb{Q}(N)$ (Abg. von $\mathbb{Q}(N)$ unter Multiplikation).

(c) Berechnen Sie die Automorphismengruppe von L über $\mathbb{Q}$.

Zunächst zeigen wir, dass $L|\mathbb{Q}$ eine Galois-erweiterung ist. (Das geht wie in Aufgabe H25T2A3, lassen wir aus.) Es gilt $\mathbb{Q}(N) = \mathbb{Q}(\sqrt{5}, i)$. (Man muss $\sqrt{5}, i \in \mathbb{Q}(N)$ und $N \subseteq \mathbb{Q}(\sqrt{5}, i)$ gilt, auch das wird nicht ausgeführt. Der Erweiterungsgrad von $L|\mathbb{Q}$ ist gleich 4 (zeigt man wie oben).)

n muss auch
 ein. Wenden
 e $x^2 - 5$ und
 $\in \{\pm\sqrt{5}\}$ und
 (L) Betrachte
 $\rightarrow \{\pm\sqrt{5}\} \times \{\pm i\}$
 $L = \mathbb{Q}(\sqrt{5}, i)$ ist
 $(\sqrt{5}, i)$ eindeu-
 also injektiv.
 $\{\pm i\}$ ist surjektiv.
 s. σ von $\text{Aut } \mathbb{Q}(L)$
 durch

Weil $L/\mathbb{Q}$ galois'sch ist, gilt

$$|\text{Aut}_{\mathbb{Q}}(L)| = |\text{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4.$$

Wie in H25T2A3 leitet man aus der
 Existenz der beiden Zwischenkörper $\mathbb{Q}(\sqrt{5})$
 und $\mathbb{Q}(i)$ von $L/\mathbb{Q}$ ab, dass $\text{Aut}_{\mathbb{Q}}(L) =$
 $\text{Gal}(L/\mathbb{Q})$ isomorph zu $(\mathbb{Z}/2\mathbb{Z})^2$ ist.

Möglicherweise ist die Aufgabenstellung so
 gemeint, dass nicht nur der Isomorphietyp von
 $\text{Aut}_{\mathbb{Q}}(L)$, sondern auch die Elemente dieser Gruppe
 angeg. werden sollen. In diesem Fall gehen wir
 folgendermaßen vor:

Allgemein gilt: Ist $g \in \mathbb{Q}[x]$, $\sigma \in \text{Aut}_{\mathbb{Q}}(L)$ und

$$\sigma_3 = -\sqrt{5},$$

$$\sigma_3(i) = -i$$

$$= -i. \text{ (Es ist}$$

$$\sigma_2 \text{ und } \sigma_4$$

enkörper von
konjug.

et man zunächst,
(L) genau drei Un-
stet, und demen-
vom Grad 2 über $\mathbb{Q}$
 $\mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(i)$ herleitet.

$x \in L$ Nullstelle von g , dann muss auch
 $\sigma(x)$ eine Nullstelle von g sein. Wenden
wir dies auf die Polynome $x^2 - 5$ und
 $x^2 + 1$ an, so folgt $\sigma(\sqrt{5}) \in \{\pm\sqrt{5}\}$ und
 $\sigma(i) \in \{\pm i\} \forall \sigma \in \text{Aut}_{\mathbb{Q}}(L)$. Betrachte
nun die Abb. $\phi: \text{Aut}_{\mathbb{Q}}(L) \rightarrow \{\pm\sqrt{5}\} \times \{\pm i\}$,
 $\sigma \mapsto (\sigma(\sqrt{5}), \sigma(i))$. Wegen $L = \mathbb{Q}(\sqrt{5}, i)$ ist
jedes $\sigma \in \text{Aut}_{\mathbb{Q}}(L)$ durch $\sigma(\sqrt{5}), \sigma(i)$ eindeu-
tig bestimmt, die Abbildung also injektiv.
Wegen $|\text{Aut}_{\mathbb{Q}}(L)| = 4 = |\{\pm\sqrt{5}\} \times \{\pm i\}|$ ist surjektiv.
Die vier Elemente $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ von $\text{Aut}_{\mathbb{Q}}(L)$
sind also eindeutig bestimmt durch

Weil L
 $|\text{Aut}_{\mathbb{Q}}(L)|$
Wie in H
Existenz
und $\mathbb{Q}(i)$
 $\text{Gal}(L|\mathbb{Q})$
Möglicherweise
generiert, das
 $\text{Aut}_{\mathbb{Q}}(L)$, s
angeg. wird
folgendermaßen
Allgemein g

$$\sigma_1(\sqrt{5}) = \sqrt{5}, \sigma_1(i) = i, \sigma_2(\sqrt{5}) = -\sqrt{5},$$

$$\sigma_2(i) = i, \sigma_3(\sqrt{5}) = \sqrt{5}, \sigma_3(i) = -i$$

$$\text{bzw. } \sigma_4(\sqrt{5}) = -\sqrt{5}, \sigma_4(i) = -i. (\text{Es ist}$$

leicht zu sehen, dass $\sigma_1 = \text{id}_L$ und σ_4
 $= \sigma_2 \sigma_3 = \sigma_3 \sigma_2$ gilt.)

(b) Bestimmen Sie alle Zwischenkörper von
 $L/\mathbb{Q}$ sowie deren Inklusionen.

Wie bei H25T2A3 begründet man zunächst,
 dass $G = \text{Gal}(L/\mathbb{Q}) = \text{Aut}_{\mathbb{Q}}(L)$ genau drei Un-
 tergruppen der Ordnung zwei besitzt, und demzu-
 folge genau drei Zwischenkörper vom Grad 2 über $\mathbb{Q}$
 existieren, wobei es sich um $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i\sqrt{5})$ und $\mathbb{Q}(i)$ handelt.

Sei nun K ein bel. Zwischenkörper von $L|\mathbb{Q}$. Gradformel
 $\Rightarrow 4 = [L:\mathbb{Q}] = [L:K] \cdot [K:\mathbb{Q}] \Rightarrow [K:\mathbb{Q}] \mid 4 \Rightarrow$

$[K:\mathbb{Q}] \in \{1, 2, 4\}$. Im Fall $[K:\mathbb{Q}] = 2$ gilt

$K \in \{\mathbb{Q}(\sqrt{5}), \mathbb{Q}(i\sqrt{5}), \mathbb{Q}(i)\}$, und $K = \mathbb{Q}$ im Fall $[K:\mathbb{Q}] = 1$.

Im Fall $[K:\mathbb{Q}] = 4$ ist $[L:K] = 1$ und $K = L$.

Auf Grund der unterschiedlichen Grade gilt $L, \mathbb{Q} \notin \{\mathbb{Q}(\sqrt{5}), \mathbb{Q}(i\sqrt{5}), \mathbb{Q}(i)\}$ und $L \neq \mathbb{Q}$. Insgesamt hat $L|\mathbb{Q}$ also genau 5 verschiedene Zwischenkörper.

Allgemein gilt: Sind M, K beides Zwischenkörper von $L|\mathbb{Q}$ mit $K \subsetneq M$, dann gilt auf Grund der Gradformel $[M:\mathbb{Q}] = [M:K] \cdot [K:\mathbb{Q}]$, also $[K:\mathbb{Q}] \mid [M:\mathbb{Q}]$. Im Fall $[K:\mathbb{Q}] = [M:\mathbb{Q}]$

□

folgt $[M:K] = 1$ und $M = K$ $\Downarrow$ Also muss
 $[K:\mathbb{Q}]$ ein echter Teiler von $[M:\mathbb{Q}]$ sein. Daraus
folgt, dass neben den trivialen Inklusionen $K \subseteq K$ für
die Zwischenkörper nur die Inklusionen $\mathbb{Q} \subseteq K$ für
 $K \in \{\mathbb{Q}(\sqrt{5}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{5})\}$, $K \subseteq L$ für $K \in \{\mathbb{Q}(\sqrt{5}), \mathbb{Q}(i),$
 $\mathbb{Q}(i\sqrt{5})\}$ und $\mathbb{Q} \subseteq L$ möglich sind. Dass $\mathbb{Q}$ in jedem Zwischen
körper liegt, ist offensichtlich, da jeder der Körper nach Def.
Erweiterung von $\mathbb{Q}$ ist. Die übrigen Inklusionen ergeben sich
aus $\sqrt{5}, i, i\sqrt{5} \in L$. $\square$