Aufgabe 9 der Probeklausur

Sei $f \in \mathbb{Q}[X]$ normiert und separabel, seien $x_1, \dots, x_n$ die (alle) Nullstellen von f. Sei $\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_4)$ zyklisch von Ordnung 4.

Behauptung. *Die Gleichung*

$$X^2 + 1 = 0$$

besitzt keine Lösung in $K := \mathbb{Q}(x_1, \dots, x_4)$.

Beweis (Ausarbeitung der Lehrstuhllösung). Zunächst eine Vorüberlegung: Das Polynom f ist nicht nur separabel, sondern auch irreduzibel. Denn da die Galoisgruppe der Nullstellen von f nach Voraussetzung zyklisch ist, gilt insbesondere, dass die Wirkung der Galoisgruppe transitiv auf den Nullstellen ist (d. h., dass es für alle $1 \leq i, j \leq 4$ eine Symmetrie σ der Galoisgruppe mit $\sigma(i) = j$ gibt). Somit sind aber alle vier Nullstellen zueinander galoisch konjugiert. (Denn: Zwei Zahlen aus K sind genau dann zueinander galoisch konjugiert, wenn es eine Symmetrie der Galoisgruppe gibt, die bei Multiplikation mit ihr die eine Zahl auf die andere abbildet.) Das geht nur, wenn f irreduzibel ist.

Insbesondere ist somit klar, dass f das gemeinsame Minimalpolynom der x_i ist, und dass die x_i jeweils vom Grad 4 über $\mathbb{Q}$ sind. Außerdem ist klar, dass x_1 ein primitives Element der x_i ist, denn es gilt:

$$\left.\begin{aligned} &\mathbb{Q}(x_1) \subseteq \mathbb{Q}(x_1, \dots, x_4) \\ &[\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_1, \dots, x_4) : \mathbb{Q}] = 4 \end{aligned}\right\} \quad \Rightarrow \quad \mathbb{Q}(x_1) = \mathbb{Q}(x_1, \dots, x_4)$$

Die beiden Lösungen der Gleichung sind i und $-i$. Würde K eine dieser beiden Zahlen enthalten, dann auch die andere, da K als Körper unter Negativenbildung abgeschlossen ist.

Eine weitere Vorüberlegung: Eine der Nullstellen x_i muss nicht-reell sein. Denn wären alle Nullstellen reell, so wäre K eine Teilmenge von $\mathbb{R}$ und würde somit sicher nicht i enthalten. Ohne Beschränkung der Allgemeinheit sei x_1 eine der nicht-reellen Nullstellen.

Nun zum Hauptteil des Beweises, wir nehmen die Widerspruchsannahme an, dass i ein Element von K ist. Wir müssen irgendwie die spezielle Voraussetzung an die Galoisgruppe ausnutzen; unser Plan dazu, ist, den Hauptsatz der Galoistheorie zu verwenden!

Es ist nämlich klar, dass (unter der Widerspruchsannahme) $\mathbb{Q}(i)$ eine Zwischenerweiterung von K ist,

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq K,$$

wobei natürlich $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ gilt.

Somit ist $\mathrm{Gal}_{\mathbb{Q}(i)}(x_1, \dots, x_4)$ eine Untergruppe von $\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_4)$ vom Index 2. Man weiß nun, dass die Gruppe $\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_4)$ genau eine Untergruppe vom Index 2 besitzt, da sie zyklisch ist.

[Denn: Wir können $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_4)$ schreiben als $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_4) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, wobei σ ein (nach Voraussetzung existenter) Erzeuger von $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_4)$ ist. Die einzige Untergruppe von Ordnung 2 ist dann $\{\mathrm{id}, \sigma^2\}$.]

Nach dem Hauptsatz der Galoistheorie gibt es somit auch nur eine Zwischenerweiterung von $\mathbb{Q}(x_1, \ldots, x_4)$ vom Grad 2.

Wir werden nun folgende Strategie verfolgen: Etwas unmotiviert werden wir eine weitere Zwischenerweiterung L vom Grad 2 konstruieren. Da es nur eine solche Zwischenerweiterung gibt, muss dann $L = \mathbb{Q}(i)$ gelten; von L wird aber klar sein, dass L die Zahl i nicht enthält, womit dann der Widerspruch erreicht ist.

Dazu betrachten wir nun zunächst das Minimalpolynom $g \in \mathbb{Q}(i)[X]$ von x_1 über $\mathbb{Q}(i)$. Nach der Vorüberlegung ist klar, dass g Grad 2 hat, denn es gilt mit der Gradformel

$$4 = [\mathbb{Q}(x_1, \ldots, x_4) : \mathbb{Q}] = [\mathbb{Q}(x_1, \ldots, x_4) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(x_1) : \mathbb{Q}(i)].$$

Damit können wir auch das Polynom f in einer anderen Form angeben, es gilt nämlich:

$$f(X) = g(X) \cdot \overline{g(X)}$$

Das hat folgenden Grund: Das Produkt $g\overline{g}$ ist normiert, hat nur rationale Koeffizienten, besitzt x_1 als Nullstelle und hat denselben Grad (nämlich 4) wie das Minimalpolynom von x_1 über $\mathbb{Q}$ (also f). Daraus folgt schon, dass $g\overline{g}$ das Minimalpolynom von x_1 ist.

Somit ist klar, dass die Zahl $\overline{x_1}$ eine weitere Nullstelle von f ist. (Sie ist nämlich eine Nullstelle vom Faktor $\overline{g}$.)

Wir definieren nun

$$L := \mathbb{Q}(x_1 + \overline{x_1}, x_1\overline{x_1})$$

und zeigen:

a) L ist eine Zwischenerweiterung von K.

b) L hat Index 2 in K.

c) L enthält nicht i.

Damit ist der Beweis dann abgeschlossen, denn wegen der oben angesprochenen Eindeutigkeit muss L gleich $\mathbb{Q}(i)$ sein, da es nur eine Zwischenerweiterung vom Grad 2 gibt. Somit gilt $i \in \mathbb{Q}(i) = L$ im Widerspruch zu c).

a) Da $\overline{x_1}$ auch eine der vier Nullstellen von f ist, sind die Zahlen $x_1 + \overline{x_1}$ und $x_1\overline{x_1}$ Elemente von L.

c) Klar, denn da $x_1 + \overline{x_1}$ und $x_1\overline{x_1}$ beides reelle Zahlen sind (die erste ist einfach der doppelte Realteil von x_1, die zweite das Quadrat des Betrags von x_1), gilt $L \subseteq \mathbb{R}$.

b) Es ist $(X - x_1)(X - \overline{x_1}) = X^2 - (x_1 + \overline{x_1}) + x_1\overline{x_1}$ das Minimalpolynom von x_1 über L. Denn es ist normiert, hat Koeffizienten nur aus L und ist irreduzibel. Irreduzibel ist es deswegen, da es keine Nullstellen in L besitzt (da es ein Polynom vom Grad 2 ist, ist diese Schlussweise ja zulässig): Denn $x_1 \in \mathbb{C} \setminus \mathbb{R}$, während $L \subseteq \mathbb{R}$.

Somit folgt mit der Gradformel aus

$$4 = [\mathbb{Q}(x_1, \ldots, x_4) : \mathbb{Q}] = [\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_1) : L] \cdot [L : \mathbb{Q}] = 2 \cdot [L : \mathbb{Q}]$$

in der Tat, dass $[L : \mathbb{Q}] = 2$ gilt. □