

Bemerkung zu Aufgabe 4.2.

Satz:

Seien $p_1, \dots, p_r$ paarweise verschiedene Primzahlen.

Dann gilt:

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}) : \mathbb{Q}] = 2^r.$$

Beweis:

Definiere

$$K_i := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_i}) \quad 1 \leq i \leq r$$

$$K_0 := \mathbb{Q}.$$

Genügt zu zeigen: $[K_{i+1} : K_i] = 2 \quad \forall 0 \leq i < r. \quad (*)$

Dann folgt aus dem Gradsatz:

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}) : \mathbb{Q}] = [K_r : K_{r-1}] \cdot \dots \cdot [K_1 : K_0] = 2^r.$$

Um $(*)$ zu zeigen, genügt es

$$\sqrt{p_{i+1}} \notin K_i \quad \forall 0 \leq i < r \quad (**)$$

zu zeigen. Denn dann ist für ein i mit $0 \leq i < r$

$$X^2 - p_{i+1} \in K_i[X]$$

irreduzibel, also aus Gradgründen das Minimalpolynom von $\sqrt{p_{i+1}}$ über K_i und damit $(*)$ gezeigt.

Um (**) zu zeigen führen wir eine (endliche) Induktion nach i . Die Behauptung $B(i)$ ist für $0 \leq i < r$:

$$\underline{B(i)}: \left[\begin{array}{l} \text{Sind } j_1, \dots, j_s \in \mathbb{N} \text{ mit} \\ i < j_1 < \dots < j_s \leq r \\ \text{gegeben, so ist } \sqrt{p_{j_1} \dots p_{j_s}} \notin K_i. \end{array} \right.$$

Beachte: Ist $B(i)$ für ein i richtig, dann erhalten wir insbesondere für $s=1$ und $j_1=i+1$:

$$\sqrt{p_{i+1}} \notin K_i$$

also auch $[K_{i+1} : K_i] = 2$ (vgl. Vorüberlegungen).

Zur Induktion:

- Induktionsanfang: $i=0$.

Seien $j_1, \dots, j_s$ die Zahlen aus $B(0)$. Betrachte

$$X^2 - p_{j_1} \dots p_{j_s} \in \mathbb{Q}[X] = K_0[X].$$

Eisenstein (z.B. mit $p=p_{j_1}$) und Gauß liefern Irreduzibilität dieses Polynoms.

$$\Rightarrow \sqrt{p_{j_1} \dots p_{j_s}} \notin \mathbb{Q} = K_0.$$

ok.

- Induktionsschritt: „ $(i-1) \rightarrow i$ “ und es gelte $i < r$.

↗ $\exists$ Indizes $j_1, \dots, j_s$ mit $i < j_1 < \dots < j_s \leq r$ und
 $\sqrt{p_{j_1} \dots p_{j_s}} \in K_i$.

Nach Konstruktion: $K_i = K_{i-1}(\sqrt{p_i}) = K_{i-1}[\sqrt{p_i}]$

$$\text{I.V.: } [K_i : K_{i-1}] = 2 \Rightarrow \{a + b\sqrt{p_i} \mid a, b \in K_{i-1}\}$$

$\Rightarrow \exists \alpha, \beta \in K_{i-1}$ mit

$$\sqrt{p_{j_1} \dots p_{j_s}} = \alpha + \beta \sqrt{p_i}$$

$$\Rightarrow p_{j_1} \dots p_{j_s} = \alpha^2 + \beta^2 p_i + 2\alpha\beta \sqrt{p_i}$$

$\Rightarrow 2\alpha\beta = 0$, d.h. $\alpha = 0$ oder $\beta = 0$.

- Ist $\alpha = 0$, dann: $p_i p_{j_1} \dots p_{j_s} = \beta^2 p_i^2$

$$\Rightarrow \sqrt{p_i p_{j_1} \dots p_{j_s}} = \beta \cdot p_i \in K_{i-1} \quad \text{⚡}$$

$B_{(i-1)}$ mit Indizes
 $(i-1) < i < j_1 < \dots < j_s \leq r$.

- Ist $\beta = 0$, dann:

$$\sqrt{p_{j_1} \dots p_{j_s}} = \alpha \in K_{i-1} \quad \text{⚡}$$

$B_{(i-1)}$ mit Indizes
 $(i-1) < j_1 < \dots < j_s \leq r$.

In jedem Fall ergibt sich ein Widerspruch. $\Rightarrow B_{(i)}$ gilt.

Anwendung:

$$(i) \left. \begin{array}{l} [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 2^3 \\ [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2^2 \end{array} \right\} \Rightarrow \sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

(ii) Können sogar zeigen, dass in der Situation aus dem Satz gilt:

$$\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}) / \mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^r.$$