Lösung 10

Lösbarkeit durch Radikale, Norm

1. Zeigen Sie, dass $L|\mathbb{Q}$ eine radikale Körpererweiterung ist.

   (a) $L = \mathbb{Q}(\sqrt[5]{1+\sqrt{3}})$

   (b) $L = \mathbb{Q}(\sqrt[3]{1-\sqrt{5}}, \sqrt[7]{\sqrt{2}+\sqrt{3}})$

2. Sei $E|K$ eine endliche Galoiserweiterung mit Galoisgruppe $G := \mathrm{Gal}(E|K)$. Für $x \in E$ ist die *Norm* N von x als

$$N(x) := \prod_{\sigma \in G} \sigma(x)$$

   definiert. Zeigen Sie, dass

   (a) $N(E) \subset K$, und

   (b) $N(xy) = N(x)N(y)$.

   Berechnen Sie N für $E = \mathbb{Q}(i)$ und $E = \mathbb{Q}(\sqrt{2})$ als Körpererweiterungen von $K = \mathbb{Q}$.

3. Zeigen Sie, dass die folgenden Gleichungen durch Radikale lösbar sind (ohne diese zu lösen):

   (a) $X^4 - 2X^2 - 21 = 0$,

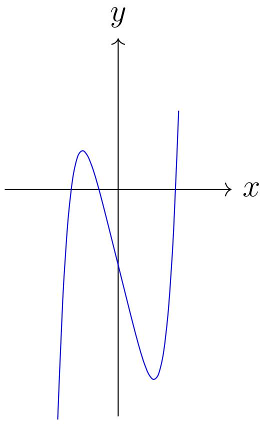
   (b) $X^6 - 2X^3 - 2 = 0$.

4. Zeigen Sie, dass $X^5 - p^2X - p \in \mathbb{Q}[X]$ mit p prim nicht durch Radikale lösbar ist.

   Lösung: Wir wollen Theorem 2.20 verwenden, um die Galoisgruppe des Polynoms auszurechnen. Das Polynom hat grad 5 (prim) und ist irreduzibel nach Eisenstein mit der Primzahl p. Damit genügt es zu zeigen, dass $X^5 - p^2X - p$ genau drei reelle Nullstellen hat. Die Ableitung ist $5X^4 - p^2$ und hat damit genau zwei reelle Nullstellen, nämlich $\pm\sqrt[4]{\frac{p^2}{5}}$ (die anderen zwei Nullstellen sind $\pm i\sqrt[4]{\frac{p^2}{5}}$). Die zweite Ableitung ist $20X^3$ und damit hat das Polynom bei $\sqrt[4]{\frac{p^2}{5}}$ ein lokales Minimum, bei $-\sqrt[4]{\frac{p^2}{5}}$ ein lokales Maximum und bei $X = 0$ einen Wendepunkt. Der Wendepunkt liegt bei $(0,-p)$. Damit reicht es zu zeigen, dass der Wert am lokalen Maximum positiv ist. Wir haben

$$\left(-\sqrt[4]{\frac{p^2}{5}}\right)^5 + p^2\sqrt[4]{\frac{p^2}{5}} - p = -\frac{p^2}{5}\frac{\sqrt{p}}{\sqrt[4]{5}} + p^2\frac{\sqrt{p}}{\sqrt[4]{5}} - p = p\left(\frac{4p\sqrt{p}}{5\sqrt[4]{5}} - 1\right),$$

und damit genügt es zu zeigen, dass $p\sqrt{p} > \frac{5\sqrt[4]{5}}{4} \approx 1,869$. Dies gilt für alle Primzahlen p, da es für 2 gilt und der Ausdruck auf der linken Seite monoton steigend ist, der rechte jedoch konstant in p. Damit sieht der Graph von $X^5 - p^2X - p$ in etwa so aus: Nach dem Zwischenwertsatz gibt es daher genau 3 reelle Nullstellen.



Damit ist gezeigt, dass die Galoisgruppe von $X^5 - p^2X - p$ isomorph zu S_5 ist, und S_5 ist nicht auflösbar. Das bedeutet, dass das Polynom nicht durch Radikale lösbar ist.

5. Zeigen Sie, dass die Galoisgruppe von

$$f(X) = (X^2+4)(X-2)(X-4)\cdots(X-2(p-2)) + 2 \in \mathbb{Q}(X)$$

mit p prim gleich S_p ist.

Lösung: Wir wollen wieder Theorem 2.20 verwenden. Wir bemerken zunächst, dass f Grad p hat. Nach Eisenstein mit $q = 2$ ist f irreduzibel, da der konstante Term genau $4(-2)^{p-2}(p-2)! + 2$ ist und damit nicht durch 4 teilbar. Wir müssen nun nur noch zeigen, dass f genau $p-2$ reelle Nullstellen hat um zu schliessen, dass die Galoisgruppe isomorph zu S_p ist. Dazu bemerken wir, dass f an den Stellen $X = 1, 3, 5, \ldots, 2(p-2)+1$ abwechselnd negative und positive Werte annimmt. Bei Werten kleiner als 1 ist f immer negativ, bei Werten grösser als $2(p-2)+1$ immer positiv. Dazwischen müssen daher reelle Nullstellen liegen nach dem Zwischenwertsatz. Da es genau $p-2$ Wechsel der Vorzeichen gibt, haben wir genau $p-2$ reelle Nullstellen gefunden.

6. (Hilbert 90) Angenommen $E|K$ ist eine (endliche) Galoiserweiterung mit $G := \mathrm{Gal}(E|K)$ zyklisch. Sei $\sigma \in G$ ein Erzeuger. Zeigen Sie, dass $N(u) = 1$ genau dann, wenn ein $z \in E^\times$ existiert mit $z\sigma(z)^{-1} = u$.

   Hinweis für $\Longrightarrow$: Sei $G = \{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\}$. Definieren Sie $\delta_0, \delta_1, \ldots, \delta_{n-1}$, so dass $\sigma(\delta_i) = u^{-1}\delta_{i+1}$ für $0 \leqslant i \leqslant n-2$ und $\delta_{n-1} = 1$. Wählen Sie $y \in E$ und definieren Sie $z := \delta_0 y + \delta_1\sigma(y) + \ldots + \delta_{n-1}\sigma^{n-1}(y)$.

   Lösung: Ist $z \in E^\times$ mit $z\sigma(z)^{-1} = u$, so ist

$$N(u) = N(z)N(\sigma(z^{-1})) = N(z)N(z^{-1}) = 1.$$

   Für die andere Richtung verwenden wir den Hinweis. Wir bemerken zuerst, dass u nicht Null ist, da $N(u) = 1$, und damit invertierbar. Wir definieren $\delta_{n-1} := 1$ und $\delta_i := \sigma^{n-1}(u^{-1})\sigma^{n-1}(\delta_{i+1})$. Dann gilt $\sigma(\delta_i) = \sigma^n(u^{-1})\sigma^n(\delta_{i+1}) = u^{-1}\delta_{i+1}$. Als geschlossene Form geschrieben erhalten wir für alle $0 \leqslant i \leqslant n-1$

$$\delta_i := \prod_{j=1}^{n-i-1} \sigma^{n-j}(u^{-1}).$$

   Wir berechnen

$$\delta_0 = \prod_{j=1}^{n-1} \sigma^{n-j}(u^{-1}) = \prod_{j=1}^{n-1} \sigma^{j}(u^{-1}) = u\prod_{j=0}^{n-1} \sigma^{j}(u^{-1}) = uN(u^{-1}) = u,$$

   da $N(u) = N(u^{-1}) = 1$. Für $y \in E$ sei $z(y) := \delta_0 y + \delta_1\sigma(y) + \ldots + \delta_{n-1}\sigma^{n-1}(y)$. Damit haben wir

$$\begin{aligned} u\sigma(z(y)) &= u\sigma(\delta_0 y + \delta_1\sigma(y) + \ldots + \delta_{n-1}\sigma^{n-1}(y)) \\ &= u(u^{-1}\delta_1\sigma(y) + u^{-1}\delta_2\sigma^2(y) + \ldots + u^{-1}\delta_{n-1}\sigma^{n-1}(y) + u^{-1}uy) \\ &= \delta_0 y + \delta_1\sigma(y) + \ldots + \delta_{n-1}\sigma^{n-1}(y) = z(y). \end{aligned}$$

   Wir müssen noch zeigen, dass ein $y \in E$ existiert mit $z(y) \neq 0$ ist (dies ist dann das gesuchte $z \in E^\times$). Aber dies folgt aus dem Satz von Dedekind (Prop. IV-5), da $z(y)$ eine Linearkombination der Potenzen von σ ist, und diese linear unabhängig sind, und somit $z(y)$ nicht die Nullabbildung ist. Damit existiert $y \in E$ existiert mit $z := z(y) \neq 0$ und $z\sigma(z)^{-1} = u$.