Musterlösung 28

Auflösbare Körpererweiterungen

1. Sei $p > 11$ eine Primzahl. Zeige, dass die Gleichung $X^5 - pX + p = 0$ über $\mathbb{Q}$ nicht durch Radikale auflösbar ist.

   Lösung: Sei $f(X) = X^5 - pX + p \in \mathbb{Q}[X]$. Wir untersuchen den Graphen von f, aufgefasst als Funktion $\mathbb{R} \to \mathbb{R}$, mithilfe von Methoden aus der Analysis I. Die erste Ableitung $f'(X) = 5X^4 - p$ hat genau zwei reelle Nullstellen, nämlich $\pm\sqrt[4]{\frac{p}{5}}$. Es gilt $f\left(\sqrt[4]{\frac{p}{5}}\right) < 0$ und $f\left(-\sqrt[4]{\frac{p}{5}}\right) > 0$. Weitere lokale Extrema gibt es nicht, daher hat f genau drei reelle und zwei nichtreelle Nullstellen. Also folgt aus Serie 24 Aufgabe 3, dass die Galoisgruppe von f gleich S_5 ist. Da diese Gruppe nicht auflösbar ist, folgt mit dem Satz von Abel-Ruffini, dass f nicht durch Radikale auflösbar ist.

2. Seien $\varepsilon, \delta \in \{\pm 1\}$. Zeige, dass jedes Polynom $f \in \mathbb{Q}[X]$ vom Grad $n \leqslant 9$ mit der Eigenschaft $f(X) = \varepsilon X^n f(\delta X^{-1})$ auflösbar durch Radikale ist. (Vergleiche Serie 24 Aufgabe 5.)

   Lösung: Die Voraussetzung impliziert, dass der konstante Koeffizient von f gleich $\pm$ dem höchsten Koeffizienten ist; insbesondere ist er ungleich null. Also ist jede Nullstelle $\alpha \in \mathbb{C}$ von f ungleich null. Weiter ist die Abbildung $\varphi\colon \alpha \mapsto \delta\alpha^{-1}$ eine Permutation der Menge der Nullstellen mit $\varphi^2 = \mathrm{id}$, welche zudem die Multiplizität der Nullstellen erhält.

   Wird eine Nullstelle α_0 auf sich abgebildet, so erfüllt diese die Gleichung $\alpha_0^2 = \delta$. Im Fall $\delta = 1$ ist dann $\alpha_0 \in \{\pm 1\}$ und somit $f(X) = (X - \alpha_0) \cdot g(X)$ für ein Polynom $g \in \mathbb{Q}[X]$ vom Grad $n-1$. Dieses erfüllt

   $$g(X) = \frac{f(X)}{X - \alpha_0} = \frac{\varepsilon X^n f(X^{-1})}{-\alpha_0 X(X^{-1} - \alpha_0)} = -\frac{\varepsilon}{\alpha_0} \cdot X^{n-1} g(X^{-1}),$$

   also die entsprechende Eigenschaft. Da f und g denselben Zerfällungskörper haben, genügt es, die Aussage für g anstatt f zu beweisen.

   Im Fall $\delta = -1$ ist $\{\alpha_0, \overline{\alpha_0}\} = \{\pm i\}$, und beides sind Nullstellen von f. Somit ist $f(X) = (X^2+1) \cdot g(X)$ für ein Polynom $g \in \mathbb{Q}[X]$ vom Grad $n-2$. Dieses erfüllt

   $$g(X) = \frac{f(X)}{X^2+1} = \frac{\varepsilon X^n f(-X^{-1})}{X^2(X^{-2}+1)} = \varepsilon X^{n-2} g(-X^{-1}),$$

also wieder die entsprechende Eigenschaft. Ist $K \subset \mathbb{C}$ der Zerfällungskörper von g, so ist $K(i) \subset \mathbb{C}$ der Zerfällungskörper von f. Somit ist letzterer auflösbar über $\mathbb{Q}$, wenn ersterer es ist, und es genügt wieder, die Aussage für g anstatt f zu beweisen.

Durch Induktion über den Grad können wir uns damit auf den Fall reduzieren, dass die Abbildung $\varphi\colon \alpha \mapsto \delta\alpha^{-1}$ keine Nullstelle festlässt. Dann ist n gerade, und die komplexen Nullstellen sind Paare α_k, $\delta\alpha_k^{-1}$ für $1 \leqslant k \leqslant m := n/2$. Die Rechnung

$$\frac{f(X)}{X^m} = \prod_{k=1}^{m} \frac{(X-\alpha_k)(X-\delta\alpha_k^{-1})}{X} = \prod_{k=1}^{m} \Big(X + \delta X^{-1} - \alpha_k - \delta\alpha_k^{-1} \Big)$$

zeigt nun, dass $f(X) = X^m \cdot h(X + \delta X^{-1})$ ist für ein Polynom h vom Grad m. Da f Koeffizienten in $\mathbb{Q}$ hat, gilt dies auch für h. Wegen $n \leqslant 9$ ist jetzt aber $m \leqslant 4$ und folglich h auflösbar durch Radikale. Die Nullstellen von f ergeben sich dann aus den Nullstellen β_k von h durch Lösen der Gleichung $X + \delta X^{-1} = \beta_k$, welche zu der quadratischen Gleichung $X^2 - \beta_k X + \delta = 0$ äquivalent ist. Sie sind somit durch Radikale über dem Zerfällungskörper von h ausdrückbar, und deshalb ist auch f durch Radikale auflösbar.

3. Sei $f(X)$ ein normiertes Polynom vom Grad 3 in einer Variablen mit reellen Koeffizienten ohne mehrfache Nullstellen, und sei Δ seine Diskriminante. Zeige:

   (a) Es gilt $\Delta > 0$, falls alle Nullstellen von f reell sind, andernfalls $\Delta < 0$.

   (b) Falls f genau eine reelle Nullstelle hat, so enthält die Lösungsformel dafür nur reelle Quadrat- und dritte Wurzeln.

   (c) Im Gegensatz dazu erfordert die Lösungsformel ausgerechnet dann eine dritte Wurzel aus einer nicht-reellen komplexen Zahl, wenn f drei reelle Nullstellen hat (*“Casus irreducibilis”*).

   *(d) Versuche zu erklären, wieso der Umstand aus (c) unvermeidbar ist, also weshalb die Nullstellen von f, selbst wenn sie reell sind, im Allgemeinen nicht mit reellen Radikalen ausgedrückt werden können.

Lösung: (a) Seien x_1, x_2, x_3 die Nullstellen von f. Falls x_1, x_2, x_3 reell sind, so ist

$$\Delta = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 > 0.$$

Hat f andererseits nicht-reelle Nullstellen, so ist genau eine Nullstelle reell, und die anderen beiden sind zueinander komplex konjugiert. Sei ohne Beschränkung der Allgemeinheit x_1 die reelle Nullstelle. Dann ist

$$\begin{aligned} \Delta &= (x_1 - x_2)^2 (x_1 - \overline{x_2})^2 (x_2 - \overline{x_2})^2 \\ &= \underbrace{\Big((x_1 - x_2)\overline{(x_1 - x_2)} \Big)^2}_{|x_1 - x_2|^4} \underbrace{(x_2 - \overline{x_2})^2}_{-4\,\mathrm{Im}(x_2)^2} < 0. \end{aligned}$$

(b) und (c): Verwende die Notationen aus der Vorlesung. Laut Vorlesung ist die Lösungsformel für kubische Gleichungen gegeben durch

$$y_i = \zeta^i \cdot \sqrt[3]{q - \sqrt{-\frac{1}{4 \cdot 27}\Delta}} + \zeta^{-i} \cdot \sqrt[3]{q + \sqrt{-\frac{1}{4 \cdot 27}\Delta}}.$$

Wir sehen, dass unter der dritten Wurzel genau dann eine reelle Zahl steht, wenn $\Delta < 0$ gilt. Dies ist mit (a) genau dann der Fall, wenn f genau eine reelle Nullstelle hat.

(d) Nehmen wir an, dass eine allgemeine Lösungsformel für den Fall (c) existiert, welche nur reelle Wurzeln enthält. Dann gilt diese Formel insbesondere dann, wenn f irreduzibel über einem gegebenen Unterkörper $K \subset \mathbb{R}$ ist, was wir also nun annehmen. Die Formel bedeutet, dass ein Radikalturm

$$K \subset K_0 := K(\sqrt{\Delta}) \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R}$$

existiert mit $x_1, x_2, x_3 \in K_n$. Dabei können wir ohne Beschränkung der Allgemeinheit annehmen, dass jedes $K_i = K_{i-1}(\sqrt[p_i]{\alpha_i})$ ist für eine Primzahl p_i und ein $\alpha_i \in K_{i-1}$. Sei m minimal, sodass eine der Nullstellen x_ν in K_m liegt. Da f irreduzibel über K ist, gilt $x_\nu \notin K_0$ und somit $m \geqslant 1$. Da dann keine der drei Nullstellen von f in K_{m-1} liegt, ist f wegen $\deg f = 3$ irreduzibel über K_{m-1}. Wegen $[K_m/K_{m-1}]$ prim und $K_{m-1}(x_\nu) \subset K_m$ folgt dann $K_{m-1}(x_\nu) = K_m$, das heisst, K_m ist ein Stammkörper von f über K_{m-1}. Aber wir wissen bereits, dass $K_0(x_\nu) = K(\sqrt{\Delta}, x_\nu)$ alle drei Nullstellen von f enthält. Daher gilt das Gleiche für K_m, und somit ist K_m ein Zerfällungskörper von f über K_{m-1}. Er ist also galoissch vom Grad 3 über K_{m-1}. Nach Konstruktion gilt nun aber $K_m = K_{m-1}(\sqrt[3]{\alpha_m})$ mit $\alpha_m \in K_{m-1}$, wobei $X^3 - \alpha_m \in K_{m-1}[X]$ irreduzibel ist und somit insbesondere $\alpha_m \neq 0$. Da K_m normal über K_{m-1} ist, muss er also auch die anderen beiden Nullstellen von $X^3 - \alpha_m$ enthalten, das heisst, die beiden nicht reellen dritten Wurzeln aus α_m, im Widerspruch zu $K_m \subset \mathbb{R}$.