# 1 Lösungen

## 1.1 Aufgabe 1

Sei $L/K$ eine Körpererweiterung vom Grad $p$ und $p$ prim. Dann gilt für $\alpha \in L \setminus K$ die Aussage $K(\alpha) = L$.
Der Körper $L(\alpha)$ ist ein Zwischenkörper der Erweiterung $L/K$, deshalb gilt nach dem Gradsatz

$$p = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] .$$

Nun ist $K(\alpha) \neq K$ also $[K(\alpha) : K] > 1$. Daraus folgt dann, weil $p$ prim ist, dass $[K(\alpha) : K] = p$ gelten muss. Also $[L : K(\alpha)] = 1$, woraus sofort $L = K(\alpha)$ folgt.

## 1.2 Aufgabe 2

Seien $K \subset L \subset M$ Körper, $M$ algebraisch über $K$ und $\alpha \in M$.
**Behauptung:** $\deg_L(\alpha) \leq \deg_K(\alpha)$
Es ist $\deg_L(\alpha) = \deg Irr(\alpha, L)$ der Grad des Minimalpolynoms von $\alpha$ über $L$. Dieses Existiert, da auch die Erweiterung $M/L$ algebraisch ist.
Angenommen $\deg_L(\alpha) > \deg_K(\alpha)$. Nun sei $f \in K[X]$ das Minimalpolynom von $\alpha$ über $K$. Wir fassen $f$ als Polynom über $L$ auf. Das Polynom $f$ hat $\alpha$ als Nullstelle und kleineren Grad als das Minimalpolynom von $\alpha$ über $L$. Das ist ein Widerspruch.

## 1.3 Aufgabe 3

Sei $\alpha$ algebraisch über $\mathbb{Q}$. Wir zeigen, dass $\overline{\alpha}$ ebenfalls algebraisch über $\mathbb{Q}$ ist.
Eine Zahl $\alpha \in \mathbb{C}$ ist genau dann algebraisch über $\mathbb{Q}$, wenn es ein rationales Polynom $f$ positiven Grades gibt mit $f(\alpha) = 0$.
Nun gilt aber $0 = \overline{0} = \overline{f(\alpha)} = f(\overline{\alpha})$ also ist auch $\overline{\alpha}$ algebraisch über $\mathbb{Q}$.
Nach Satz 14.8.2 sind Summen und Produkte von algebraischen Elementen wieder algebraisch, also ist $\frac{1}{2}(\alpha + \overline{\alpha}) = Re(\alpha)$ algebraisch über $\mathbb{Q}$.
Da $\alpha \cdot \overline{\alpha}$ algebraisch über $\mathbb{Q}$ ist (14.8.2), gibt es ein rationales Polynom $g = \sum_{k=0}^{n} c_k X^k$ mit $g(\alpha \cdot \overline{\alpha}) = 0$.
Sei $\tilde{g} := \sum_{k=0}^{n} c_k X^{2k}$, dann ist $\tilde{g}(\sqrt{\alpha \cdot \overline{\alpha}}) = 0$, also ist $|\alpha| = \sqrt{\alpha \cdot \overline{\alpha}}$ algebraisch über $\mathbb{Q}$.

## 1.4 Aufgabe 4

Seien $K \subset L$ Körper und $\phi : L \to L$ ein Körperautomorphismus, der $K$ fix lässt. Wir zeigen, dass das Minimalpolynom von $\alpha$ über $K$ und das Minimalpolynom $\phi(\alpha)$ über $K$ übereinstimmen.

Sei $f = \sum_{k=0}^{n} c_n X^n$ das Minimalpolynom von $\alpha$ über $K$, dann gilt

$$0 = \phi(0) = \phi(f(\alpha)) = \phi(\sum_{k=0}^{n} c_n \alpha^n) = \sum_{k=0}^{n} \phi(c_n)\phi(\alpha)^n = \sum_{k=0}^{n} c_n \phi(\alpha)^n = f(\phi(\alpha))$$

und damit teilt $f$ das Minimalpolynom von $\phi(\alpha)$ (Satz 14.5.b). Das Minimalpolynom von $\phi(\alpha)$ ist aber irreduzibel (14.5.a) und damit müssen die beiden normierten Polynome übereinstimmen.

## 1.5 Aufgabe 5

Wir betrachen $q = X^9 - X \in \mathbb{F}_3[X]$. Es gilt

$$\begin{aligned} q &= X(X^8 - 1) = X(X^4 - 1)(X^4 + 1) = X(X^2 - 1)(X^2 + 1)(X^4 + 1) \\ &= X(X - 1)(X + 1)(X^2 + 1)(X^4 + 1) \end{aligned}$$

Die Polynome $X, X - 1$ und $X + 1$ sind irreduzibel (das sind Polynome von Grad 1 nämlich immer), die Polynome $X^2 + 1$ und $X^4 + 1$ haben keine Nullstellen in $\mathbb{F}_3$. Damit ist zumindest das erste Polynom irreduzibel (,weil sein Grad kleiner gleich 3 ist). Das Polynom $X^4 + 1$ lässt sich, wenn es reduzibel ist nur als Produkt von zwei Polynomen vom Grad 2 schreiben (diese sind dann automatisch irreduzibel, weil $X^4 + 1$ sonst eine Nullstelle hätte).
Wir wählen den Ansatz $X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d)$. Man erhält hieraus $X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$.

Wir betrachten nun zwei Wahlen eines $\mathbb{F}_3$-irreduzblen Grad zwei Polynoms $p$ zur Dartellung von $\mathbb{F}_9 \cong \mathbb{F}_3/(p)$,

1. Sei $p = X^2 - X - 1$. Setze $\alpha := \overline{X} \in \mathbb{F}_3[X]/(p)$. Dann ist $\alpha$ ein Erzeuger von $\mathbb{F}_9^\times$:

$$\begin{aligned} \alpha^2 &= \alpha + 1 \\ \alpha^3 &= \alpha^2 + \alpha = 2\alpha + 1 = -\alpha + 1 \\ \alpha^4 &= -\alpha^2 + \alpha = -1 \\ \alpha^5 &= -\alpha \\ \alpha^6 &= -\alpha^2 = -\alpha - 1 \\ \alpha^7 &= -\alpha^2 - \alpha = \alpha - 1 \\ \alpha^8 &= \alpha^2 - \alpha = 1 \end{aligned}$$

   Damit ist also $\mathbb{F}_3[X]/(p) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^7\}$.
   Die Bahnen des Frobeniusautomorphimus $F : x \mapsto x^3$ sind (beachte $\alpha^8 = 1$):

$$\{0\}, \{1\}, \{2\}, \{\alpha, \alpha^3\}, \{\alpha^2, \alpha^6\}, \{\alpha^5, \alpha^7\}$$

Wir rechnen nun

$$\begin{aligned}(X-\alpha)(X-\alpha^3) &= X^2-(\alpha+\alpha^3)X+\alpha^4 = X^2+X-1\\ (X-\alpha^2)(X-\alpha^6) &= X^2-(\alpha^2+\alpha^6)X+\alpha^8 = X^2+1\\ (X-\alpha^5)(X-\alpha^7) &= X^2-(\alpha^5+\alpha^7)X+\alpha^{12} = X^2-X-1\end{aligned}$$

2. Sei $p = X^2+1$. Setze $\beta := \overline{X} \in \mathbb{F}_3[X]/(p)$. Dann ist $\beta^2 = -1$, also $\beta$ kein Erzeuger von $\mathbb{F}_9^\times$, aber $1+\beta$ ist einer: Die Folge der ersten acht Potenzen von $(1+\beta)$ ist

$$1+\beta, -\beta, 1-\beta, 2, 2-\beta, \beta, \beta-1, 1$$

Die Bahnen des Frobeniushoms sind wieder die drei Elemente des Fixkörpers $\{0\},\{1\},\{2\}$ zusammen mit den drei Bahnen der Länge zwei, die den Nullstellenmengen der $\mathbb{F}_3$-irreduziblen Grad zwei Polynome entsprechen:

$$\{\beta,-\beta\},\{1+\beta,1-\beta\},\{2+\beta,2-\beta\}.$$