Übungsblatt 8

Aufgabe 1

a) Gibt es einen Körper mit 6 Elementen?

b) Gibt es einen Körper K und ein lineares Gleichungssystem über K, welches genau 6 Lösungen besitzt?

c) Gibt es einen Körper K und ein lineares Gleichungssystem über K, welches genau 9 Lösungen besitzt?

Aufgabe 2

Seien p eine Primzahl, $n \in \mathbb{N}_{\geq 1}$ und K ein Körper mit p^n Elementen.

a) Zeigen Sie, dass $\operatorname{char} K = p$ gilt.

b) Bestimmen Sie die Ordnung des Frobenius-Automorphismus $\sigma : a \mapsto a^p$ von K in der Gruppe der bijektiven Abbildungen von K nach K.

Aufgabe 3

Sei $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ der kleinste Teilkörper von $\mathbb{C}$, welcher $\sqrt{2}$ und $\sqrt{3}$ enthält.

a) Zeigen Sie, dass die Elemente $1, \sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ über $\mathbb{Q}$ linear unabhängig sind.

b) Zeigen Sie, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\,;\, a, b, c, d \in \mathbb{Q}\}$ gilt, und geben Sie zu jedem Element $w = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})^\times$ das Inverse w^{-1} als Linearkombination von $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ an.

c) Zeigen Sie, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ gilt.

Aufgabe 4

Sei $p > 2$ eine Primzahl, sei $\zeta = e^{\frac{2\pi i}{p}}$, und sei $\varepsilon = (-1)^{\frac{p-1}{2}}$. Wir wollen einsehen, dass $\mathbb{Q}(\zeta)$ eine Quadratwurzel von εp enthält:

$$\mathbb{Q}(\sqrt{\varepsilon p}) \subseteq \mathbb{Q}(\zeta)\ .$$

Setzen Sie hierzu $f = 1 + X + X^2 + \cdots + X^{p-1} \in \mathbb{Q}[X]$, und lösen Sie die folgenden Teilaufgaben:

a) Bestimmen Sie den Grad von $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$, und zeigen Sie, dass f über $\mathbb{Q}(\zeta)$ die Linearfaktorzerlegung

$$f(X) = \prod_{i=1}^{p-1} (X - \zeta^i)$$

besitzt.

b) Folgern Sie aus Teil a), dass in $\mathbb{Q}(\zeta)$ die Gleichungen

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i) \quad \text{und} \quad \prod_{1 \leq i \neq j \leq p-1} (\zeta^i - \zeta^j) = \prod_{i=1}^{p=1} f'(\zeta^i)$$

gelten. (Bitte wenden.)

c) Zeigen Sie, dass in $\mathbb{Q}(\zeta)$ die Gleichungen

$$p\zeta^{i(p-1)} = (\zeta^i - 1) \cdot f'(\zeta^i)$$

gelten, für $1 \leq i \leq p-1$. Hinweis: Verwenden Sie die Gleichung $X^p - 1 = (X-1) \cdot f(X)$.

d) Verwenden Sie die Resultate aus b) und c), um in $\mathbb{Q}(\zeta)$ die Gleichung

$$p^{p-1} = p \prod_{1 \leq i \neq j \leq p-1} (\zeta^i - \zeta^j)$$

zu zeigen. Verifizieren Sie ferner in $\mathbb{Q}(\zeta)$ die Gleichung

$$\prod_{1 \leq i \neq j \leq p-1} (\zeta^i - \zeta^j) \;=\; \varepsilon \left(\prod_{i<j} (\zeta^i - \zeta^j) \right)^2 .$$

Folgern Sie aus diesen beiden Gleichungen, dass εp in $\mathbb{Q}(\zeta)$ eine Quadratwurzel besitzt.