Serie 13

KÖRPERERWEITERUNGEN (ABGABE BIS 19.02.2021)

1. Sei K ein Körper und $f \in K[X]$ mit $\deg(f) > 0$. Sei L der Zerfällungskörper von f über K. Zeigen Sie, dass $[L : K] \leqslant \deg(f)!$.

2. (a) Sei K ein Körper der Charakteristik $\neq 2$ und $L|K$ eine Körpererweiterung vom Grad 2. Zeigen Sie, dass $\alpha \in L$ existiert, so dass $\alpha^2 \in K$ und $L = K(\alpha)$. Was ist das Minimalpolynom von α über K?

   (b) Sei K ein Körper der Charakteristik 2, und sei $L|K$ eine Körpererweiterung. Zeigen Sie, dass $[L : K] = 2$ genau dann, wenn $L = K(a)$ für ein $a \in L \setminus K$ mit $a^2 \in K$ oder $a^2 + a \in K$.

   (c) Sei $L = K(\alpha)$ eine Körpererweiterung über einem Körper K, so dass $[L : K]$ ungerade ist. Zeigen Sie, dass $L = K(\alpha^2)$.

3. (a) Finden Sie für die folgenden Werte von $\alpha \in \mathbb{C}$ das Minimalpolynom von α über $\mathbb{Q}$.

   i. $\alpha = \frac{1}{2}(1 + \sqrt{5})$,

   ii. $\alpha = \sqrt{2 + \sqrt[3]{2}}$,

   iii. $\alpha = \lambda + i\lambda$, mit $\lambda \in \mathbb{R}_{>0}$, $\lambda^4 = 5$,

   iv. $\alpha = \sqrt{3} - \sqrt[3]{3}$. *Hinweis:* Betrachten Sie $(\alpha - \sqrt{3})^3$.

   (b) Sei K ein Körper und x ein Element eines Erweiterungskörpers von K, so dass x transzendent über K ist. Zeigen Sie, dass x^n für jedes $n \geqslant 1$ transzendent über K ist, und es gilt $[K(x) : K(x^n)] = n$.

4. Sei F ein endlicher Körper. Wir nennen $x \in F$ ein Quadrat in F, falls $y \in F$ existiert mit $y^2 = x$.

   (a) Angenommen $\operatorname{char}(F) = 2$. Zeigen Sie, dass jedes Element von F ein Quadrat in F ist.

   (b) Nun nehmen wir an, dass $\operatorname{char}(F) = p \geqslant 3$. Sei

   $$S = \{\alpha \in F \mid \exists\, b \in F : \alpha = b^2\} \text{ und } S' = S \setminus \{0\}.$$

   Zeigen Sie, dass S' ist eine Untergruppe vom Index 2 in $F^\times$ und, dass $2 \cdot |S| > |F|$. *Hinweis:* Die Abbildung $x \mapsto x^2$ von $F^\times$ ist nicht injektiv.

   (c) Folgern Sie, dass für jeden endlichen Körper F, jedes Element in F als Summe von Quadraten in F geschrieben werden kann.

(d) Sei $F = \mathbb{F}_p$ mit $p \geqslant 3$. Zeigen Sie, dass $-1 \in \mathbb{F}_p$ ein Quadrat in $\mathbb{F}_p$ ist, genau dann, wenn $p \equiv 1 \pmod 4$.

5. (a) Zeigen Sie, dass das Polynom $P = X^3 + 3X + 3$ irreduzibel in $\mathbb{F}_5[X]$ ist.
   (b) Sei α eine Nullstelle von P in einem algebraischen Abschluss L von $\mathbb{F}_5$ und $\mathbb{F}_{125} = \mathbb{F}_5(\alpha)$. Berechnen Sie die Matrix des Frobeniusautomorphismus' $\varphi : \mathbb{F}_{125} \to \mathbb{F}_{125}$ in der Basis $(1, \alpha, \alpha^2)$.
   (c) Schreiben Sie das Element $\beta = \frac{1}{1-\alpha} \in \mathbb{F}_{125}$ als eine $\mathbb{F}_5$-Linearkombination von 1, α und α^2.
   (d) Zeigen Sie, dass α ein Erzeuger der zyklischen Gruppe $\mathbb{F}_{125}^\times$ ist.

6. Sei $L|K$ eine endliche Körpererweiterung.
   (a) Für $x \in L$, zeigen Sie, dass die Abbildung $M_x : L \to L$, $y \mapsto xy$ K-linear ist.
   (b) Zeigen Sie, dass die Abbildung $r_{L|K} : L \to \mathrm{End}_K(L)$, $x \mapsto M_x$ ein Ringhomomorphismus ist.
   (c) Betrachten Sie die Abbildungen

$$\begin{aligned} \mathrm{Tr}_{L/K} &: L \to K,\ x \mapsto \mathrm{Tr}(M_x), && \text{(Spurabbildung)} \\ \mathrm{N}_{L/K} &: L \to K,\ x \mapsto \det(M_x). && \text{(Normabbildung)} \end{aligned}$$

   Zeigen Sie, dass $\mathrm{Tr}_{L/K}$ K-linear ist und, dass $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$ für alle $x, y \in L$ und $\mathrm{N}_{L/K}(x) = 0$ genau dann, wenn $x = 0$.
   (d) Seien $L_1|L_2|K$ iterierte endliche Körpererweiterungen. Zeigen Sie, dass

$$\mathrm{Tr}_{L_1/K} = \mathrm{Tr}_{L_2/K} \circ \mathrm{Tr}_{L_1/L_2}\,.$$

   Hinweis: Beschreiben Sie eine K-Basis von L_1 durch eine K-Basis von L_2 und eine L_2-Basis of L_1. Evaluieren Sie anschliessend die rechte Seite an $\alpha \in L_1$.
   (e) Zeigen Sie, dass falls $x \in L$ mit $L = K(x)$ und Minimalpolynom

$$X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in K[X],$$

   dann ist $\mathrm{Tr}_{L/K}(x) = -a_{d-1}$ und $\mathrm{N}_{L/K}(x) = (-1)^d a_0$.
   Hinweis: $(1, x, \ldots, x^{d-1})$ ist eine K-Basis of L.
   (f) Sei p eine Primzahl. Sei $\zeta := e^{\frac{2\pi i}{p}} \in \mathbb{C}$ und betrachten Sie das Polynomial

$$f := \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1 \in \mathbb{Q}[X].$$

   Zeigen Sie, dass f irreduzibel ist und folgern Sie, dass $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Der Körper $\mathbb{Q}(\zeta)$ heisst der *p-te Kreisteilungskörper*.
   Sei nun p ungerade und $K = \mathbb{Q}(\zeta)$. Berechnen Sie $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta)$, $\mathrm{N}_{K/\mathbb{Q}}(\zeta)$ und $\mathrm{N}_{K/\mathbb{Q}}(\zeta - 1)$.