Lösung 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 $a \in L \smallsetminus K$ 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 $\mathrm{char}(F) = 2$. Zeigen Sie, dass jedes Element von F ein Quadrat in F ist.

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

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

   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.

Lösung: Im Folgenden bezeichen wir die Elemente von $\mathbb{F}_5$ mit den ganzen Zahlen mit $5 = 0$.

(a) Da das Polynom $P \in \mathbb{F}_5[X]$ Grad 3 hat, hat jede echte Faktorisierung von P einen lineare Faktor. Das heisst P ist irreduzibel genau dann, wenn P keine Nullstelle in $\mathbb{F}_5$ hat. Da $P(0) = 3$, $P(1) = 2$, $P(2) = 2$, $P(3) = 4$ und $P(4) = 4$, folgern wir, dass P keine Nullstelle in $\mathbb{F}_5$ hat, und damit ist P irreduzibel in $\mathbb{F}_5$.

(b) Da α eine Nullstelle von P ist, haben wir

$$\begin{aligned} \alpha^3 &= -3\alpha - 3 = 2(\alpha + 1) \text{ and} \\ (\alpha + 1)^3 &= \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3(\alpha^2 + 1), \end{aligned}$$

was impliziert, dass

$$\alpha^9 = -\alpha^2 - 1.$$

Um die Matrix von $\varphi : x \mapsto x^5$ bezüglich der Basis $(1, \alpha, \alpha^2)$ zu berechnen, wobei α eine Nullstelle von P ist, schreiben wir die Bilder von 1, α und α^2 unter φ als $\mathbb{F}_5$-Linearkombinationen von 1, α und α^2. Wir erhalten:

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(\alpha) &= \alpha^5 = \alpha^2 \cdot 2 \cdot (\alpha + 1) = 2\alpha^3 + 2\alpha^2 = -1 - \alpha + 2\alpha^2 \\ \varphi(\alpha^2) &= \alpha \cdot \alpha^9 = -\alpha^3 - \alpha = -2 + 2\alpha \end{aligned}$$

Die Matrix assoziiert zu φ bezüglich der Basis $(1, \alpha, \alpha^2)$ ist

$$M_\varphi = \begin{pmatrix} 1 & -1 & -2 \\ 0 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$

(c) Angenommen $\beta = \lambda + \mu\alpha + \nu\alpha^2$ für $\lambda, \mu, \nu \in \mathbb{F}_5$. Dann liefert die Bedingung $1 = \beta(1 - \alpha)$

$$1 = \lambda + (\mu - \lambda)\alpha + (\nu - \mu)\alpha^2 - \nu\alpha^3 = \lambda + 3\nu + (3\nu + \mu - \lambda)\alpha + (\nu - \mu)\alpha^2,$$

was äquivalent zu

$$\begin{cases} \lambda + 3\nu = 1 \\ 3\nu + \mu - \lambda = 0 \\ \nu - \mu = 0 \end{cases}$$

ist. Rückwärtsauflösen der Gleichungen liefert $\mu = \nu$, $\lambda = 4\nu$ und $7\nu = 1$, so dass die eindeutige Lösung $(\lambda, \mu, \nu) = (2, 3, 3)$ ist, und $\beta = 2 + 3\alpha + 3\alpha^2$.

(d) Es gilt $|\mathbb{F}_{125}^\times| = 124 = 4 \cdot 31$, und nach dem Theorem von Lagrange, angewandt auf die Untergruppe $\langle\alpha\rangle$, sehen wir, dass die Ordnung von α ein Teiler von 124 ist. Wir wollen zeigen, dass $\mathrm{ord}_{\mathbb{F}_{125}^\times}(\alpha) = 124$, und dies können wir tun, indem wir zeigen, dass α^4 und α^{62} nicht 1 sind, da jeder echte Teiler von 124 entweder 4 oder 62 teilt. Es gilt $\alpha^4 = 2(\alpha^2 + \alpha) \neq 1$, und damit bleibt zu überprüfen, dass $\alpha^{62} \neq 1$. Wir haben

$$\alpha^{62} = \alpha^{-1}(\alpha^9)^7 = -\alpha^{-1}(\alpha^2 + 1)^7.$$

Um weiterzurechnen bemerken wir, dass

$$\begin{aligned} (\alpha^2 + 1)^3 &= \alpha^6 + 3\alpha^4 + 3\alpha^2 + 1 = 4(\alpha + 1)^2 + \alpha^2 + \alpha + 3\alpha^2 + 1 = 3\alpha^2 - \alpha, \\ (\alpha^2 + 1)^6 &= (3\alpha^2 - \alpha)^2 = -\alpha^4 - \alpha^3 + \alpha^2 = -\alpha^2 + \alpha - 2, \text{ and} \\ (\alpha^2 + 1)^7 &= (-\alpha^2 + \alpha - 2)(\alpha^2 + 1) = -\alpha^4 - \alpha^2 + \alpha^3 + \alpha - 2\alpha^2 - 2 = \alpha. \end{aligned}$$

Dann ist

$$\alpha^{62} = -\alpha^{-1}\alpha = -1 \neq 1,$$

und wir folgern, dass α $\mathbb{F}_{125}^\times$ erzeugt.

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

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

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

$$X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in K[X],$$

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 $\mathrm{N}_{K/\mathbb{Q}}(\zeta - 1)$.

Lösung:

(a) Die K-Linearität der Abbildung M_x ist einfach zu verifizieren. In der Tat ist M_x additiv nach der Distributivität der Multiplikation bezüglich Addition und M_x respektiert die Skalarmultiplikation nach der Kommutativität der Multiplikation in L.

(b) Wir bemerken, dass $m_0 = 0$ und $m_1 = \mathrm{id}_L$. Für $x, y, z \in L$ haben wir $m_{x+y}(z) = (x+y)z = xz+yz = m_x(z)+m_y(z)$ und $m_{xy}(z) = (xy)z = x(yz) = m_x(m_y(z)) = (m_x \circ m_y)(z)$. Dies bedeutet, dass $r_{L/K}$ sowohl Addition als auch Multiplikation respektiert und wir folgern, dass $r_{L/K}$ ein Ringhomomorphismus ist. Da $r_{L/K}$ nicht die Nullabbildung ist ($r_{L/K}$ sendet $1 \mapsto id_L \neq 0$) und L ein Körper ist, ist der Kern gleich (0), und damit ist $r_{L/K}$ injektiv.

(c) Wir zeigen zunächst die Linearität von $\mathrm{Tr}_{L/K}$. Sei $n = [L : K]$ und fixiere eine K-Basis $\mathcal{B}$ für L. Nach linearer Algebra gibt es einen K-linearen Ringisomorphismus $\varphi : \mathrm{End}_K(L) \to M_n(K)$. Die Spurabbildung $\mathrm{tr} : M_n(K) \to K$ ist K-linear. Nach Konstruktion gilt dann $\mathrm{Tr}_{L/K} = \mathrm{tr} \circ \varphi \circ r_{L/K}$, was K-linear ist als Komposition von K-linearen Abbildungen.

Was die Norm betrifft haben wir $\mathrm{N}_{L/K} = \det \circ \varphi \circ r_{L/K}$. Da jede dieser Abbildungen die Multiplikation respektiert, tut dies auch $\mathrm{N}_{L/K}$. Ausserdem haben wir $\mathrm{N}_{L/K}(x) = 0$ genau dann, wenn $\det(m_x) = 0$, was äquivalent dazu ist, zu sagen, dass M_x kein invertierbarer Endomorphismus ist und dies passiert genau dann, wenn $x = 0$ (da für $x \neq 0$ haben wir $m_{x^{-1}} = m_x^{-1}$).

(d) Sei $\mathcal{B}_1 = (e_1, \ldots, e_k)$ eine L_2-Basis für L_1 und $\mathcal{B}_2 = (f_1, \ldots, f_l)$ eine K-Basis für L_2. Dann ist

$$\mathcal{B} := (e_1f_1, e_1f_2, \ldots, e_1f_l, e_2f_1, \ldots, e_2f_l, \ldots, e_kf_1, \ldots, e_kf_l)$$

eine K-Basis für L_1.
Für $\alpha \in L_1$ finden wir Koeffizienten $\lambda_{ij} \in L_2$, $1 \leqslant i, j \leqslant k$, so dass für jedes i gilt, dass

$$\alpha \cdot e_i = \sum_{j=1}^{k} \lambda_{ij} e_j.$$

Dann finden wir für jedes i, j wie oben und $1 \leqslant s, t \leqslant l$ Koefficienten $\mu_{ijst} \in L_2$, so dass für jedes i, j und s gilt, dass

$$\lambda_{ij} \cdot f_s = \sum_{t=1}^{l} \mu_{ijst} f_t.$$

Wenn wir diese zwei Gleichheiten zusammensetzen erhalten wir für jedes i und t wie oben,

$$\alpha \cdot e_i f_s = \sum_{j=1}^{k} \sum_{t=1}^{l} \mu_{ijst} e_j f_t.$$

Die Matrix, die zu M_α als eine L_2-lineare Abbildung von L_1 bezüglich der Basis $\mathcal{B}_1$ korrespondiert, ist

$$[m_\alpha]_{L_1/L_2} = {}^T(\lambda_{ij})_{i,j},$$

und damit ist $\mathrm{Tr}_{L_1/L_2}(\alpha) = \sum_{i=1}^{k} \lambda_{ii}$. Ausserdem sind die Matrixkoeffizienten von M_α als eine K-lineare Abbildung von L_1 bezüglich der Basis $\mathcal{B}$

$$[m_\alpha]_{L_1/K} = {}^T(\mu_{ijst})_{(i,s),(j,t)},$$

wobei der Zeilenindex das Tupel (i, s) ist und der Spaltenindex das Tupel (j, t), und diese sind lexicographisch geordnet und damit ist $\mathrm{Tr}_{L_1/K}(\alpha) = \sum_{i=1}^{k} \sum_{s=1}^{l} \mu_{iiss}$.
Für jedes i, j wie oben ist die Matrix, die zu $M_{\lambda_{i,j}}$ als eine K-lineare Abbildung von L_2 bezüglich der Basis $\mathcal{B}_2$ korrespondiert,

$$[m_{\lambda_{i,j}}]_{L_2/K} = {}^T(\mu_{ijst})_{s,t},$$

und damit ist $\mathrm{Tr}_{L_2/K}(\lambda_{ij}) = \sum_{s=1}^{l} \mu_{ijss}$.
Zusammenfassend erhalten wir

$$\mathrm{Tr}_{L_2/K}(\mathrm{Tr}_{L_1/L_2}(\alpha)) = \mathrm{Tr}_{L_2/K}(\sum_{i=1}^{k} \lambda_{ii}) = \sum_{i=1}^{k} \mathrm{Tr}_{L_2/K}(\lambda_{ii}) = \sum_{i=1}^{k} \sum_{s=1}^{l} \mu_{iiss} = \mathrm{Tr}_{L_1/K}(\alpha),$$

was zu zeigen war.

(e) Da $L \cong K[X]/(m_x(\mathbb{Q}))$ als Körpererweiterung von K und $(1, x, \ldots, x^{d-1})$ eine K-Basis von L ist, interessieren wir uns für die Matrix $M = (\lambda_{ij})_{0 \leqslant i,j \leqslant d-1}$ assoziiert zu M_x. Für $j = 0, \ldots, d-2$, haben wir $x \cdot x^j = x^{j+1}$, so dass

$$\lambda_{ij} = \begin{cases} 1 & \text{falls } i = j+1 \\ 0 & \text{ansonsten.} \end{cases}, \text{ für } j = 0, \ldots, d-2.$$

Ausserdem ist $x \cdot x^{d-1} = x^d = -a_0 - a_1 x - \cdots - a_{d-1} x^{d-1}$, so dass

$$\lambda_{i,(d-1)} = -a_i.$$

Wir haben herausgefunden, dass

$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Es gilt $\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(M) = -a_{d-1}$ und $\mathrm{N}_{L/K}(x) = \det(M) = (-1)^d a_0$ nach Entwicklung nach der ersten Zeile.

(f) Betrachte den eindeutigen Ringhomomorphismus $\gamma : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]$, der $\mathbb{Q} \ni a \mapsto a$ und $X \mapsto X + 1$ sendet. Dies ist ein Ringisomorphismus mit Inversem definiert durch $X \mapsto X - 1$. Damit ist f irreduzibel genau dann, wenn $g := \gamma(f)$ irreduzibel ist. Wir bemerken, dass

$$Xg = \gamma(X-1)\gamma(f) = \gamma(X^p - 1) = (X+1)^p - 1,$$

und damit

$$g = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = \sum_{h=1}^{p-1} \binom{p}{h+1} X^h.$$

Da $p \big| \binom{p}{h+1}$ für $h = 0, \ldots, p-2$, aber $p \nmid \binom{p}{(p-1)+1} = 1$ und $p^2 \nmid \binom{p}{0+1} = p$, erfüllt das Polynom g die Voraussetzung des Eisensteinkriteriums, und damit ist g irreduzibel in $\mathbb{Q}[X]$. Es folgt, dass auch f irreduzibel in $\mathbb{Q}[X]$ ist.

Wir bemerken zuerst, dass

$$f(\zeta) = \frac{\zeta^p - 1}{\zeta - 1} = \frac{1-1}{\zeta - 1} = 0.$$

Da f irreduzibel ist, folgern wir, dass $\mathbb{Q}[X]/(f) \cong \mathbb{Q}(\zeta)$. Dies ist auch ein Isomorphismus von $\mathbb{Q}$-Vektorräumen und damit ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}[X]/(f) : \mathbb{Q}] = \deg(f) = p - 1$.

Nach obigen Überlegungen folgt, dass das Minimalpolynom von ζ genau das Polynom $f = \frac{X^p-1}{X-1}$ ist. Nach Aufgabenteil (e) ist damit $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta) = -1$ und $\mathrm{N}_{K/\mathbb{Q}}(\zeta) = 1$, da p ungerade ist. Wir bemerken, dass $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta - 1)$, und damit hat das Minimalpolynom von $\zeta - 1$ Grad $p - 1$.

Da $\zeta - 1$ Nullstelle von $f(X + 1)$ ist, welches irreduzibel vom Grad $p - 1$ ist, erhalten wir

$$m_{\zeta-1}(\mathbb{Q}) = \frac{(X+1)^p - 1}{X},$$

dessen konstanter Koeffizient gerade p ist. Damit ist $N_{L/K}(\zeta - 1) = p$.