Musterlösung 16

1. Zu jedem Polynom $f = \sum_{k=0}^{d} c_k X^k \in K[X]$ bezeichne $\overline{f}$ das Polynom $\sum_{k=0}^{d} (-1)^k c_k X^k$ und $\widetilde{f}$ das Polynom $\sum_{k=0}^{d} c_{d-k} X^k$. Für jedes Polynom f und jedes Element ω einer beliebigen Erweiterung von K gilt

$$\overline{f}(-\omega) = \sum_{k=0}^{d} (-1)^k c_k (-\omega)^k = \sum_{k=0}^{d} c_k \omega^k = f(\omega),$$

sowie im Falle $\omega \neq 0$

$$\widetilde{f}(\omega^{-1}) = \sum_{k=0}^{d} c_{d-k} \omega^{-k} = \omega^{-d} \sum_{k=0}^{d} c_{d-k} \omega^{d-k} = \omega^{-d} f(\omega).$$

Sei also $m_\alpha = X^n + \sum_{k=0}^{n-1} a_k X^k$ das Minimalpolynom von α über K. Wegen $\alpha \neq 0$ gilt $a_0 \neq 0$, da m_α sonst ein Vielfaches des normierten Polynoms X wäre und wegen seiner Irreduzibilität also gleich X wäre, was aber der Gleichung $m_\alpha(\alpha) = 0$ widerspricht. Es sind nun $m_{-\alpha} := (-1)^n \overline{m_\alpha}$ und $m_{\alpha^{-1}} := a_0^{-1} \widetilde{m_\alpha} \in K[X]$ normierte Polynome mit $m_{-\alpha}(-\alpha) = 0$ und $m_{\alpha^{-1}}(\alpha^{-1}) = 0$. Zudem sind sie von minimalem Grad mit dieser Eigenschaft: Gäbe es ein Polynome g von kleinerem Grad mit $g(-\alpha) = 0$, so wäre $\overline{g}(\alpha) = 0$ mit $\deg \overline{g} < n$, im Widerspruch zur Definition von m_α (analog für α^{-1}). Somit sind $m_{-\alpha}$ und $m_{\alpha^{-1}}$ die Minimalpolynome von $-\alpha$, beziehungsweise α^{-1}.

2. Nach einem Satz der Vorlesung ist eine Körpererweiterung genau dann algebraisch, wenn sie von algebraischen Elementen erzeugt wird. Wenn α und β algebraisch sind, ist also jedes Element von $K(\alpha, \beta)$ algebraisch. Insbesondere gilt dies für $\alpha + \beta$ und $\alpha \cdot \beta$; die eine Richtung der Aussage ist damit also bewiesen.

   Nehmen wir jetzt an, seien $\alpha + \beta$ und $\alpha \cdot \beta$ algebraisch und betrachten wir die Körpererweiterung $K' = K(\alpha+\beta, \alpha\cdot\beta)$ von K. Nach dem oben erwähnten Satz ist K'/K algebraisch. Ausserdem ist das Polynom $X^2 - (\alpha+\beta)X + \alpha\cdot\beta \in K'[X] \backslash \{0\}$ ein annullierendes Polynom von α und β, das heisst sie sind algebraisch über K'. Folglich ist $K(\alpha, \beta)/K'$ algebraisch und als algebraische Erweiterung einer algebraischen Erweiterung ist daher auch $K(\alpha, \beta)/K$ algebraisch. Insbesondere sind α und β algebraisch über K.

3. Sei R ein Unterring von L mit $K \subset R$. Als Unterring eines Körpers ist R nullteilerfrei und nicht der Nullring. Sei $\alpha \in R \backslash \{0\}$. Wir werden zeigen, dass α in R ein Inverses besitzt. Da $\alpha \in R \subset L$ ist und L algebraisch über K ist, ist α algebraisch

über K. Sei $p = \sum_{k=0}^{n} c_k X^k \in K[X]$ das Minimalpolynom von α; wegen $\alpha \neq 0$ ist $c_0 \neq 0$. Es gilt $0 = p(\alpha) = \sum_{k=0}^{n} c_k \alpha^k$, also

$$1 = \alpha \cdot \Big(- c_0^{-1} \sum_{k=1}^{n} c_k \alpha^{k-1} \Big)$$

und somit ist

$$-c_0^{-1} \sum_{k=1}^{n} c_k \alpha^{k-1} \in R$$

ein Inverses von α in R. Damit wurde bewiesen, dass R ein Körper ist.

Als Gegenbeispiel wenn L/K nicht algebraisch ist, finden wir $L = K(X)$ für einen beliebigen Körper K und $R = K[X]$.

4. (a) Sei $s = P(t)/Q(t) \in K' \smallsetminus K$ für teilerfremde Polynome $P(X)$, $Q(X) \in K[X]$ mit $Q \neq 0$. Dann ist t eine Nullstelle des Polynoms $F(X) := P(X) - s \cdot Q(X) \in K'[X]$. Wir werden zeigen, dass dieses Polynom nicht identisch verschwindet. Sei dafür $b \in K$ der höchste nicht-verschwindende Koeffizient von $Q(X)$, und $a \in K$ der Koeffizient derselben Potenz von X in $P(X)$. Wenn $F(X)$ verschwindet, muss $a - sb = 0$ sein, also $s = a/b \in K$, im Widerspruch zur Annahme. Da $F(X)$ nicht verschwindet, ist t algebraisch über K'. Man überlegt nun, dass gilt $L = K(t) = K'(t)$. Nach einem Satz der Vorlesung ist dies schliesslich eine algebraische Erweiterung von K', wie zu zeigen war.

   Eine Konsequenz von (a) ist, dass s nicht algebraisch über K ist. Denn wäre es algebraisch über K, so wären sowohl $K(s)/K$ als auch $L/K(s)$ algebraisch, also wäre L/K algebraisch. Aber $t \in L$ ist nicht algebraisch über K.

   (b) Ist $s \in K$, so müssen P und Q konstant sein. In diesem Fall ist $[L/K(s)] = [L/K] = \infty$. Sei also $s \notin K$. Die obige Überlegung zeigt dann genauer, daß $\deg(F) = \deg(Q)$ ist, falls $\deg(Q) \geqslant \deg(P)$ ist. In dem Fall $\deg(Q) < \deg(P)$ gilt dagegen offensichtlich $\deg(F) = \deg(P)$. Also ist $\deg(F)$ stets das Maximum der Grade von P und von Q. Wir werden zeigen, dass F irreduzibel in $K(s)[X]$ ist. Dann ist es bis auf einen Faktor in $K(s)^\times$ das Minimalpolynom von t über $K(s)$, und sein Grad ist gleich dem gesuchten Körpergrad $[L/K(s)]$.

   Da s nicht algebraisch über K ist, können wir für die folgende Überlegung s als formale Unbestimmte auffassen. Nach Konstruktion liegt F in $K[s, X]$, was wir als Polynomring in zwei unabhängigen Variablen auffassen können. Dieser hat eindeutige Primfaktorzerlegung (siehe Algebra I). Es genügt daher zu beweisen, daß F als Element von $K[s, X]$ irreduzibel ist. Da F linear in s ist, kann es in $K[s, X]$ höchstens einen in s konstanten Faktor abspalten. Da aber P und Q als teilerfremd vorausgesetzt wurden, ist auch das nicht möglich.

(c) Sei $s = P(t)/Q(t) \in L$ das Bild von t unter einem Element von $\mathrm{Aut}_K(L)$. Dann gilt $L = K(s)$, also $[L/K(s)] = 1$, und aus (b) folgt, dass P und Q höchstens linear sind. Das heißt, der Automorphismus ist gegeben durch die angegebene Formel. Umgekehrt definiert diese Formel einen solchen Automorphismus genau dann, wenn Zähler und Nenner teilerfremd und nicht beide konstant sind. Man zeigt leicht, daß dies äquivalent ist zu der Bedingung $ad - bc \neq 0$.

5. Wir nehmen (ad absurdum) an, die Erweiterung $\mathbb{R}/\mathbb{Q}$ hätte eine abzählbare Transzendenzbasis $(t_1, t_2, \ldots)$. Für jedes $n \geqslant 1$ ist der Körper $\mathbb{Q}(t_1, \ldots, t_n)$ nach Aufgabe 5. (a) von Serie 14 abzählbar. Daraus folgt, dass auch der Körper

$$K := \mathbb{Q}(t_1, \ldots) = \bigcup_{n=1}^{\infty} \mathbb{Q}(t_1, \ldots, t_n)$$

als abzählbare Vereinigung von abzählbaren Mengen abzählbar ist. Die Erweiterung $\mathbb{R}/K$ ist algebraisch, weil $(t_1, \ldots)$ eine Transzendenzbasis von $\mathbb{R}/\mathbb{Q}$ ist; somit ist $\mathbb{R} \subset \overline{K}$. Aber $\overline{K}$ ist nach Aufgabe 5. (b) von Serie 14 abzählbar; Widerspruch. Somit hat die Erweiterung $\mathbb{R}/\mathbb{Q}$ keine abzählbare Transzendenzbasis.