Lösung zu Zettel 11, Aufgaben 3 und 4

Jendrik Stelzner

30. Januar 2017

Aufgabe 3

Die K-linearen Körperhomomorphismen $K(t) \to K(t)$ sind nach der universellen Eigenschaft des Quotientenkörpers genau die eindeutigen Fortsetzungen der K-linearen, injektiven Ringhomomorphismen $K[T] \to K(t)$.

Die K-linearen Ringhomomorphismen $K[T] \to K(t)$ sind genau die Einsetzhomomorphismen von Elementen aus $K(t)$, wobei jedes Element einen anderen Einsetzhomomorphismus liefert. Die injektiven Einsetzhomomorphismen entsprechen dabei genau den Elementen aus $K(t)$, die transzendent über K sind. Dabei ist nach Aufgabe 2 ein Element $q \in K(t)$ genau dann transzendent über K, wenn $q \notin K$.

Ingesamt erhalten wir, dass die K-linearen Körperhomomorphismen $K(t) \to K(t)$ genau die Einsetzhomomorphismen $p \mapsto p(q)$ für $q \in K(t)$ mit $q \notin K$ sind.

Behauptung 1. 1. Ist $q \in K(t)$ mit $q \notin K$, so ist der entsprechende Einsetzhomomorphismus $\varphi\colon K(t) \to K(t)$, $p \mapsto p(q)$ genau dann ein Automorphismus, wenn q von der Form $q = (at+b)/(ct+d)$ mit $a \neq 0$ oder $c \neq 0$ ist.

2. Für ein beliebiges Element $(at+b)/(ct+d) \in K(t)$ gilt genau dann $(at+b)/(ct+d) \notin K$, wenn
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K).$$

Beweis. 1. Da Körperhomomorphismen immer injektiv sind, ist φ genau dann ein Automorphismus, wenn φ surjektiv ist. Dabei gilt $\operatorname{im}\varphi = K(q)$. Ist $q = f/g$ mit teilerfremden $f, g \in K[T]$, so gilt nach Aufgabe 2, dass
$$[K(t) : \operatorname{im}\varphi] = [K(t) : K(q)] = \max\{\deg f, \deg g\}.$$

Folglich ist φ genau dann surjektiv, also $[K(t) : \operatorname{im}\varphi] = 1$, wenn $f = at+b$ und $g = ct+d$ mit $a \neq 0$ oder $c \neq 0$.

2. Es gilt $c \neq 0$ oder $d \neq 0$, und deshalb

$$
\begin{aligned}
& \frac{at+b}{ct+d} \in K \\
\iff & \frac{at+b}{ct+d} = \lambda \quad \text{für ein } \lambda \in K \\
\iff & at+b = c\lambda t + d\lambda \quad \text{für ein } \lambda \in K \\
\iff & \begin{cases} a &= c\lambda \\ b &= d\lambda \end{cases} \quad \text{für ein } \lambda \in K \\
\iff & \begin{pmatrix} a \\ b \end{pmatrix} \text{ und } \begin{pmatrix} c \\ d \end{pmatrix} \text{ sind linear abhängig} \\
\iff & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin \mathrm{GL}_2(K).
\end{aligned}
$$

□

Insgesamt erhalten wir somit, dass die K-linearen Körperautomorphismen $K(t) \to K(t)$ genau die Einsetzhomomorphismen von Elementen $q \in K(t)$ der Form $q = (at+b)/(ct+d)$ mit

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$$

sind. Wir haben also eine surjektive Abbildung

$$\Phi\colon\ \mathrm{GL}_2(K) \to \mathrm{Gal}(K(t)/K), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(p \mapsto p\left(\frac{at+b}{ct+d}\right)\right).$$

Diese Abbildung ist ein Gruppenantimorphismus, d.h. es gilt

$$\Phi(S_1)\Phi(S_2) = \Phi(S_2 S_1) \quad \text{für alle } S_1, S_2 \in \mathrm{GL}_2(K).$$

Sind nämlich

$$S_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{und} \quad S_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

so gilt

$$
\begin{aligned}
(\Phi(S_1)\Phi(S_2))(t) &= \Phi(S_1)(\Phi(S_2)(t)) = \Phi(S_1)\left(\frac{a't+b'}{c't+d'}\right) = \frac{a'\Phi(S_1)(t)+b'}{c'\Phi(S_1)(t)+d'} \\
&= \frac{a'\frac{at+b}{ct+d}+b'}{c'\frac{at+b}{ct+d}+d'} = \frac{a'(at+b)+b'(ct+d)}{c'(at+b)+d'(ct+d)} = \frac{(a'a+b'c)t+(a'b+b'd)}{(c'a+d'c)t+(c'b+d'd)} \\
&= \Phi\left(\begin{pmatrix} a'a+b'c & a'b+b'd \\ c'a+d'c & c'b+d'd \end{pmatrix}\right)(t) = \Phi(S_2S_1)(t).
\end{aligned}
$$

Es gilt $\ker \Phi = K^\times \cdot I$, denn

$$\begin{aligned}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \ker \Phi &\iff \Phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \mathrm{id} \iff \Phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)(t) = t \\ &\iff \frac{at+b}{ct+d} = t \iff at+b = ct^2+dt \iff a = d, b = c = 0.\end{aligned}$$

Somit induziert Φ einen Antiisomorphismus von Gruppen

$$\overline{\Phi}\colon\ \mathrm{PGL}_2(K) \to \mathrm{Gal}(K(t)/K), \quad \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \mapsto \Phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).$$

Bemerkung 2. Dass Φ ein Gruppenantimorphismus, aber kein Gruppenhomomorphismus ist, lässt sich dadurch reparieren, dass man Φ durch die Abbildung

$$\Psi\colon\ \mathrm{GL}_2(K) \to \mathrm{Gal}(K(t)/K), \quad S \mapsto \Phi(S)^{-1} = \Phi(S^{-1})$$

ersetzt. Für jede Gruppe G ist die Abbildung $(-)^{-1}\colon G \to G$, $g \mapsto g^{-1}$ ein Antiisomorphismus, also ist Φ als Komposition zweier Gruppenantimorphismen ein Gruppenhomomorphismus. Dabei gilt $\ker \Psi = \ker \Phi$, weshalb Ψ einen Isomorphismus von Gruppen

$$\overline{\Psi}\colon\ \mathrm{PGL}_2(K) \to \mathrm{Gal}(K(t)/K), \quad \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \mapsto \Psi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).$$

induziert. Dieser ist konkret durch

$$\begin{aligned}\overline{\Psi}\left(\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}\right)(p) &= \Phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\right)(p) = \Phi\left(\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\right)(p) \\ &= \Phi\left(\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\right)(p) = p\left(\frac{dt-b}{-ct+a}\right)\end{aligned}$$

gegeben.

Aufgabe 4

Es sei

$$C_n(K) \coloneqq \{\omega \in K \mid \omega^n = 1\}$$

die Gruppe der n-ten Einheitswurzeln in K; es handelt sich um eine Untergruppe von $K^\times$. Nach Aufgabe 3 ergibt sich für jedes $\omega \in C_n(K)$ ein K-linearer Körperautomorphismus

$$\sigma_\omega\colon K(t) \to K(t), \quad p(t) \mapsto p(\omega t).$$

Dabei gilt $\sigma_{\omega_1} \circ \sigma_{\omega_2} = \sigma_{\omega_1\omega_2}$ für alle $\omega_1, \omega_2 \in C_n(K)$, weshalb die Abbildung

$$\Phi\colon C_n(K) \to \mathrm{Gal}(K(t)/K), \quad \omega \mapsto \sigma_\omega$$

ein Gruppenhomomorphismus ist. Da $\Phi(\omega)(t) = \sigma_\omega(t) = \omega t$ ist Φ injektiv, und wir zeigen, dass im $\Phi = \mathrm{Gal}(K(t)/K(t^n))$; damit liefert die Zuordnung $\omega \mapsto \sigma_\omega$ einen Isomorphismus $C_n(K) \to \mathrm{Gal}(K(t)/K(t^n))$.

Es gilt im $\Phi \subseteq \mathrm{Gal}(K(t)/K(t^n))$, denn für jedes $\omega \in C_n(K)$ gilt

$$\sigma_\omega(t^n) = \sigma_\omega(t)^n = (\omega t)^n = \omega^n t^n = t^n$$

und somit $\sigma_\omega|_{K(t^n)} = \mathrm{id}_{K(t^n)}$.

Ist andererseits $\sigma \in \mathrm{Gal}(K(t)/K(t^n)) \subseteq \mathrm{Gal}(K(t)/K)$, so gibt es nach Aufgabe 3 ein eindeutiges Element $q \in K(t)$ mit $q \notin K$, so dass $\sigma(p) = p(q)$ für alle $p \in K(t)$. Wegen der $K(t^n)$-Linearität von σ muss dabei

$$q^n = \sigma(t)^n = \sigma(t^n) = t^n.$$

Die Surjektivität von Φ nach $\mathrm{Gal}(K(t)/K(t^n))$ folgt deshalb aus der folgenden Aussage:

Behauptung 3. Ist $q \in K(t)$ mit $q^n = t^n$, so ist $q = \omega t$ mit $\omega \in C_n(K)$.

Beweis. Es sei $\mathcal{P} \subseteq K[T]$ ein Repräsentantensystem der Primelemente von $K[T]$. Wir können o.B.d.A. davon ausgehen, dass $t \in \mathcal{P}$. Dann gibt es eine eindeutige Darstellung

$$q = \omega \prod_{p \in \mathcal{P}} p^{\nu_p}$$

mit $\omega \in K^\times$ und $\nu_p \in \mathbb{Z}$ für alle $p \in \mathcal{P}$, wobei $\nu_p = 0$ für fast alle $p \in \mathcal{P}$. Es gilt

$$t^n = q^n = \omega^n \prod_{p \in \mathcal{P}} p^{n\nu_p} = \omega^n t^{n\nu_t} \prod_{p \in \mathcal{P} \setminus \{t\}} p^{n\nu_p},$$

und aus der Eindeutigkeit dieser Darstellung für t^n ergibt sich, dass $\omega^n = 1$, $\nu_t = 1$ und $\nu_p = 0$ für alle $\in \mathcal{P} \setminus \{t\}$. Also ist $q = \omega t$ mit $\omega \in C_n(K)$. □

Die Galoisgruppe der Körpererweiterung $K(t)/K(t^n)$ ist also die Gruppe der n-ten Einheitswurzeln. Nach Aufgabe 2 gilt $[K(t) : K(t^n)] = n$ (und das Minimalpolynom von t über $K(t^n)$ ist $X - t^n \in K(t^n)[X]$), also ist $K(t)/K(t^n)$ genau dann galoisch, wenn $|C_n(K)| = n$. Da $C_n(K)$ die Nullstellenmenge des Polynoms $X^n - 1 \in K[X]$ ist, gilt dies genau dann, wenn das Polynom $X^n - 1 \in K[X]$ vollständig in Linearfaktoren zerfällt, und alle Nullstellen paarweise verschieden sind, d.h. wenn das Polynom zerfällt und seperabel ist.

Gilt $p := \mathrm{char}(K) > 0$ und $n = p^r$, so gilt

$$X^n - 1 = X^{p^r} - 1^{p^r} = (X-1)^{p_r}.$$

In diesem Fall ist also $\mathrm{Gal}(K(t)/K(t^n)) \cong C_n(K) \cong 1$.