Musterlösung 19

Körperhomomorphismen und Zerfällungskörper

1. Sei L/K eine algebraische Körpererweiterung. Zeige, dass jeder Körperhomomorphismus $\varphi\colon L \to L$ über K ein Automorphismus ist.

   Lösung: Wir wissen bereits, dass φ injektiv ist. Für die Surjektivität sei $a \in L$ beliebig. Sei $m_{a,K}(X) \in K[X]$ sein Minimalpolynom über K, und sei S die Menge aller Nullstellen von $m_{a,K}(X)$ in L. Für jedes $b \in S$ gilt dann $m_{a,K}(\varphi(b)) = \varphi(m_{a,K}(b)) = \varphi(0) = 0$ und somit $\varphi(b) \in S$. Daher induziert φ eine Abbildung $S \to S$. Da φ injektiv und S endlich ist, ist die induzierte Abbildung $S \to S$ folglich auch surjektiv. Also existiert $b \in S$ mit $\varphi(b) = a$, und wir folgern $a \in \varphi(K)$. Somit ist φ surjektiv, und daher ein Isomorphismus.

2. (a) Zeige, dass $\mathrm{id}_{\mathbb{R}}$ der einzige Körperendomorphismus von $\mathbb{R}$ ist.

(*b) Zeige, dass $\mathbb{C}$ überabzählbar viele Körperendomorphismen hat.

(**c) Zeige, dass die Kardinalität in (b) echt grösser als die von $\mathbb{R}$ ist.

Lösung: (a) Sei φ ein Körperendomorphismus von $\mathbb{R}$. Da $\mathbb{Q}$ der Primkörper von $\mathbb{R}$ ist, gilt $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

Wir zeigen nun, dass φ streng monoton ist: Seien $x, y \in \mathbb{R}$ mit $x > y$. Wegen $x - y > 0$ existiert dann ein $z \in \mathbb{R}$ mit $z^2 = x - y$. Dann ist $\varphi(z)^2 = \varphi(x) - \varphi(y)$, und da φ injektiv ist, gilt $\varphi(z) \neq 0$. Daraus folgt $\varphi(x) - \varphi(y) > 0$, also $\varphi(x) > \varphi(y)$, und somit ist φ streng monoton.

Für jedes $x \in \mathbb{R}$ und jedes $\varepsilon > 0$ existieren $x_1, x_2 \in \mathbb{Q}$ mit

$$x - \varepsilon < x_1 < x < x_2 < x + \varepsilon.$$

Wegen der Monotonie von φ und mit $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ folgt

$$x - \varepsilon < x_1 = \varphi(x_1) < \varphi(x) < \varphi(x_2) = x_2 < x + \varepsilon.$$

Daraus folgt $|x - \varphi(x)| < \varepsilon$. Da $\varepsilon > 0$ beliebig war, muss also $\varphi(x) = x$ sein.

(b) Sei $\mathcal{T}$ eine Transzendenzbasis von $\mathbb{C}/\mathbb{Q}$. Laut Vorlesung ist $\mathcal{T}$ überabzählbar; genauer gilt $\mathrm{card}(\mathcal{T}) = \mathrm{trdeg}_{\mathbb{R}/\mathbb{Q}} = \mathrm{card}(\mathbb{R})$. Betrachte eine beliebige Permutation σ von $\mathcal{T}$. Da $\mathcal{T}$ algebraisch unabhängig über $\mathbb{Q}$ ist, lässt sich σ zu einem eindeutigen Automorphismus φ von $\mathbb{Q}(\mathcal{T})$ fortsetzen.

Sei nun $\mathbb{C}_\varphi := \mathbb{C}$, betrachtet als Oberkörper von $\mathbb{Q}(\mathcal{T})$ vermöge der Einbettung $\varphi\colon \mathbb{Q}(\mathcal{T}) \hookrightarrow \mathbb{C}$. Da $\mathbb{C}/\mathbb{Q}(\mathcal{T})$ algebraisch ist, und $\mathbb{C}$ und folglich $\mathbb{C}_\varphi$ algebraisch abgeschlossen ist, existiert nach dem Satz aus Abschnitt 5.7 der Vorlesung ein Homomorphismus $\psi\colon \mathbb{C} \to \mathbb{C}_\varphi$ über $\mathbb{Q}(\mathcal{T})$. Nach Definition von $\mathbb{C}_\varphi$ ist dieser nichts anderes als eine Fortsetzung von φ zu einem Endomorphismus von $\mathbb{C}$. Somit ist die Anzahl der Körperendomorphismen von $\mathbb{C}$ grösser oder gleich der Anzahl der Permutationen von $\mathcal{T}$.

Fixiere ein $t_0 \in \mathcal{T}$. Für jedes $t \in \mathcal{T} \smallsetminus \{t_0\}$ betrachte die Permutation, welche t_0 und t vertauscht und alle übrigen Elemente festhält. Diese Konstruktion liefert insgesamt $\mathrm{card}(\mathcal{T} \smallsetminus \{t_0\})$ verschiedene Permutationen. Da $\mathcal{T}$ unendlich ist, gilt aber $\mathrm{card}(\mathcal{T} \smallsetminus \{t_0\}) = \mathrm{card}(\mathcal{T})$. Damit ist (b) gezeigt.

(c) Da $\mathcal{T}$ unendlich ist, gilt $\mathrm{card}(\mathcal{T} \times \{0,1\}) = \mathrm{card}(\mathcal{T})$, das heisst, es existiert eine bijektive Abbildung $\beta\colon \mathcal{T} \times \{0,1\} \to \mathcal{T}$. Für jede Abbildung $u\colon \mathcal{T} \to \{0,1\}$ betrachte die Permutation von $\mathcal{T} \times \{0,1\}$, die gegeben ist durch

$$(t,i) \mapsto \begin{cases} (t,i) & \text{falls } u(t) = 0, \\ (t,1-i) & \text{falls } u(t) = 1. \end{cases}$$

Via β entspricht diese einer Permutation von $\mathcal{T}$. Für verschiedene u sind diese Permutationen ebenfalls verschieden. Nach demselben Argument wie in (b) ist die gesuchte Kardinalität daher $\geqslant \mathrm{card}(\{0,1\}^{\mathcal{T}}) > \mathrm{card}(\mathcal{T}) = \mathrm{card}(\mathbb{R})$.

Bemerkung: Die oben konstruierten Endomorphismen von $\mathbb{C}$ sind tatsächlich sogar Automorphismen. Denn da $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{Q}(\mathcal{T})$ ist, ist jede Fortsetzung eines Automorphismus von $\mathbb{Q}(\mathcal{T})$ zu einem Endomorphismus von $\mathbb{C}$ bereits ein Automorphismus, was man genauso zeigt wie im Beweis der Eindeutigkeit des algebraischen Abschlusses oder wie in Aufgabe 1.

Es existieren aber auch nicht surjektive Endomorphismen von $\mathbb{C}$, und solche können auf dieselbe Art wie oben konstruiert werden; beispielsweise lässt sich jede injektive aber nicht surjektive Abbildung $\mathcal{T} \to \mathcal{T}$ zu einem Endomorphismus von $\mathbb{C}$ fortsetzen, der dann automatisch nicht surjektiv ist. Daraus folgt, dass $\mathbb{C}$ viele echte Unterkörper hat, die isomorph zu $\mathbb{C}$ sind.

*3. Finde für jedes $n \geqslant 1$ ein Beispiel einer Körpererweiterung vom Grad n mit trivialer Automorphismengruppe.

Lösung: Sei $K := \mathbb{F}_2(T)$. Nach dem Eisensteinkriterium bezüglich des Primelements T ist das Polynom $X^n - T \in \big(\mathbb{F}_2[T]\big)[X]$ irreduzibel, und nach Gauss ist es somit auch irreduzibel in $K[X]$. Sei L ein Stammkörper von $X^n - T$ über K, das heisst $L = K(S)$ für ein $S \in L$ mit $S^n - T = 0$. Nach Konstruktion ist $[L/K] = n$. Wir stellen zudem fest, dass L über $\mathbb{F}_2$ von S erzeugt wird, und dass S transzendent über $\mathbb{F}_2$ ist; das heisst, L ist der Körper der rationalen Funktionen über $\mathbb{F}_2$ in der Variablen S.

Sei nun φ ein Automorphismus von L über K. Dann ist $\varphi(S)$ ebenfalls eine Nullstelle des Polynoms $X^n - T$. Für $\alpha := \frac{\varphi(S)}{S}$ gilt also

$$\alpha^n = \Big(\frac{\varphi(S)}{S}\Big)^n = \frac{\varphi(S)^n}{S^n} = \frac{T}{T} = 1.$$

Schreiben wir andererseits $\alpha = \frac{p}{q}$ für teilerfremde Polynome $p, q \in \mathbb{F}_2[S]$, so folgt $\frac{p^n}{q^n} = \alpha^n = 1$, aber da p und q und somit auch p^n und q^n teilerfremd waren, sind $p, q \in \mathbb{F}_2$, also auch $\alpha \in \mathbb{F}_2$ und somit $\alpha = 1$.

Somit haben wir gezeigt, dass $\varphi(S) = S$ ist, und daraus folgt $\varphi = \mathrm{id}_L$.

Bemerkung: Für n ungerade funktioniert dasselbe Argument auch über $\mathbb{R}$ anstelle von $\mathbb{F}_2$, da dann 1 die einzige n-te Einheitswurzel in $\mathbb{R}$ und somit auch in $\mathbb{R}[S]$ ist.

Ein weiteres Beispiel in Charakteristik 0 erhält man (mit n ungerade) nach demselben Prinzip auch mit $K := \mathbb{Q}$ und $L := \mathbb{Q}(\sqrt[n]{2})$.

Man kann zudem zeigen, dass es in jeder Charakteristik und zu jedem $n > 2$ Erweiterungen vom Grad n mit trivialer Automorphismengruppe gibt.

4. (a) Beweise, dass $(X^2 - 2X - 2)(X^2 + 1)$ und $X^5 - 3X^3 + X^2 - 3$ dieselben Zerfällungskörper K über $\mathbb{Q}$ haben, und finde $[K/\mathbb{Q}]$.

   (b) Bestimme den Grad eines Zerfällungskörpers des Polynoms $X^3 + X^2 + 1$ über $\mathbb{Q}$ und über $\mathbb{F}_2$.

Lösung: (a) Das erste Polynom zerlegt sich über $\mathbb{C}$ in die Linearfaktoren

$$(X^2 - 2X - 2)(X^2 + 1) = (X - 1 + \sqrt{3})(X - 1 - \sqrt{3})(X - i)(X + i).$$

Es besitzt also den Zerfällungskörper $K := \mathbb{Q}(\sqrt{3}, i) \subset \mathbb{C}$. Das zweite Polynom zerlegt sich zu

$$\begin{aligned} &X^5 - 3X^3 + X^2 - 3 \\ &\quad = (X^2 - 3)(X^3 + 1) \\ &\quad = (X - \sqrt{3})(X + \sqrt{3})(X + 1)(X - \tfrac{1}{2}(-1 + i\sqrt{3}))(X - \tfrac{1}{2}(-1 - i\sqrt{3})). \end{aligned}$$

Es besitzt also den Zerfällungskörper $L := \mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3})) \subset \mathbb{C}$. Die Erzeugenden von L sind offenbar in K enthalten, also gilt $L \subset K$. Umgekehrt sind wegen

$$i = (2(\frac{1}{2}(-1 + i\sqrt{3})) + 1)\frac{\sqrt{3}}{3}$$

die Erzeugenden von K in L enthalten, also haben wir $K = L$.

Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$ ist $X^2 - 3$, also gilt $[\mathbb{Q}(\sqrt{3})/\mathbb{Q}] = 2$. Da i nicht in der reellen Erweiterung $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ liegt, ist $X^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(\sqrt{3})$. Folglich gilt $[\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}(\sqrt{3})] = 2$. Wegen der Multiplikativität des Körpergrades haben wir also

$$[K/\mathbb{Q}] = [K/\mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3})/\mathbb{Q}] = 4.$$

(b) *Über $\mathbb{Q}$:* Das Polynom $f(X) := X^3 + X^2 + 1$ ist ganzzahlig und normiert. Jede rationale Nullstelle ist somit ganz und ein Teiler des konstanten Koeffizienten. Aber ± 1 sind keine Nullstellen; also hat f keine Nullstelle in $\mathbb{Q}$. Wegen $\deg(f) = 3$ ist es deshalb schon irreduzibel über $\mathbb{Q}$.

Da $\deg(f) = 3$ ungerade ist, besitzt f mindestens eine reelle Nullstelle a. Um zu untersuchen, ob die anderen beiden Nullstellen ebenfalls in $\mathbb{R}$ liegen, wenden wir Methoden der Analysis an. Die erste Ableitung von f ist $f'(X) = 3X^2 + 2X = X(3X + 2)$; also hat f die beiden lokalen Extrema $f(0) = 1$ und $f(-\frac{2}{3}) = \frac{31}{27}$. Da beide Werte grösser als 0 sind, kann f keine weitere reelle Nullstelle haben.

Insbesondere liegen die beiden übrigen Nullstellen $b, c \in \mathbb{C}$ von f nicht in $\mathbb{Q}(a)$. Für den Zerfällungskörper $L := \mathbb{Q}(a, b, c)$ von f gilt daher

$$[L/\mathbb{Q}] = [L/\mathbb{Q}(a)] \cdot [\mathbb{Q}(a)/\mathbb{Q}] = 2 \cdot 3 = 6.$$

Über $\mathbb{F}_2$: Durch Einsetzen von 0 und 1 sehen wir, dass $f(X) := X^3 + X^2 + 1$ keine Nullstelle in $\mathbb{F}_2$ hat und somit irreduzibel über $\mathbb{F}_2$ ist. Folglich ist

$$L := \mathbb{F}_2[X]/(X^3 + X^2 + 1)$$

ein Stammkörper von f über $\mathbb{F}_2$. Sei $x \in L$ die Restklasse von X. In jedem Körper der Charakteristik 2 ist Quadrieren ein Endomorphismus, insbesondere ist $f(x^2) = f(x)^2 = 0$ in L. Wegen $x \neq 0, 1$ gilt andererseits $x^2 \neq x$. Also hat das kubische Polynom f schon die zwei verschiedenen Nullstellen $x, x^2 \in L$; es zerfällt daher bereits über L in Linearfaktoren. Also ist L schon ein Zerfällungskörper von f über $\mathbb{F}_2$. Wegen der Irreduzibilität folgt schliesslich $[L/\mathbb{F}_2] = 3$.

5. Sei K ein Körper und sei $f \in K[X]$ ein Polynom vom Grad $n \geqslant 1$. Sei L ein Zerfällungskörper von f über K. Beweise:

   (a) Es gilt $[L/K] | n!$.

   (b) Im Fall $[L/K] = n!$ ist f irreduzibel über K.

   Lösung: (a) Wir verwenden Induktion über n. Für $n = 1$ ist f ein lineares Polynom und daher gilt $[L/K] = 1$, woraus die Aussage direkt folgt. Sei also $n \geqslant 2$. Wir unterscheiden zwei Fälle:

   Sei f irreduzibel und $a \in L$ eine Nullstelle von f. Dann ist f das Minimalpolynom von a über K und es gilt $[K(a)/K] = n$. Ausserdem lässt sich f über $K(a)$ faktorisieren als $f(X) = (X - a)g(X)$ mit $\deg(g) = n - 1$. Offensichtlich ist L ein Zerfällungskörper von g über $K(a)$. Nach Induktionsvoraussetzung gilt also $[L/K(a)] \,\big|\, \deg(g)! = (n-1)!$. Durch Multiplizieren auf beiden Seiten mit n erhält man

   $$[L/K] = [L/K(a)] \cdot [K(a)/K] \,\big|\, (n-1)! \cdot n = n!.$$

   Nehmen wir jetzt an, das Polynom f sei reduzibel und seien $f_1, f_2 \in K[X] \smallsetminus K$ mit $f = f_1 f_2$. Dann gilt $n_1 := \deg(f_1) \geqslant 1$ und $n_2 := \deg(f_2) \geqslant 1$ und $n = n_1 + n_2$. Sei K_1 ein Zerfällungskörper von f_1 über K. Nach Induktionsvoraussetzung gilt dann $[K_1/K] \,\big|\, n_1!$. Ausserdem ist L ein Zerfällungskörper von f_2 über K_1. Nach Induktionsvoraussetzung gilt also $[L/K_1] \,\big|\, n_2!$, und wegen der Multiplikativität des Körpergrades folgt daraus $[L/K] \,\big|\, n_1! n_2!$. Der Binomialkoeffizient $\binom{n_1+n_2}{n_1} = \frac{(n_1+n_2)!}{n_1! n_2!}$ ist eine ganze Zahl, also gilt $n_1! n_2! \,\big|\, (n_1 + n_2)! = n!$. Demnach gilt

   $$[L/K] \,\big|\, n!.$$

   (b) Da für ein reduzibles f wie oben gilt $[L/K] \,\big|\, n_1! n_2!$ und $n_1! n_2! < n!$, folgt die Aussage.