Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE
UNIVERSITÄT
DARMSTADT

WS 08/09 13. Januar 2009

Algebra

11. Übung mit Lösungshinweisen

Aufgabe 50 Es sei $\mathbb{K}$ ein Körper.

(a) Sei $f \in \mathbb{K}[X]$ ein separables Polynom. Zeige, daß der Zerfällungskörper von f eine separable Erweiterung von $\mathbb{K}$ ist.

(b) Sei umgekehrt $\mathbb{L}/\mathbb{K}$ eine separable Erweiterung und $f \in \mathbb{K}[X]$ ein Polynom, so daß $\mathbb{L}$ der Zerfällungskörper von f über $\mathbb{K}$ ist. Ist dann auch f separabel?

Lösung: (a) Sei $\mathbb{L}$ der Zerfällungskörper von f und $\overline{\mathbb{K}}$ ein algebraischer Abschluß von $\mathbb{K}$. Es ist $\mathbb{L} = \mathbb{K}(a_1, ..., a_n)$, wobei $a_1, ..., a_n$ die paarweise verschiedenen Nullstellen in $\overline{\mathbb{K}}$ bezeichne. Es reicht (nach Skript) zu zeigen, daß jedes a_i separabel ist.
Da a_i eine Nullstelle von f ist, teilt $m_{a_i,\mathbb{K}}$ das Polynom f, also hat $m_{a_i,\mathbb{K}}$ nur einfache Nullstellen in $\overline{\mathbb{K}}$, somit ist a_i separabel über $\mathbb{L}$.

(b) Die Erweiterung $\mathbb{C}/\mathbb{R}$ ist separabel, aber $\mathbb{C}$ ist der Zerfällungskörper von $(X^2+1)^2$, ein nicht separables Polynom in $\mathbb{R}[X]$. Somit gilt die Umkehrung von (a) nicht.

Aufgabe 51 Es habe $\mathbb{K}$ Charakteristik $p > 0$ und es sei $\mathbb{K}(a)/\mathbb{K}$ eine algebraische Körpererweiterung. Zeige, daß folgende Aussagen äquivalent sind:

(1) Das Minimalpolynom f von a ist separabel.

(2) $\mathbb{K}(a) = \mathbb{K}(a^p)$.

Lösung: (1) $\Rightarrow$ (2) Ist f nicht separabel, dann ist $f' = 0$, also $f(X) = g(X^p)$ für ein $g \in \mathbb{K}[X]$ nach H13. Wir erhalten $\deg(g) < \deg(f)$ und es gilt

$$g(a^p) = f(a) = 0.$$

Somit folgt

$$[\mathbb{K}(a^p) : \mathbb{K}] \leq \deg(g) < \deg(f) = [\mathbb{K}(a) : \mathbb{K}].$$

Damit ist $\mathbb{K}(a) \neq \mathbb{K}(a^p)$.
(2) $\Rightarrow$ (1) Ist $\mathbb{K}(a^p)$ eine echte Teilmenge von $\mathbb{K}(a)$, dann hat das Minimalpolynom g von a über $\mathbb{K}(a^p)$ den Grad

$$\deg(g) = [\mathbb{K}(a) : \mathbb{K}(a^p)] > 1.$$

Da a Nullstelle von $X^p - a^p \in \mathbb{K}(a^p)[X]$ ist, folgt, daß g das Polynom $X^p - a^p$ teilt. Aber:

$$X^p - a^p = (X - a)^p \in \mathbb{K}(a)[X],$$

somit hat g eine mehrfache Nullstelle in $\mathbb{K}(a)$. Da a eine Nullstelle von f ist, teilt g das Polynom f und f muß ebenfalls eine mehrfache Nullstelle haben, also ist f nicht separabel.

Aufgabe 52 Bestimme alle $\mathbb{Q}$-Automorphismen von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Welche Elemente sind gemeinsame Fixpunkte aller $\mathbb{Q}$-Automorphismen?

LÖSUNG: Die Erweiterung $\mathbb{L} := \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ ist separabel, also gibt es genau 4 $\mathbb{Q}$-Homomorphismen

$$\rho_i : \mathbb{L} \to \overline{\mathbb{Q}}$$

und, da $\mathbb{L}/\mathbb{Q}$ normal ist, folgt

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{L}) = [\mathbb{L} : \mathbb{Q}]_s = 4.$$

Betrachten wir die $\mathbb{Q}(\sqrt{3})$-Automorphismen von $\mathbb{L}$. Diese müssen die Nullstellen des Minimalpolynoms von $\sqrt{2} \in \mathbb{L}$ invariant lassen. Also kommt neben der Identität nur die $\mathbb{Q}(\sqrt{3})$-lineare Abbildung

$$\sigma : \mathbb{L} \to \mathbb{L}, \quad \sigma(a + b \cdot \sqrt{2}) := a - b \cdot \sqrt{2}$$

in Frage. Diese Abbildung ist ein $\mathbb{Q}$-Automorphismus von $\mathbb{L}$.
Analog erhalten wir einen $\mathbb{Q}$-Automorphismus von $\mathbb{L}$ durch

$$\tau : \mathbb{L} \to \mathbb{L}, \quad \sigma(a + b \cdot \sqrt{3}) := a - b \cdot \sqrt{3},$$

wobei a und b Koeffizienten aus $\mathbb{Q}(\sqrt{2})$ sind.
Diese Automorphismen erfüllen die Relationen

$$\sigma^2 = \tau^2 = \mathrm{id}, \quad \sigma \circ \tau = \tau \circ \sigma, \quad \sigma \neq \tau \neq \mathrm{id}.$$

Damit folgt

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{L}) = \{\mathrm{id}, \sigma, \tau, \sigma \circ \tau\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Gemeinsame Fixpunkte aller Automorphismen sind offensichtlich nur die Elemente aus $\mathbb{Q}$, also ein 1-dimensionaler Teilraum von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Aufgabe 53 Finde alle primitiven Elemente der Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

LÖSUNG: Wir kennen bereits alle $\mathbb{Q}$-Automorphismen der normalen Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Wir betrachten nun Elemente der Form

$$\alpha = a\sqrt{2} + b\sqrt{3} + c\sqrt{6}.$$

Kennen wir unter den Elementen dieser Form die primitiven Elemente, so kennen wir alle primitiven Elemente, da Addition von $\mathbb{Q}$-Skalaren in jedem Körper $\mathbb{Q}(\alpha)$ möglich ist.
Sei α wie oben und f dessen Minimalpolynom. Da unsere Erweiterung normal ist, zerfällt das Minimalpolynom f in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ in Linearfaktoren. Weiter ist die Erweiterung separabel, also hat auch das irreduzible Minimalpolynom nur einfache Nullstellen. Somit ist unser Element genau dann primitiv, wenn sein Minimalpolynom Grad 4 hat, denn der Grad des Minimalpolynoms ist der Grad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Aus

$$4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

folgt dann, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\alpha)] = 1$, also $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.
Vorüberlegung: Hat ein Polynom $g \in \mathbb{Q}[X]$ eine Nullstelle $\beta \in \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so hat das Polynom g auch für jeden Automorphismus $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ das Element $\sigma(\beta)$ als Nullstelle in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Somit ist die Nullstellenmenge von f gleich der Menge

$$\{\alpha, \sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha)\},$$

denn, wie wir uns leicht klar machen können, ist das Polynom

$$\prod_{i=0}^{3} (X - \sigma_i(\alpha))$$

ein Polynom aus $\mathbb{Q}[X]$: Seine Koeffizienten sind Fixpunkte aller 4 Automorphismen, also rationale Zahlen, wie aus voriger Aufgabe klar wurde.
Nun sehen wir

$$\begin{aligned} \alpha = \sigma_0(\alpha) &= a\sqrt{2} + b\sqrt{3} + c\sqrt{6} \\ \sigma_1(\alpha) &= -a\sqrt{2} + b\sqrt{3} - c\sqrt{6} \\ \sigma_2(\alpha) &= a\sqrt{2} - b\sqrt{3} - c\sqrt{6} \\ \sigma_3(\alpha) &= -a\sqrt{2} - b\sqrt{3} + c\sqrt{6}. \end{aligned}$$

Sind nun zwei der drei $\mathbb{Q}$-Skalare a, b, c von α nun ungleich 0, so liefert obiger Katalog 4 verschiedene Elemente von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Damit ist in diesem Fall α ein primitives Element.
Ist nur einer der drei Skalare ungleich 0, so ist α kein primitives Element. Dies sehen wir aus

$$(X - a\sqrt{2}) \cdot (X + a\sqrt{2}) = X^2 - 2a^2 \in \mathbb{Q}[X],$$

$$(X - b\sqrt{3}) \cdot (X + b\sqrt{3}) = X^2 - 3b^2 \in \mathbb{Q}[X],$$

$$(X - c\sqrt{6}) \cdot (X + c\sqrt{6}) = X^2 - 6c^2 \in \mathbb{Q}[X].$$

Ist keiner der Skalare ungleich 0, so ist offensichtlich $\mathbb{Q}(\alpha) = \mathbb{Q}$, ein langweiliger Fall.

Aufgabe 54 Berechne den Körper $\mathbb{F}_9$ und bestimme die Ordnung der Elemente aus $\mathbb{F}_9^\times$.

LÖSUNG: Der Körper $\mathbb{F}_9$ ist bis auf $\mathbb{Z}_3$-Isomorphie eindeutig. Wir realisieren ihn dadurch, daß wir aus $\mathbb{Z}_3[X]$ ein irreduzibles Polynom vom Grad 2 rausfaktorisieren. Als solche kommen die Polynome

$$X^2 + 1, X^2 + X + 2, X^2 + 2X + 2$$

in Frage. Wir führen das Verfahren für $X^2 + 1$ durch.
$\mathbb{F}_9$ besteht somit aus dem Elementen

$$\{0, 1, 2, X, X + 1, X + 2, 2X, 2X + 1, 2X + 2\}.$$

Die Multiplikationstabelle rechne ich hier nicht vor, wichtig ist die Relation $X^2 = 2 = -1$ zu verwenden.
Als Vektorraum ist $\mathbb{F}_9$ isomorph zu $\mathbb{Z}_3 \cdot \mathbb{1} \oplus \mathbb{Z}_3 \cdot X$.
Es gibt 4 Elemente der Ordnung 8:

$$X + 1, 2X + 1, 2X + 2, X + 2.$$

Die Elemente der Ordnung 4 sind die Quadrate davon:

$$2X, X.$$

Schließlich ist 2 das Element der Ordnung 2 und 1 das Element der Ordnung 1.

Hausübungen

Aufgabe H21 (Automorphismen normaler separabler Erweiterungen) Es sei $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[X]$ ein separables Polynom und $\mathbb{L}$ ein Zerfällungskörper von f. Zeige, daß folgende Aussagen äquivalent sind:

(1) Die Gruppe $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ operiert transitiv auf den Nullstellen von f in $\mathbb{L}$.

(2) Das Polynom f ist irreduzibel.

LÖSUNG: Es seien $a_1, ..., a_n$ die Nullstellen von f in $\mathbb{L}$. Wir kennen die Äquivalenz folgender Aussagen:

(1) $m_{a_i,\mathbb{K}} = m_{a_j,\mathbb{K}}$.

(2) Es gibt ein $\varphi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ mit $\varphi(a_i) = a_j$.

(1) $\Rightarrow$ (2) : Operiert die Gruppe transitiv, so gibt es für jedes i ein $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ mit

$$m_{a_1,\mathbb{K}} = m_{\sigma(a_1),\mathbb{K}} = m_{a_i,\mathbb{K}}.$$

Damit ist $m_{a_1,\mathbb{K}}$ das Minimalpolynom aller seiner Nullstellen, also irreduzibel.
(2) $\Rightarrow$ (1) : Ist f irreduzibel, so ist f für jedes a_i das Minimalpolynom, also gibt es für i, j auch einen $\mathbb{K}$-Automorphismus φ mit $\varphi(a_i) = a_j$. Damit operiert die Automorphismengruppe transitiv.

Aufgabe H22 (Endliche Erweiterungen endlicher Körper) Es sei p eine Primzahl.

(a) Es sei $\mathbb{K}$ ein Körper mit Charakteristik p. Zeige, daß jede endliche Erweiterung $\mathbb{L}/\mathbb{K}$, deren Erweiterungsgrad nicht von p geteilt wird, separabel ist.

(b) Es seien $\mathbb{K}_1$ und $\mathbb{K}_2$ Zwischenkörper einer Körpererweiterung $\mathbb{L}/\mathbb{Z}_p$. Zeige, daß folgende Aussagen äquivalent sind:

 (1) $|\mathbb{K}_1| = |\mathbb{K}_2|$.

 (2) $\mathbb{K}_1 = \mathbb{K}_2$.

LÖSUNG: (a) Für alle $a \in \mathbb{L}$ ist $[\mathbb{K}(a) : \mathbb{K}] = \deg(m_{a,\mathbb{K}})$ ein Teiler von $[\mathbb{L} : \mathbb{K}]$. Da $[\mathbb{L} : \mathbb{K}]$ nicht von p geteilt wird, wird somit auch $\deg(m_{a,\mathbb{K}})$ nicht von p geteilt. Somit folgt

$$m'_{a,\mathbb{K}} \neq 0,$$

also ist a separabel. Da $a \in \mathbb{L}$ beliebig war, ist jedes Element aus $\mathbb{L}$ separabel, also ist $\mathbb{L}/\mathbb{K}$ eine separable Erweiterung.

(b) Angenommen, $\mathbb{K}_1$ und $\mathbb{K}_2$ besitzen q Elemente. Da die Einheitengruppe von $\mathbb{K}_1$ und $\mathbb{K}_2$ zyklisch ist, ist jedes Element $x \in \mathbb{K}_1$ und $y \in \mathbb{K}_2$ Nullstelle des Polynoms

$$X^q - X \in \mathbb{L}[X].$$

Dieses hat jedes Element aus $\mathbb{K}_1$ und jedes Element aus $\mathbb{K}_2$ als Nullstelle. Da obiges Polynom jedoch maximal q Nullstellen haben kann, folgt, $\mathbb{K}_1 = \mathbb{K}_2$.