Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 20. Januar 2009

Algebra

12. Übung mit Lösungshinweisen

Aufgabe 55 Sei $\mathbb{K}$ ein endlicher Körper. Zeige, daß für jedes Element $a \in \mathbb{K}$ Elemente $b, c \in \mathbb{K}$ existieren mit $a = b^2 + c^2$.

LÖSUNG: Hat $\mathbb{K}$ Charakteristik 2, so ist jedes Element ein Quadrat, da die Abbildung

$$\mathbb{K} \ni x \to x^2 \in \mathbb{K}$$

ein Automorphismus ist. Somit ist $x = x + 0$ eine mögliche Darstellung.
Es habe also $\mathbb{K}$ eine Charakteristik ungleich 2. Betrachte die multiplikative Einheitengruppe $\mathbb{K}^\times$. Da diese abelsch ist, ist die Abbildung

$$\varphi : \mathbb{K}^\times \ni x \to x^2 \in \mathbb{K}^\times$$

ein Gruppenhomomorphismus. Somit gilt

$$\mathrm{im}(\varphi) \cong \mathbb{K}^\times / \ker(\varphi).$$

Da der Kern dieser Abbildung genau aus $\{-1, 1\}$ besteht, erhalten wir

$$|\mathrm{im}(\varphi)| = \frac{|\mathbb{K}^\times|}{|\{-1,1\}}|,$$

also enthält die Menge der invertierbaren Quadrate genau $\frac{q-1}{2}$ Elemente, wobei q die Anzahl der Elemente von $\mathbb{K}$ bezeichne. Da 0 ebenfalls ein Quadrat ist, gibt es genau $\frac{q+1}{2}$ Qadratzahlen in $\mathbb{K}$.
Sei $a \in \mathbb{K}$. Definiere die Menge

$$N_a := \{a - b^2 : b \in \mathbb{K}\}.$$

Diese Menge enthält ebenfalls $\frac{q+1}{2}$ Elemente. Somit kann der Schnitt von N_a mit den Quadratzahlen nicht leer sein, da jede dieser beiden Mengen mehr als die Hälfte aller Elemente enthält. Ist d im Schnitt beider Mengen, so gibt es ein c mit

$$c^2 = d = a - b^2.$$

Somit erhalten wir

$$a = b^2 + c^2$$

und da a beliebig war, folgt die Behauptung.

Aufgabe 56 Entscheide, ob die Erweiterung $\mathbb{R}/\mathbb{Q}$ galoissch ist und bestimme die Gruppe $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$.

LÖSUNG: Ist $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ und $\mathbb{R} \ni x \geq 0$, so gibt es ein $y \in \mathbb{R}$ mit $x = y^2$. Also gilt auch

$$\sigma(x) = \sigma(y)^2 \geq 0.$$

Insofern bildet σ die positiven Elemente in positive Elemente ab.
Weiter erhalten wir durch folgende Rechnung

$$\begin{aligned} a \geq b &\Leftrightarrow (a-b) \geq 0 \\ &\Leftrightarrow \sigma(a-b) \geq 0 \\ &\Leftrightarrow \sigma(a) \geq \sigma(b), \end{aligned}$$

daß σ eine monotone Abbildung ist.
Sei $(x_n)_{n\in\mathbb{N}}$ eine Nullfolge in $\mathbb{R}$, $\mathbb{Q} \ni \epsilon > 0$, $N_0 \in \mathbb{N}$ und $|x_n| < \epsilon$ für $n > N_0$, dann gilt

$$-\epsilon < x_n < \epsilon,$$

also auch

$$-\sigma(\epsilon) < \sigma(x_n) < \sigma(\epsilon).$$

Da σ Elemente aus $\mathbb{Q}$ fix läßt, erhalten wir

$$-\epsilon < \sigma(x_n) < \epsilon,$$

also ist auch $(\sigma(x_n))$ eine Nullfolge in $\mathbb{R}$. Damit können wir leicht folgern, daß σ eine stetige $\mathbb{Q}$-lineare Abbildung von $\mathbb{R}$ nach $\mathbb{R}$ ist. Da σ auf einer in $\mathbb{R}$ dichten Menge die Identität ist, ist auf Grund der Stetigkeit $\sigma = \mathrm{id}$. Die Gruppe $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ ist somit die triviale Gruppe $\{\mathrm{id}_{\mathbb{R}}\}$.

Aufgabe 57 Betrachte das Polynom $f(X) = X^3 - 7 \in \mathbb{Q}[X]$ und den Zerfällungskörper $\mathbb{L}$ von f.

(a) Zeige, daß die Galoisgruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{Q})$ isomorph zur D_3, der Diedergruppe mit 6 Elementen, ist.
Hinweis: *Finde einen $\mathbb{Q}$-Automorphismus von $\mathbb{L}$ der Ordnung 2 und einen der Ordnung 3.*

(b) Finde alle Untergruppen der Galoisgruppe und die zugehörigen Zwischenkörper von $\mathbb{L}/\mathbb{Q}$. Welche dieser Zwischenkörper sind ebenfalls galoissch über $\mathbb{Q}$?

(c) Finde ein primitives Element der Erweiterung.

LÖSUNG: (a) Die Nullstellen von f sind die komplexen Zahlen

$$\{\alpha, \alpha \cdot \beta, \alpha \cdot \beta^2\},$$

wobei $\alpha := \sqrt[3]{7}$ und $\beta := -\frac{1}{2} + \frac{1}{2}\sqrt{3} \cdot i = e^{\frac{2}{3}\pi \cdot i}$ bezeichne. Wir erhalten somit

$$\mathbb{L} = \mathbb{Q}(\alpha, \beta).$$

Weiter gilt $[\mathbb{L} : \mathbb{Q}] = 6$, denn $\mathbb{Q}(\alpha)$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 3 und $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Da $\mathbb{Q}(\alpha)(\beta)$ echt komplexe Zahlen enthält, ist dies eine Erweiterung vom Grad mindestens 2. Andererseits ist β Nullstelle des Polynoms $X^2 + X + 1$, somit gilt $[\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\beta)] = 2$. Da $\mathbb{L}/\mathbb{Q}$ galoissch ist (normal und separabel), gilt

$$|\mathrm{Gal}(\mathbb{L}, \mathbb{K})| = 6.$$

Da es insgesamt nur 3 Isomorphieklassen von Gruppen mit 6 Elementen gibt, ist unsere Gruppe isomorph zu $\mathbb{Z}_6, \mathbb{Z}_3 \oplus Z_2$ oder $D_3 = S_3$.
Nun suchen wir die erzeugenden $\mathbb{Q}$-Automorphismen. Wir betrachten den $\mathbb{Q}(\beta)$-Automorphismus

$$\sigma : \mathbb{L} \to \mathbb{L}, \sigma(\sqrt[3]{7}) := \sqrt[3]{7} \cdot \beta.$$

Diesen muß es geben, da $\sqrt[3]{7}$ und $\sqrt[3]{7} \cdot \beta$ beides Nullstellen des Minimalpolynoms von α sind. Realisiert wird er durch

$$\mathbb{Q}(\beta)(\alpha) \cong \mathbb{Q}(\beta)[X]/(f) \cong \mathbb{Q}(\beta)(\alpha \cdot \beta).$$

Wir sehen

$$\sigma^2(\alpha) = \alpha \cdot \beta^2 \neq \alpha, \quad \sigma^3(x) = x,$$

also hat σ Ordnung 3. Setze analog einen zweiten Automorphismus τ von $\mathbb{L}$, welcher $\mathbb{Q}(\alpha)$ fix läßt, durch

$$\tau(\beta) := \overline{\beta} = \beta^2.$$

Diese Abbildung permutiert die Nullstellen des Minimalpolynoms $X^2 + X + 1$ von β und ist somit der eindeutige $\mathbb{Q}(\alpha)$-Automorphismus, der nicht trivial ist.
Beide angegebenen Automorphismen kommutieren nicht:

$$\begin{aligned}
\sigma \circ \tau(\alpha) &= \sigma(\alpha) \\
&= \alpha \cdot \beta \\
\tau \circ \sigma(\alpha) &= \sigma(\alpha \cdot \beta) \\
&= \alpha \cdot \beta^2.
\end{aligned}$$

Somit ist die Galoisgruppe nicht kommutativ und zur D_3 isomorph.

(b) Die echten Untergruppen der Gruppe D_3 sind die vier Gruppen

$$< \tau >, < \sigma >, < \tau \circ \sigma >, < \tau \circ \sigma^2 > .$$

Die Untergruppe $< \tau >$ hat 3 Elemente, alle anderen Untergruppen haben 2 Elemente. Wir erhalten leicht

$$\mathrm{Fix}(< \tau >) = \mathbb{Q}(\alpha),$$
$$\mathrm{Fix}(< \sigma >) = \mathbb{Q}(\beta).$$

Für die Gruppe $< \tau \circ \sigma >$ ist das Element $\alpha \cdot \beta$ ein Fixelement und der Körper $\mathbb{Q}(\alpha \cdot \beta)$ der Fixkörper. Dieser hat Erweiterungsgrad 3 über $\mathbb{Q}$.
Für die Gruppe $< \tau \circ \sigma^2 >$ ist das Element $\alpha \cdot \beta^2$ ein Fixelement und der Körper $\mathbb{Q}(\alpha^2 \cdot \beta)$ der Fixkörper. Dieser hat Erweiterungsgrad 3 über $\mathbb{Q}$.
Fixkörper der trivialen Gruppe ist natürlich ganz $\mathbb{L}$.
Die Normalteiler von D_3 sind die Untergruppen $\{\mathbb{1}\}, D_3, < \sigma >$. Die ersten beiden Gruppen sind offensichtlich normal, die Untergruppe $< \sigma >$ ist daher normal, da sie Index 2 hat. Alle 3 Untergruppen mit Index 3 sind nicht normal, da sie zueinander konjugiert sind, was man leicht durch Konjugation mit σ nachrechnet.
Hilfreich ist es, eine Präsentation von D_3 zu kennen. Diese ist

$$D_3 =< \sigma, \tau | \sigma^3 = \tau^2 = \mathbb{1}, \sigma \cdot \tau = \tau \cdot \sigma^2 > .$$

Als Fazit sehen wir, daß der Zwischenkörper $\mathrm{Fix}(< \sigma >) = \mathbb{Q}(\beta)$ der einzige galoissche echte Zwischenkörper der Erweiterung $\mathbb{L}/\mathbb{Q}$ ist. Dieser ist in der Tat der Zerfällungskörper von $X^2 + X + 1$ und damit normal und separabel.

(c) Ein primitives Element ist z. B. $\alpha + \beta$, da dieses Element als Bahn unter $\mathrm{Gal}(\mathbb{L}, \mathbb{Q})$ eine sechselementige Menge besitzt.

Aufgabe 58 Es sei $\mathbb{L}$ ein Körper und G eine Untergruppe von $\mathrm{Aut}(\mathbb{L})$. Weiter setze

$$\mathbb{K} := \mathbb{L}^G = \{a \in \mathbb{L} : \sigma(a) = a \text{ für alle } \sigma \in G\}$$

den Fixkörper unter G.
Zeige, ist G nicht endlich, $\mathbb{L}/\mathbb{K}$ aber algebraisch, so ist $\mathbb{L}/\mathbb{K}$ eine unendliche Galoiserweiterung und G ist eine Untergruppe der Galoisgruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$.

LÖSUNG: Ist $a \in \mathbb{L}$, so gibt es ein maximales System von Automorphismen $\sigma_1, ..., \sigma_r$, so daß $\sigma_1(a), ..., \sigma_r(a)$ paarweise verschiedene Elemente von $\mathbb{L}$ sind. Dies folgt daher, daß $\sigma(a)$ immer eine Nullstelle des Minimalpolynoms von a über $\mathbb{K}$ sein muß für jeden Automorphismus $\sigma \in G$. Weiter permutiert jedes $\sigma \in G$ obige Menge, also folgt, daß das Polynom

$$f := \prod_{k=1}^{r}(X - \sigma_k(a))$$

Koeffizienten in $\mathbb{K}$ hat, denn es gilt $f = \sigma_*(f)$ für jedes $\sigma \in G$. Also ist a Nullstelle eines separablen Polynoms und somit ist die Erweiterung separabel.
Weiter ist $\mathbb{L}/\mathbb{K}$ normal, da $\mathbb{L}$ der Zerfällungskörper aller Polynome von obigem Typ ist. Also ist $\mathbb{L}/\mathbb{K}$ eine Galoiserweiterung. Offensichtlich ist G eine Untergruppe von $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$, eine Gruppe, welche viel größer sein kann, als G.

Hausübungen

Aufgabe H23 (Algebraischer Abschluß) Sei $p > 0$ eine Primzahl. Wir starten mit

$$\mathbb{F}_p := \mathbb{Z}_p$$

und wählen rekursiv für jedes $n \in \mathbb{N}$ einen Oberkörper $\mathbb{F}_{p^{(n+1)!}}$ von $\mathbb{F}_{p^{n!}}$ mit $p^{(n+1)!}$ Elementen. Damit erhalten wir eine Kette von Körpern

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq ...$$

Wir setzen

$$\mathbb{F}_{p^\infty} := \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}.$$

(a) Erkläre auf $\mathbb{F}_{p^\infty}$ eine Addition und Multiplikation, welche $\mathbb{F}_{p^\infty}$ zu einem Körper macht und die Körperoperationen jedes $\mathbb{F}_{p^{n!}} \subseteq \mathbb{F}_{p^\infty}$ fortsetzt.

(b) Zeige, daß $\mathbb{F}_{p^\infty}$ algebraisch abgeschlossen ist.

(c) Zeige, daß $\mathbb{F}_{p^\infty}$ ein algebraischer Abschluß von $\mathbb{Z}_p$ ist.

LÖSUNG: (a) Sind $x, y \in \mathbb{F}_{p^\infty}$, so existiert ein $n \in \mathbb{N}$ mit $x, y \in \mathbb{F}_{p^{n!}}$. Somit definiere $x + y$, bzw. $x \cdot y$ als das entsprechende Ergebnis in $\mathbb{F}_{p^{n!}}$.
Dann ist $x+y$, bzw. $x \cdot y$ wohldefiniert, denn ist $x, y \in \mathbb{F}_{p^{m!}}$, so ist $\mathbb{F}_{p^{m!}} \subseteq \mathbb{F}_{p^{n!}}$ oder $\mathbb{F}_{p^{n!}} \subseteq \mathbb{F}_{p^{m!}}$ und das Ergebnis $x + y$, bzw. $x \cdot y$ stimmt in $\mathbb{F}_{p^{m!}}$ mit dem in $\mathbb{F}_{p^{n!}}$ überein.
Weiter ist jeder Körper $\mathbb{F}_{p^{n!}}$ ein Unterkörper von $\mathbb{F}_{p^\infty}$.

(b) Sei $f \in \mathbb{F}_{p^\infty}[X]$ ein nicht konstantes Polynom und $\mathbb{K}$ ein Erweiterungskörper von $\mathbb{F}_{p^\infty}$, in welchem f eine Nullstelle α besitzt. Sind $a_0, ..., a_n$ die Koeffizienten von f, so ist dann

$$\mathbb{Z}_p(a_0, ..., a_n, \alpha)/\mathbb{Z}_p$$

eine endliche Erweiterung und somit $\mathbb{L} := \mathbb{Z}_p(a_0, ..., a_n, \alpha)$ ein endlicher Körper, also $|\mathbb{L}| = p^m$ für ein $m \in \mathbb{N}$. Somit gilt

$$\mathbb{L} \subseteq \mathbb{F}_{p^{m!}},$$

da m die Zahl $m!$ teilt. Also folgt

$$\alpha \in \mathbb{L} \subseteq \mathbb{F}_{p^{m!}} \subseteq \mathbb{F}_{p^\infty},$$

also ist $\mathbb{F}_{p^\infty}$ algebraisch abgeschlossen.

(c) Wir zeigen noch, daß $\mathbb{F}_{p^\infty}/\mathbb{Z}_p$ algebraisch ist. Ist $x \in \mathbb{F}_{p^\infty}$, so ist $x \in \mathbb{F}_{p^{n!}}$ für ein $n \in \mathbb{N}$, also

$$[\mathbb{Z}_p(x) : \mathbb{Z}_p] \leq [\mathbb{F}_{p^{n!}} : \mathbb{Z}_p] = n!.$$

Damit ist $\mathbb{F}_{p^\infty}$ eine algebraische und algebraisch abgeschlossene Erweiterung von $\mathbb{Z}_p$, also ein algebraischer Abschluß.

Aufgabe H24 (Abelsche Erweiterungen) Es seien $p_1, ..., p_n$ paarweise verschiedene Primzahlen und $\mathbb{L} := \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$. Zeige, daß $\mathbb{L}/\mathbb{Q}$ galoissch ist und bestimme die Galoisgruppe $G := \mathrm{Gal}(\mathbb{L}, \mathbb{Q})$.

LÖSUNG: Wir zeigen per Induktion $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}), \mathbb{Q}) \cong \bigoplus_{k=1}^n \mathbb{Z}_2$. Weiter zeigen wir, daß diese Gruppe von den Abbildungen erzeugt werden, welche genau eine Wurzel auf ihr negatives abbilden und die dazu algebraisch unabhängigen Wurzeln fest lassen.
Ist $n = 1$, so ist $\mathbb{L}$ eine Erweiterung von Grad 2 über $\mathbb{Q}$ und damit galoissch. Die Galoisgruppe ist somit $\mathbb{Z}_2$ und wird vom Flip auf der Menge $\{\sqrt{p}, -\sqrt{p}\}$ erzeugt.

Betrachte $n+1$. Dann wissen wir aus H18, daß $X^2 - p_{n+1}$ über $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$ irreduzibel ist. Somit existieren genau zwei $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$-Automorphismen von $\mathbb{L}$. Wir bezeichnen den nichttrivialen von beiden mit σ_{n+1}. Weiter ist nach Induktionsvorraussetzung $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}), \mathbb{Q})$ zu $\bigoplus_{k=1}^n \mathbb{Z}_2$ isomorph und wird erzeugt von $\sigma_1, ..., \sigma_n$, den Automorhpismen, die jeweils $\sqrt{p_i}$ auf $-\sqrt{p_i}$ abbilden. Diese Erzeuger kommutieren offensichtlich mit der Abbildung σ_{n+1}. Wir erhalten somit in $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ zwei Untergruppen, zum einen die Gruppe $H_n \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}), \mathbb{K})$, deren Elemente wir durch triviale Wirkung auf $\sqrt{p_{n+1}}$ fortsetzen und zum anderen die Gruppe $N := <\sigma_{n+1}> \cong \mathbb{Z}_2$. Diese Untergruppen erfüllen die Relation

$$H_n \cap N = \{\mathrm{id}\}$$

und die erzeugte Gruppe $H_n \cdot N$ ist abelsch. Also gilt

$$H_n \cdot N \cong H_n \oplus N$$

und wir erhalten

$$|H_n \oplus N| = |H_n| \cdot |N| = 2^n \cdot 2 = 2^{n+1}.$$

Damit gilt bereits

$$\mathrm{Gal}(\mathbb{L}, \mathbb{K}) = H_n \cdot N$$

und aus der Induktionsvorraussetzung erhalten wir

$$\mathrm{Gal}(\mathbb{L}, \mathbb{K}) = H_n \cdot N \cong H_n \oplus \mathbb{Z}_2 \cong \left(\bigoplus_{k=1}^{n} \mathbb{Z}_2 \right) \oplus \mathbb{Z}_2 \cong \bigoplus_{k=1}^{n+1} \mathbb{Z}_2.$$