Übungsblatt 10: Körpererweiterungen und Automorphismen

1. Grundlagen

1.1. Zeigen Sie, dass die Menge der Zahlen $\{\log(p) : p \text{ Primzahl }\}$ im $\mathbb{Q}$-Vektorraum $\mathbb{R}$ linear unabhängig ist. Folgern Sie $|\mathbb{R} : \mathbb{Q}| = \infty$.

1.2. (a) Zeigen Sie, dass die Menge der algebraischen Zahlen über $\mathbb{Q}$ abzählbar ist.
(b) Zeigen Sie, dass die Menge der reellen Zahlen überabzählbar ist.
(c) Folgern Sie die Existenz von reellen transzendenten Zahlen.

2. Körpererweiterungen

S 2.1. (2 Punkte) Sind die Erweiterungen $\mathbb{Q}[\sqrt{7}]$ und $\mathbb{Q}[\sqrt{11}]$ isomorph?

2.2. Bestimmen Sie die Dimension von $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ über $\mathbb{Q}$.
Finden Sie fünf Zwischenkörper der Körpererweiterung $\mathbb{Q}[\sqrt{2},\sqrt{3}]|\mathbb{Q}$.

2.3. Sei $a+bi \in \mathbb{C}$ algebraisch über $\mathbb{Q}$. Zeigen Sie, dass dann auch $a-bi$, a und b algebraisch über $\mathbb{Q}$ sind.

V 2.4. Sei $E|K$ eine Körpererweiterung mit $|E : K| < \infty$.
(a) Es ist E algebraisch über K und $E = K[\alpha_1,\dots,\alpha_r]$ für geeignete $\alpha_i \in E$.
(b) Sei $|E : K| = p$ eine Primzahl, dann gilt sogar $E = K[\xi]$ für ein $\xi \in E \setminus K$.
(c) Sei $|E : K| = 2$ und $\operatorname{char}(K) \neq 2$. Zeigen Sie, dass es ein Element $a \in E$ gibt mit $a \notin K$, $a^2 \in K$. Somit ist $E = K[a]$ und $(1,a)$ ist eine Basis von E über K.

2.5. Eine Erweiterung $E|K$ ist genau dann algebraisch, wenn jeder Teilring R mit $K \subset R$ auch ein Körper ist.

V 2.6. Sei $E|K$ eine Körpererweiterung und $\alpha,\beta \in E$ seien algebraisch über K.
(a) Zeigen Sie, dass $|K[\alpha,\beta] : K| \leq |K[\alpha] : K| \cdot |K[\beta] : K|$ gilt.
(b) Sind $|K[\alpha] : K|$ und $|K[\beta] : K|$ teilerfremd, so gilt in (a) Gleichheit.

2.7. Man bestimme die algebraischen Erweiterungen von $\mathbb{C}$ und von $\mathbb{R}$.
Man gebe Beispiele nicht-algebraischer Erweiterungen von $\mathbb{C}$ und von $\mathbb{R}$.

2.8. Angenommen $e \in \mathbb{R}$ sei transzendent über $\mathbb{Q}$. Ist e dann auch transzendent über jeder algebraischen Erweiterung von $\mathbb{Q}$?

2.9. Jede einfache transzendente Körpererweiterung $E|K$ hat unendlich viele Zwischenkörper.

3. Zerfällungskörper

3.1. Sei $\xi = e^{2\pi i/p}$ eine Nullstelle des Polynoms $X^p - 1$ für eine Primzahl p.
Ist $\mathbb{Q}[\xi]$ der Zerfällungskörper von $X^p - 1$ über $\mathbb{Q}$?

S 3.2. (6 Punkte)
(a) Zeigen Sie, dass $\mathbb{Q}[\sqrt[3]{2}, j]$ mit $j = e^{2\pi i/3}$ ein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ ist.
(b) Welche Dimension haben $\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[j\sqrt[3]{2}]$ und $\mathbb{Q}[j^2\sqrt[3]{2}]$ als $\mathbb{Q}$-Vektorräume? Bestimmen Sie eine Basis von $\mathbb{Q}[\sqrt[3]{2}]$ über $\mathbb{Q}$.
(c) Warum ist $\mathbb{Q}[\sqrt[3]{2}]$ kein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$?
(d) Finden Sie das Minimalpolynom von j über $\mathbb{Q}$.
(e) Bestimmen Sie die Dimension von $\mathbb{Q}[j]$ und $\mathbb{Q}[\sqrt[3]{2}, j]$ über $\mathbb{Q}$.
(f) Bestimmen Sie sechs Zwischenkörper der Erweiterung $\mathbb{Q}[\sqrt[3]{2}, j]|\mathbb{Q}$.

3.3. Man zeige, dass $E = \mathbb{Q}[i, \sqrt[4]{2}]$ ein Zerfällungskörper von $X^4 + 2$ über $\mathbb{Q}$ ist. Ist E auch ein Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$? Man bestimme den Grad $|E : \mathbb{Q}|$ und finde eine Basis von E über $\mathbb{Q}$.

4. Körperautomorphismen

4.1. Seien K und L Körper und $\sigma : K \to L$ ein Körperhomomorphismus. Zeigen Sie, dass σ injektiv ist und K und L die gleiche Charakteristik haben.

4.2. Sei K ein Körper und $\sigma : K \to K$ ein Körperautomorphismus.
(a) Zeigen Sie, dass σ den Primkörper von K punktweise festlässt. Folgern Sie daraus, dass $\mathbb{F}_p$ und $\mathbb{Q}$ nur die Identität als Körperautomorphismen haben.
(b) Zeigen Sie weiter, dass auch $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_\mathbb{R}\}$ gilt. *Hinweis:* Es ist $x \geq 0 \Leftrightarrow \exists\, r \in \mathbb{R} : x = r^2$. Folgern Sie daraus, dass σ stetig ist.
(c) Bestimmen Sie alle Automorphismen $\sigma : \mathbb{C} \to \mathbb{C}$ mit $\sigma(\mathbb{R}) = \mathbb{R}$.

4.3. Sei $E|K$ eine Körpererweiterung und $\sigma\colon E \to E$ ein Automorphismus von $E|K$. Für alle Polynome $P \in K[X]$ und $x \in E$ gilt $P(\sigma(x)) = \sigma(P(x))$. Folgern Sie, dass für eine Nullstelle a von P auch $\sigma(a)$ eine Nullstelle von P ist.

V 4.4. (a) Ist $E|K$ algebraisch, dann ist jeder Körperhomomorphismus $\sigma\colon E \to E$ über K ein Automorphismus.
(b) Geben Sie zu einem Körper K eine Erweiterung $E|K$ und einen Körperhomomorphismus $\sigma\colon E \to E$ über K an, der kein Automorphismus ist.

V 4.5. Sei $K \subset \mathbb{C}$ und $K[a]$ eine Erweiterung von Grad 2 mit $a^2 \in K$ (siehe Aufgabe 2.4). Zeigen Sie, dass $\sigma : K[a] \to K[a] : x + ya \mapsto x - ya$ ein nichttrivialer Körperautomorphismus ist und zeigen Sie, dass $\mathrm{Aut}(K[a]|K) = \{\mathrm{id}, \sigma\}$.

4.6. Bestimmen Sie alle Automorphismen von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

5. Endliche Körper

S 5.1. (5 Punkte) Sei $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$.
(a) Begründen Sie, warum $\mathbb{F}_9$ ein Körper ist und $\mathbb{F}_3$ als Teilkörper enthält. Zeigen Sie, dass $(1, X)$ eine Basis von $\mathbb{F}_9$ als Vektorraum über $\mathbb{F}_3$ ist.
(b) Ist die additive Gruppe von $\mathbb{F}_9$ zu $\mathbb{Z}/_9$ oder zu $\mathbb{Z}/_3 \times \mathbb{Z}/_3$ isomorph? Gibt es dann sogar einen Ringisomorphismus zu $\mathbb{Z}/_9$ oder zu $\mathbb{Z}/_3 \times \mathbb{Z}/_3$?
(c) Bestimmen Sie die Ordnungen der Elemente in $\mathbb{F}_9^\times$.
(d) Bestimmen Sie das Bild eines allgemeinen Elementes $a + bX \in \mathbb{F}_9$ unter dem Frobenius-Homomorphismus $x \mapsto x^3$.
(e) Ist $\mathbb{F}_9$ isomorph zu $\mathbb{F}_3[Y]/(Y^2 + Y + 1)$ oder zu $\mathbb{F}_3[Z]/(Z^2 + Z - 1)$? Geben Sie gegebenenfalls einen Isomorphismus κ an. *Hinweis:* Betrachten Sie κ zuerst als lineare Abbildung von $\mathbb{F}_3$-Vektorräumen und zeigen Sie anschließend noch $\kappa(X^2) = \kappa(X)^2$.

5.2. Zeigen Sie, dass ein endlicher Körper nie algebraisch abgeschlossen sein kann.
Hinweis: Jeder endliche Körper F hat eine Primzahl p als Charakteristik. Zu dem Polynom $P = X^{p^n} - X$ in $F[X]$ berechne man $\mathrm{ggT}(P, P')$ und leite hieraus die Anzahl der verschiedenen Nullstellen von P ab.

5.3. Geben Sie einen unendlichen Körper K mit Charakteristik $p > 0$ an, so dass der Frobenius-Homomorphismus $x \mapsto x^p$
(a) injektiv, aber nicht surjektiv ist,
(b) ein Automorphismus von K ist.