

8. Übung Algebra II

1. Aufgabe Einfache Artin-Schreier-Erweiterungen

(4 Punkte)

Sei K ein Körper, $\text{Char} K = p > 0$ und $f(t) = t^p - t - a \in K[t]$ irreduzibel. Zeige folgende Aussagen:

(a) Der Zerfällungskörper E von f ist galoissch über K und es gilt $E = K(b)$ mit $f(b) = 0$.

(b) Durch

$$\phi : G(E/K) \rightarrow \mathbb{Z}/p\mathbb{Z}, \quad \sigma \mapsto \phi(\sigma) \text{ mit } \sigma(b) = b + \phi(\sigma)$$

wird ein Isomorphismus definiert. Die Erweiterung E/K ist zyklisch von der Ordnung p .

2. Aufgabe Automorphismen

(4 Punkte)

(a) Sei $K = \mathbb{F}_{p^n}$ gegeben mit p Primzahl und $G := \text{Aut}_{\mathbb{F}_p}(K)$. Ist G zyklisch? Wenn ja, welche Ordnung hat G ? Gib einen Erzeuger an.

(b) Sei $K = \mathbb{Q}(\zeta)$ wobei $\zeta \in \mathbb{C}$ eine primitive n -te Einheitswurzel ist. Zeige, dass $\text{Aut}_{\mathbb{Q}}(K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ gilt.

3. Aufgabe Unendliche Galoiserweiterungen

(4 Punkte)

Sei $K := \bigcup_{i=1}^{\infty} \mathbb{F}_{p^{l^i}}$ mit p, l Primzahl. Dann ist K eine unendliche Galoiserweiterung von $\mathbb{F}_p$. Ferner sei eine l -adische Reihe $\sum_{k=0}^{\infty} \lambda_k l^k$ mit $\lambda_k = 1$ für $k = 0, 1, 2, \dots$ gegeben und $a_n := \sum_{k=0}^n \lambda_k l^k$. Wir definieren nun eine Abbildung $\tau : K \rightarrow K$ mit $\tau(x) = x^{p^{a_i}}$ wenn $x \in \mathbb{F}_{p^{l^i}}$ wobei i minimal ist. Wir wissen bereits, dass τ ein Automorphismus von K ist. Zeige

(a) $\tau \in \overline{\langle \sigma \rangle} = \mathcal{G}_{K/\mathbb{F}_p} \circ \mathcal{F}_{K/\mathbb{F}_p}(\langle \sigma \rangle)$

(b) $\tau \notin \langle \sigma \rangle$.

4. Aufgabe Praktische Aufgabe

(4 + 10 Punkte)

Sei $p > 2$ Primzahl und $q = p^m$ mit $m \in \mathbb{N}$. Schreibe einen Algorithmus, der ein gegebenes normiertes quadratfreies Polynom f vom Grad n aus $\mathbb{F}_q[x]$ faktorisiert. Gehe dazu folgendermaßen vor:

- (a) Betrachte den Vektorraum $R := \mathbb{F}_q[x]/(f)$ der Dimension n über $\mathbb{F}_q$ und die $\mathbb{F}_q$ -lineare Abbildung

$$\beta: R \longrightarrow R, \quad a \longmapsto a^q - a. \quad (1)$$

Eine Basis des $\mathbb{F}_q$ -Vektorraumes R ist $1 \bmod f, x \bmod f, \dots, x^{n-1} \bmod f$. Ist $f = f_1 \cdots f_r$ die Faktorisierung von f in paarweise verschiedene irreduzible Faktoren $f_i \in \mathbb{F}_q[x]$, so ist

$$R \cong \mathbb{F}_q[x]/(f_1) \times \cdots \times \mathbb{F}_q[x]/(f_r). \quad (2)$$

- (b) Nun gilt für $a \in R$:

$$a \in \ker(\beta) \Leftrightarrow \chi(a) = (a_1, \dots, a_r)$$

mit $a_i \in \mathbb{F}_q$, $i = 1, \dots, r$ wobei χ der Isomorphismus von (2) ist.

- (c) Berechne nun den Kern von β mittels der Darstellungsmatrix. Ist dann $b_1, \dots, b_r$ eine Basis des Kern von β , so bilde $a := \sum_{i=1}^r c_i b_i$ mit $c_i \in \mathbb{F}_q$ zufällig gewählt.

- (d) Berechne nun den $\text{ggT}(f, a)$ und $\text{ggT}(b-1, f)$ wobei $b := a^{(q-1)/2} \bmod f$ ist.

Warum funktioniert dieser Algorithmus?

Hinweis: Die praktische Aufgabe kann bis zum 09.01.2008 bearbeitet werden. Es gibt 10 Extrapunkte für die richtige Bearbeitung dieser Aufgabe.