Übungen zur Algebra I

Wintersemester 2020/21

Universität Heidelberg
Mathematisches Institut
Prof. Dr. A. Schmidt
Dr. M. Leonhardt

Blatt 10
Abgabetermin: Freitag, 29.01.2021, 9:15 Uhr

Aufgabe 1. *(Galoisgruppe)* (6 Punkte) Es sei $f = X^4 + 2X^2 + 2 \in \mathbb{F}_3[X]$. Bestimmen Sie einen Zerfällungskörper L von f über $\mathbb{F}_3$ sowie die Galoisgruppe und sämtliche Zwischenkörper von $L/\mathbb{F}_3$.

Aufgabe 2. *(Kreisteilungspolynome)* (6 Punkte, je 3 Punkte)

(a) Es sei $\Phi_n(X) \in \mathbb{Z}[X]$ das n-te Kreisteilungspolynom. Zeigen Sie $\Phi_{2n}(X) = \Phi_n(-X)$ für ungerade $n \geq 3$. *(Hinweis: Vergleichen Sie Grade und Nullstellen der beiden Polynome.)*

(b) Es sei K ein beliebiger Körper und $n \in \mathbb{N}$ nicht durch $\mathrm{char}(K)$ teilbar. Wir betrachten

$$\Psi_n(X) := \prod_{\substack{\zeta \in \mu_n(\overline{K}) \\ \text{primitiv}}} (X - \zeta) \in \overline{K}[X].$$

Außerdem sei $\Phi_n(X) = \sum_{i=0}^n a_i X^i$ und $\overline{\Phi}_n(X) = \sum_{i=0}^n \overline{a}_i X^i \in K[X]$, wobei $\overline{a}_i \in K$ das Bild von $a_i \in \mathbb{Z}$ unter dem eindeutigen Ringhomomorphismus $\mathbb{Z} \to K$ ist. Zeigen Sie $\Psi_n(X) = \overline{\Phi}_n(X)$. *(Hinweis: Argumentieren Sie wie in Variante 2 des Beweises von 4.46.)*

Aufgabe 3. *(Diskriminante)* (6 Punkte) Es sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Weiter sei $f \in K[X]$ ein Polynom vom Grad $n \geq 1$ und $\alpha_1, \dots, \alpha_n$ die Nullstellen von f in $\overline{K}$. Wir definieren

$$\delta_f := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in \overline{K}$$

und nennen $\Delta_f := a_n^{2n-2} \delta_f^2 \in \overline{K}$ die *Diskriminante* von f, wobei a_n der Leitkoeffizient von f sei.

(a) (1 Punkt) Zeigen Sie, dass $\Delta_f \neq 0$ genau dann, wenn f separabel ist.

(b) (1 Punkt) Zeigen Sie, dass für quadratische $f = aX^2 + bX + c$ (mit $a \neq 0$) gilt: $\Delta_f = b^2 - 4ac$.

(c) (2 Punkte) Für den Rest der Aufgabe sei f separabel. Es sei L der Zerfällungskörper von f in $\overline{K}$. Wir fassen $G := \mathrm{Gal}(L/K)$ wie üblich als Untergruppe der $\mathfrak{S}_n$ auf via

$$\varphi \colon G \hookrightarrow \mathfrak{S}_n, \quad \sigma \mapsto \varphi(\sigma) \quad \text{gegeben durch} \quad \sigma(\alpha_i) = \alpha_{\varphi(\sigma)(i)} \text{ für alle } i \in \{1, \dots, n\}.$$

Zeigen Sie $\sigma(\delta_f) = \mathrm{sgn}(\varphi(\sigma)) \cdot \delta_f$.

(d) (1 Punkt) Folgern Sie $\Delta_f \in K$.

(e) (1 Punkt) Nun sei $\mathrm{char}(K) \neq 2$. Zeigen Sie, dass $\varphi(G) \subset \mathfrak{A}_n := \ker(\mathrm{sgn})$ genau dann, wenn $\Delta_f \in (K^\times)^2$.

Aufgabe 4. *(Quadratisches Reziprozitätsgesetz)* (6 Punkte) Es seien p, q zwei verschiedene ungerade Primzahlen. Für zu q teilerfremdes $a \in \mathbb{Z}$ definieren wir das *Legendre-Symbol* durch

$$\left(\frac{a}{q}\right) := \begin{cases} 1, & \text{falls } a \bmod q \in (\mathbb{F}_q^\times)^2, \\ -1, & \text{falls } a \bmod q \notin (\mathbb{F}_q^\times)^2. \end{cases}$$

Ziel dieser Aufgabe ist ein Beweis des *Quadratischen Reziprozitätsgesetzes* (1), welches eine Beziehung herstellt zwischen der Frage, ob p ein Quadrat modulo q ist, und der Frage, ob q ein Quadrat modulo p ist. Es gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1, & \text{falls } p, q \equiv 3 \pmod 4, \\ 1, & \text{sonst.} \end{cases} \tag{1}$$

Unser Beweis[1] beruht auf der Untersuchung des Zerfällungskörpers L des Polynoms $f = X^p - 1$ über $\mathbb{F}_q$ und insbesondere der Frage, ob das Bild der Galoisgruppe $G := \mathrm{Gal}(L/\mathbb{F}_q)$ unter der üblichen Einbettung $G \hookrightarrow \mathfrak{S}_p$ (durch Wirkung auf den Nullstellen von f) in der alternierenden Gruppe $\mathfrak{A}_p$ liegt. Zeigen Sie:

(a) (1 Punkt) Das Legendre-Symbol ist *multiplikativ*, d.h. für $a, b \in \mathbb{Z}$ teilerfremd zu q gilt $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$. Außerdem gilt

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } q \equiv 1 \pmod 4, \\ -1, & \text{falls } q \equiv 3 \pmod 4. \end{cases}$$

(Hinweis: Blatt 6, Aufgabe 3(c).)

(b) (2 Punkte) Das Bild von G in $\mathfrak{S}_p$ ist genau dann in $\mathfrak{A}_p$ enthalten, wenn

$$1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

(Hinweis: Benutzen Sie Aufgabe 3 sowie (ohne Beweis) die Formel $\Delta_f = (-1)^{n(n-1)/2}((1-n)^{n-1}b^n + n^n c^{n-1})$ für Polynome der Form $f = X^n + bX + c$.)

Nun sei $\sigma \in G$ der q-Frobenius, d.h. $\sigma(x) = x^q$ für alle $x \in L$. Nach Wahl einer primitiven p-ten Einheitswurzel ζ_p können wir die Nullstellen μ_p von f mit $\mathbb{Z}/p\mathbb{Z}$ identifizieren und die von σ auf $\mathbb{Z}/p\mathbb{Z}$ induzierte Permutation π is gerade die Multiplikation mit q, d.h. $\pi(a) = qa$ für $a \in \mathbb{Z}/p\mathbb{Z}$ (dies alles ist nicht zu zeigen, siehe Satz 4.50 aus der Vorlesung). Es sei $k := \mathrm{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(q)$. Zeigen Sie:

(c) (1 Punkt) Es gilt $\mathrm{sgn}(\pi) = (-1)^{(k-1)\frac{(p-1)}{k}}$.

(Hinweis: Bestimmen Sie die Zykeldarstellung von π, indem sie zunächst den Zykel, in dem $1 \in \mathbb{Z}/p\mathbb{Z}$ liegt, bestimmen. Was wissen Sie dann über das Signum von Zykeln der Länge k?)

(d) (2 Punkte) Folgern Sie aus (c), dass das Bild von G genau dann in $\mathfrak{A}_p$ enthalten ist, wenn

$$1 = \left(\frac{q}{p}\right),$$

und folgern Sie (1) mit Hilfe von (b).

(Hinweis: Wählen Sie einen Erzeuger γ von $\mathbb{F}_p^\times$. Welche Potenzen von γ sind Quadrate in $\mathbb{F}_p^\times$?)

[1] Es gibt mehr als 200 verschiedene Beweise des Quadratischen Reziprozitätsgesetzes. Die ersten acht vollständigen Beweise stammen von Gauß.