Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie
Sommersemester 2016

Prof. Dr. Marco Hien
Ingo Blechschmidt

Übungsblatt 10 zur Algebraischen Zahlentheorie

Aufgabe 1. *Das inverse galoissche Problem im abelschen Fall*

a) Sei $n \geq 1$. Finde eine galoissche Erweiterung K von $\mathbb{Q}$ mit $\mathrm{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}/(n)$.

Hinweis. Finde nach Dirichlets Satz eine Primzahl p mit $p \equiv 1$ modulo n und konstruiere K als geeigneten Fixkörper von $\mathbb{Q}(\zeta_p)$ über $\mathbb{Q}$.

b) Sei A eine endliche abelsche Gruppe. Finde eine galoissche Erweiterung K von $\mathbb{Q}$ mit $\mathrm{Gal}(K|\mathbb{Q}) \cong A$.

Hinweis. Wir können $A \cong \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_r)$ schreiben und nach Dirichlets Satz *verschiedene* Primzahlen p_i mit $p_i \equiv 1$ modulo n_i finden. Wir können dann die gesuchte Erweiterung K als den Fixkörper der Erweiterung $\mathbb{Q}(\zeta_{p_1} \cdots \zeta_{p_r})|\mathbb{Q}$ bezüglich einer geeigneten Untergruppe seiner Galoisgruppe finden. Diese ist unkanonisch isomorph zu $\mathbb{Z}/(p_1 - 1) \times \cdots \times \mathbb{Z}/(p_r - 1)$.

c) Löse Teilaufgabe b) für nichtkommutative endliche Gruppen.

Aufgabe 2. *Für Matthias S.*

Seien p und q Primzahlen mit $p \neq q$. Seien ζ_p und ζ_q entsprechende primitive Einheitswurzeln.

♡ a) Erinnere dich, wie man für $n \geq 1$ zeigt, dass $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$.

b) Zeige ohne viel Mühe: $\mathbb{Q}(\zeta_p, \zeta_q) = \mathbb{Q}(\zeta_{pq})$.

Hinweis. Dein Beweis zeigt allgemeiner, dass $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{\mathrm{kgV}(n,m)})$.

c) Zeige: $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$.

Hinweis. Auch diese Behauptung gilt allgemeiner (mit ggT statt kgV), ist dann aber etwas komplizierter zu beweisen. Es gibt mehrere Beweise der spezialisierten Behauptung. Interessant ist zum Beispiel folgender: Erinnere dich, dass sich p in $\mathbb{Q}(\zeta_p)$ mit $r = f = 1$ zerlegt. Zeige, dass sich p in $\mathbb{Q}(\zeta_q)$ mit $e = 1$ zerlegt. Folgere, dass sich p in $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q)$ mit $r = e = f = 1$ zerlegt. Wieso genügt das?

Aufgabe 3. *Ein Kriterium für die Unmöglichkeit einer Potenzbasis*

Sei K ein Zahlkörper vom Grad n. Existiere eine Primzahl $p < n$, welche in K unverzweigt ist. Zeige, dass kein $\alpha \in K$ mit $\mathcal{O}_K = \mathbb{Z}[\alpha]$ existiert.

Aufgabe 4. *Endlich etwas Konzeptionelles zum Eisenstein-Kriterium*

Ein normiertes Polynom $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ heißt genau dann *Eisensteinsch* bei einer Primzahl p, wenn alle a_i durch p teilbar, der konstante Koeffizient a_0 aber nicht durch p^2 teilbar ist. Man lernt, dass solche Polynome stets irreduzibel sind.

a) Sei ϑ eine Nullstelle eines solchen Polynoms. Zeige, dass p in $\mathbb{Q}(\vartheta)$ rein verzweigt ist.

Tipp. Sei $\mathfrak{p}$ einer der Primidealfaktoren von $(p) \subseteq \mathcal{O}_K$. Sei e sein Verzweigungsindex; es gilt also $(p) \subseteq \mathfrak{p}^e$ und wir hoffen, $e = n$ nachweisen zu können. Zeige, dass $a_i \vartheta^i$ für $i = 1, \ldots, n-1$ in $\mathfrak{p}^{e+1}$ liegt. Zeige weiter, dass a_0 (zwar in $\mathfrak{p}^e$, aber) nicht in $\mathfrak{p}^{e+1}$ liegt. Folgere, dass ϑ^n nicht in $\mathfrak{p}^{e+1}$ liegt. Beobachte, dass ϑ^n aber in $\mathfrak{p}^n$ liegt. Sei fertig.

b) Welche Primzahlen muss man also nur untersuchen, wenn man das Eisenstein-Kriteriums anwenden möchte? Ist deine Antwort sogar robust gegen Verschiebungen des Polynoms, also dem Übergang zu $f(X - a)$?

♡ **Aufgabe 5.** *Eine Knobelaufgabe vom Erfinders des Blogs*

Für welche Primzahlen p ist $1/p$ ein Dezimalbruch mit Periodenlänge 10?