Algebra und Zahlentheorie

Blatt 10

Abgabe: 24.01.2023, 14 Uhr

Gruppennummer angeben!

Aufgabe 1 (6 Punkte)**.**

(a) Für $p \neq 3$ eine ungerade Primzahl, zeige mit Hilfe des quadratischen Reziprozitätsgesetzes, dass 3 genau dann ein Quadrat modulo p ist, wenn p kongruent zu 1 oder 11 modulo 12 ist.

HINWEIS: Wende den chinesischen Restssatz auf $\mathbb{Z}/12\mathbb{Z}$ an.

(b) Zeige für ungerade Primzahlen $p_1, \ldots, p_k$, dass jeder Primfaktor von $N = 3(p_1 \ldots p_k)^2 - 4$ kongruent zu 1 oder 11 modulo 12 ist.

(c) Schließe daraus, dass es unendlich viele Primzahlen gibt, welche kongruent zu 11 modulo 12 sind.

Aufgabe 2 (10 Punkte)**.**

(a) Sei $k \subset K$ eine normale Körpererweiterung und a ein Element aus K, welches Nullstelle eines separablen Polynoms $P(T)$ mit Koeffizienten aus k ist. Wir nehmen an, dass die natürliche Wirkung der Gruppe $\mathrm{Aut}(K/k)$ der k-Automorphismen von K auf den Nullstellen von $P(T)$ in K transitiv ist. Zeige, dass $P(T)$ irreduzibel über k ist.

(b) Sei F ein Körper positiver Charakteristik p. Zeige, dass die Abbildung $\begin{array}{rccc}\varphi: & F & \to & F \\ & x & \mapsto & x^p - x\end{array}$ ein additiver Gruppenhomomorphismus ist. Bestimme ihren Kern.

Sei nun $a \neq 0_{\mathbb{F}_p}$ ein Element des endlichen Körpers $\mathbb{F}_p$ und betrachte das Polynom $P(T) = T^p - T - a$.

(c) Ist $P(T)$ separabel?

(d) Sei $K \supset \mathbb{F}_p$ ein Zerfällungskörper von $P(T)$. Zeige, dass die vom Frobenius-Automorphismus erzeugte Untergruppe H von $\mathrm{Gal}(K/\mathbb{F}_p)$ transitiv auf den Nullstellen von $P(T)$ wirkt.

(e) Schließe daraus, dass $K = \mathbb{F}_p(\alpha)$, mit α einer Nullstelle von $P(T)$ in K.

(f) Zeige, dass die Abbildung $\begin{array}{rccc}\varphi: & \mathrm{Gal}(K/\mathbb{F}_p) & \to & \mathbb{Z}/p\mathbb{Z} \\ & \sigma & \mapsto & \sigma(\alpha) - \alpha\end{array}$ ein wohldefinierter Gruppenisomorphismus ist.

Insbesondere ist die Galoisgruppe $\mathrm{Gal}(K/\mathbb{F}_p)$ abelsch.

Aufgabe 3 (4 Punkte)**.**

Sei R_0 der Teilkörper von $\mathbb{R}$ aus der Aufgabe 3 auf Blatt 8. Zeige, dass jedes Polynom von ungeradem Grad mit Koeffizienten aus R_0 eine Nullstelle in R_0 besitzt.

Schließe daraus, dass es keine endliche algebraische Körpererweiterung $R_0 \subset K$ derart gibt, dass $[K : R_0]$ ungerade ist.

Die Übungsblätter können zu zweit eingereicht werden. Abgabe der Übungsblätter im Fach im Keller des mathematischen Instituts.