Übungen zur Algebra

Prof. Dr. Helmut Maier, Dr. Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Donnerstag, 2. Februar 2017, vor den Übungen

1. Es sei $p > 2$ eine Primzahl, $a \in \mathbb{Z}$ mit $p \nmid a$ und ζ_p eine primitive p- te Einheitswurzel.
   Weiter sei $\sqrt[p]{a^i} \notin \mathbb{Q}$ für $i \in \{1, \dots, p-1\}$ und $L = \mathbb{Q}(\sqrt[p]{a}, \zeta_p)$. Zeige:
   (a) Es ist $L/\mathbb{Q}$ eine Galoiserweiterung und $[L\colon \mathbb{Q}] = p \cdot (p-1)$.
   (b) Es existiert ein Isomorphismus zwischen der Galoisgruppe $G(L/\mathbb{Q})$ und
   $$AG(p) = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} : r \in (\mathbb{Z}/p\mathbb{Z})^*,\ s \in \mathbb{Z}/p\mathbb{Z} \right\}.$$
   (c) Jede Untergruppe von $G(L/\mathbb{Q})$ ist zu einer der Gruppentypen $N(V)$ bzw. $U(r,s)$ isomorph, wobei diese die Struktur
   $$N(V) = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} : r \in V,\ s \in \mathbb{Z}/p\mathbb{Z} \right\}$$
   mit einer Untergruppe $V \leq (\mathbb{Z}/p\mathbb{Z})^*$ und
   $$U(r,s) = \left\langle \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \right\rangle$$
   mit $r \in (\mathbb{Z}/p\mathbb{Z})^*$ und $s \in \mathbb{Z}/p\mathbb{Z}$ besitzen.
   (d) Es sei $p = 31$ und $a = 3$. Finde Zwischenkörper Z_i von L und $\mathbb{Q}$, die folgendes erfüllen:
      i. $Z_1 \subset \mathbb{R}$ und $[L\colon Z_1] = 2$
      ii. $[Z_2\colon \mathbb{Q}] = 5$.

   (14 Punkte)

2. Es sei $p > 2$ eine Primzahl und $k \in \mathbb{Z}$.
   (a) Es sei $ggT(k,p) = 1$. Zeige, dass ganze Zahlen x und y mit $x^2 + y^2 \equiv k \bmod p$ existieren.
   (b) Es sei $ggT(k,p) = 1$.
   Zeige, dass für $p \equiv 1 \bmod 4$ die Kongruenz $x^2 + y^2 \equiv k \bmod p$ genau $p-1$ inkongruente Lösungen besitzt und für $p \equiv 3 \bmod 4$ genau $p+1$ Lösungen.
   (c) Es sei $ggT(k,p) > 1$.
   Zeige, dass eine Lösung für $p \equiv 3 \bmod 4$ und $2p-1$ Lösungen für $p \equiv 1 \bmod 4$ existieren.
   (d) Es sei q eine zu p verschiedene ungerade Primzahl, ζ_p eine primitive p- te Einheitswurzel sowie
   $$G_p := \sum_{m=0}^{p-1} \zeta_p^{m^2}$$
   die Gaußsche Summe. Zeige in $\mathbb{F}_q(\zeta_p)$:
   $$G_p^2 = \begin{cases} p & \text{für } p \equiv 1 \bmod 4 \\ (-1)^{(p-1)/2} \cdot p & \text{für } p \equiv 3 \bmod 4 \end{cases}$$

   (10 Punkte)