Spieß

10. Übung zur Vorlesung Algebra 1

Sommersemester 2007 Abgabe: Do, 5.7.07

Aufgabe 1. Sei p eine ungerade Primzahl und $\zeta_p = e^{2\pi i/p}$. Zeigen Sie, dass der Kreisteilungskörper $\mathbb{Q}(\zeta_p)$ einen eindeutig bestimmten Teilkörper L vom Grad $[L : \mathbb{Q}] = \frac{p-1}{2}$ besitzt; dieser wird von dem Element $\zeta_p + \zeta_p^{p-1}$ erzeugt wird und es gilt $L = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$.

Aufgabe 2. Für $n \in \mathbb{N}$ sei $\Phi_n \in \mathbb{Z}[X]$ das n-te Kreisteilungspolynom. Sei p eine Primzahl die n nicht teilt. Zeigen Sie:

(a) Zeigen Sie, dass für $k \in \mathbb{Z}$ gilt:

$$\Phi(k) \equiv 0 \mod p \quad \Leftrightarrow \quad \overline{k} \text{ hat Ordnung } n \text{ in } (\mathbb{Z}/p\mathbb{Z})^*.$$

(b) Sei $P(\Phi_n)$ die Menge aller Primzahlen p mit $p \nmid n$ und so dass $\Phi_n \mod p\mathbb{Z}[X]$ eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzt. Zeigen Sie, dass $P(\Phi_n)$ eine unendliche Menge ist. Folgern Sie, dass es unendlich viele Primzahlen p gibt mit $p \equiv 1 \mod n$. (Hinweis: Sind $p_1, \ldots, p_k \in P(\Phi_n)$ schon gefunden, so wähle man ein $m \in \mathbb{N}$ so, dass gilt $\Phi_n(mp_1 \cdots p_k) > 1$. Folglich besitzt $\Phi_n(mp_1 \cdots p_k)$ einen Primteiler p).

Aufgabe 3. Sei p eine Primzahl und $a \in \mathbb{Q}$ ein Element, dass keine p-te Wurzel in $\mathbb{Q}$ besitzt. Sei $K/\mathbb{Q}$ der Zerfällungskörper von $X^p - a \in \mathbb{Q}[X]$. Zeigen Sie:

(a) $K = \mathbb{Q}(\alpha, \zeta)$, wobei ζ eine primitive p-te Einheitswurzel und $\alpha^p = a$ ist.

(b) Für $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ gibt es Elemente $b(\sigma), d(\sigma) \in \mathbb{Z}/p\mathbb{Z}$ mit $\sigma(\alpha) = \alpha\zeta^{b(\sigma)}$ und $\sigma(\zeta) = \zeta^{d(\sigma)}$.

(c) Die Abbildung

$$\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}), \sigma \mapsto \begin{pmatrix} 1 & 0 \\ b(\sigma) & d(\sigma) \end{pmatrix}$$

ist ein Gruppenmonomorphismus mit Bild $\{\begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \mid b \in \mathbb{Z}/p\mathbb{Z}, c \in (\mathbb{Z}/p\mathbb{Z})^*\}$.

Aufgabe 4. Bestimmen Sie die Galoisgruppe der folgenden Polynome.

(a) $X^4 + 2$ in $\mathbb{F}_3[X]$.

(b) $X^4 + 2$ in $\mathbb{F}_5[X]$.