Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2013/14
4. Dezember 2013

Endliche Körper
Übungsblatt 4

Aufgabe 13

a) Man zeige: Das Polynom $f(X) := X^3 - X + 1$ ist irreduzibel über dem Körper $\mathbb{F}_3[i] \cong \mathbb{F}_9$ (vgl. Aufgabe 1).

Durch Adjunktion einer Nullstelle ξ von $f(X)$ zu $\mathbb{F}_3[i]$ erhält man den Körper

$$\mathbb{F}_3[i, \xi] \cong \mathbb{F}_{9^3} = \mathbb{F}_{3^6} = \mathbb{F}_{729}.$$

b) Man zeige, dass $\mathbb{F}_3[i, \xi] = \mathbb{F}_3[i\xi]$ und bestimme das Minimalpolynom $f_0(X)$ von $i\xi$ über $\mathbb{F}_3$.

c) Welches sind die anderen Nullstellen von $f_0(X)$? Man benutze zur Darstellung die Basis $(1, i, \xi, i\xi, \xi^2, i\xi^2)$ von $\mathbb{F}_3[i, \xi]$ über $\mathbb{F}_3$.

Aufgabe 14

Die Körpererweiterung $F_{7^3} \supset \mathbb{F}_7$ werde konstruiert als $\mathbb{F}_{7^3} = \mathbb{F}_7(\xi)$, wobei ξ eine Nullstelle des Polynoms $X^3 - 2$ ist, vgl. Aufgabe 4.
Man bestimme eine Normalbasis von $\mathbb{F}_{7^3}$ über $\mathbb{F}_7$.

Aufgabe 15

Sei $q = p^n$ eine Primzahlpotenz und $F(X) \in \mathbb{F}_q[X]$ ein Polynom vom Grad $d \geq 1$. Es gelte $F'(X) = 0$.
Man zeige: Es gibt eine ganze Zahl $k \geq 1$ und ein Polynom $f(X) \in \mathbb{F}_q[X]$, so dass

$$F(X) = f(X)^{p^k} \quad \text{und} \quad f'(X) \neq 0.$$

Aufgabe 16*

Sei $p \geq 5$ eine Primzahl und ϕ die Abbildung

$$\phi : \mathbb{F}_p \to \mathbb{F}_p\,, \quad x \mapsto \phi(x) := x^3 + x.$$

Man beweise: Das Bild $\mathrm{Im}(\phi)$ besteht genau aus $\texttt{round}(2p/3)$ Elementen. Dabei bezeichnet $\texttt{round}(c) \in \mathbb{Z}$ die der Zahl $c \in \mathbb{Q}$ nächstgelegene ganze Zahl.