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

SS 2006
24. Mai 2006

Endliche Körper, Übungsblatt 3

Aufgabe 9

Sei $f(X) \in K[X]$ ein irreduzibles Polynom vom Grad n über dem Körper K und $K_1 \supset K$ eine Körper-Erweiterung, deren Grad $m := [K_1 : K]$ zu n teilerfremd ist.

Man beweise: Das Polynom $f(X)$ bleibt auch in $K_1[X]$ irreduzibel.

Aufgabe 10

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 11

a) Im Körper $\mathbb{F}_{3^6} = \mathbb{F}_{729}$ sei ζ eine Primitivwurzel, d.h. erzeugendes Element der multiplikativen Gruppe. Man bestimme in Abhängigkeit von $\nu = 0, 1, \ldots, 727$ den Grad des Minimalpolynoms von ζ^ν über $\mathbb{F}_3$.

b)* Man bestimme (mit Computer-Unterstützung) im Körper $\mathbb{F}_3[i, \xi]$ explizit eine Primitivwurzel.

Aufgabe 12

Sei $q = p^n$ eine Primzahlpotenz und $F(X) \in \mathbb{F}_q[X]$ ein Polynom vom Grad ≥ 1. Es gelte $F'(X) = 0$.

Man zeige: Es gibt eine ganze Zahl $k \geq 1$ und ein Polynom $f(X) \in \mathbb{F}_q[X]$ mit

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

Abgabetermin: Mittwoch, 31. Mai 2006, 14 Uhr