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

SS 2006
10. Mai 2006

# Endliche Körper, Übungsblatt 2

## Aufgabe 5

a) Man zeige, dass die beiden Polynome

$$\begin{aligned} P_1(X) &:= X^4 + X + 1, \\ P_2(X) &:= X^4 + X^3 + 1 \end{aligned}$$

irreduzibel über dem Körper $\mathbb{F}_2$ sind.

In den Körpern $K_1 := \mathbb{F}_2[X]/(P_1(X))$ und $K_2 := \mathbb{F}_2[X]/(P_2(X))$ seien die Basen $1, \xi_\nu, \xi_\nu^2, \xi_\nu^3$ eingeführt, wobei

$$\xi_\nu := X \bmod P_\nu(X) \in K_\nu, \quad \nu = 1, 2.$$

b) Bekanntlich sind die Körper $K_1$ und $K_2$ isomorph (beide sind isomorph zu $\mathbb{F}_{16}$). Man konstruiere einen expliziten Isomorphismus $\phi : K_1 \to K_2$ mit Angabe der Matrix von $\phi$ bzgl. der oben genannten Basen.

## Aufgabe 6

Im Körper $K := \mathbb{F}_2[X]/(X^4+X+1)$ (vgl. vorherige Aufgabe) gebe man eine Primitivwurzel $g$ (erzeugendes Element von $K^*$) an und stelle eine Tabelle des Zech-Logaritmus zur Basis $g$ auf.

## Aufgabe 7

a) Welches ist der kleinste Körper (d.h. mit der geringsten Anzahl von Elementen) irgend einer Charakteristik $p \nmid 144$, der eine primitive 144-te Einheitswurzel enthält?

b) Was ist der kleinste Körper, wenn man zusätzlich verlangt, dass seine Charakteristik gleich 5 ist?

## Aufgabe 8

Sei $q = p^n$ eine Primzahlpotenz und $G := \mathrm{Aut}(\mathbb{F}_q^*)$ die Automorphismen-Gruppe der multiplikativen Gruppe des Körpers $\mathbb{F}_q$.

a) Man zeige, dass $G$ abelsch ist. Aus wievielen Elementen besteht $G$ ?

b) Ist $G$ stets zyklisch? (Beweis oder Gegenbeispiel)

c) Man zeige, dass jeder Automorphismus der additiven Gruppe von $\mathbb{F}_q$ ein $\mathbb{F}_p$-Vektorraum-Automorphismus ist. Aus wievielen Elementen besteht $\mathrm{Aut}(\mathbb{F}_q, +)$ ?

---

**Abgabetermin:** Mittwoch, 17. Mai 2006, 14 Uhr