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

WS 2013/14
30. Okt. 2013

Endliche Körper

Übungsblatt 2

Aufgabe 5

Sei K ein endlicher Körper mit q Elementen, $m \geq 2$ eine natürliche Zahl und $s := \gcd(q-1, m)$. Man beweise:

Für $a \in K^*$ ist die Gleichung $x^m = a$ in K genau dann lösbar, wenn

$$a^{(q-1)/s} = 1.$$

Aufgabe 6

Sei $F(X) = \sum_{\nu=0}^{n} a_\nu X^\nu$, $a_0 \neq 0$, $a_n \neq 0$, ein Polynom vom Grad $n > 0$ über einem Körper K. Man zeige: $F(X)$ ist genau dann irreduzibel, wenn das "gespiegelte" Polynom

$$G(X) = \sum_{\nu=0}^{n} a_\nu X^{n-\nu}$$

irreduzibel ist.

Aufgabe 7

a) Sei $F(X) = \sum_{\nu=0}^{n} a_\nu X^\nu \in \mathbb{F}_2[X]$, $a_n = 1$, ein irreduzibles Polynom vom Grad $n > 1$ über dem Körper $\mathbb{F}_2$. Man zeige:

(i) $a_0 = 1$.

(ii) Die Anzahl der $\nu \in \{0, 1, \ldots, n\}$ mit $a_\nu = 1$ ist ungerade.

b) Man erstelle eine Liste aller irreduziblen Polynome über $\mathbb{F}_2$ vom Grad ≤ 5.

Aufgabe 8

Sei K ein endlicher Körper mit $q = p^n$ Elementen (p prim) und $G := \mathrm{Aut}(K^*)$ die Menge aller Gruppen-Automorphismen der multiplikativen Gruppe des Körpers K.

a) Man zeige, dass G eine abelsche Gruppe ist. Aus wievielen Elementen besteht G ?

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

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