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

WS 2013/14
20. Nov. 2013

Endliche Körper

Übungsblatt 3

Aufgabe 9

Das Polynom $G(X) := X^3 - X - 2$ ist bekanntlich irreduzibel über dem Körper $\mathbb{F}_7$ (vgl. Aufgabe 4). Deshalb kann man den Körper $\mathbb{F}_{7^3} = \mathbb{F}_{343}$ konstruieren als $\mathbb{F}_{7^3} = \mathbb{F}_7(\eta)$, wobei η eine Nullstelle des Polynoms $G(X)$ ist.

a) Man bestimme die Matrix $A \in \mathrm{GL}(3, \mathbb{F}_7)$ des Frobenius-Automorphismus

$$\mathrm{frob}_7 : \mathbb{F}_{7^3} \to \mathbb{F}_{7^3}, \quad x \mapsto x^7,$$

bzgl. der Basis $1, \eta, \eta^2$ von $\mathbb{F}_{7^3}$ über $\mathbb{F}_7$ und verifiziere die Beziehung $A^3 = E$ (= Einheitsmatrix).

b) Man zeige, dass die Matrix A über dem Körper $\mathbb{F}_7$ ähnlich zu einer Diagonalmatrix ist gebe eine Basis von $\mathbb{F}_{7^3}$ über $\mathbb{F}_7$ an, bzgl. der die Matrix von frob_7 Diagonalform hat.

Aufgabe 10

Man beweise, dass das Polynom $X^4 + 1$ irreduzibel über dem Körper $\mathbb{Q}$ ist, aber reduzibel über allen endlichen Körpern.

Aufgabe 11

Sei $f(X) \in \mathbb{F}_q[X]$ ein irreduzibles Polynom vom Grad n über dem endlichen Körper $\mathbb{F}_q$. Man zeige:

a) Ist d ein Teiler von n, so zerfällt $f(X)$ über dem Körper $\mathbb{F}_{q^d}$ in d irreduzible Faktoren vom Grad n/d.

b) Ist m zu n teilerfremd, so ist $f(X)$ auch irreduzibel über dem Körper $\mathbb{F}_{q^m}$.

Aufgabe 12

a) Man bestimme den kleinsten Körper K (d.h. mit der kleinsten Anzahl von Elementen) der Charakteristik $\neq 3, 5$, in dem eine primitive 75. Einheitswurzel existiert.

b) Wieviele Elemente hat der kleinste Körper K, wenn man zusätzlich verlangt, dass er die Charakteristik 2 besitzt.