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

SS 2006
21. Juli 2006

Endliche Körper, Klausur

Alle 4 Aufgaben sollen bearbeitet werden. Die mit einem Stern markierten Teilaufgaben sind nicht obligatorisch.

Arbeitszeit: 60 Minuten.

Aufgabe 1

Man zeige: Die Abbildung

$$\psi : \mathbb{F}_{64} \to \mathbb{F}_{64}, \quad x \mapsto x^{1024},$$

ist ein Automorphismus des Körpers $\mathbb{F}_{64}$. Welches ist der Fixkörper von ψ ?

Aufgabe 2

Man bestimme den kleinsten Körper der Charakterisik 5, in dem eine primitive 13-te Einheitswurzel existiert.

Aufgabe 3

Sei $\mathbb{F}_q$ ein endlicher Körper mit $q \equiv 1 \bmod 3$.

a) Man zeige: Ein Element $a \in \mathbb{F}_q^*$ besitzt genau dann eine dritte Wurzel in $\mathbb{F}_q^*$, falls

$$a^{(q-1)/3} = 1.$$

b)* Im Fall $q \equiv 7 \bmod 9$ gebe man ein Verfahren an, wie man durch Potenzieren aus einem Element $a \in \mathbb{F}_q^*$ mit $a^{(q-1)/3} = 1$ die dritte Wurzel ziehen kann.

Aufgabe 4

a) Man beweise: Das Polynom $f(X) = X^3 - X + 1$ ist irreduzibel über dem Körper $\mathbb{F}_3$.

b) Sei ξ eine Nullstelle von $f(X)$ im Körper $\mathbb{F}_{27}$. Man berechne Norm und Spur der Elemente ξ und ξ^2 bzgl. der Körpererweiterung $\mathbb{F}_{27} \supset \mathbb{F}_3$.

c)* Man beweise (ohne alle Potenzen von ξ einzeln zu berechnen), dass ξ eine Primitivwurzel des Körpers $\mathbb{F}_{27}$ ist.