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

WS 2013/14
13. Dezember 2013

Endliche Körper
Übungsblatt 5

Aufgabe 17

Sei q eine Primzahlpotenz und $n > 1$. Sei $\mathrm{N} = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ die Norm-Abbildung. Für ein Element $\xi \in \mathbb{F}_{q^n}$ sei $f(X) = X^d + a_1 X^{d-1} + \ldots + a_d \in \mathbb{F}_q[X]$ das Minimalpolynom, d.h. das normierte Polynom kleinsten Grades mit $f(\xi) = 0$.

a) Man beweise: d ist ein Teiler von n, und es gilt

$$\mathrm{N}(\xi) = (-1)^n a_d^{n/d}.$$

b) Man gebe eine analoge Formel für die Spur von ξ an.

Aufgabe 18

Sei p eine ungerade Primzahl. Sei $\mathrm{N} : \mathbb{F}_{p^2}^* \to \mathbb{F}_p^*$ die Norm-Abbildung. Für $a \in \mathbb{F}_p^*$ sei

$$U_a := \{x \in \mathbb{F}_{p^2}^* : \mathrm{N}(x) = a\}.$$

a) Man zeige: Alle Mengen U_a bestehen aus $p + 1$ Elementen und sind Nebenklassen der Untergruppe $U_1 \subset \mathbb{F}_{p^2}^*$.

b) Der Durchschnitt $U_a \cap \mathbb{F}_p^*$ ist genau dann nicht-leer, wenn a ein Quadrat in $\mathbb{F}_p^*$ ist. In diesem Fall besteht der Durchschnitt aus 2 Elementen.

Aufgabe 19

Sei q eine Primzahlpotenz, $n > 1$ und $\xi_1, \ldots, \xi_n$ eine Basis von $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$. Eine Basis $\eta_1, \ldots, \eta_n$ heißt *dual* zur Basis $\xi_1, \ldots, \xi_n$, falls

$$\mathrm{Tr}(\xi_i \eta_j) = \delta_{ij} = \begin{cases} 1, & \text{falls } i = j, \\ 0, & \text{falls } i \neq j. \end{cases}$$

Dabei bezeichnet $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ die Spur-Abbildung.

a) Man beweise: Zu jeder Basis existiert eine duale Basis.

b) Sei $\zeta \in \mathbb{F}_{81} = \mathbb{F}_{3^4}$ eine primitive 5-te Einheitswurzel. Man zeige, dass $\zeta, \zeta^2, \zeta^3, \zeta^4$ eine Basis von $\mathbb{F}_{81}$ über $\mathbb{F}_3$ ist, und bestimme eine dazu duale Basis.

Aufgabe 20

Sei K ein Körper und $F(X) \in K[X]$ ein Polynom mit $\gcd(F(X), F'(X)) = 1$.

a) Man zeige: Der Ring $R := K[X]/(F(X))$ ist isomorph zu einem kartesischen Produkt $K_1 \times K_2 \times \ldots \times K_r$ von Erweiterungskörpern $K_i \supset K$.

b) Man bestimme die Körper K_i für den Fall $K = \mathbb{F}_3$ und $F(X) = X^{10} - 1$.
