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

SS 2006
21. Juli 2006

Endliche Körper, Klausur

Lösungen

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 ?

Lösung. Die Abbildung $\mathrm{frob}_2 \colon \mathbb{F}_{64} \to \mathbb{F}_{64}, x \mapsto x^2$, ist ein Automorphismus. Für die gegebene Abbildung ψ gilt

$$\psi = (\mathrm{frob}_2)^{10},$$

also ist auch ψ ein Automorphismus. Da $\mathbb{F}_{64} = \mathbb{F}_{2^6} \supset \mathbb{F}_2$ eine Körpererweiterung vom Grad 6 ist, hat $\sigma := (\mathrm{frob}_2 \mid \mathbb{F}_{64})$ die Ordnung 6, es gilt also

$$\psi = \sigma^{10} = \sigma^4.$$

Die von ψ erzeugte Untergruppe $\langle\psi\rangle \subset \mathrm{Gal}(\mathbb{F}_{64}/\mathbb{F}_2)$ besteht aus den Elementen

$$\psi = \sigma^4, \quad \psi^2 = \sigma^8 = \sigma^2, \quad \psi^3 = \sigma^{12} = \mathrm{id},$$

d.h. $\langle\psi\rangle$ hat die Ordnung 3, woraus folgt

$$[\mathbb{F}_{2^6} : \mathrm{Fix}(\psi)] = 3,$$

also $\mathrm{Fix}(\psi) = \mathbb{F}_{2^{6/3}} = \mathbb{F}_4$.

Aufgabe 2

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

Lösung. Genau dann enthält der Körper $\mathbb{F}_{5^n}$ eine primitive 13-te Einheitwurzel, wenn 13 ein Teiler der Ordnung der multiplikativen Gruppe $\mathbb{F}_{5^n}^*$ ist, d.h. wenn $13 \mid 5^n - 1$. Dies ist gleichbedeutend mit

$$5^n \equiv 1 \bmod 13.$$

Es ist also die Ordnung von 5 in der multiplikativen Gruppe $(\mathbb{Z}/13)^*$ zu bestimmen. Nun ist

$$5^2 = 25 \equiv -1 \bmod 13, \quad 5^3 \equiv -5 \bmod 13, \quad 5^4 = (5^2)^2 \equiv (-1)^2 \equiv 1 \bmod 13.$$

Die gesuchte Ordnung ist also gleich 4, der kleinste Körper der Charakteristik 5, der eine primitive 13-te Einheitswurzel enthält, ist $\mathbb{F}_{5^4} = \mathbb{F}_{625}$.

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.

Lösung.

a) Die angegebene Bedingung ist notwendig, denn aus $x^3 = a$ folgt $a^{(q-1)/3} = x^{q-1} = 1$.
Die Bedingung ist auch hinreichend: Sei $w \in \mathbb{F}_q^*$ eine Primitivwurzel. Dann ist $a = w^k$ mit einer ganzen Zahl k. Es gilt nach Voraussetzung

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

Also muss der Exponent $k(q-1)/3$ ein Vielfaches der Ordnung $q-1$ von w sein, etwa

$$k \cdot \frac{q-1}{3} = \nu(q-1) \quad \text{mit } \nu \in \mathbb{Z}.$$

Daraus folgt $k = 3\nu$, also ist $x := w^\nu$ eine dritte Wurzel von $a = w^{3\nu}$.

b) (Das folgende Verfahren ist analog zum Ziehen der Quadratwurzel im Fall $q \equiv 3 \bmod 4$.) Definiere

$$x := a^{(q+2)/9}.$$

Der Exponent ist ganzzahlig wegen $q \equiv 7 \bmod 9$. Damit gilt

$$x^3 = a^{(q+2)/3} = a^{(q-1)/3}\, a^1 = a, \quad \text{q.e.d.}$$

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.

Lösung. a) Es ist nur zu zeigen, dass $f(X)$ keine Nullstelle in $\mathbb{F}_3$ hat. Dies ist der Fall, es gilt $f(x) = 1$ für alle $x \in \mathbb{F}_3$.

b) Die Galoisgruppe von $\mathbb{F}_{27}$ über $\mathbb{F}_3$ ist $\{\mathrm{id}, \sigma, \sigma^2\}$, wobei $\sigma = \mathrm{frob}_3$. Für $x \in \mathbb{F}_{27}$ sind Norm und Spur definiert durch

$$\begin{aligned} \mathrm{N}(x) &= x \cdot \sigma(x) \cdot \sigma^2(x) = x^{1+3+9} = x^{13}, \\ \mathrm{Tr}(x) &= x + \sigma(x) + \sigma^2(x) = x + x^3 + x^9. \end{aligned}$$

Nun ist

$$\sigma(\xi) = \xi^3 = \xi - 1, \quad \sigma^2(\xi) = (\xi - 1)^3 = \xi^3 - 1 = \xi - 2 = \xi + 1$$

und

$$\sigma(\xi^2) = \sigma(\xi)^2 = (\xi - 1)^2 = \xi^2 - 2\xi + 1, \quad \sigma^2(\xi^2) = (\sigma^2(\xi))^2 = (\xi + 1)^2 = \xi^2 + 2\xi + 1.$$

Daraus folgt

$$\mathrm{N}(\xi) = \xi(\xi - 1)(\xi + 1) = \xi^3 - \xi = (\xi - 1) - \xi = -1$$

und

$$\mathrm{Tr}(\xi) = \xi + (\xi - 1) + (\xi + 1) = 3\xi = 0.$$

Dies hätte man auch direkt aus dem Minimalpolynom $X^3 - X + 1$ von ξ ablesen können, denn der Koeffizient von X^2 ist die negative Spur und das konstante Glied gleich $(-1)^3$ mal der Norm.

Weiter erhält man

$$\mathrm{N}(\xi^2) = \mathrm{N}(\xi)^2 = 1,$$

$$\mathrm{Tr}(\xi^2) = \xi^2 + \sigma(\xi^2) + \sigma^2(\xi^2) = \xi^2 + (\xi^2 - 2\xi + 1) + (\xi^2 + 2\xi + 1) = 2.$$

c) Es ist zu zeigen, dass ξ in der multiplikativen Gruppe $\mathbb{F}_{27}^*$ die Ordnung $27 - 1 = 26$ hat. Jedenfalls ist die Ordnung ein Teiler von 26, wir müssen also nur die Ordnungen 1, 2 und 13 ausschließen. Trivialerweise ist die Ordnung von ξ nicht 1 oder 2. Die Ordnung ist aber auch nicht 13, denn $\xi^{13} = \mathrm{N}(\xi) = -1$. Damit ist die Behauptung bewiesen.
