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

WS 2013/14
23. Okt. 2013

Endliche Körper

Übungsblatt 1

Aufgabe 1

Analog zur Konstruktion der komplexen Zahlen aus den reellen Zahlen werde für eine Primzahl $p > 2$ auf der Menge $\mathbb{F}_p[i] := \mathbb{F}_p \times \mathbb{F}_p$ eine Addition und Multiplikation definiert durch

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &:= (x_1 + x_2,\ y_1 + y_2)\\ (x_1, y_1) \cdot (x_2, y_2) &:= (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1).\end{aligned}$$

Man beweise:

a) $\mathbb{F}_p[i]$ ist mit diesen Verknüpfungen ein kommutativer Ring mit Einselement.

b) Die Menge aller Elemente der Gestalt $(x, 0)$ bildet einen zu $\mathbb{F}_p$ isomorphen Unterring von $\mathbb{F}_p[i]$. Im folgenden werde $\mathbb{F}_p$ mit diesem Unterring identifiziert.

c) Das Element $i := (0, 1)$ hat die Eigenschaft $i^2 = (-1, 0) \mathrel{\widehat{=}} -1$.

d) $\mathbb{F}_p[i]$ ist genau dann ein Körper, wenn -1 kein Quadrat in $\mathbb{F}_p$ ist, d.h. wenn $p \equiv 3 \bmod 4$.

Aufgabe 2

a) Sei p eine Primzahl mit $p \equiv 3 \bmod 4$. Man zeige: Jedes Element $x \in \mathbb{F}_p$, das keine Quadratwurzel in $\mathbb{F}_p$ besitzt, besitzt eine Quadratwurzel in $\mathbb{F}_p[i]$.

b) Man bestimme explizit von allen Nicht-Quadraten aus $\mathbb{F}_{11}$ Quadratwurzeln in $\mathbb{F}_{11}[i]$.

Aufgabe 3

Im Körper $\mathbb{F}_3[i]$ (vgl. Aufg. 1) bestimme man explizit eine primitive 8-te Einheitswurzel, d.h. ein Element $\omega \in \mathbb{F}_3[i]$ mit $\omega^8 = 1$ und $\omega^\nu \neq 1$ für $1 \leq \nu \leq 7$.

Aufgabe 4

a) Man beweise: Die Polynome

$$F(X) := X^3 - 2 \quad \text{und} \quad G(X) := X^3 - X - 2$$

sind irreduzibel über dem Körper $\mathbb{F}_7$.

b) Sei ξ eine Nullstelle des Polynoms F (in einem Erweiterungskörper von $\mathbb{F}_7$) und η eine Nullstelle des Polynoms G. Man bestimme explizit einen Körper-Isomorphismus

$$\phi : \mathbb{F}_7(\eta) \longrightarrow \mathbb{F}_7(\xi).$$