

Endliche Körper, Übungsblatt 1

Aufgabe 1

Sei p eine Primzahl. Auf der Menge $\mathbb{F}_p[i] := \mathbb{F}_p \times \mathbb{F}_p$ seien 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:

- $\mathbb{F}_p[i]$ ist mit diesen Verknüpfungen ein kommutativer Ring mit Einselement.
- 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.
- Das Element $i := (0, 1)$ hat die Eigenschaft $i^2 = (-1, 0) \hat{=} -1$.
- $\mathbb{F}_p[i]$ ist genau dann ein Körper, wenn -1 kein Quadrat modulo p ist, d.h. wenn $p \equiv 3 \pmod{4}$.

Aufgabe 2

Im Körper $\mathbb{F}_3[i]$ (vgl. Aufg. 1) bestimme man explizit eine primitive 8-te Einheitswurzel, d.h. ein Element ζ_8 mit $\zeta_8^8 = 1$ und $\zeta_8^k \neq 1$ für $1 \leq k \leq 7$.

Aufgabe 3

- Sei p eine Primzahl mit $p \equiv 3 \pmod{4}$. Man zeige: Jedes Element $x \in \mathbb{F}_p$, das keine Quadratwurzel in \mathbb{F}_p besitzt, besitzt eine Quadratwurzel in $\mathbb{F}_p[i]$.
- Man bestimme explizit von allen Nicht-Quadraten aus \mathbb{F}_{11} Quadratwurzeln in $\mathbb{F}_{11}[i]$.

Aufgabe 4

Sei K ein Körper der Charakteristik p und m eine ganze Zahl mit $0 < m < \#K$. Dabei bezeichnet $\#K$ die Anzahl der Elemente von K (darf auch ∞ sein).

Man zeige: Genau dann gilt

$$(x + y)^m = x^m + y^m \quad \text{für alle } x, y \in K,$$

wenn m eine Potenz von p ist.
