D-MATH Algebra II FS 2023
Prof. Richard Pink

Serie 22

Endliche Körper, Separable Körpererweiterungen

1. Finde für $p^r = 8, 9, 16$ das Minimalpolynom über $\mathbb{F}_p$ eines Erzeugenden von $\mathbb{F}_{p^r}^\times$.

2. (a) Zeige, dass das Polynom $f(X) = X^3 + 3X + 3$ irreduzibel in $\mathbb{F}_5[X]$ ist.
   (b) Sei α eine Nullstelle von f in einem algebraischen Abschluss von $\mathbb{F}_5$ und $\mathbb{F}_{125} := \mathbb{F}_5(\alpha)$. Berechne die Darstellungsmatrix des Frobeniusautomorphismus $\mathrm{Frob}_5 \colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ in der geordneten Basis $(1, \alpha, \alpha^2)$.
   (c) Schreibe das Element $\beta := 1/(1-\alpha) \in \mathbb{F}_{125}$ als $\mathbb{F}_5$-Linearkombination von $1, \alpha$ und α^2.
   (d) Zeige, dass α die zyklische Gruppe $\mathbb{F}_{125}^\times$ erzeugt.

3. Sei K ein Körper der Charakteristik $p > 0$ und sei $a \in K$.
   (a) Zeige, dass das Polynom $f(X) := X^p - X - a \in K[X]$ separabel ist.
   (b) Sei α eine Nullstelle von f in einem algebraisch abgeschlossenen Oberkörper L von K. Zeige
   $$\big\{\beta \in L : f(\beta) = 0\big\} \;=\; \big\{\alpha + x : x \in \mathbb{F}_p\big\}.$$
   (c) Zeige, dass im Fall $a \notin \{y^p - y : y \in K\}$ die Körpererweiterung $K(\alpha)/K$ den Grad p hat. Was geschieht im Fall $a \in \{y^p - y : y \in K\}$?
   (d) Zeige, dass im Fall $a \notin \{y^p - y : y \in K\}$ die Gruppe $\mathrm{Aut}_K(K(\alpha))$ zyklisch der Ordnung p ist.
   (e) Konstruiere auf diese Weise für $K = \mathbb{F}_p$ einen Körper der Ordnung p^p.

4. Seien p eine Primzahl und K ein endlicher Körper der Ordnung p^n mit $n > 0$. Zeige:
   (a) Im Fall $p = 2$ ist jedes Element von K ein Quadrat.
   (b) Jedes Element von K ist eine Summe von zwei Quadraten.
   (c) Für $p > 2$ ist ist -1 ein Quadrat in K genau dann, wenn $p^n \equiv 1 \mod 4$ ist.

5. Zeige, dass eine Primzahl $p > 2$ genau dann als Summe zweier Quadrate in $\mathbb{Z}$ geschrieben werden kann, wenn $p \equiv 1 \mod 4$ ist.

   Hinweis: Untersuche die Primfaktorzerlegung von p in $\mathbb{Z}[i]$. Siehe auch Serie 13, Aufgabe 2.