D-MATH
Prof. Richard Pink

Algebra II

FS 2016

Serie 21

Endliche Körper

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 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 die Mengengleichheit
   $$\{\beta \in L : f(\beta) = 0\} = \{\alpha + x : x \in \mathbb{F}_p\}.$$

   (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. Ein Ring, der alle Körperaxiome ausser vielleicht die Kommutativität der Multiplikation erfüllt, heisst eine *Divisionsalgebra* oder ein *Schiefkörper*. Der *Satz von Wedderburn* besagt, dass jeder endliche Schiefkörper kommutativ ist.

   Wähle $n \geqslant 1$. Versuche für n Stunden, selbst einen Beweis dafür zu finden. Vergleiche das Resultat mit bekannten Beweisen, wie zum Beispiel hier:
   `https://en.wikipedia.org/wiki/Wedderburn%27s_little_theorem`

Bitte wenden

*5. Sei p eine ungerade Primzahl. Für jede zu p teilerfremde ganze Zahl x ist das *Legendresymbol* $\left(\frac{x}{p}\right)$ definiert durch:

$$\left(\frac{x}{p}\right) := \begin{cases} 1 & \text{falls } \exists\, a \in \mathbb{Z} \colon x \equiv a^2 \text{ modulo } (p), \\ -1 & \text{sonst,} \end{cases}$$

was nur von der Restklasse von x modulo (p) abhängt. Das *quadratische Reziprozitätsgesetz* von Gauss besagt

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

für je zwei verschiedene ungerade Primzahlen p und q. Dies sei im Folgenden vorausgesetzt.

(a) Zeige

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \text{ modulo } (p),$$

und dass diese Kongruenz das Legendresymbol eindeutig bestimmt.

(b) Zeige, dass für alle zu p teilerfremden ganzen Zahlen x und y gilt

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right).$$

(c) Beweise den *ersten Ergänzungssatz* zum quadratischen Reziprozitätsgesetz:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

(d) Beweise den *zweiten Ergänzungssatz* zum quadratischen Reziprozitätsgesetz:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

[*Hinweis:* Setze $s := \frac{p-1}{2}$ und zeige $s! \equiv 2^s s! (-1)^{\frac{s(s+1)}{2}}$ modulo (p), unter Benutzung von $s! = (-1)^{\frac{s(s+1)}{2}} \prod_{j=1}^{s} (-1)^j j$ und $-j \equiv p - j$ modulo (p).]

(e) Finde Kongruenzbedingungen für p, die zu $\left(\frac{13}{p}\right) = 1$ äquivalent sind.

(f) Folgere, dass für eine Primzahl $p \equiv 6 \bmod (13)$ nur endlich viele $n \in \mathbb{Z}^{>0}$ existieren, so dass $n! + n^p - n + 13$ ein Quadrat in $\mathbb{Z}$ ist.

(**g) Zeige, dass für alle p und x der Wert von $\left(\frac{x}{p}\right)$ in $O(\max\{\log|x|, \log p\})$ Schritten effektiv berechnet werden kann, falls ganze Zahlen y in $O(\log|y|)$ Schritten faktorisiert werden können.