

# Endliche Körper und Codierung

Übung, LVA 405.351

C. Fuchs

## 4. Übungsblatt, WS 2018/19

07.11.2018

---

1. Sei  $K$  ein Körper mit Charakteristik  $p$  und  $n \in \mathbb{N}$  teilerfremd zu  $p$ . Zeige, dass

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

2. Faktorisierere  $x^{21} - 1$  über  $\mathbb{F}_2$ . Sie können die Faktorisierung per Hand suchen oder sich über den Berlekamp-Algorithmus (zur Faktorisierung von Polynomen über  $\mathbb{Z}_p$ ) informieren (z.B. in A. Pethő, Algebraische Algorithmen, Vieweg, 1999) und diesen anwenden.
3. Zeige, dass  $x^2 + x + 2 \in \mathbb{F}_3[x]$  ein irreduzibler Teiler des 8-ten Kreisteilungspolynoms  $Q_8(x) \in \mathbb{F}_3[x]$  ist, und bestimme dann das Minimalpolynom von  $\alpha^2$  über  $\mathbb{F}_3$ , wobei  $\alpha$  eine Nullstelle von  $x^2 + x + 2$  bezeichnet.
4. Sei  $\alpha$  eine Nullstelle von  $x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ . Gib alle zyklotomischen Nebenklassen von 2 modulo 31 und dann das Minimalpolynom von  $\alpha$ ,  $\alpha^4$  und  $\alpha^5$  an.