## Endliche Körper -Kontrollaufgaben



Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw.de, Raum

149B

Version: 1.0.1

#### Bemerkung

Dies ist nicht primärer Inhalt der Kryptovorlesungen, muss jedoch für die Prüfungen ggf. beherrscht werden, um zum Beispiel AES verstehen zu können.

1

# 1. Rechnen mit Polynomen $\overline{GF}(2^x)$

2

### Klassenraumübung

#### 1.1. Polynomarithmetik im endlichen Körper GF(2<sup>7</sup>)

Gegen sei das irreduzible Polynom:  $x^7+x+1$ . Berechnen Sie jeweils das Ergebnis:

- 1. Addition:  $(x^3 + x + 1) + (x^4 + x)$
- 2. Multiplikation:  $(x^3+x+1) imes (x^2+1)$
- 3. Multiplikation:  $(x^6) imes (x^5)$
- 4. Multiplikation:  $(x^5+x^3) imes (x^4+x+1)$

3