Übungsblatt 4

Aufgabe 1.

a) Überprüfen Sie, ob durch die Relation $\alpha^5 = \alpha^3 + \alpha^2 + \alpha + 1$ der Körper $\mathbb{F}_{32}$ definiert werden kann.

b) Überprüfen Sie, ob durch die Relation $\alpha^7 = \alpha^6 + \alpha^5 + \alpha^2 + 1$ der Körper $\mathbb{F}_{128}$ definiert werden kann.

Aufgabe 2. Wir betrachten den Körper $k = \mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha^2 + 1$ und stellen ein Element $a = r \cdot \alpha^2 + s \cdot \alpha + t \in \mathbb{F}_8$ durch das binäre Dreitupel $(r, s, t) \in \mathbb{F}_2^3$ dar. Berechnen Sie

$$a = (1,1,0) \cdot (1,1,1), \quad b = \frac{(0,1,1)}{(1,1,1)}, \quad c = \frac{(1,0,1)}{(1,1,0)}$$

und schreiben Sie das Ergebnis wieder als binäres Dreitupel.

Aufgabe 3. Wir betrachten den Körper $\mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha + 1$. Bestimmen Sie alle Lösungen x_1, x_2, x_3, $x_4 \in \mathbb{F}_8$ des linearen Gleichungssystems

$$\begin{array}{rcrcrcrcl} \alpha \cdot x_1 & + & (\alpha+1) \cdot x_2 & + & (\alpha+1) \cdot x_3 & + & (\alpha^2+\alpha) \cdot x_4 & = & 0 \\ (\alpha^2+\alpha) \cdot x_1 & + & (\alpha^2+\alpha+1) \cdot x_2 & + & (\alpha+1) \cdot x_3 & + & \alpha^2 \cdot x_4 & = & 0 \end{array}$$

Aufgabe 4. Wir betrachten den Körper $k = \mathbb{F}_{256}$ mit der Relation

$$\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$$

(wie in der Vorlesung) und identifizieren ein Element

$$a = r_7 \cdot \alpha^7 + r_6 \cdot \alpha^6 + \cdots + r_1 \cdot \alpha + r_0$$

mit dem Byte $a = (r_7,\, r_6,\, \ldots, r_1,\, r_0)$.
.Berechnen Sie

$$a = (1,\, 1,\, 0,\, 0,\, 0,\, 0,\, 1,\, 1) \cdot (0,\, 0,\, 1,\, 1,\, 1,\, 0,\, 0,\, 0)$$

und

$$b = (0,\, 1,\, 0,\, 1,\, 0,\, 1,\, 0,\, 1)^2$$

und

$$c = \frac{(0,\, 0,\, 0,\, 0,\, 0,\, 1,\, 1,\, 0)}{(1,\, 0,\, 0,\, 0,\, 1,\, 1,\, 0,\, 1)}$$

und stellen Sie das Ergebnis wieder als binäres Achttupel dar.