

# Übungsblatt 4

## Aufgabe 1

a)  $\bar{F}_{32} = \bar{F}_{2^5}$  mit  $F(x) = x^5 + x^3 + x^2 + x + 1$

-  $F(x)$  hat keine Nullstellen über  $\mathbb{F}_2$

- Falls  $F(x)$  kein Minimalpolynom ist, hat es echte Teiler, d.h.:  $F(x) = h(x) \cdot g(x)$

wobei der Grad einer der Polynome 2 und der des anderen 3 sein müsste.

Das einzige Minimalpolynom vom Grad 2 ist:  $x^2 + x + 1$ . Um  $F(x)$  und dieses Polynom auf gemeinsame Teiler zu überprüfen, berechnen wir ...

$$\begin{array}{r} (x^5 + x^3 + x^2 + x + 1) : (x^2 + x + 1) = x^3 + x^2 + x + 1 \\ x^5 + x^4 + x^3 \\ \hline x^4 + x^2 + x + 1 \\ x^4 + x^3 + x^2 \\ \hline x^3 + x + 1 \\ x^3 + x^2 + x \\ \hline x^2 + 1 \end{array} \quad \text{Rest } x$$

$\Rightarrow F(x)$  hat keine echten Teiler, also ist  $F(x)$  ein Minimalpolynom für  $\bar{F}_{32}$  und definiert  $\bar{F}_{32}$ .

b)  $\bar{F}_{2^2}$  mit  $F(x) = x^7 + x^6 + x^5 + x^2 + 1$

-  $F(x)$  hat keine Nullstellen über  $\mathbb{F}_2$

- Gibt es ein  $h(x), g(x)$ , sodass  $F(x) = h(x) \cdot g(x)$  gilt?

$\hookrightarrow$  O.B.d.A.  $\deg(h(x)) = 5 \wedge \deg(g(x)) = 2$

oder  $\deg(h(x)) = 4 \wedge \deg(g(x)) = 3$

? Gibt es so ein  $g(x)$  mit  $\deg(g(x)) = 2$ ?

$$(x^7 + x^6 + x^5 + x^2 + 1) : (x^2 + x + 1) = x^5 + 1 \quad \text{Rest } x$$

$$\begin{array}{r} x^7 + x^6 + x^5 \\ \hline x^2 + 1 \end{array} \quad \Rightarrow \text{Kein Teiler von } F(x)$$

2. Gibt es so ein  $g(x)$  mit  $\deg(g(x)) = 3$ ?

$\hookrightarrow$  Dieses Mal gibt es zwei Minimalpolynome, die beide auf echte Teiler mit  $F(x)$  getestet werden müssen. Die Polynome sind:

1.  $x^3 + x + 1 \quad 2. x^3 + x^2 + 1$

$$1. \quad (x^7 + x^6 + x^5 + x^2 + 1) : (x^3 + x + 1) = x^4 + x^3 + 1 \quad \text{Rest } x^2 + x$$

$$\begin{array}{r} x^7 + x^6 + x^5 + x^4 \\ \underline{-x^7 - x^6 - x^5} \\ x^4 + x^2 + 1 \\ \underline{-x^4 - x^3 - x^2} \\ x^3 + x + 1 \\ \underline{-x^3 - x^2 - x} \\ x^2 + x \end{array}$$

$\Rightarrow$  kein Teiler von  $F(x)$

$$2. \quad (x^7 + x^6 + x^5 + x^2 + 1) : (x^3 + x^2 + 1) = x^4 + x^2 \quad \text{Rest } 1$$

$$\begin{array}{r} x^7 + x^6 + x^4 \\ \underline{-x^7 - x^6 - x^5} \\ x^5 + x^4 + x^2 + 1 \\ \underline{-x^5 - x^4 - x^3} \\ x^3 + x^2 + 1 \\ \underline{-x^3 - x^2 - x} \\ 1 \end{array}$$

$\Rightarrow$  kein Teiler von  $F(x)$

$\Rightarrow F(x)$  ist teilerfremd und hat keine Nullstellen  
entsprechend ist es ein Minimalpolynom, welches  $\mathbb{F}_{128}$  definiert.

## Aufgabe 2

$\mathbb{F}_8$  mit  $\alpha^3 = \alpha^2 + 1$

zyklische Gruppe  $\mathbb{F}_8 \setminus \{0\}$ :

$$\begin{array}{llll} \alpha = \alpha & \alpha^3 = \alpha^2 + 1 & \alpha^5 = \alpha + 1 & \alpha^7 = 1 \\ \alpha^2 = \alpha^2 & \alpha^4 = \alpha^2 + \alpha + 1 & \alpha^6 = \alpha^2 + \alpha & \end{array}$$

$$\begin{aligned} a &= (1, 1, 0) \cdot (1, 1, 1) = (\alpha^2 + \alpha + 0) \cdot (\alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^3 + \alpha^2 + \alpha^2 + \alpha \\ &= \alpha^2 + \alpha + 1 + \alpha = \alpha^2 + 1 = \underline{(1, 0, 1)} = a \end{aligned}$$

$$b = \frac{(0, 1, 1)}{(1, 1, 1)} = \frac{\alpha + 1}{\alpha^2 + \alpha + 1} = \frac{\alpha^5}{\alpha^4} = \alpha = \underline{(0, 1, 0)} = b$$

$$c = \frac{(1, 0, 1)}{(1, 1, 0)} = \frac{\alpha^2 + 1}{\alpha^2 + \alpha} = \frac{\alpha^3}{\alpha^6} = \frac{1}{\alpha^3} = \frac{\alpha^7}{\alpha^3} = \alpha^4 = \alpha^2 + \alpha + 1 = \underline{(1, 1, 1)} = c$$

### Aufgabe 3

Fg mit  $\alpha^3 = \alpha + 1$ :

$$\alpha^4 = \alpha^2 + \alpha \quad \alpha^5 = \alpha^2 + \alpha + 1 \quad \alpha^6 = \alpha^2 + 1 \quad \alpha^7 = 1$$

LGS:

$$\left( \begin{array}{ccccc} \alpha & \alpha+1 & \alpha+1 & \alpha^2+\alpha & | 0 \\ \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha+1 & \alpha^2 & | 0 \end{array} \right) \xrightarrow{\text{II} + \alpha^2\text{I}} \left( \begin{array}{ccccc} \alpha & \alpha^3 & \alpha^3 & \alpha^4 & | 0 \\ \alpha^4 & \alpha^5 & \alpha^3 & \alpha^2 & | 0 \end{array} \right)$$

$$\left( \begin{array}{cccc} \alpha & \alpha^3 & \alpha^3 & \alpha^4 & | 0 \\ 0 & \alpha^6+\alpha^5 & \alpha^6+\alpha^3 & \alpha^4+\alpha^4 & | 0 \end{array} \right) \xrightarrow{\text{II} - \alpha^2\text{I}} \left( \begin{array}{cccc} \alpha & \alpha+1 & \alpha+1 & \alpha^2+\alpha & | 0 \\ 0 & \alpha & \alpha^2+\alpha & \alpha & | 0 \end{array} \right)$$

$x_3, x_4$  frei: Setze  $x_3 := 1, x_4 := 0 \Rightarrow (\alpha+1, \alpha+1, 1, 0)$

Dann gilt: Setze  $x_3 := 0, x_4 := 1 \Rightarrow (\alpha^2, \alpha^2+\alpha+1, 0, 1)$

Allg. Lsg.:  $\underline{r \cdot (\alpha+1, \alpha+1, 1, 0) + s \cdot (\alpha^2, \alpha^2+\alpha+1, 0, 1)}$

### Aufgabe 4

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

$$\begin{aligned}
 a &= (1, 1, 0, 0, 0, 0, 1, 1) \cdot (0, 0, 1, 1, 1, 0, 0, 0) \\
 &= (\alpha^2 + \alpha^6 + \alpha + 1) \cdot (\alpha^5 + \alpha^4 + \alpha^3) \\
 &= \alpha^{12} + \alpha^{21} + \alpha^6 + \alpha^5 + \alpha^{21} + \alpha^{20} + \alpha^5 + \alpha^4 + \alpha^{10} + \alpha^9 + \alpha^4 + \alpha^3 \\
 &= \alpha^{12} + \alpha^6 + \alpha^9 + \alpha^3 \\
 &= \alpha^4(\alpha^4 + \alpha^3 + \alpha^2 + 1) + \alpha(\alpha^4 + \alpha^3 + \alpha^2 + 1) + \alpha^6 + \alpha^3 \\
 &= \alpha^8 + \alpha^2 + \alpha^6 + \alpha^4 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + \alpha^6 + \alpha^3 \\
 &= \alpha^4 + \alpha^3 + \alpha^2 + 1 + \alpha^7 + \alpha^5 + \alpha \\
 &= \alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \\
 a &= (1, 0, 1, 1, 1, 1, 1, 1)
 \end{aligned}$$

$$\underline{b = (0, 1, 0, 1, 0, 1)^2}$$

$$\begin{aligned}
 &= (\alpha^6 + \alpha^4 + \alpha^2 + 1)(\alpha^6 + \alpha^4 + \alpha^2 + 1) \\
 &= \alpha^{12} + \alpha^{10} + \alpha^8 + \alpha^6 + \alpha^{10} + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 \\
 &\quad + \alpha^6 + \alpha^4 + \alpha^2 + 1 \\
 &= \alpha^{12} + \alpha^8 + \alpha^4 + 1 \\
 &= \alpha^8 + \alpha^2 + \alpha^6 + \alpha^4 + \alpha^8 + \alpha^4 + 1
 \end{aligned}$$

$$b = \alpha^7 + \alpha^6 + 1$$

$$\underline{b = (1, 1, 0, 0, 1, 0, 0, 1)}$$

$$c = (0, 0, 0, 0, 0, 1, 1, 0) / (1, 0, 0, 0, 1, 1, 0, 1)$$
$$= (\alpha^2 + \alpha) / (\alpha^7 + \alpha^6 + \alpha^5 + 1)$$

Um das Inverse von  $(\alpha^7 + \alpha^6 + \alpha^5 + 1)$  zu berechnen, nutze ich Euklid mit  $F(\alpha) = \alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1$ :

$$i=0: \frac{(\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1)}{\alpha^8 + \alpha^4 + \alpha^3 + \alpha} : (\alpha^7 + \alpha^6 + \alpha^5 + 1) = \alpha \quad \text{Rest: } \alpha^2 + \alpha + 1$$

$$i=1: \frac{(\alpha^7 + \alpha^6 + \alpha^5 + 1)}{\alpha^7 + \alpha^6 + \alpha^5} : (\alpha^2 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^2 \quad \text{Rest: } 1$$
$$\frac{\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1}{\alpha^6 + \alpha^5 + \alpha^4} : (\alpha^4 + \alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha^2 \quad 1$$

$$\Rightarrow 1 = (\alpha^7 + \alpha^6 + \alpha^5 + 1) - (\alpha^5 + \alpha^4 + \alpha^2) \cdot (\alpha^2 + \alpha + 1)$$
$$= (\alpha^7 + \alpha^6 + \alpha^5 + 1) - (\alpha^5 + \alpha^4 + \alpha^2) \cdot ((\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1) - \alpha(\alpha^7 + \alpha^6 + \alpha^5 + 1))$$
$$= -(\alpha^5 + \alpha^4 + \alpha^2) F(\alpha) + (\alpha^6 + \alpha^5 + \alpha^3 + 1) \cdot (\alpha^7 + \alpha^6 + \alpha^5 + 1)$$

$$1 \equiv (\alpha^6 + \alpha^5 + \alpha^3 + 1) (\alpha^7 + \alpha^6 + \alpha^5 + 1)$$

$$\Rightarrow (\alpha^7 + \alpha^6 + \alpha^5 + 1)^{-1} = (\alpha^6 + \alpha^5 + \alpha^3 + 1)$$

$$\Rightarrow c = (\alpha^2 + \alpha) \cdot (\alpha^6 + \alpha^5 + \alpha^3 + 1)$$

$$= \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

$$= \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$$

$$= \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1$$

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