# Lösung 9 (BCH Codes)

a) $0, 1, D, D+1, D^2, D^2+1, D^2+D, D^2+D+1, D^3, D^3+1, D^3+D, D^3+D+1, D^3+D^2, D^3+D^2+1, D^3+D^2+D, D^3+D^2+D+1$

Die Addition in einem erweiterten Galois-Feld entspricht einer einfachen Polynomaddition. Das Ergebnis einer Polynommultiplikation könnte jedoch auch außerhalb der Menge aller gültigen Elemente liegen. Für zwei beliebige Polynome $a(D), b(D) \in GF(2^4)$ gilt daher:

$$\begin{aligned} + &: a(D) + b(D) \\ \cdot &: (a(D) \cdot b(D)) \ mod \ f(D). \end{aligned}$$

Im folgenden seien die Elemente im $GF(2^4)$ als Binärvektoren gegeben: $\vec{x} = x_3x_2x_1x_0 = x_3D^3 + x_2D^2 + x_1D + x_0$.

| + | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
| 0001 | 0001 | 0000 | 0011 | 0010 | 0101 | 0100 | 0111 | 0110 | 1001 | 1000 | 1011 | 1010 | 1101 | 1100 | 1111 | 1110 |
| 0010 | 0010 | 0011 | 0000 | 0001 | 0110 | 0111 | 0100 | 0101 | 1010 | 1011 | 1000 | 1001 | 1110 | 1111 | 1100 | 1101 |
| 0011 | 0011 | 0001 | 0001 | 0000 | 0111 | 0110 | 0101 | 0100 | 1011 | 1010 | 1001 | 1000 | 1111 | 1110 | 1101 | 1100 |
| 0100 | 0100 | 0101 | 0110 | 0111 | 0000 | 0001 | 0010 | 0011 | 1100 | 1101 | 1110 | 1111 | 1000 | 1001 | 1010 | 1011 |
| 0101 | 0101 | 0100 | 0111 | 0110 | 0001 | 0000 | 0011 | 0010 | 1101 | 1100 | 1111 | 1110 | 1001 | 1000 | 1011 | 1010 |
| 0110 | 0110 | 0111 | 0100 | 0101 | 0010 | 0011 | 0000 | 0001 | 1110 | 1111 | 1100 | 1101 | 1010 | 1011 | 1000 | 1011 |
| 0111 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 | 0000 | 1111 | 1110 | 1101 | 1100 | 1011 | 1010 | 1001 | 1000 |
| 1000 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |
| 1001 | 1001 | 1000 | 1011 | 1010 | 1101 | 1100 | 1111 | 1110 | 0001 | 0000 | 0011 | 0010 | 0101 | 0100 | 0111 | 0110 |
| 1010 | 1010 | 1011 | 1000 | 1001 | 1110 | 1111 | 1100 | 1101 | 0010 | 0011 | 0000 | 0001 | 0110 | 0111 | 0100 | 0101 |
| 1011 | 1011 | 1010 | 1001 | 1000 | 1111 | 1110 | 1101 | 1100 | 0011 | 0010 | 0001 | 0000 | 0111 | 0110 | 0101 | 0100 |
| 1100 | 1100 | 1101 | 1110 | 1111 | 1000 | 1001 | 1010 | 1011 | 0100 | 0101 | 0110 | 0111 | 0000 | 0001 | 0010 | 0011 |
| 1101 | 1101 | 1100 | 1111 | 1110 | 1001 | 1000 | 1011 | 1010 | 0101 | 0100 | 0111 | 0110 | 0001 | 0000 | 0011 | 0010 |
| 1110 | 1110 | 1111 | 1100 | 1101 | 1010 | 1011 | 1000 | 1001 | 0110 | 0111 | 0100 | 0101 | 0010 | 0011 | 0000 | 0001 |
| 1111 | 1111 | 1110 | 1101 | 1100 | 1011 | 1010 | 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 | 0000 |

| · | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |
| 0001 | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
| 0010 | 0000 | 0010 | 0100 | 0110 | 1000 | 1010 | 1100 | 1110 | 1111 | 1101 | 1011 | 1001 | 0111 | 0101 | 0011 | 0001 |
| 0011 | 0000 | 0011 | 0110 | 0101 | 1100 | 1111 | 1010 | 1001 | 0111 | 0100 | 0001 | 0010 | 1011 | 1000 | 1101 | 1110 |
| 0100 | 0000 | 0100 | 1000 | 1100 | 1111 | 1011 | 0111 | 0011 | 0001 | 0101 | 1001 | 1101 | 1110 | 1010 | 0110 | 0010 |
| 0101 | 0000 | 0101 | 1010 | 1111 | 1011 | 1110 | 0001 | 0100 | 1001 | 1100 | 0011 | 0110 | 0010 | 0111 | 1000 | 1101 |
| 0110 | 0000 | 0110 | 1100 | 1010 | 0111 | 0001 | 1011 | 1101 | 1110 | 1000 | 0010 | 0100 | 1001 | 1111 | 0101 | 0011 |
| 0111 | 0000 | 0111 | 1110 | 1001 | 0011 | 0100 | 1101 | 1010 | 0110 | 0001 | 1000 | 1111 | 0101 | 0010 | 1011 | 1100 |
| 1000 | 0000 | 1000 | 1111 | 0111 | 0001 | 1001 | 1110 | 0110 | 0010 | 1010 | 1101 | 0101 | 0011 | 1011 | 1100 | 0100 |
| 1001 | 0000 | 1001 | 1101 | 0100 | 0101 | 1100 | 1000 | 0001 | 1010 | 0011 | 0111 | 1110 | 1111 | 0110 | 0010 | 1011 |
| 1010 | 0000 | 1010 | 1011 | 0001 | 1001 | 0011 | 0010 | 1000 | 1101 | 0111 | 0110 | 1100 | 0100 | 1110 | 1111 | 0101 |
| 1011 | 0000 | 1011 | 1001 | 0010 | 1101 | 0110 | 0100 | 1111 | 0101 | 1110 | 1100 | 0111 | 1000 | 0011 | 0001 | 1010 |
| 1100 | 0000 | 1100 | 0111 | 1011 | 1110 | 0010 | 1001 | 0101 | 0011 | 1111 | 0100 | 1000 | 1101 | 0001 | 1010 | 0110 |
| 1101 | 0000 | 1101 | 0101 | 1000 | 1010 | 0111 | 1111 | 0010 | 1011 | 0110 | 1110 | 0011 | 0001 | 1100 | 0100 | 1001 |
| 1110 | 0000 | 1110 | 0011 | 1101 | 0110 | 1000 | 0101 | 1011 | 1100 | 0010 | 1111 | 0001 | 1010 | 0100 | 1001 | 0111 |
| 1111 | 0000 | 1111 | 0001 | 1110 | 0010 | 1101 | 0011 | 1100 | 0100 | 1011 | 0101 | 1010 | 0110 | 1001 | 0111 | 1000 |

b) Es handelt sich bei $\gamma = \alpha^2 + 1$ um ein primitives Element gdw., $\gamma^i \ mod \ f(\alpha)$, $0 \leq i \leq 14$, alle Elemente im $GF(2^4)$ erzeugt.

| $i$ | $\gamma^i \bmod f(\alpha) = (\alpha^2+1)^i \bmod f(\alpha)$ | $i$ | $\gamma^i \bmod f(\alpha) = (\alpha^2+1)^i \bmod f(\alpha)$ |
|---|---|---|---|
| 0 | $1$ | 8 | $\alpha+1$ |
| 1 | $\alpha^2+1$ | 9 | $\alpha^3+\alpha^2+\alpha+1$ |
| 2 | $\alpha^3+\alpha^2+\alpha$ | 10 | $\alpha^3+\alpha^2+1$ |
| 3 | $\alpha^3$ | 11 | $\alpha^2+\alpha+1$ |
| 4 | $\alpha^3+1$ | 12 | $\alpha^2$ |
| 5 | $\alpha^3+\alpha^2$ | 13 | $\alpha^3+\alpha+1$ |
| 6 | $\alpha$ | 14 | $\alpha^2+\alpha$ |
| 7 | $\alpha^3+\alpha$ | 15 | $1$ |

c)

$$
\begin{aligned}
m_1(D) &= (D-\gamma)(D-\gamma^2)(D-\gamma^4)(D-\gamma^8) \\
&= (D^2-(\gamma+\gamma^2)D+\gamma^3)(D^2-(\gamma^4+\gamma^8)D+\gamma^12) \\
&= D^4 - \underbrace{(\gamma+\gamma^2+\gamma^4+\gamma^8)}_{s_1} D^3 + \underbrace{(\gamma^3+\gamma^5+\gamma^6+\gamma^9+\gamma^{10}+\gamma^{12})}_{s_2} D^2 \\
&\qquad - \underbrace{(\gamma^7+\gamma^{11}+\gamma^{13}+\gamma^{14})}_{s_3} D + \gamma^{15} \\
&= D^4+D^3+1 = m_2(D) = m_4(D) \\
m_3(D) &= (D-\gamma^3)(D-\gamma^6)(D-\gamma^{12})(D-\gamma^{24}) \\
&= (D-\gamma^3)(D-\gamma^6)(D-\gamma^{12})(D-\gamma^9) \\
&= (D^2-(\gamma^3+\gamma^6)D+\gamma^9)(D^2-(\gamma^9+\gamma^{12})D+\gamma^{21}) \\
&= D^4 - \underbrace{(\gamma^3+\gamma^6+\gamma^9+\gamma^{12})}_{t_1} D^3 + \underbrace{(\gamma^9+\gamma^{12}+\gamma^{15}+\gamma^{15}+\gamma^{18}+\gamma^{21})}_{t_2} D^2 \\
&\qquad - \underbrace{(\gamma^{18}+\gamma^{21}+\gamma^{24}+\gamma^{27})}_{t_3} D + \gamma^{30} \\
&= D^4+D^3+D^2+D+1
\end{aligned}
$$

$$
\begin{aligned}
s_1 &= \gamma+\gamma^2+\gamma^4+\gamma^8 \\
&= (\alpha^2+1)+(\alpha^3+\alpha^2+\alpha)+(\alpha^3+1)+(\alpha+1) \\
&= 1 \\
s_2 &= \gamma^3+\gamma^5+\gamma^6+\gamma^9+\gamma^{10}+\gamma^{12} \\
&= (\alpha^3)+(\alpha^3+\alpha^2)+(\alpha)+(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+1)+(\alpha^2) \\
&= 0 \\
s_3 &= \gamma^7+\gamma^{11}+\gamma^{13}+\gamma^{14} \\
&= (\alpha^3+\alpha)+(\alpha^2+\alpha+1)+(\alpha^3+\alpha+1)+(\alpha^2+\alpha) \\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
t_1 &= \gamma^3 + \gamma^6 + \gamma^9 + \gamma^{12} \\
&= (\alpha^3) + (\alpha) + (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^2) \\
&= 1 \\
t_2 &= \gamma^9 + \gamma^{12} + \gamma^{15} + \gamma^{15} + \gamma^{18} + \gamma^{21} \\
&= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^2) + (1) + (1) + (\alpha^3) + (\alpha) \\
&= 1 \\
t_3 &= \gamma^{18} + \gamma^{21} + \gamma^{24} + \gamma^{27} \\
&= (\alpha^3) + (\alpha) + (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^2) \\
&= 1
\end{aligned}
$$

d)

$$
\begin{aligned}
g(D) &= KGV(m_1(D), \cdots, m_{2t}(D)) = KGV(m_1(D), m_2(D), m_3(D), m_4(D)) \\
&= m_1(D) \cdot m_3(D) = (D^4 + D^2 + 1)(D^4 + D^3 + D^2 + D + 1) \\
&= D^8 + D^4 + D^2 + D + 1
\end{aligned}
$$

$$
\begin{aligned}
N &= 15 \\
N - K &= grad\{g(D)\} = 8 \\
K &= 7 \\
R &= {}^{K}\!/_{N} = {}^{7}\!/_{15}
\end{aligned}
$$