Lösung 8 (BCH Codes)

a) $f(D)$ muss ein irreduzibles Polynom vom Grad 5 sein. Weiterhin können irreduzible Polynome keine Wurzel $\alpha \in [0,1]$ besitzen, da sie ansonsten den Faktor $(D-\alpha)$ hätten. Somit kann $f_1(D)$ ausgeschlossen werden, da es vom Grad 4 ist. Das Polynom $f_3(D)$ kann ausgeschlossen werden, weil es die Wurzel $\alpha = 0$ besitzt:

$f_2(0) = 0^5 + 0^4 + 0^3 + 0^2 + 1 = 1$ $\quad$ $f_2(1) = 1^5 + 1^4 + 1^3 + 1^2 + 1 = 1$

$f_3(0) = 0^5 + 0^4 + 0^3 + 1 = 1$ $\quad$ $f_3(1) = 1^5 + 1^4 + 1^3 + 1 = 0$

Somit bleibt das Polynom $f_2(D) = D^5 + D^4 + D^3 + D^2 + 1$ als einziger Kandidat übrig.

b)

i	$\alpha^i \ mod \ f(\alpha)$	i	$\alpha^i \ mod \ f(\alpha)$	i	$\alpha^i \ mod \ f(\alpha)$
0	1	11	$\alpha^2+\alpha+1$	22	$\alpha^4+\alpha^2+1$
1	α	12	$\alpha^3+\alpha^2+\alpha$	23	$\alpha^3+\alpha^2+\alpha+1$
2	α^2	13	$\alpha^4+\alpha^3+\alpha^2$	24	$\alpha^4+\alpha^3+\alpha^2+\alpha$
3	α^3	14	$\alpha^4+\alpha^3+\alpha^2+1$	25	$\alpha^4+\alpha^3+1$
4	α^4	15	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	26	$\alpha^4+\alpha^2+\alpha+1$
5	α^2+1	16	$\alpha^4+\alpha^3+\alpha+1$	27	$\alpha^3+\alpha+1$
6	$\alpha^3+\alpha$	17	$\alpha^4+\alpha+1$	28	$\alpha^4+\alpha^2+\alpha$
7	$\alpha^4+\alpha^2$	18	$\alpha+1$	29	α^3+1
8	$\alpha^3+\alpha^2+1$	19	$\alpha^2+\alpha$	30	$\alpha^4+\alpha$
9	$\alpha^4+\alpha^3+\alpha$	20	$\alpha^3+\alpha^2$	31	1
10	α^4+1	21	$\alpha^4+\alpha^3$	32	α

c) Allgemein: Die Ordnung m eines Elements α^i ist die kleinste positive ganze Zahl, für die $(\alpha^i)^m = e$ gilt. Weiterhin ist m ein Faktor von $2^n - 1$.

Primitive Elemente haben die Ordnung $2^n - 1$.

Für das $GF(2^5)$ gilt: $2^n - 1 = 2^5 - 1 = 31$ ist eine Primzahl.
Da die Ordnung aller Elemente Faktoren von 31 sind gilt also: $ord(\alpha^i) = 1$ oder $ord(\alpha^i) = 31$.
Offensichtlich kann nur für das Element $\alpha^i = \alpha^0 = 1$ die Bedingung $(\alpha^i)^1 = 1$ gelten. Alle anderen Elemente müssen somit die Ordnung $2^n - 1 = 31$ besitzen. Daraus folgt, dass das $GF(2^5)$ insgesamt $32 - 2 = 30$ (nach Abzug des Nullpolynoms) primitive Elemente besitzt.

d)

$$x + \alpha y = \alpha^3 \tag{1}$$
$$(1+\alpha^3)x + y = \alpha^3 + \alpha + 1 \tag{2}$$

$(1) \cdot \alpha^{30}$:

$$\alpha^{30}x + y = \alpha^2 \tag{3}$$

$(2) + (3)$:

$$\begin{aligned}
& & (\alpha^{30} + \alpha^3 + 1)x &= \alpha^3 + \alpha^2 + \alpha + 1 & (4)\\
&\Rightarrow & (\alpha^4 + \alpha^3 + \alpha + 1)x &= \alpha^3 + \alpha^2 + \alpha + 1 & (5)\\
&\Rightarrow & \alpha^{16}x &= \alpha^{23} & (6)\\
&\Rightarrow & x &= \alpha^{23-16} = \alpha^7 & (7)
\end{aligned}$$

In (1) einsetzen:

$$\begin{aligned}
& & \alpha^7 + \alpha y &= \alpha^3 & (8)\\
&\Rightarrow & \alpha y &= \alpha^7 + \alpha^3 = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^{13} & (9)\\
&\Rightarrow & y &= \alpha^{13-1} = \alpha^{12} & (10)
\end{aligned}$$

Überprüfung des Ergebnisses:

$$\begin{aligned}
\alpha^7 + \alpha \cdot \alpha^{12} &= \alpha^4 + \alpha^2 + \alpha^4 + \alpha^3 + \alpha^2\\
&= \alpha^3\\
(1 + \alpha^3)\alpha^7 + \alpha^{12} &= \alpha^7 + \alpha^{10} + \alpha^{12}\\
&= \alpha^4 + \alpha^2 + \alpha^4 + 1 + \alpha^3 + \alpha^2 + \alpha\\
&= \alpha^3 + \alpha + 1
\end{aligned}$$

e)

$\beta = \alpha^7 \;,\; \beta^2 = \alpha^{14} \;,\; \beta^4 = \alpha^{28} \;,\; \beta^8 = \alpha^{56} \;,\; \beta^{16} = \alpha^{112} \;,\; \beta^{32} = \alpha^{224} = \alpha^7$

$$
\begin{aligned}
\Rightarrow m_1(D) &= (D-\alpha^7)(D-\alpha^{14})(D-\alpha^{28})(D-\alpha^{56})(D-\alpha^{112}) \\
&= D^5 - (\alpha^7+\alpha^{14}+\alpha^{28}+\alpha^{56}+\alpha^{112})D^4 \\
&\quad + (\alpha^{21}+\alpha^{35}+\alpha^{42}+\alpha^{63}+\alpha^{70}+\alpha^{84}+\alpha^{119}+\alpha^{126}+\alpha^{140}+\alpha^{168})D^3 \\
&\quad - (\alpha^{49}+\alpha^{77}+\alpha^{91}+\alpha^{98}+\alpha^{133}+\alpha^{147}+\alpha^{154}+\alpha^{175}+\alpha^{182}+\alpha^{196})D^2 \\
&\quad + (\alpha^{105}+\alpha^{161}+\alpha^{189}+\alpha^{203}+\alpha^{210})D - \alpha^{217} \\
&= D^5 - \underbrace{(\alpha^7+\alpha^{14}+\alpha^{19}+\alpha^{25}+\alpha^{28})}_{t_1} D^4 \\
&\quad + \underbrace{(\alpha+\alpha^2+\alpha^4+\alpha^8+\alpha^{11}+\alpha^{13}+\alpha^{16}+\alpha^{21}+\alpha^{22}+\alpha^{26})}_{t_2} D^3 \\
&\quad - \underbrace{(\alpha^5+\alpha^9+\alpha^{10}+\alpha^{15}+\alpha^{18}+\alpha^{20}+\alpha^{23}+\alpha^{27}+\alpha^{29}+\alpha^{30})}_{t_3} D^2 \\
&\quad + \underbrace{(\alpha^3+\alpha^6+\alpha^{12}+\alpha^{17}+\alpha^{24})}_{t_4} D - 1 \\
&= D^5 + D^3 + D^2 + D + 1 = m_2(D)
\end{aligned}
$$

$$
\begin{aligned}
t_1 &= (\alpha^4+\alpha^2+\alpha) + (\alpha^4+\alpha^3+1) + (\alpha^4+\alpha^2) + (\alpha^4+\alpha^3+\alpha^2+1) + (\alpha^2+\alpha) = 0 \\
t_2 &= (\alpha^4+\alpha^2+1) + (\alpha^4) + (\alpha) + (\alpha^2+\alpha+1) + (\alpha^3+\alpha^2+1) + (\alpha^4+\alpha^3) + \\
&\quad (\alpha^4+\alpha^3+\alpha+1) + (\alpha^4+\alpha^3+\alpha^2) + (\alpha^4+\alpha^2+\alpha+1) + (\alpha^2) = 1 \\
t_3 &= (\alpha^3+1) + (\alpha^2+1) + (\alpha+1) + (\alpha^4+\alpha^3+\alpha^2+\alpha+1) + (\alpha^4+1) + \\
&\quad (\alpha^3+\alpha^2+\alpha+1) + (\alpha^3+\alpha^2) + (\alpha^4+\alpha) + (\alpha^3+\alpha+1) + (\alpha^4+\alpha^3+\alpha) = 1 \\
t_4 &= (\alpha^3+\alpha^2+\alpha) + (\alpha^4+\alpha+1) + (\alpha^4+\alpha^3+\alpha^2+\alpha) + (\alpha^3+\alpha) + (\alpha^3) = 1
\end{aligned}
$$

$$g(D) = KGV(m_1(D), m_2(D)) = m_1(D) = D^5 + D^3 + D^2 + D + 1$$

$$
\begin{aligned}
N &= 31 \\
N-K &= grad\{g(D)\} = 5 \\
K &= 26 \\
R &= {}^{K}\!/_{N} = {}^{26}\!/_{31}
\end{aligned}
$$

Aus der Beziehung $N = 2^{N-K} - 1$ und $t = 1$ folgt, dass es sich um einen Hamming-Code handelt. Es gilt $d = 2t + 1 = 3$.