Aufgabe 1: Für die Konstruktion des Körpers $GF(2^5)$ wird das primitive Polynom $p(x) = x^5 + x^3 + 1$ benutzt. Ergänzen Sie die fehlenden 5-Tupel in der nachfolgenden Tabelle.

i	α^i	α^4	α^3	α^2	α^1	α^0
0	1	0	0	0	0	1
1	α	0	0	0	1	0
2	α^2	0	0	1	0	0
3	α^3	0	1	0	0	0
4	α^4	1	0	0	0	0
5	α^5	0	1	0	0	1
6	α^6					
7	α^7					
8	α^8					
9	α^9					
10	α^{10}					
11	α^{11}					
12	α^{12}					
13	α^{13}					
14	α^{14}	0	0	0	1	1
15	α^{15}					
16	α^{16}					
17	α^{17}					
18	α^{18}					
19	α^{19}					
20	α^{20}					
21	α^{21}					
22	α^{22}					
23	α^{23}					
24	α^{24}					
25	α^{25}					
26	α^{26}					
27	α^{27}					
28	α^{28}					
29	α^{29}					
30	α^{30}					

Aufgabe 2: Addieren Sie mit der Tabelle aus Aufgabe 1 die folgenden Elemente:

$$\alpha^{14} + \alpha^{3} =$$

$$\alpha^{14} + \alpha^{18} =$$

$$\alpha^{14} + \alpha^{28} =$$

Aufgabe 3: Multiplizieren Sie in dem Körper von Aufgabe 1 die folgenden Elemente:

$$\alpha^{11} \cdot \alpha^{14} =$$

$$\alpha^{29} \cdot \alpha^{3} =$$

$$\alpha^{21} \cdot \alpha^{-25} =$$

Hinweis: Im Ergebnis sollen die Exponenten jeweils aus der Menge $\{0, 1, 2, \ldots 30\}$ sein.

Aufgabe 4: Sie wollen einen binären BCH-Code der Länge $n = 63$ konstruieren, der mindestens 6 Fehler korrigieren kann.

a.) Ergänzen Sie die folgende Zeile:

Für die Mindestdistanz gilt $d \geq$ entworfende Distanz = .

b.) Geben Sie die relevanten Kreisteilungsklassen an:

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16, 32\} \\ C_3 &= \{3, 6, 12, 24, 48, 33\} \\ &= \{\quad\quad\quad\quad\quad\quad\} \\ &= \{\quad\quad\quad\quad\quad\quad\} \\ &= \{\quad\quad\quad\quad\quad\quad\} \\ &= \{\quad\quad\quad\quad\quad\quad\} \end{aligned}$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

$$g(x) = m_1(x) \cdot m_3(x) \cdot \quad .$$

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

e.) Bestimmen Sie die Minimalpolynome von α und α^9.

$$m_1(x) =$$

$$m_9(x) =$$

Hinweis: Benutzen Sie zur Bestimmung von $m_1(x)$ und $m_9(x)$ den Körper $GF(2^6)$ mit dem primitiven Polynom x^6+x+1. Es gilt $p(\alpha) = 0$ und $\alpha^9 + \alpha^{18} + \alpha^{36} = 1$.

Aufgabe 5: Lösen Sie mit der quadratischen Lösungsformel die Gleichung

$$\alpha^{13} \cdot z^2 + z + \alpha^2 = 0$$

im Körper $GF(2^4)$ mit $p(x) = x^4 + x + 1$ wobei $p(\alpha) = 0$.

$$z_1 =$$
$$z_2 = \quad .$$

Aufgabe 6: Gegeben sei der Körper $GF(2^6)$, konstruiert mit dem primitiven Polynom $p(x) = x^6 + x + 1$, $p(\alpha) = 0$. Das Goppa Polynom $G(z) = z^2 + z + 1$ mit

$$L = GF(2^6) - \{\text{Nullstellen von } G(z) \text{ in } GF(2^6)\}$$

bestimmt einen binären Goppa Code.

Ergänzen Sie nachfolgend die Gleichung bzw. Ungleichungen für Länge n, Mindestdistanz d sowie Anzahl der Informationsstellen k des Codes.

$$n = |L| =$$
$$d \geq$$
$$k \geq \quad .$$

Aufgabe 7: Die nachfolgend angegebene Prüfmatrix $\mathbf{H}$ beschreibt einen nichtbinären $[12, 10, 3]$ Hamming Code über $GF(11)$ in systematischer Form.

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 \end{pmatrix}$$

a.) Bestimmen Sie die zugehörige Generatormatrix $\mathbf{G}$.

$$\mathbf{G} =$$

b.) Decodieren Sie die Vektoren

$$\mathbf{r_1} = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$$

$$\mathbf{r_2} = (0, 1, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0)$$

zu den nächsten Codewörtern $\mathbf{c_1}$ und $\mathbf{c_2}$:

$$\mathbf{c_1} =$$

$$\mathbf{c_2} =$$

c.) Codieren Sie die Nachrichtenvektoren

$$\mathbf{m_a} = (1, 2, 3, 4, 0, 0, 0, 0, 0, 0)$$

$$\mathbf{m_b} = (2, 2, 2, 2, 0, 0, 0, 0, 0, 0).$$

$$\mathbf{c_a} =$$

$$\mathbf{c_b} =$$

Aufgabe 8: Decodieren Sie den Binärvektor

$$\mathrm{r} = (r_0, r_1, \ldots, r_{15}) = (0,0,0,0,1,0,0,0,0,1,0,0,0,0,0,1)$$

zum nächsten Codewort des binären $[16, 8, 5]$ Goppa Codes, der mit dem Goppa Polynom $G(z) = z^2 + z + \alpha^3$ gebildet wird, wobei α Wurzel des primitiven Polynoms $x^4 + x + 1$ ist. Für die α_i gilt $\alpha_0 = 0$, $\alpha_i = \alpha^{i-1}$, $i = 1, 2, \ldots, 15$.

Hinweis: Es handelt sich um den Code, der in der Vorlesung behandelt wurde (siehe z.B. Aufgabe 21, Vorlesung vom 18.01.2008, Folie 16).

a.) Bestimmen Sie zunächst das Syndrom $S(z)$:

$$S(z) =$$

b.) Bestimmen Sie mit dem Syndrom $S(z)$ das Polynom $T(z)$:

$$T(z) =$$

c.) Bestimmen Sie sodann $R(z) = \sqrt{T(z) + z} \bmod G(z)$:

$$R(z) =$$

d.) Bestimmen Sie schließlich das Fehlerstellenpolynom $\sigma(z)$:

$$\sigma(z) =$$

e.) Finden Sie mittels der Nullstellen von $\sigma(z)$ den Fehlervektor $\mathbf{e}$ und das Codewort $\mathbf{c}$:

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Hinweis: Zur Nullstellensuche siehe auch Aufgabe 5.

Aufgabe 9: Decodieren Sie das Polynom

$$r(x) = 4x^2 + 5$$

zum nächsten Codewort des $[5, 3, 5]$ negazyklischen Codes über $GF(11)$, der mit dem Generatorpolynom $g(x) = (x - 2) \cdot (x - 2^3)$ erzeugt wird.

Hinweis: Es handelt sich um den Code, der in der Vorlesung behandelt wurde (siehe z.B. Aufgabe 24, Folie 16, 18.01.2008).

a.) Bestimmen Sie zunächst den bekannten Teil des Syndroms $\tilde{S}(z)$:

$$\tilde{S}(z) =$$

b.) Bestimmen Sie sodann das Polynom $U(z)$:

$$U(z) =$$

c.) Bestimmen Sie die relevanten Terme des Polynoms $1 + T(z)$:

$$1 + T(z) =$$

d.) Bestimmen Sie dann die Polynome $\phi(z)$ und $\omega(z)$

$$\phi(z) = \qquad\qquad \omega(z) =$$

e.) Bestimmen Sie schließlich das Fehlerstellenpolynom $\sigma(z)$:

$$\sigma(z) =$$

f.) Finden Sie mittels der Nullstellen von $\sigma(z)$ das Fehlerpolynom $e(x)$ und das Codewortpolynom $c(x)$:

$$e(x) =$$

$$c(x) =$$