Computational Algebra 3/02/14

1. Determine the splitting field of
   (a) $x^3 - x + 1$ over $\mathbb{F}_3$
   (b) $(x^2 + x + 1)(x^3 + x + 1)$ over $\mathbb{F}_2$

2. Find a primitive element of $\mathbb{F}_9$.

3. Decompose $x^8 - 1$ in irreducible factors in $\mathbb{F}_3$.

4. Construct a cyclic $[8, 3]$ code $\mathcal{C}$ over $\mathbb{F}_3$ and find an idempotent element of $\mathcal{C}$

5. Construct a cyclic code $\mathcal{C}$ over $\mathbb{F}_3$ of length 8 which can be used to correct up to 2 errors.

6. Consider the primitive element α of $\mathbb{F}_{16}$ satisfing $\alpha^4 = 1 + \alpha$. The elements of $\mathbb{F}_{16}$ are listed in the table below.

0000	0	1000	α^3	1011	α^7	1110	α^{11}
0001	1	0011	α^4	0101	α^8	1111	α^{12}
0010	α	0110	α^5	1010	α^9	1101	α^{13}
0100	α^2	1100	α^6	0111	α^{10}	1001	α^{14}

   Consider the BCH code of dimensions $[15, 7]$ over $\mathbb{F}_2[x]$ (with $b = 1$) with defining set $T = \{1, 2, 3, 4, 6, 8, 9, 12\}$. Using the primitive 15-root of unity α form the previous table, the generator polynomial of $\mathcal{C}$ is $g(x) = 1 + x^4 +^6 +x^7 + x^8$. Suppose $\mathcal{C}$ is used to transmit a codeword and $y(x)$ is received. Correct the received word using the Peterson-Gorenstein-Zierler Decoding Algorithm, in case $y(x) = 1 + x^2 + x^3 + x^7 + x^9 + x^{10}$ or $y(x) = 1 + x^4 + x^7 + x^9 + x^{10}$. Verify that the correct word is actually a codeword.

7. Give the definition of $\mathbb{Z}_4$-linear code. Give the definition of $\mathbb{Z}_4$-linear code of type $4^{k_1}2^{k_2}$.