COMPUTATIONAL ALGEBRA 24/02/14

1. Determine the splitting field of
   (a) $x^3 - x^2 - x$ over $\mathbb{F}_3$
   (b) $(x^3 - x^2 - x)(x^4 - x^2 - 1)$ over $\mathbb{F}_3$

2. Let K the smallest field of characteristic 2 containing a primitive 7-th root of unity.
   (a) Determine the number of elements of K.
   (b) Find a primitive element of K.
   (c) Determine all the primitive elements of K.

3. Decompose $x^8 - x$ in irreducible factors in $\mathbb{F}_2$.

4. (a) Find a primitive element of $\mathbb{F}_{13}$.
   (b) Construct a Reed-Solomon code $\mathcal{C}$ of dimensions $[12, 7]$ over $\mathbb{F}_{13}$.
   (c) Determine the minimal distance of $\mathcal{C}$.
   (d) Find a parity check matrix for $\mathcal{C}$.

5. 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 belove.

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 $[15, 5]$ over $\mathbb{F}_2[x]$ (with $b = 1$) with defining set $T = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12\}$. Using the primitive 15-root of unity α form the previous table, the generator polynomial of $\mathcal{C}$ is $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. 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 $y(x) = x^4 + x^5 + x^7 + x^9 + x^{10} + x^{12}$. Verify that the correct word is actually a codeword. Correct the same $y(x)$ using the Sugiyama Decoding Algorithm.

6. (a) Give the definition of $\mathbb{Z}_4$-linear code.
   (b) What are the Hamming, Lee and Euclidean distances between the vectors (30012221) and (20202213) in $\mathbb{Z}_4^8$?