Computational Algebra 18/02/15

1. Determine the splitting field of
   (a) $(x^3 - x + 1)(x^2 + 1)$ over $\mathbb{F}_3$
   (b) $x^4 + x^3 + x - 1$ over $\mathbb{F}_3$
   (c) $x^3 - x$ over $\mathbb{F}_4$

2. (a) Construct the field $\mathbb{F}_9$;
   (b) Find the primitive elements of $\mathbb{F}_9$;
   (c) Is it true that a primitive 3^{th}-root of the unit over $\mathbb{F}_3$ is contained in $\mathbb{F}_9$? If yes, find such a root.
   (d) Is it true that a primitive 4^{th}-root of the unit over $\mathbb{F}_3$ is contained in $\mathbb{F}_9$? If yes, find such a root.

3. (a) Construct a cyclic code $\mathcal{C}$ over $\mathbb{F}_3$ of length 8 and dimension 4.
   (b) Find a generator polynomial and a check polynomial for $\mathcal{C}$.
   (c) What can be said about the minimum distance of $\mathcal{C}$?

4. Decompose $x^{16} - x$ in irreducible factors over $\mathbb{F}_2$.

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 $y(x) = 1+x+x^5+x^6+x^7+x^{12}$. Verify that the correct word is actually a codeword. Correct the same $y(x)$ using the Sugiyama Decoding Algorithm.

6. Give the definition of a cyclic code of length m over $\mathbb{F}_q$. Show that the cyclic codes of length m over $\mathbb{F}_q$ correspond to the ideals of the ring $\mathbb{F}_q[x]/(x^m - 1)$.