ECE 259A: Problem Set #3

1. Let $\alpha \in GF(2^9)$, and let the minimal polynomial of $\alpha$ be $x^9 + x + 1$. Find the order of $\alpha$.

2. (a) Prove that $f(x) = x^3 + x^2 + 2$ is irreducible over $GF(3)$.
   (b) Let $\alpha$ denote the root of $f(x)$, and assume that $f(x)$ is used to construct $GF(27)$. Compute $(2\alpha + 1)(\alpha^2 + 2)$ in $GF(27)$.
   (c) What are the possible multiplicative orders of the elements of $GF(27)$?
   (d) What is the order of $\alpha$?

3. (a) Prove that each element $\beta$ of $GF(p^m)$ has a unique $p$-th root, that is $\gamma \in GF(p^m)$ such that $
\gamma^p = \beta$.
   (b) What are all the square roots of 1 in a field of characteristic two? In a field of odd characteristic?
   (c) Show that if $\alpha$ and $\beta$ are primitive elements in a field of odd characteristic, then $\alpha\beta$ is not primitive.
   (d) Find primitive elements $\alpha$ and $\beta$ in some field of characteristic two, such that $\alpha\beta$ is also primitive.

4. (a) Find a polynomial of degree 2 which is irreducible over $GF(2)$, and use this polynomial to construct $GF(4)$.
   (b) Find a polynomial of degree 2 which is irreducible over $GF(4)$, and use this polynomial along with the result of (a) to construct $GF(16)$.

5. The polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $GF(2)$. Let $\alpha$ denote the root of $f(x)$.
   (a) Show that $\alpha$ is not primitive in the field $GF(2)[x]/f(x)$.
   (b) Show that $\alpha + 1$ is primitive in this field.
   (c) Find the minimal polynomial $g(x)$ of $\alpha + 1$.
   (d) Find an isomorphism mapping between $GF(2)[x]/f(x)$ and $GF(2)[x]/g(x)$.

6. (a) Express the polynomial $x^6 - 1$ as a product of monic polynomials that are irreducible over $GF(2)$. How many monic polynomials divide $x^6 - 1$ over $GF(2)$?
   (b) Repeat (a) with "GF(2)" replaced by "GF(3)".

7. Let $\beta = \alpha^i$, where $\alpha$ is a primitive element of $GF(p^m)$. Prove that the minimal polynomial of $\beta$ is $M_{\beta}(x) = \prod_{j \in C_i}(x - \alpha^j)$, where $C_i$ is the cyclotomic coset mod $p^m - 1$ containing $i$. 