ECE 259A: Problem Set #3

1. Let $\alpha \in \text{GF}(2^9)$, 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 $\text{GF}(3)$.
   (b) Let $\alpha$ denote the root of $f(x)$, and assume that $f(x)$ is used to construct $\text{GF}(27)$. Compute $(2\alpha + 1)(\alpha^2 + 2)$ in $\text{GF}(27)$.
   (c) What are the possible multiplicative orders of the elements of $\text{GF}(27)$?
   (d) What is the order of $\alpha$?

3. (a) Prove that each element $\beta$ of $\text{GF}(p^m)$ has a unique $p$-th root, that is $\gamma \in \text{GF}(p^m)$ 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 $\text{GF}(2)$, and use this polynomial to construct $\text{GF}(4)$.
   (b) Find a polynomial of degree 2 which is irreducible over $\text{GF}(4)$, and use this polynomial along with the result of (a) to construct $\text{GF}(16)$.

5. The polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\text{GF}(2)$. Let $\alpha$ denote the root of $f(x)$.
   (a) Show that $\alpha$ is not primitive in the field $\text{GF}(2)[x]/f(x)$.
   (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 $\text{GF}(2)[x]/f(x)$ and $\text{GF}(2)[x]/g(x)$.

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