EE5160: Error Control Coding
Problem Set 2

1. a) Construct GF(8) using $p(X) = X^3 + X + 1$.
   b) Construct GF(8) using $p(X) = X^3 + X^2 + 1$.
   c) Show that the two fields obtained in a) and b) are isomorphic.

2. Let β be a nonzero element of GF(q^m). Let e be the smallest non-negative integer such that $\beta^{q^e} = \beta$. Prove that e divides m.

3. Prove that the extension field GF(p^m) of the prime field GF(p) is an m-dimensional vector space over GF(p).

4. Consider the Galois field GF(2^5) given by Table 2.10. Find the minimum polynomials of α^5 and α^7.

5. If $q-1$ is a prime, prove that every nonzero element of GF(q) not equal to the unit element 1 is primitive.