1. Let $F$ be a field of characteristic $p$ and order $q = p^m$ for some integer $m \geq 1$.

   (a) Prove that (since $p$ is a prime) $p$ divides $\binom{p}{j}$ for $j = 1, 2, \ldots, p - 1$.

   (b) Prove that for any $\alpha, \beta \in F$, we have $(\alpha + \beta)^p = \alpha^p + \beta^p$, and hence, by induction, $(\alpha + \beta)^{p^j} = \alpha^{p^j} + \beta^{p^j}$ for any $j \geq 1$.

   (c) Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial in $F[x]$. Use part (a) and induction on the degree, $n$, to prove that $(f(x))^q = f(x^q)$, meaning that

   $$\left( \sum_{i=0}^{n} a_i x^i \right)^q = \sum_{i=0}^{n} a_i (x^q)^i.$$  

   (d) Use part (b) and induction on $j$ to prove that $(f(x))^{q^j} = f(x^{q^j})$ for any $j \geq 1$.

2. Let $F$ be a field of order $q$, and let $K$ be an extension field of $F$. Let $\beta \in K$ be a nonzero element of degree $d$ over $F$.

   (a) Prove that $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{d-1}}$ are all distinct elements of $K$.

   (b) For positive integers $j$, prove that $\beta^{q^j} = \beta$ iff $d \mid j$. [Hint: Write $j = sd + r$ with $0 \leq r < d$.]

   (c) Deduce from (b) that if $K$ has order $q^m$, then $d \mid m$.

3. Let $\alpha$ be a primitive element in $F_{2^m}$.

   (a) For $m > 2$, prove that the degree (over $F_2$) of $\alpha^2$ is equal to $m$.

   [Hint: If $d = \deg(\alpha^3)$, then $\text{ord}(\alpha^3) \mid (2^d - 1)$. In particular, $\text{ord}(\alpha^3) \leq (2^d - 1)$. From Problem 5 of HW assignment 4, we have that $\text{ord}(\alpha^3) = \frac{2^m - 1}{\gcd(2^m - 1)} \geq \frac{2^m - 1}{3}$. Combining these inequalities, deduce that $d > m - 2$. Now, using Problem 2(c) above, eliminate the possibility that $d = m - 1$.]

   (b) Generalize the argument above to show that for $1 \leq j \leq 2^{\lceil m/2 \rceil}$, we have $\text{deg}_{F_2}(\alpha^j) = m$.

4. Consider the code $C$ consisting of all binary vectors in the nullspace of the matrix

   $$H = \begin{bmatrix}
   1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
   1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \alpha^{-7} & \alpha^{-8} & \alpha^{-9} & \alpha^{-10} & \alpha^{-11} & \alpha^{-12} & \alpha^{-13} & \alpha^{-14}
   \end{bmatrix},$$

   where $\alpha$ is a primitive element of $F_{16}$.

   (a) What is the dimension of $C$?

   (b) What is the minimum distance of $C$? [Hint: $1 + \alpha^5 + \alpha^{10} = 0$.]