1. Let $\mathbb{F}$ 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 $\alpha, \beta \in \mathbb{F}$, 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 $\mathbb{F}[x]$. Use part (a) and induction on the degree, $n$, to prove that $\left( f(x) \right)^q = f(x^q)$, 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 $\left( f(x) \right)^{q^j} = f(x^{q^j})$ for any $j \geq 1$.

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

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

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

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

   (a) For $m > 2$, prove that the degree (over $\mathbb{F}_2$) of $\alpha^3$ is equal to $m$. [Hint: If $d = \deg(\alpha^3)$, then ord($\alpha^3$) $\mid (2^d - 1)$. In particular, ord($\alpha^3$) $\leq (2^d - 1)$. From Problem 3 of HW assignment 6, we have that ord($\alpha^3$) $= \frac{2^m - 1}{\gcd(3, 2^m - 1)} \geq \frac{2^m - 1}{3}$. Combining these inequalities, deduce that $d > m - 2$. Now, using Problem 2(b) above, eliminate the possibility that $d = m - 1$.]

   (b) Generalize the argument above to show that for $1 \leq j \leq 2^{[m/2]}$, we have deg$_{\mathbb{F}_2}(\alpha^j) = m$.

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

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

   where $\alpha$ is a primitive element of $\mathbb{F}_{2^4}$.

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

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