Assignment of Chapter 7

1. If $p(x) = x^3 + x + 1$ is the primitive polynomial of $\mathbb{F}_8 = \{0, 1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6\}$, and the element σ is the root of $p(x)$, please
   (a) Show the addition table of $\mathbb{F}_8$.
   (b) Solve the equation
   $$\begin{bmatrix} \sigma^3 & \sigma^6 \\ 1 & \sigma^2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ \sigma^2 \end{bmatrix}.$$
   (c) Determine the roots of polynomial $p(x) = \sigma^4 x^3 + \sigma^2 x^2 + \sigma^5 x + \sigma^6$.
   (d) Given polynomials $f(x) = x^4 + \sigma x^3 + \sigma^3$ and $g(x) = \sigma^2 x^2 + \sigma^2 x$, compute $f(x)/g(x)$ and $f(x) \mod g(x)$.
2. Consider the finite field $\mathbb{F}_8$ as in *Question* 1. Given a $(7, 3)$ RS code defined over the $\mathbb{F}_8$, please
   (a) Determine the RS codeword of the message vector $(\sigma^4, \sigma^3, 1)$ through evaluating the message polynomial with code locators $1, \sigma, \sigma^2, \ldots, \sigma^6$.
   (b) Determine the generator matrix of the $(7, 3)$ RS code.
   (c) Prove that any three columns of the generator matrix are linearly independent.
   Solution tip: RS codes are maximum distance separable (MDS) codes.