Problem 8.16 :

(a) The generator polynomial of degree $4 = n - k$ should divide the polynomial $p^6 + 1$. Since the polynomial $p^6 + 1$ assumes the factorization

$$p^6 + 1 = (p+1)^3(p+1)^3 = (p+1)(p+1)(p^2+p+1)(p^2+p+1)$$

we find that the shortest possible generator polynomial of degree 4 is

$$g(p) = p^4 + p^2 + 1$$

The i^{th} row of the generator matrix $\mathbf{G}$ has the form

$$\mathbf{g}_i = \begin{bmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & p_{i,1} & \cdots & p_{i,4} \end{bmatrix}$$

where the 1 corresponds to the i-th column (to give a systematic code) and the $p_{i,1}, \ldots, p_{i,4}$ are obtained from the relation

$$p^{6-i} + p_{i,1}p^3 + p_{i,2}p^2 p_{i,3}p + p_{i,4} = p^{6-i}(\bmod p^4 + p^2 + 1)$$

Hence,

$$\begin{aligned} p^5 \bmod p^4 + p^2 + 1 &= (p^2+1)p \bmod p^4 + p^2 + 1 = p^3 + p \\ p^4 \bmod p^4 + p^2 + 1 &= p^2 + 1 \bmod p^4 + p^2 + 1 = p^2 + 1 \end{aligned}$$

and therefore,

$$\mathbf{G} = \left(\begin{array}{cc|cccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right)$$

The codewords of the code are

$$\begin{aligned} \mathbf{c}_1 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\ \mathbf{c}_2 &= \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \\ \mathbf{c}_3 &= \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \\ \mathbf{c}_4 &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

(b) The minimum distance of the linear $(6,2)$ cyclic code is $d_{\min} = w_{\min} = 3$. Therefore, the code can correct

$$e_c = \frac{d_{\min} - 1}{2} = 1 \text{ error}$$