PROBLEM 1. .

a) Rate $= \frac{\log(5)}{6}$

b) Since (111111, 101010 are in C but not their summation, this code is not linear.

c) 101100, 101010 have the minimum distance amoung all the pairs of codewords so the minimum distance is 2.

d) Since $d_{\text{min}} = 2$, this code can correct up to 1 erasure. It can not correct errors and it can detect up to 1 error.

e)
   1. Both codewords 111111, 010011 agree with ?1??11 and therefore we can not correct it.
   2. The only codeword which starts with 0 and ends with 1 is 010011 and so we can correct it to 010011.

f) The closest codeword to 111100 is 101100 and therefore the minimum number of errors that channel could introduce is 1. The farthest codeword to it is 000000 and the maximum number of errors that channel could introduce is 4.

PROBLEM 2. Suppose that $0 \neq x = (x_1, x_2, \ldots, x_n) \in \mathcal{C}$. Therefore $xH^T = 0$. This means that $(x_1, x_2, \ldots, x_n)H^T = x_1.v_1^T + x_2.v_2^T + \ldots + x_n.v_n^T = 0$. Since we assumed that any d columns of H are linearly independent, we can not have fewer than $d+1$ of x_i's being non-zero. So, x has at least $d+1$ nonzero entries. Hence, the Hamming weight of any nonzero codeword is at least $d+1$.

PROBLEM 3. a) Let $\mathcal{C}$ be an (n,k) binary linear code with minimum distance $2d+2$. Take an element x of $\mathcal{C}$ of Hamming weight $2d+2$. Suppose that the first entry of this vector is nonzero. Remove the first entry of all the vectors in $\mathcal{C}$. It is clear that the result is also a binary linear code of length $n-1$. Since the minimum distance of $\mathcal{C}$ is $2d+2 > 3$ enev after removing one coordinate, still all the codewords are different and therefore the number of codewords does not change. So, the result is in fact an $(n-1,k)$ binary linear code. Finally, for the minimum distance of the resulting code, since the Hamming weight of x in $\mathcal{C}$ is $2d+2$, after removing a nonzero coordinate of it, its Hamming weight becomes $2d+1$ and this is indeed the minimum Hamming weight among all the Hamming weights of nonzero codewords.

b) Let $\mathcal{C}$ be an (n, k) binary linear code with minimum distance $2d+1$. We will construct an $(n+1, k)$ binary linear code with minimum distance $2d+2$ as follows. Take any vector $x = (x_1, x_2, \ldots, x_n) \in \mathcal{C}$ define $f(x) = (x_0, x_1, x_2, \ldots, x_n)$ where $x_0 = x_1 + x_2 + \ldots + x_n \pmod 2$. It is easy to see that this code is a binary linear code of the same number of elements as $\mathcal{C}$. We only have to check the minimum Hamming weight of the nonzero codewords. To see this, first notice that the Hamming weight of $f(x)$ is at least as large as the Hamming weight of x. Therefore the minimum distance of the new code is at least $2d+1$. But notice that non of the new codewords have Hamming weight equal to $2d+1$. In fact, the summation of all the entries of $f(x)$ is equal to $x_0 + x_1 + \ldots + x_n = (x_1 + x_2 + \ldots + x_n) + x_1 + x_2 + \ldots + x_n = 0$. This means that the number of entries of $f(x)$ which are equal to 1 is an even number. It means that the Hamming weight of $f(x)$ is always an even number and can not be equal to $2d+1$. So, the minimum distance of the designed code is at $2d+2$.

Problem 4. (a) $5^0 \equiv 1 \bmod 7$, $5^1 \equiv 5 \bmod 7$, $5^2 \equiv 4 \bmod 7$, $5^3 \equiv 6 \bmod 7$, $5^4 \equiv 2 \bmod 7$, $5^5 \equiv 3 \bmod 7$. Since $\phi(7) = 6$ and $\gcd(5, 7) = 1$, from the Euler's theorem we have,

$$5^6 \equiv \bmod 7$$

(b) One can see from the previous part that $5^k \not\equiv 1 \bmod 7$ for $0 < k < 6$. Since $\phi(7) = 6$, and $\gcd(5^k, 7) = 1$ for any k we have from the Euler's theorem,

$$5^{6k} = (5^k)^6 \equiv 1 \bmod 7$$

(c) Clearly,

$$\begin{aligned}(5^k - 1)(1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) &= 5^k(1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) \\ &\quad - (1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) \\ &= 5^{6k} - 1 = 0\end{aligned}$$

The last equality follows from the previous part. This implies that

$$(5^k - 1) \sum_{i=0}^{5} 5^{ki} = 0$$

Again, from the previous part we know that $5^k \not\equiv 1 \bmod 7$ for $0 < k < 6$, this implies that

$$\sum_{i=0}^{5} 5^{ki} = 0$$

for $0 < k < 6$. For $k = 0$ we have

$$\sum_{i=0}^{5} 5^{ki} = 1 + 1 + 1 + 1 + 1 + 1 \equiv 6 \bmod 7$$

(e) From the definition of Fourier transform we have,

$$\hat{u}_i = \sum_{l=0,1,\ldots,5} u_l 3^{il}$$

Performing all computations modulo 7, we have

$$\begin{aligned}
\hat{u}_0 &= \sum_{l=0,1,\ldots,5} u_l 3^{0l} = \sum_{l=0,1,\ldots,5} u_l = 0 \\
\hat{u}_1 &= \sum_{l=0,1,\ldots,5} u_l 3^{1l} = 3 \\
\hat{u}_2 &= \sum_{l=0,1,\ldots,5} u_l 3^{2l} = 6 \\
\hat{u}_3 &= \sum_{l=0,1,\ldots,5} u_l 3^{3l} = 4 \\
\hat{u}_4 &= \sum_{l=0,1,\ldots,5} u_l 3^{4l} = 2 \\
\hat{u}_5 &= \sum_{l=0,1,\ldots,5} u_l 3^{5l} = 5
\end{aligned}$$

(f) From the definition of the inverse Fourier transform we have

$$u_j = 6 \sum_{i=0,1,\ldots,5} \hat{u}_i 5^{ij}$$

Since $\hat{u}_i$ is the i^{th} component of the Fourier transform of u, we use the its definition to get

$$u_j = 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 3^{il} 5^{ij}$$

Since $5 \cdot 3 \equiv 1 \bmod 7$, 3 is the inverse of 5, i.e. $3 = 5^{-1}$ modulo 7. Thus we have

$$\begin{aligned} u_j &= 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 5^{-il} 5^{ij} = 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 5^{i(j-l)} \\ &= \sum_{l=0,1,\ldots,5} u_l 6 \sum_{i=0,1,\ldots,5} (5^{(j-l)})^i \end{aligned}$$

where in the last equality we exchanged the order of two summations.

Now using the results of part (c) we know that $j = l$ implies $\sum_{i=0,1,\ldots,5} (5^{(j-l)})^i = 6 \bmod 7$ and $6 \cdot 6 = 36 \equiv 1 \bmod 7$. Also for $j \neq l$ we have

$$\sum_{i=0,1,\ldots,5} (5^{(j-l)})^i = \sum_{i=0,1,\ldots,5} (5^{ki})$$

where $0 < |k| < 6$. Thus if $k > 0$ then from the results of part (c) we have that

$$\sum_{i=0,1,\ldots,5} (5^{ki}) = 0$$

if $k < 0$, then we know that $5^{-1} = 3$, thus

$$\sum_{i=0,1,\ldots,5} (5^{ki}) = \sum_{i=0,1,\ldots,5} (3^{-ki})$$

Here $0 < -k < 6$. One can easily verify that the results of part (c) are valid if we replace 5 by 3, thus we get

$$\sum_{i=0,1,\ldots,5} (3^{-ki}) = 0$$

and hence

$$u_j = \sum_{l=0,1,\ldots,5} u_l 6 \sum_{i=0,1,\ldots,5} (5^{(j-l)})^i = u_j$$

(g) (i) Cyclic convolution y, of two vectors u, v is given by,

$$y[n] = \sum_{m=0,1,\ldots,5} u[m] v[n - m \bmod 6]$$

Note that here the signals are periodic with period 6. Thus we have

$$
\begin{aligned}
y[0] &= \sum_{m=0,1,\ldots,5} u[m]v[-m \bmod 6] \\
&= u[0]v[0] + u[1]v[5] + u[2]v[4] + u[3]v[3] + u[4]v[2] + u[5]v[1] = 5 \\
y[1] &= \sum_{m=0,1,\ldots,5} u[m]v[1-m \bmod 6] \\
&= u[0]v[1] + u[1]v[0] + u[2]v[5] + u[3]v[4] + u[4]v[3] + u[5]v[2] = 2 \\
y[2] &= \sum_{m=0,1,\ldots,5} u[m]v[2-m \bmod 6] \\
&= u[0]v[2] + u[1]v[1] + u[2]v[0] + u[3]v[5] + u[4]v[4] + u[5]v[3] = 5 \\
y[3] &= \sum_{m=0,1,\ldots,5} u[m]v[3-m \bmod 6] \\
&= u[0]v[3] + u[1]v[2] + u[2]v[1] + u[3]v[0] + u[4]v[5] + u[5]v[4] = 2 \\
y[4] &= \sum_{m=0,1,\ldots,5} u[m]v[4-m \bmod 6] \\
&= u[0]v[4] + u[1]v[3] + u[2]v[2] + u[3]v[1] + u[4]v[0] + u[5]v[5] = 5 \\
y[5] &= \sum_{m=0,1,\ldots,5} u[m]v[5-m \bmod 6] \\
&= u[0]v[5] + u[1]v[4] + u[2]v[3] + u[3]v[2] + u[4]v[1] + u[5]v[0] = 2
\end{aligned} \tag{1}
$$

(ii) Fourier transform of u is given by

$$
\begin{aligned}
\hat{u}_0 &= \sum_{l=0,1,\ldots,5} u_l 3^{0l} = \sum_{l=0,1,\ldots,5} u_l = 0 \\
\hat{u}_1 &= \sum_{l=0,1,\ldots,5} u_l 3^{1l} = 3 \\
\hat{u}_2 &= \sum_{l=0,1,\ldots,5} u_l 3^{2l} = 6 \\
\hat{u}_3 &= \sum_{l=0,1,\ldots,5} u_l 3^{3l} = 4 \\
\hat{u}_4 &= \sum_{l=0,1,\ldots,5} u_l 3^{4l} = 2 \\
\hat{u}_5 &= \sum_{l=0,1,\ldots,5} u_l 3^{5l} = 5
\end{aligned}
$$

The Fourier transform of v is given by

$$\hat{v}_0 = \sum_{l=0,1,\ldots,5} v_l 3^{0l} = \sum_{l=0,1,\ldots,5} v_l = 2$$
$$\hat{v}_1 = \sum_{l=0,1,\ldots,5} v_l 3^{1l} = 0$$
$$\hat{v}_2 = \sum_{l=0,1,\ldots,5} v_l 3^{2l} = 0$$
$$\hat{v}_3 = \sum_{l=0,1,\ldots,5} v_l 3^{3l} = 4$$
$$\hat{v}_4 = \sum_{l=0,1,\ldots,5} v_l 3^{4l} = 0$$
$$\hat{v}_5 = \sum_{l=0,1,\ldots,5} v_l 3^{5l} = 0$$

Multiplying $\hat{u}$ and $\hat{v}$ component wise we get

$$\hat{w}_0 = \hat{u}_0\hat{v}_0 = 0$$
$$\hat{w}_1 = \hat{u}_1\hat{v}_1 = 0$$
$$\hat{w}_2 = \hat{u}_2\hat{v}_2 = 0$$
$$\hat{w}_3 = \hat{u}_3\hat{v}_3 = 16 = 2 \bmod 7$$
$$\hat{w}_4 = \hat{u}_4\hat{v}_4 = 0$$
$$\hat{w}_5 = \hat{u}_5\hat{v}_5 = 0$$

We take the inverse Fourier transform of $\hat{w} = (000200)$ is given by $w = (525252)$ which matches the original calculation in equation (1).

(h) (a) For the canonical definition of RS codes, we consider n non-zero distinct elements $(a_0, a_1, \ldots, a_{n-1})$ of the field F_q where $n < q$. Then we consider all polynomials $A(x)$ of degree at most $k-1$ and then evaluate $(A(a_0), A(a_1), \ldots, A(a_{n-1}))$ to form the code of length n and dimension k. Here $n = 6$ and $q = 7$. Thus clearly the only 6 non-zero distinct elements are $1, 2, 3, 4, 5, 6$. Also since $k = 2$ we have that $A(x) = c_1 + c_2 x$ where both $c_1, c_2 \in F_7$. Thus there are 49 codewords.

Now we know from the previous part (a) that 3 is a *generator* of the field F_7, i.e. 3^i for $0 \le i \le 5$ covers all the non-zero elements of the field F_7. Indeed this is easily checked: $3^0 \equiv 1 \bmod 7, 3^1 \equiv 3 \bmod 7, 3^2 \equiv 2 \bmod 7, 3^3 \equiv 6 \bmod 7, 3^4 \equiv 4 \bmod 7, 3^5 \equiv 5 \bmod 7$. Now consider the Fourier transform of the set $\hat{c} = (c_1, c_2, 0, 0, 0)$ for $c_1, c_2 \in F_7$. We have

$$\begin{aligned}\hat{\hat{c}}_i &= \sum_{j=0,1,\ldots,5} \hat{c}_j 3^{ij} \\ &= c_1 + c_2 3^i\end{aligned}$$

The equivalence of the definitions is now got as follows: let the 6 distinct, non-zero elements required for the canonical definition of RS codes be given by

$$a_0 = 3^0 \equiv 1; a_1 = 3^1 \equiv 3; a_2 = 3^2 \equiv 2; a_3 = 3^3 \equiv 6; a_4 = 3^4 \equiv 4; a_5 = 3^5 \equiv 5.$$

Thus according to the canonical definition of RS codes, a codeword is given by

$$y_i = c_1 + c_2 3^i$$

which is exactly the Fourier transform of the set $\hat{c} = (c_1, c_2, 0, 0, 0, 0)$.

(b) Code is generated by the generator matrix G as follows: consider the vector $u = (u_1, \ldots, u_k)$, where k is the dimension of the code and each $u_i \in F_q$. Then a codeword x is given by $u \cdot G$. Here $k = 2, q = 7$. Thus we have $u = (u_1, u_2)$ and the codeword x is given by

$$x_i = u_1 g_{1i} + u_2 g_{2i} \bmod 7 \tag{2}$$

where (g_{1i}, g_{2i}) is the i^{th} column of the matrix G.
From the Fourier transform definition of the RS code, we see that

$$x_i = u_1 + u_2 3^i$$

where $u_1, u_2 \in F_7$. Thus together with equation (2), this implies that the i^{th} column of G is given by $(1, 3^i)$. One easily verifies that G is thus given by

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}.$$

(c) The codeword is given by

$$x_i = 1 + 4 \cdot 3^i \bmod 7$$

Thus

$$x_0 = 5; x_1 = 6; x_2 = 2; x_3 = 4; x_4 = 3; x_5 = 0$$

Thus the transmitted codeword is given by $(5, 6, 2, 4, 3, 0)$.

(d) Let us denote the codeword by $x = (x_0, x_1, x_2, x_3, x_4, x_5)$. Using the generator matrix definition of the code we get,

$$c_1 + 3c_2 = 4 \tag{3}$$
$$c_1 + 6c_2 = 6 \tag{4}$$
$$c_1 + 4c_2 = 0 \tag{5}$$

Solving equation (1), (2) we get $c_1 = 2, c_2 = 3$. Thus the transmitted codeword is given by (541603).