Question 1.

(a) No. Let $C = \{010, 101, 111\}$, then $0 \cdot 010 = 000 \notin C$.

(b) No. Let $C = \{0\}$, then $C' = \{1\}$ which is not a linear code, since $0 \cdot 1 = 0 \notin C'$.

(c) Yes. We need to verify linear code axioms:

(i) Observe $a \otimes b = a + b$ under $\mathbb{F}_2^n$. Let $c_1, c_1' \in C_1$ and $c_2, c_2' \in C_2$, then:

$$\begin{aligned}(c_1 \otimes c_2) + (c_1' \otimes c_2') &= (c_1 + c_2) + (c_1' + c_2') \\ &= (c_1 + c_1') + (c_2 + c_2') \\ &= c_1'' + c_2'' \\ &= c_1'' \otimes c_2'' \in C'',\end{aligned}$$

where $c_1'' \in C_1$ and $c_2'' \in C_2$. So the axiom of additive closure holds.

(ii) Observe $0 \cdot a = 0^n$ and $1 \cdot a = a$ under $\mathbb{F}_2^n$. So we need to check only that $0^n \in C''$. Since $0^n \in C_1$ and $0^n \in C_2$, then $0^n \otimes 0^n = 0^n \in C''$. So the axiom of scalar multiplication closure holds.

Question 2.

(a) We can read out the $n = 5$ and $k = 2$ directly from the generating matrix G. With a little effort, since the code contains only four words, we can also see that the codeword with smallest weight is 01010 and therefore $d = 2$.

(b) The code C has 4 codewords: $\{00000, 10101, 01010, 11111\}$. The array has dimension $q^{n-k} = 2^3 = 8$ by $q^k = 4$. A standard (Slepian) array is given as follows:

00000	10101	01010	11111
10000	00101	11010	01111
01000	11101	00010	10111
00100	10001	01110	11011
00001	10100	01011	11110
10010	00111	11000	01101
00011	10110	01001	11100
00110	10011	01100	11001

(c) We can find the word 11110 which is decoded to the first row in its column – codeword 00111.

Question 3.

(a) Yes.

Code generated by G_1 is $C_1 = \{0000, 1001, 0101, 1100\}$

Code generated by G_2 is $C_2 = \{0000, 1010, 0011, 1001\}$

We can get code C_1 by doing permutation of 2nd and 3th and of 1st and 4th columns on the code words of C_2.

(b) Yes.

Code generated by G_1 is $C_1 = \{00000, 11000, 01010, 00101, 01111, 10010, 11101, 10111\}$.

Code generated by G_2 is $C_2 = \{00000, 11110, 10010, 01111, 11101, 01100, 10001, 00011\}$.

We can get code C_1 by doing permutation of 2nd and 5th columns on the code words of C_2.

(c) Two codes are permutation equivalent if they are equal up to a fixed permutation on the code word coordinates, so we can generate the code words and try all the possible permutations and then decide if they are permutation equivalent. All the combinations have a finite and fixed number.

Question 4.

Consider the binary linear code C with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

(a) Find the parity-check matrix of C.

To get the parity check matrix I first edit the generator G matrix to normal form.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \sim$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right] = [\ I_3 \mid A\ ]$$

Then parity matrix H is created as:

$$H = [\ -A^T \mid I_3\ ] = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(b) Find the syndrome of the word 100001.

To find the syndrome I have to multiply received word $w = 100001$ with the matrix H.

$$w \cdot H^T = (010)$$

Syndrome of this word is 010.

Question 5.

$\{1001, 0111, 1110\}$

(a) Third word is linear combination of the first two. Generator matrix for binary linear code containing these words can look like this:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

This code is also the smallest possible, because vectors in matrix G are linearly independent. $\mathrm{C} = \{0000, 1001, 1110, 0111\}$ $|C| = 2^2$

(b) These words are linearly independent in GF(3). Generator matrix for such a code can look like this:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

This matrix generates the smallest ternary linear code C_3. $|C_3| = 3^3$

Question 6.

Proof. We know that $x = x_1x_2 \dots x_{12} \in C \iff xH^\top = \mathbf{0} = \underbrace{(0, \dots, 0)}_{12 \text{ zeros}}$. If $H_i^\top$ denotes the i-th column in $H^\top$, then this is iff $\bigwedge\limits_{1 \le i \le 12} x \cdot H_i^\top = 0$.

We can sum up these equations into one and see that the following must hold

$$\sum_{1 \le i \le 12} 3x_i \equiv \sum_{1 \le i \le 12} x_i \equiv 0 \pmod 2$$

However, this only holds iff we have an even number indices $i \in \{1, \dots, 12\}$ s.t. $x_i = 1$. □

Question 7.

Consider code C_1 and its dual $C_1^\perp$. Consider an operation O that transforms C_1 into equivalent code C_2. We will show that for each such operation, there is a corresponding equivalent operation O' that transforms $C_1^\perp$ into $C_2^\perp$.

There are two types of operations that we have to consider:

(a) permutation of the words or positions of the code

Permutation of words is trivial case. Permutation of words in C_1, doesn't affect $C_1^\perp$ so in this case, the corresponding operation on $C_1^\perp$ is to do nothing.
Permutation of positions of the code does affect dual code. To make things simpler, we can decompose permutation into sequence of swapping of two columns. Now, when we swap two columns in C_1 to obtain C_2, we swap columns on same positions in $C_1^\perp$ to obtain $C_2^\perp$ to ensure that same pairs of symbols will be multiplied with each other as before swapping. Thus the scalar product will remain the same (zero) for all pairs of codewords.

(b) multiplication of symbols appearing in a fixed position by a non-zero scalar

Consider $v_1v_2v_3 \dots v_n \in C_1$ and $u_1u_2u_3 \dots u_n \in C_1^\perp$ and suppose that to obtain C_2, column i of v was multiplied by non-zero scalar x. Before, i-th column added v_iu_i to the sum. Now it would add xv_iu_i so naturally, the sum wouldn't be zero anymore. To fix this in $C_2^\perp$, column i of u can be multiplied by modular inverse of x (mod q), denoted as x^{-1}. It holds that $x^{-1}x = 1$ (mod q) and modular inverse exists for all numbers that share no prime factors with q, which are actually all numbers $1, 2, \dots q-1$ since we assume that q is a prime. So now given columns will again be adding $xv_ix^{-1}u_i = v_iu_i$ to the sum. Thus the scalar product will remain the same (zero) for all pairs of codewords.

For any equivalent codes C_1 and C_2, there is a sequence of operations a) and b) that can transform one code into the other. We can map all of those operations to the corresponding operations on dual codes as shown above. Described operations on dual codes are again operations of type either a) or b) (swapping rows = permutation of positions and multiplying by modular inverse = multiplying by non-zero scalar). So $C_1^\perp$ and $C_2^\perp$ are equivalent because one can be obtained from the other by sequence of operations a) and b).