Q. 1. Show whether the groups $G_{10}$ and $G_7$ are cyclic or not. If so, determine their generators.

Proof. The subgroups generated by the elements of $G_7$ are

\[
\langle [1]_7 \rangle = \{[1]_7\}, \\
\langle [2]_7 \rangle = \{[1]_7, [2]_7, [4]_7, [6]_7\}, \\
\langle [3]_7 \rangle = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}, \\
\langle [4]_7 \rangle = \{[1]_7, [4]_7\}, \\
\langle [5]_7 \rangle = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}, \\
\langle [6]_7 \rangle = \{[1]_7, [6]_7\}.
\]

Therefore $G_7 = \langle [1]_7 \rangle = \langle [5]_7 \rangle$ and $G_7$ is cyclic.

Over $G_{10} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$, we have

\[
\langle [1]_{10} \rangle = \{[1]_{10}\}, \\
\langle [3]_{10} \rangle = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}, \\
\langle [7]_{10} \rangle = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}, \\
\langle [9]_{10} \rangle = \{[1]_{10}, [9]_{10}\}.
\]

Therefore $G_{10} = \langle [1]_{10} \rangle = \langle [7]_{10} \rangle$ and $G_{10}$ is cyclic. \(\Box\)

Q. 2. Let $(G, \ast)$ and $(H, \circ)$ be two groups. Consider the cartesian product $G \times H$ with the operation $(g_1, h_1)(g_2, h_2) = (g_1 \ast g_2, h_1 \circ h_2)$ for all $(g_1, h_1), (g_2, h_2) \in G \times H$. Show that $G \times H$ is a group. Prove that $G \times H$ is Abelian (commutative) if and only if both $G$ and $H$ are Abelian.

Proof. First, we show that $G \times H$ is a group. We go through the four group axioms.

1. For all $(g_1, h_1), (g_2, h_2) \in G \times H$, we have $(g_1, h_1)(g_2, h_2) = (g_1 \ast g_2, h_1 \circ h_2)$ and $g_1 \ast g_2 \in G$, $h_1 \circ h_2 \in H$. So $(g_1, h_1)(g_2, h_2) \in G \times H$. This shows that $G \times H$ is closed under the group operation.

2. For all $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$, we have

\[
[(g_1, h_1)(g_2, h_2))(g_3, h_3)] = (g_1 \ast g_2, h_1 \circ h_2)(g_3, h_3) = ((g_1 \ast g_2) \ast g_3, (h_1 \circ h_2) \circ h_3).
\]

Notice that $(g_1 \ast g_2) \ast g_3 = g_1 \ast (g_2 \ast g_3)$ since $G$ is a group. Similarly, $(h_1 \circ h_2) \circ h_3) = h_1 \circ (h_2 \circ h_3)$. So, continuing from the last equation

\[
((g_1 \ast g_2) \ast g_3, (h_1 \circ h_2) \circ h_3) = (g_1 \ast (g_2 \ast g_3), h_1 \circ (h_2 \circ h_3))
\]

\[
= (g_1, h_1)(g_2 \ast g_3, h_2 \circ h_3)
\]

\[
= (g_1, h_1)[(g_2, h_2)(g_3, h_3)].
\]

Therefore, the group operation is associative.

3. The identity element is $(e_G, e_H)$ where $e_G$ is the identity element in $(G, \ast)$ and $e_H$ is the identity element in $(H, \circ)$.

4. The inverse of $(g, h) \in G \times H$ is $(g', h') \in G \times H$ where $g'$ is the inverse of $g$ with respect to $\ast$ in $G$ and $h'$ is the inverse of $h$ with respect to $\circ$ in $H$. Since all four axioms are satisfied, we conclude that $G \times H$ is a group.
Now let us show the second part of the question. Let \((g_1, h_1), (g_2, h_2) \in G \times H\). Then,
\[
(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)
\]
and
\[
(g_2, h_2)(g_1, h_1) = (g_2 * g_1, h_2 \circ h_1).
\]
By definition, \(G \times H\) is commutative if and only if \((g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)\). The latter holds if and only if \((g_1 + g_2, h_1 \circ h_2) = (g_2 + g_1, h_2 \circ h_1)\), that is, if and only if \(g_1 + g_2 = g_2 + g_1\) and \(h_1 \circ h_2 = h_2 \circ h_1\), in other words, \(G\) and \(H\) both are commutative. (4 pts)

Q. 3. Show that \(\mathbb{Z} \times \mathbb{Z}\) is not cyclic.

Proof. The standard group operation on \(\mathbb{Z} \times \mathbb{Z}\) is given by \((a,b)(c,d) = (a+c, b+d)\) for \((a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}\). We will say that \(\mathbb{Z} \times \mathbb{Z}\) is cyclic if and only if it can be generated by a single element \((x,y) \in \mathbb{Z} \times \mathbb{Z}\). That is, if any \((a,b) \in \mathbb{Z} \times \mathbb{Z}\) can be written as \((a,b) = (nx, ny)\) for some \(n \in \mathbb{Z}\). The equality \((a,b) = (nx, ny)\) has a solution for \(n\) if and only if \(n = \frac{a}{2}\) and \(n = \frac{b}{2}\). The common divisor of all integers is 1 (or \(-1\)). So, \(x, y\) must be 1 or \(-1\). However, \((1,1)\) can only generate the elements of the form \((a, a) \in \mathbb{Z} \times \mathbb{Z}\) and \((1,-1)\) can generate the elements of the form \((a,-a) \in \mathbb{Z} \times \mathbb{Z}\). Therefore, \(\mathbb{Z} \times \mathbb{Z}\) is not cyclic. (1 pt)

Q. 4. Consider \(\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}\) as a group with the addition defined by \((a,b) + (c,d) = (a+b, c+d)\) for all \((a,b), (c,d) \in \mathbb{R}^2\). Show that the function \(f: \mathbb{R}^2 \to \mathbb{R}^2\) given by \(f(x,y) = (x,x)\) is a group homomorphism.

Proof. The condition for \(f\) to be a group homomorphism is that
\[
f((a,b) + (c,d)) = f(a,b) + f(c,d)
\]
for all \((a,b), (c,d) \in \mathbb{R}^2\). By the assumption, \(f((a,b) + (c,d)) = f(a+c, b+d) = (a+c, a+c)\).

On the other hand,
\[
f(a,b) + f(c,d) = (a,a) + (c,c) = (a+c, a+c)
\]
Therefore, \(f((a,b) + (c,d)) = f(a,b) + f(c,d)\) and \(f\) is a group homomorphism. (1 pt)

Q. 5. Exercise 5.3.3. Let \(G\) be any group and \(g\) be an element of \(G\). Define the function \(f: G \to G\) by \(f(a) = g^{-1}ag\) for \(a \in G\). Show that \(f\) is an isomorphism \(G\) to itself.

Proof. First of all, \(f\) is a group homomorphism since for any \(a, b \in G\), we have
\[
f(ab) = g^{-1}abg = g^{-1}agg^{-1}bg = (g^{-1}ag)(g^{-1}bg) = f(a)f(b).
\]
So, we need to show that \(f\) is bijective.

Let \(a, b \in G\) and assume that \(f(a) = f(b)\). Then
\[
g^{-1}ag = g^{-1}bg \iff ag = bg \iff a = b.
\]
Hence, \(f\) is one-to-one.

Now, let \(b \in G\). Then \(g^{-1}ag = b\) if and only if \(ag = gb\), and the latter holds if and only if \(a = gb^{-1}\). Hence \(b = f(a)\) for \(a = gb^{-1} \in G\), and \(f\) is surjective.

Therefore \(f\) is an isomorphism of \(G\) to itself. (3 pts)

Q. 6. Exercise 5.2.4. Let \(H\) be a subgroup of the group \(G\) and let \(a\) be an element of \(G\). Fix an element \(b\) in \(aH\) (so \(b = ah\) for some \(h \in H\)). Show that
\[
H = \{b^{-1}c \mid c \in aH\}.
\]

Proof. Let us denote the set \(\{b^{-1}c \mid c \in aH\}\) by \(K\) and show that \(H = K\).

Let \(\ell \in H\) then \(b\ell = ah\ell\). By Multiplying both sides of \(b\ell = ah\ell\) on the left by \(b^{-1}\) we get \(\ell = b^{-1}ah\ell\). Since \(h\ell \in H\), we have \(ah\ell \in aH\). As a result, \(\ell\) has the form \(\ell = b^{-1}c\) for \(c = ah\ell\). So, \(\ell \in K\). Therefore, \(H \subseteq K\).

Let \(k \in K\). Then \(k = b^{-1}c\) for some \(c \in aH\), (or \(c = ah_1\) for some \(h_1 \in H\)). So,
\[
k = (ah)^{-1}c = (ah)^{-1}ah_1 = h_{-1}a^{-1}ah_1 = h_{-1}h_1.
\]
Since \(h, h_1 \in H\) and \(H\) is a subgroup, \(hh_1 \in H\). So, \(k \in H\). Hence, \(K \subseteq H\).

Consequently, \(H = K\). (2 pts)
Q. 7. Exercise 5.4.1. Show that the check digit at the end of an ISBN code can detect an error made by interchanging two adjacent digits.

Proof. Let us assume that \( n \) is the correct integer calculated by \( \sum_{i=2}^{10} 10^i \cdot a_i \) and \( b \) is the check digit. Suppose that \( a_i \) and \( a_{i+1} \) are exchanged. Then,

\[
\begin{align*}
n' &= 10 \cdot a_{10} + 9 \cdot a_9 + \cdots + (i + 1) \cdot a_i + i \cdot a_{i+1} + \cdots + 2 \cdot a_2 \\
&= 10 \cdot a_{10} + 9 \cdot a_9 + \cdots + (i + 1) \cdot a_{i+1} + i \cdot a_i + \cdots + 2 \cdot a_2 - a_{i+1} + a_i
\end{align*}
\]

The value of the check digit after the error is equal to

\[
b' \equiv -n' \mod 11 \equiv -n + a_{i+1} - a_i \equiv b + a_{i+1} - a_i.
\]

Therefore, the code detects the error if and only if \( b' \neq b \), that is, if and only if \( a_{i+1} - a_i \neq 0 \). Since exchanging \( a_{i+1} \) with \( a_i \) when \( a_{i+1} = a_i \) is not error, we conclude that the code detects that type error.

(2 pts)

Q. 8. For each of the following generator matrices, find the minimum distance and determine the number of errors that it can detect and correct.

\[
M_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},
\]

\[
M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},
\]

\[
M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.
\]

Proof. Consider \( M_1 \). Then 100 is mapped to 100 \( \cdot M_1 = 1001101 = w_1 \), 010 to 010 \( \cdot M_1 = 01001101 = w_2 \) and 001 to 001 \( \cdot M_1 = 00100111 = w_3 \). The minimum weight among \( w_1, w_2, w_3 \) is 4. The rest of the codewords are of the form \( \alpha w_1 + \beta w_2 + \gamma w_3 \) for \( \alpha, \beta, \gamma \in \{0, 1\} \). However, it is not possible to produce a codeword of weight 3 or less by that formula. Therefore the minimum distance between the codewords is 4. The code can detect 3 errors and correct 1 error.

By a similar discussion, we find that the minimum distance between the codewords produced by the code generated by \( M_2 \) is 3. So, it can detect 2 errors and correct 1.

Let us consider \( M_3 \). We have 1000 \( \cdot M_3 = 1000111, 0100 \cdot M_3 = 0100110, 0010 \cdot M_3 = 0010101 \) and 0001 \( \cdot M_3 = 0001110 \). The minimum weight among those codewords is 3. However, if we consider the rest of the codewords, we observe that the weight of

\[
0100110 + 0001110 = 0101000
\]

is 2. Therefore the minimum distance is 2 and the code can detect 1 error but correct none.

(3 pts)

Q. 9. Exercise 5.4.3. Let \( f : \mathbb{B}^3 \to \mathbb{B}^9 \) be a coding function given by

\[
f(abc) = ab \bar{c} \bar{a} \bar{b} \bar{c} \bar{a} \bar{b} \bar{c}
\]

for \( abc \in \mathbb{B}^3 \) where \( \bar{x} = 1 \) if \( x = 0 \) and \( \bar{x} = 0 \) if \( x = 1 \). List the eight codewords of \( f \). Show that \( f \) does not give a group (linear) code.
Proof. The code maps

000 ↦→ 00000111
100 ↦→ 10010011
010 ↦→ 01001010
001 ↦→ 00100110
110 ↦→ 11011001
101 ↦→ 10110101
011 ↦→ 01101100
111 ↦→ 11111100.

However, \( f \) is not a linear code since the sum of the two codewords 010010101 + 110110001 = 100100100 is not a codeword.

Q. 10. Write down the complete coset decoding table for the code generated by the matrix

\[
\begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0
\end{pmatrix}
\]

A message is encoded using the letter equivalents

00 = G, 10 = S, 01 = Z, 11 = Y,

and received as

101111, 111111, 011110, 111101, 010000, 101101.

Correct and decode the received message.

Proof. We see that by the code

00 ↦→ 000000
10 ↦→ 101011
01 ↦→ 010110
11 ↦→ 111101.

The coset decoding table can be formed as follows.

<table>
<thead>
<tr>
<th>000000</th>
<th>101011</th>
<th>010110</th>
<th>111101</th>
</tr>
</thead>
<tbody>
<tr>
<td>100000</td>
<td>101011</td>
<td>110110</td>
<td>011101</td>
</tr>
<tr>
<td>010000</td>
<td>111110</td>
<td>000110</td>
<td>101101</td>
</tr>
<tr>
<td>001000</td>
<td>100110</td>
<td>011110</td>
<td>110101</td>
</tr>
<tr>
<td>000100</td>
<td>101011</td>
<td>010010</td>
<td>111001</td>
</tr>
<tr>
<td>000010</td>
<td>101001</td>
<td>010100</td>
<td>111111</td>
</tr>
<tr>
<td>000001</td>
<td>101101</td>
<td>010111</td>
<td>111100</td>
</tr>
<tr>
<td>100001</td>
<td>001010</td>
<td>110111</td>
<td>011100</td>
</tr>
<tr>
<td>100010</td>
<td>001001</td>
<td>110100</td>
<td>011111</td>
</tr>
<tr>
<td>101010</td>
<td>000011</td>
<td>111011</td>
<td>010101</td>
</tr>
<tr>
<td>110000</td>
<td>011011</td>
<td>100110</td>
<td>001101</td>
</tr>
<tr>
<td>110001</td>
<td>111110</td>
<td>000111</td>
<td>101100</td>
</tr>
<tr>
<td>011100</td>
<td>100111</td>
<td>011010</td>
<td>110001</td>
</tr>
<tr>
<td>001100</td>
<td>101110</td>
<td>010011</td>
<td>111000</td>
</tr>
<tr>
<td>000101</td>
<td>101101</td>
<td>010011</td>
<td>111100</td>
</tr>
</tbody>
</table>

We observe that in the received message 111101 is a codeword. For the rest of the words, we locate them in the coset decoding table and note the column leader. So, the words

101111, 111111, 011110, 111101, 010000, 101101

are corrected into

101011, 111110, 010110, 111101, 000000, 111101.

The encoded message is formed by the first two digits of those: 10, 11, 01, 11, 00, 11 which translates into SYZYGY.

(3 pts)