1. Let $G$ be a group of order $pq$ where $p$ and $q$ are prime numbers.

(i) Let $H$ be a proper subgroup of $G$. What are the possible values of $|H|$?

Solution. By a theorem of Lagrange, $|H|$ must divide $|G|$. Since the only divisors of $|G|$ are 1, $p$, $q$ and $pq = |G|$, and the order of a proper subgroup of a finite group is strictly smaller than the order of the group, we conclude that $|H| \in \{1, p, q\}$.

(ii) Show that every proper subgroup of $G$ is cyclic.

Solution. If $|H| = 1$ then $H$ consists of the identity element only and is cyclic. Otherwise, by (i), $|H|$ is a prime number say $p$. Let $h$ be an element of $H$ different from the identity element which exists since we assume that $|H| > 1$. Since $H$ is a group, $\langle h \rangle$ is a subgroup of $H$. Again, by a theorem of Lagrange, $|\langle h \rangle| > 1$ is a divisor of $|H| = p$ and therefore equals $p$, $p$ being prime. Thus, $|H| = |\langle h \rangle|$ and so $H = \langle h \rangle$ and therefore $H$ is cyclic.

2. Let

\[
\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}
\]

be permutations in $S_6$.

(i) Compute $\tau^2 \sigma$;

Solution. First, we compute $\tau^2$.

\[
\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix}
\]

Then

\[
\tau^2 \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}
\]

(ii) Express $\sigma$, $\tau$ and $\tau^2$ as products of disjoint cycles;

Solution. We have $\sigma : 1 \to 3 \to 4 \to 5 \to 6 \to 2 \to 1$. Thus $\sigma$ has only one orbit $O_{1,\sigma}$ and $\sigma = (1, 3, 4, 5, 6, 2)$.

Since $\tau : 1 \to 2 \to 4 \to 3 \to 1, \tau : 5 \to 6 \to 5$, we conclude that $\tau$ has two orbits, $O_{1,\tau}$ and $O_{5,\tau}$ and $\tau = (1, 2, 4, 3)(5, 6)$.

Finally, $\tau^2 : 1 \to 4 \to 1, 2 \to 3 \to 2, 5 \to 5$ and $6 \to 6$. Thus, $\tau^2$ has 4 orbits, $O_{1,\tau^2}$, $O_{2,\tau^2}$, $O_{5,\tau^2}$ and $O_{6,\tau^2}$ and $\tau^2 = (1, 4)(2, 3)$. 


(iii) Compute $|\langle \tau^2 \rangle|$.  

**Solution.** By (ii), $\tau^2 = (1,4)(2,3)$. Since $\tau^2$ is a product of two disjoint cycles of order 2 (2 disjoint transpositions), the order of $\tau^2$, which is equal $|\langle \tau^2 \rangle|$, is 2.

3.

(i) List all possible orders of subgroups of $\mathbb{Z}_{12}$;  

**Solution.** By a theorem of Lagrange, the order of a subgroup of $\mathbb{Z}_{12}$ divides $|\mathbb{Z}_{12}| = 12$. Since the divisors of 12 are 1, 2, 3, 4, 6, 12, these are the possible orders of subgroups of $\mathbb{Z}_{12}$.

(ii) Find all subgroups of $\mathbb{Z}_{12}$;  

**Solution.** Since $\mathbb{Z}_{12}$ is cyclic, all its subgroups are cyclic and for every divisor $d$ of $|\mathbb{Z}_{12}|$ there exists a unique subgroup $H$ of $\mathbb{Z}_{12}$ of order $d$. Indeed, $\langle 12/d \rangle$ is obviously a subgroup of $\mathbb{Z}_{12}$ of order $d$ and if $k \in \{0, 1, \ldots, 11\}$ generates a subgroup of order $d$ then $k$ must be divisible by $12/d$ and so is contained in $\langle 12/d \rangle$.

Thus, the proper subgroups of $\mathbb{Z}_{12}$ are $\{0\}$, $\langle 6 \rangle = \{0, 6\}$, $\langle 4 \rangle = \{0, 4, 8\}$, $\langle 3 \rangle = \{0, 3, 6, 9\}$ and $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$.

(iii) Draw the subgroup diagram for the subgroups of $\mathbb{Z}_{12}$.

**Solution.**

```
\begin{center}
\begin{tikzpicture}
  \node (12) {$\mathbb{Z}_{12}$};
  \node (6) [below left of=12] {$\langle 6 \rangle \cong \mathbb{Z}_2$};
  \node (4) [below right of=12] {$\langle 4 \rangle \cong \mathbb{Z}_3$};
  \node (3) [below left of=4] {$\langle 3 \rangle \cong \mathbb{Z}_4$};
  \node (2) [below right of=4] {$\langle 2 \rangle \cong \mathbb{Z}_6$};
  \node (0) [above of=3] {$\{0\}$};

  \path
    (12) edge (6)
    (12) edge (4)
    (6) edge (3)
    (6) edge (2)
    (4) edge (3)
    (4) edge (2)
    (0) edge (3)
    (0) edge (2);
\end{tikzpicture}
\end{center}
```
4. Let \( A = \{ e, a, b, c \} \) be a set of cardinality 4.

(i) Complete the following table

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td></td>
<td>e</td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

to a multiplication table of a group of order 4 in at least two different ways. Is any of these groups abelian?

**Solution.** The crucial point in this argument is that left and right multiplication maps \( \lambda_x : g \mapsto xg \) and \( \rho_x : g \mapsto gx \) are permutations. In particular, if our table defines a group structure on the set, every element has to appear in every row and every column exactly once.

Since \( a \) appears already in the 1st row of the 2nd column of our table, it cannot appear anywhere else in that column, in particular in the row containing \( b \). Since \( e \) already appears in that row, the only possibility left for \( b \ast a \) is \( c \). Then we will have only one possible choice for \( b \ast c \), namely \( a \). A similar argument shows that \( a \ast b = c \) and \( c \ast b = a \). Thus, we obtain the following table

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td></td>
<td>a</td>
<td></td>
</tr>
</tbody>
</table>

Now we have two possible choices for \( a \ast a \): \( a \ast a = b \) or \( a \ast a = e \).

Suppose first that \( a \ast a = b \). Then using the same argument as before (every line and every column must contain each element of the group exactly once) we obtain

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

Then \( \langle A, \ast \rangle \) is isomorphic to \( \langle \mathbb{Z}_4, +_4 \rangle \). Indeed, define \( \psi : A \to \mathbb{Z}_4 \) as \( \psi(e) = 0 \), \( \psi(a) = 1 \), \( \psi(b) = 2 \) and \( \psi(c) = 3 \). Then it is easy to see that \( \psi(x \ast y) = \psi(x) +_4 \psi(y) \) for all \( x, y \in A \). Since \( \psi \) is obviously bijective, it is an isomorphism of binary structures, which in particular implies that \( \langle A, \ast \rangle \) is a group.
Suppose that \( a \ast a = e \). Then the permutation argument yields the following table

\[
\begin{array}{c|cccc}
  \ast & e & a & b & c \\
  \hline 
  e & e & a & b & c \\
  a & a & e & c & b \\
  b & b & c & e & a \\
  c & c & b & a & e \\
\end{array}
\]

This table has the property that for all \( x \in A \), \( x \ast x = e \). One of the ways of showing that this table is a multiplication table of a group is to observe that the map \( \phi : A \to \mathbb{Z}_2 \times \mathbb{Z}_2 \) defined by \( \phi(e) = (0, 0) \), \( \phi(a) = (1, 0) \), \( \phi(b) = (1, 1) \) and \( \phi(c) = (0, 1) \) is bijective and satisfies \( \phi(x \ast y) = \phi(x) + \phi(y) \). Thus, \( \phi \) is an isomorphism of binary structures and therefore \( \langle A, \ast \rangle \) is a group.

Both tables are symmetric with respect to the main diagonal and so both operations are commutative, that is the corresponding groups are abelian.

(ii) Is there another way of making the above table into a multiplication table of a group? Why?

\textit{Solution.} There is no other way since any other completion would require putting an element twice in the same row or in the same column and thus the result cannot be a multiplication table of a group.

This agrees with the already established fact that there are only 2 non-isomorphic groups of order 4.

5. **Bonus problem.** Let \( G \) be a finite group of order \( 2n \), \( n \in \mathbb{Z}^+ \).

(i) Show that \( G \) contains at least one element of order 2;

\textit{Solution.} Suppose that for all \( g \in G \), \( g \neq e \), \( g^{-1} \neq g \), that is, \( g^2 \neq e \). Fix \( g_1 \in G \), \( g_1 \neq e \). Since \( G \) is a group, \( G \) contains \( g_1 \) and \( g_1^{-1} \notin \{e, g_1\} \). If \( G = \{e, g_1, g_1^{-1}\} \) then we have a contradiction since \( |G| = 2n \) for some \( n \). So, we must have \( g_2 \in G \) which is not in the set \( \{e, g_1, g_1^{-1}\} \). Then \( g_2^{-1} \in G \) and is not in the set \( \{e, g_1, g_1^{-1}, g_2\} \). Continuing this way we conclude that \( G \) has an odd order which is a contradiction. Thus, there exists an element \( g \in G \) such that \( g^{-1} = g \).

(ii) Suppose that \( G \) is abelian and \( n \) is odd. Show that \( G \) contains a unique element of order 2.

\textit{Solution.} Suppose that \( g_1 \neq g_2 \in G \) are of order 2. In particular, \( g_1, g_2 \neq e \). Since \( G \) is abelian, \( (g_1g_2)^2 = g_1^2g_2^2 = e \) while \( g_1g_2 \neq e \) (for otherwise \( g_2 = g_1^{-1} = g_1 \)). Then \( H = \{e, g_1, g_2, g_1g_2\} \) is a subgroup of \( G \). Indeed, we only need to check that it is closed under multiplication, for it obviously contains the inverse of any of its elements and \( e \). Since \( g_1g_2 \in H \), we only need to check that \( g_1(g_1g_2) = g_1^2g_2 = g_2 \in H \) and \( g_2(g_1g_2) = g_1g_2^2 = g_1 \in H \).
Since $H$ is a subgroup of $G$ and $|H| = 4$, the order of $G$ must be divisible by 4 by a theorem of Lagrange. But $G = 2(2k + 1) = 4k + 2 \equiv 2 \pmod{4}$ and so is not divisible by 4, which is a contradiction.

(iii) Give a counterexample to (ii) if $G$ is not abelian

*Solution.* Consider $G = S_3$. It contains 3 distinct transpositions, namely $(1, 2)$, $(2, 3)$ and $(1, 3)$ which are all of order 2. The reason of that is, of course, that $(1, 2)(2, 3) \neq (2, 3)(1, 2)$ which in particular implies that the order of $(1, 2)(2, 3)$ can be different from 2. Indeed, $(1, 2)(2, 3) = (1, 2, 3)$ which is of order 3. One can actually prove that the smallest subgroup of $G$ containing both $(1, 2)$ and $(2, 3)$ is $G$ itself.