1. Through this question, you will classify all groups of order less than or equal to 7 up to isomorphism. This means that for each \( 1 \leq n \leq 7 \), you will find a list of groups of order \( n \) such that any other group of order \( n \) must be isomorphic to some group in this list.

(a) Show that there is a unique group of order 1 up to isomorphism.

*Solution:* Let \( G_1, G_2 \) be two groups of order 1. There must be \( e_1 \in G_1, e_2 \in G_2 \) the unique (and hence identity) elements of the respective groups. Define \( \varphi : G_1 \rightarrow G_2 \) by \( \varphi(e_1) = e_2 \).

This is a well-defined bijection between the underlying sets of the group. Moreover it respects the group operations: for any \( x, y \in G_1 \) \( x = y = xy = e_1 \) hence \( \varphi(xy) = \varphi(e_1) = e_2 = e_2 e_2 = \varphi(x) \varphi(y) \).

Thus \( G_1 \cong G_2 \) and we have shown that any two groups of order 1 are isomorphic.

(b) Show that there is a unique group of any prime order up to isomorphism. Thus, deduce that for \( n = 2, 3, 5, 7 \), there is a unique group of order \( n \) up to isomorphism.

*Solution:* Let \( p \) be a prime number and \( G \) a group of order \( p \). We will show that \( G \cong \mathbb{Z}_p \). To do so, it is sufficient to prove that \( G \) is a cyclic group since any cyclic group of order \( p \) is isomorphic to \( \mathbb{Z}_p \) (Theorem 3.5.2 in Beachy and Blair). Thus, we look for a generator of \( G \). Let \( a \neq e \in G \) (must exist since \( |G| > 1 \)). Then \( o(a) \mid p \) but \( o(a) \neq 1 \). Since \( p \) is prime, we conclude that \( o(a) = p \). Thus, \( |\langle a \rangle| = p \) and since \( \langle a \rangle \subseteq G \), it must be that \( \langle a \rangle = G \). Thus, any group of order \( p \) is cyclic and hence isomorphic to \( \mathbb{Z}_p \).

Since 2, 3, 5, 7 are each prime numbers, the above argument applies in each case and we deduce that (up to isomorphism) there are unique groups of each of these orders.

(c) To classify groups of order 4, show that any group of order 4 is isomorphic either to \( \mathbb{Z}_4 \) or \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

*Solution:* Let \( G \) be a group of order 4. We consider two cases: either \( G \) contains an element of order 4 or it does not. In the first case, \( G \) is cyclic. Therefore, it is isomorphic to \( \mathbb{Z}_4 \) (by Theorem 3.5.2). On the other hand, if \( G \) has no element of order 4 then each non-identity element has order 2. (Why? The order of an element in \( G \) divides the order of the group and hence is either 1, 2, or 4.) We will show that this implies \( G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \).

Let \( a, b, c \in G \) be the nonidentity elements. Define \( \varphi : G \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \) by \( \varphi(e) = ([0], [0]) \quad \varphi(a) = ([0], [1]) \quad \varphi(b) = ([1], [0]) \quad \varphi(c) = ([1], [1]) \).

This is a well-defined bijection so it remains to prove it respects the group operations. For any \( x \in G \),

\[
\varphi(ex) = \varphi(xe) = \varphi(x)\varphi(e)
\]

since \( \varphi(e) \) is the identity in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). Observe that for any \( x, y \in G \) which are distinct nonidentity elements,

\[
xy = yx = z
\]
where \( z \) is the third nonidentity element in the group. Why? If we assume for a contradiction that \( xy = x \), then applying the cancellation law on the left gives \( y = e \) (contradicting the assumption that \( y \) is not the identity). The same argument with the cancellation law on the right shows that \( xy \neq y \). Also, note that for any \( x \in G \), \( x^2 = e \) by assumption on the order. Thus, it suffices to check that

\[
\varphi(a) = \varphi(b)\varphi(c) \quad \varphi(b) = \varphi(a)\varphi(c) \quad \varphi(c) = \varphi(a)\varphi(b)
\]

and

\[
\varphi(a)^2 = ([0], [0]) \quad \varphi(b)^2 = ([0], [0]) \quad \varphi(c)^2 = ([0], [0]).
\]

These are all true by the definition of \( \varphi \) and hence we have shown that \( \varphi \) is a group isomorphism.

(d) To classify groups of order 6, use your work from questions 15 (week 4), 16, and the hint from question 17 in section 3.3 of Beachy and Blair.

**Solution:** We will show that any group of order 6 is either isomorphic to \( \mathbb{Z}_6 \) or \( S_3 \). Let \( G \) be a group of order 6. If \( G \) is cyclic then it is isomorphic to \( \mathbb{Z}_6 \). So, suppose \( G \) is not cyclic. By question 15 in section 3.3 of Beachy and Blair, there is \( b \in G \) with \( o(b) = 2 \). Moreover, since any element in \( G \) has order either 1, 2, 3, or 6 and \( G \) is not cyclic, question 15 also gives that there is \( a \in G \) with \( o(a) = 3 \). By question 16 of the same section, since \( G \) is not cyclic, \( ab \neq ba \). We can write each element in \( G \) in terms of \( e, a, b \) by noticing that we get 6 distinct elements

\[ e, a, a^2, b, ab, a^2b. \]

Why? First, \( e, a, a^2, b \) are distinct because \( ab \neq ba \). By the cancellation law and since \( a, b, e \) are distinct: \( ab \neq a, ab \neq b, ab \neq a^2 \). Moreover, \( ab \neq e \) because \( b = b^{-1} \). Similarly applying the cancellation law, we see that \( a^2b \neq e, a^2, b, ab \).

Since \( G \) is a group, it is closed under multiplication and hence \( ba \in G \). But \( G = \{e, a, a^2, b, ab, a^2b\} \), so it must be the case that \( ba \) is one of these elements. By the cancellation law, \( ba \neq e, a, a^2, b \) and by assumption, \( ba \neq ab \). Therefore, \( ba = a^2b \). Thus, we conclude that the multiplication table of \( G \) is

\[
\begin{array}{cccccccc}
  & e & a & a^2 & b & ab & a^2b \\
 e & e & a & a^2 & b & ab & a^2b \\
a & a & a^2 & e & ab & a^2b & b \\
a^2 & a^2 & e & a & a^2b & b & ab \\
ab & ab & b & a^2b & a & e & a^2 \\
ab^2 & ab^2 & ab & b & a^2 & a & e \\
\end{array}
\]

because \( abab = a(a^2b)b = a^3b^2 = e \) and \( aba = a(a^2)b = b \) and \( aba^2 = a(a^2)b = a^3a^2b = a^2b \), and \( aba^2b = a(a^2b)ab = bab = a^2b^2 = a^2 \), etc.

We define \( \varphi : G \rightarrow S_3 \) as follows

\[
\varphi(e) = (1) \quad \varphi(a) = (1\ 2\ 3) \quad \varphi(b) = (1\ 2)
\]

and \( \varphi(a^2), \varphi(ab), \varphi(a^2b) \) defined so as to respect the group operations:

\[
\varphi(a^2) = (1\ 3\ 2) \quad \varphi(ab) = (1\ 3) \quad \varphi(a^2b) = (2\ 3).
\]

This is clearly a well-defined bijection. Using the multiplication table for \( S_3 \) (Table 3.3.3 on page 116 of Beachy and Blair), we see that \( \varphi \) respects the group operations.
2. Fix some $n \geq 2$. In this problem, you will find all subgroups of the group $\mathbb{Z}_n$. As a consequence, you will prove that every subgroup of $\mathbb{Z}_n$ is cyclic, equal to $\langle [d]_n \rangle$ for some positive divisor $d$ of $n$.

(a) Show that if $d \geq 1$ and $d \mid n$, then $\langle [d]_n \rangle$ has exactly $\frac{n}{d}$ elements. Describe these elements.

*Solution:* By definition, $\langle [d]_n \rangle$ is the set of all (distinct) multiples of $[d]_n$ in $\mathbb{Z}_n$ (because $\mathbb{Z}_n$ is additive). Since $d \mid n$, there is some (positive) number $C = \frac{n}{d}$ such that $n = Cd$. Thus, $$\langle [d]_n \rangle = \{ [d]_n, [2d]_n , [3d]_n, \ldots, [Cd]_n \}$$ because $[Cd]_n = [n]_n = [0]_n$ and hence $[(C + 1)d]_n = [Cd]_n + [d]_n = [d]_n$ is already in the set.

(b) Let $H$ be any subgroup whatsoever of $\mathbb{Z}_n$ (don’t assume $H$ is cyclic). Show that there must be a positive integer $m$ such that $[m]_n \in H$. Thus it makes sense to let $d$ be the smallest positive integer such that $[d]_n \in H$, using the well-ordering principle. Prove that $d \mid n$.

*Solution:* Suppose $H$ is a subgroup of $\mathbb{Z}_n$. Then $[0]_n \in H$ since a subgroup must include the identity. But, for any multiple $\alpha n$ of $n$, $[0]_n = [\alpha n]_n$. Thus, the set of positive representatives of congruence classes in $H$ is nonempty. By the well-ordering principle, let $d$ be the smallest element of this set. That is, $d \in \mathbb{N} \neq 0$ and

$$[d]_n \in H.$$ 

Using the division algorithm, there are $q \in \mathbb{Z}$ and $0 \leq r < d$ such that $n = qd + r$. Then, $$[r]_n = [n - qd]_n = [n]_n - q[d]_n = [0]_n - q[d]_n.$$ 

But, $[0]_n \in H$ and $[d]_n \in H$ so since $H$ is closed under addition and subtraction $[r]_n \in H$. Our assumption that $d$ is the smallest positive representative of a congruence class in $H$ then requires $r = 0$. This means that $n = qd$, hence that $d \mid n$.

(c) Again let $H$ be any subgroup of $\mathbb{Z}_n$ and let $d$ be defined as in part (b). Prove that $H$ is equal to the cyclic subgroup $\langle [d]_n \rangle$ of $\mathbb{Z}_n$.

*Solution:* Let $H$ and $d$ be as specified. Since $[d]_n \in H$, $\langle [d]_n \rangle \subseteq H$. For the reverse set inclusion, we need to show that any $[c]_n \in H$ can be written as a multiple of $[d]_n$ and hence is in $\langle [d]_n \rangle$. Let $[c]_n \in H$. By the division algorithm there is $q \in \mathbb{Z}$ and $0 \leq r < d$ such that $c = qd + r$. Arguing as in part (b), we see that $[r]_n \in H$. But (as before), this implies that $r = 0$. Therefore, $c = qd$ and $[c]_n = q[d]_n$. Thus, $H = \langle [d]_n \rangle$. 