1. True or False. Please briefly justify your response.

T  F  If $H$ is a subgroup of $G$ and $H$ is cyclic, then $G$ is cyclic.
Let $G = \{1, -1, i, -i, j, -j, k, -k\}$ and $H = \{1, -\}$ = $\langle -1 \rangle$.
So $H$ is cyclic, but $G$ is not.

T  F  If $a \neq e$ and $a^7 = e$, then $|a| = 7$.
If $a^7 = e$, then $|a|$ divides 7. Thus $|a| = 1$ or 7. Since $a \neq e$, $|a| \neq 1$. Thus $|a| = 7$.

T  F  If $|G| = |G'|$, then $G$ is isomorphic to $G'$.
Let $G = \mathbb{Z}_4$ and $G'$ = the Klein 4 group. These two groups have the same order, but they are not isomorphic because $\mathbb{Z}_4$ is cyclic and the Klein 4 group is not.

T  F  If $\phi : G \rightarrow G'$ is a homomorphism, then $\ker \phi \neq \emptyset$.
Since $\phi$ is a homomorphism, $\phi(e) = e'$. Thus $e \in \ker \phi$, so $\ker \phi \neq \emptyset$.

2. Let $G = \langle a \rangle$ where $|a| = 15$.

(a) List all elements that generate $G$.

Generators of $G$ are the elements $a^k$ where $(k, 15) = 1$.
Thus the generators are $a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$.

(b) List all subgroups of $G$.
The subgroups are the subgroups generated by $a^k$ where $k$ is a positive divisor of 15. Thus the distinct subgroups are:

$$\langle a \rangle = G$$
$$\langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}\}$$
$$\langle a^5 \rangle = \{e, a^5, a^{10}\}$$
$$\langle a^{15} \rangle = \{e\}$$

(c) List all elements in $G$ of order 5?

$$|a^k| = \frac{15}{(k, 15)}$$
$$5 = \frac{15}{(k, 15)}$$

$(k, 15) = 3$
$k = 3, 6, 9, 12$

Thus $a^3, a^6, a^9$ and $a^{12}$ all have order 5.

(d) Are there any elements of order 2 in $G$? Justify.

If the order of $a^k$ is 2, then we would need $\frac{15}{(k, 15)} = 2$. However, this would imply $(k, 15) = 7.5$ which is a contradiction. Thus $G$ does not contain any elements of order 2.
3. Let \( \phi : G \to G' \) be a homomorphism.

(a) Prove that \( |\phi(a)| \) divides \( |a| \).

Let \( |a| = n \). Then \( a^n = e \). Therefore we have \( (\phi(a))^n = \phi(a^n) = \phi(e) = e' \). Since \( \phi(a)^n = e' \), then \( |\phi(a)| \) divides \( n \).

(b) Prove that if \( \phi \) is an isomorphism, then \( |\phi(a)| = |a| \).

Let \( |a| = n \). Since any isomorphism is a homomorphism, we have shown above that \( \phi(a)^n = e' \). Let \( k \) be a positive integer such that \( \phi(a)^k = e' \). Then \( \phi(e') = e \) and \( \phi(a^k) = \phi(a)^k = e' \). Thus \( \phi(a^k) = \phi(e) \) and since \( \phi \) is one to one this implies \( a^k = e \). Since the order of \( a^k \) is \( n \), then \( a^k = e \) implies \( n \leq k \). Thus we have shown that \( n \) is the smallest positive integer such that \( \phi(a)^n = e' \). Hence \( |\phi(a)| = n \).

4. (a) Prove \( U(\mathbb{Z}_{10}) \) is cyclic.

\[ U(\mathbb{Z}_{10}) = \{ [1], [3], [7], [9] \}. \]

\[ [3]^3 = [27] = [7] \]
\[ [3]^4 = [7][3] = [21] = [1] \]

Thus \( |[3]| = 4 \) and so \( \langle [3] \rangle = \{ [1], [3], [3]^2, [3]^3 \} = \{ [1], [3], [7], [9] \} = U(\mathbb{Z}_{10}) \).

(b) Prove or disprove that \( U(\mathbb{Z}_{10}) \) is isomorphic to the Klein Four group.

\( V = \{ e, a, b, c \} \) where \( a^2 = b^2 = c^2 = e \), so \( |a| = |b| = |c| = 2 \). Since \( V \) has no element of order 4, then \( V \) is not cyclic. However, by part (a), \( U(\mathbb{Z}_{10}) \) is cyclic. Thus \( V \) is not isomorphic to \( U(\mathbb{Z}_{10}) \).

5. Prove that any cyclic group of order \( n \) is isomorphic to \( \mathbb{Z}_n \).

Let \( G = \langle a \rangle \). So \( |a| = n \). Define \( \phi : G \to \mathbb{Z}_n \) by \( \phi(a^k) = [k] \).

Let’s first show \( \phi \) is well-defined. Suppose \( a^k = a^l \). Then \( k \equiv l \pmod{\text{\textit{n}}} \) since \( |a| = n \). Thus \( [k] = [l] \), and hence \( \phi(a^k) = \phi(a^l) \). Thus \( \phi \) is well-defined.

Now let’s show \( \phi \) is a homomorphism. Let \( a^k, a^l \in G \).

\[ \phi(a^ka^l) = \phi(a^{k+l}) = [k+l] = [k] + [l] = \phi(a^k) + \phi(a^l) \]

Thus \( \phi \) is a homomorphism.

Next we’ll show \( \phi \) is one-to-one. Let \( a^k, a^l \in G \) such that \( \phi(a^k) = \phi(a^l) \). Thus \( [k] = [l] \) and hence \( k \equiv l \pmod{\text{\textit{n}}} \). Therefore \( a^k = a^l \), so \( \phi \) is one-to-one.

Finally we’ll show \( \phi \) is onto. Let \( [k] \in \mathbb{Z}_n \). Then \( a^k \in G \) and \( \phi(a^k) = [k] \). Therefore \( \phi \) is onto.

Thus \( \phi \) is an isomorphism and hence \( G \cong \mathbb{Z}_n \).

6. Let \( \phi : G \to G' \) be a homomorphism.

(a) Prove \( \ker \phi = \{ e \} \) if and only if \( \phi \) is one-to-one.

(\( \Rightarrow \)) Assume \( \ker \phi = \{ e \} \). Let \( a, b \in G \) such that \( \phi(a) = \phi(b) \). Therefore we have the following:

\[ \phi(a) = \phi(b) \]
\[ \phi(a)\phi(b)^{-1} = e' \]
\[ \phi(a)\phi(b^{-1}) = e' \]
\[ \phi(ab^{-1}) = e' \]

Thus \( ab^{-1} \in \ker \phi \) and since \( \ker \phi = \{ e \} \) we have that \( ab^{-1} = e \). Multiplying on the right by \( b \) we get \( a = b \). Thus \( \phi \) is one-to-one.
(⇐) Assume \( \phi \) is one-to-one. Since \( \phi \) is a homomorphism, \( \phi(e) = e' \), so \( \{e\} \subseteq \ker \phi \). Let \( a \in \ker \phi \). Then \( \phi(a) = e' = \phi(e) \). Since \( \phi \) is one-to-one, \( a = e \). Thus \( \ker \phi = \{e\} \).

(b) Suppose \( \ker \phi = \{e, g\} \) and \( \phi(a) = b \). Find another element in \( G \) that maps to \( b \).

\[
\phi(ag) = \phi(a)\phi(g) = be' = b
\]

Thus \( ag \in G \) maps to \( b \) and \( ag \neq a \) since \( g \neq e \).