1. Let $H = \{a + bi : a, b \in \mathbb{R}, ab \geq 0\}$. Prove or disprove that $H$ is a subgroup of $\mathbb{C}$ under addition.

Solution. Note that $1, -i \in H$, but $1 + (-i) \notin H$. So, $H$ is not a subgroup.

2. Let $H$ be a non-trivial subgroup of $\mathbb{Z}$. Then $H$ has some nonzero elements $a$ so that $a, -a \in H$, and one of them is positive. As a result, the set of positive numbers in $H$ is non-empty. By the well ordering property of $H$, there is a smallest positive integer $k$ in $H$. We claim that every element $x \in H$ is an integral multiple of $k$. It then follows that $H = k\mathbb{Z} = \langle k \rangle$.

Suppose our claim is not true. Then there is $h = kq + r \in H$ with $0 < r < k$. Note that $k, h \in H$ so that $r = h - qk = h - k - k - \cdots - k \in H$, which contradicts the assumption that $k$ is the smallest positive integer in $H$. Our claim follows.

3. Let $H$ be a non-trivial subgroup of $\mathbb{Z}_n$. Suppose $H$ has elements $\bar{h}_1, \ldots, \bar{h}_m = 0$ with $0 < h_1 < h_2 < \cdots < h_m = n$ so that $h_1$ is the smallest positive integer satisfy $\bar{h}_1 \in H$. We claim that $h_s = \ell_s h_1 = h_1 + \cdots + h_1$ ($h_s$ times) for some positive integer $\ell_s$ for $s = 2, \ldots, m$. It will then follow that $H = \langle \bar{h}_1 \rangle$.

Suppose our claim is not true. Then there is $h_s = \ell_s h_1 + r$ with $0 < r < h_1$. Note that $h_s, h_1 \in H$ so that $\bar{r} = \bar{h}_s - \ell_s \bar{h}_1 = \bar{h}_s - \bar{h}_1 - \cdots - \bar{h}_1 \in H$, which contradicts the assumption that $h_1$ is the smallest positive integer satisfying $h_1 \in H$.

4. Determine the subgroup lattice of $\mathbb{Z}_8$.

Solution. By checking gcd$(8, k)$ for $k = 1, \ldots, 7$, we see that there are four subgroups in $\mathbb{Z}_8$:

$$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle, \quad \langle 2 \rangle = \langle 6 \rangle, \quad \langle 4 \rangle, \quad \langle 0 \rangle.$$ 

The lattice diagram (in horizontal form) is: $\langle 1 \rangle - \langle 2 \rangle - \langle 4 \rangle - \langle 0 \rangle$.

5. Let $a$ and $b$ be elements of a group such that $|a| = 4, |b| = 2$, and $a^3b = ba$. Find $|ab|$.

Solution. We prove that $|ab| = 2$. Note that $(ab)(ab) = a(ba)b = a(a^3b)b = a^4b^2 = e$. So, $|ab| = 1$ or $2$. If $|ab| = 1$, then $a$ is the inverse of $b$ so that $4 = |a| = |b| = 2$, which is absurd. So, $|ab| = 2$.

6. Suppose $G$ is a group with $n$ elements, and $H$ is a subgroup of $G$ with $m$ elements.

(a) Suppose $H \neq G$ and $g_1 \in G - H$. Let $g_1H = \{g_1h : h \in H\}$.

Show that $H \cap g_1H = \emptyset$ so that $|H \cup g_1H| = 2m$. (Here you need to argue $|g_1H| = m$.)

(b) Suppose $H \cup g_1H \neq G$ and $g_2 \notin (H \cup g_1H)$.

Show that $(H \cup g_1H) \cap g_2H = \emptyset$ so that $|H \cup g_1H \cup g_2H| = 3m$.

(c) Show that $G$ is a disjoint union of $H \cup g_1H \cup g_2H \cdots g_kH$ for some $g_1, \ldots, g_k \in G$ so that $n/m$ is a positive integer.

Solution. Let $H = \{h_1, \ldots, h_m\}$ with $h_m = e$.

(a) Let $g_1 \in G - H$, and $g_1H = \{g_1h_1, \ldots, g_1h_m\}$. We claim that $H \cap g_1H = \emptyset$. If it is not true, then there are $i, j$ such that $g_1h_i = h_j$ so that $g = h_jh_i^{-1} \in H$, which is a contradiction.
Note that if \( g_i h_i = g_j h_j \), then \( h_i = h_j \) by the cancellation law. Thus, \( g_1 H \) has \( m \) elements, and \( H \cup g_1 H \) has \( 2m \) elements.

(b) If there is \( g_2 \in G - (H \cup g_1 H) \), let \( g_2 H = \{g_2 h_1, \ldots, g_2 h_m\} \). We claim that \( g_2 H \cap (H \cup g_1 H) = \emptyset \). If not, \( g_2 h_i = h_j \) or \( g_2 h_i = g_1 h_j \) for some \( i, j \). Thus, \( g_2 = h_j h_i^{-1} \) or \( g_2 = g_1 h_j h_i^{-1} \) so that \( g_2 \in H \cup g_1 H \). Now, \( g_2 H \) has \( m \) elements so that \( H \cup g_1 H \cup g_2 H \) has \( 3m \) elements.

(c) We can repeat the arguments in (a) and (b) as follows. If \( H, g_1 H, \ldots, g_r H \) are constructed and their union has \( (r + 1)m \) elements, and if \( g_{r+1} \in G - (H \cup g_1 H \cup \cdots \cup g_r H) \), then \( g_{r+1} H = \{g_{r+1} h_1, \ldots, g_{r+1} h_m\} \) are different from those in \( H \cup g_1 H \cup \cdots \cup g_r H \). If not, then \( g_{r+1} h_i = h_j \) or \( g_{r+1} h_i = g_k h_j \) for some \( \ell \in \{1, \ldots, r\} \). But then \( g_{r+1} = h_j h_i^{-1} \) or \( g_{r+1} = g_k h_j h_i^{-1} \in g_k H \), which contradicts the fact that \( g_{r+1} \in G - (H \cup g_1 H \cup \cdots \cup g_r H) \).

Hence, we can repeat this process, and construct \( H, g_1 H, g_2 H, \ldots, g_k H \) until all the elements in \( G \) are exhausted. It follows that \( n = (k + 1)m \).

7. (a) Suppose a group \( G \) has order \( p \), which is a prime. Then \( p \geq 2 \) and there is \( a \in G \) not equal to \( e \). Then \( H = \langle a \rangle \leq G \), and \( H \) has order larger than one. By Problem 6, \(|H|\) is a factor of \( p \) and not equal to \( 1 \). Thus, \(|H| = p \) and \( G = H = \langle a \rangle \) is cyclic.

(b) Let \( a, b \in G \). Suppose \(|a| = n \) and \(|b| = m \) such that \( \gcd(m, n) = 1 \). Let \( H = \langle a \rangle \cap \langle b \rangle \) has order \( k \). Then \( H \leq \langle a \rangle \) implies that \( k \) is a factor of \( n \), and \( H \leq \langle b \rangle \) implies that \( k \) is a factor of \( m \). Hence, \( k \) is a common divisor of \( n \) and \( m \). Thus, \( k = 1 \) and \( H = \{e\} \).

8. Suppose \(|G| = 24 \) and \( G \) is cyclic. If \( a^8 \neq e \) and \( a^{12} \neq e \), show that \( G = \langle a \rangle \).

Solution. Note that the order of \( a \in G \) must be a factor of \( 24 \) so that \(|a| \in \{1, 2, 4, 6, 8, 12, 24\} \). If \(|a| = 1, 2, 4, 8, \)., then \( a^8 = e \); if \(|a| = 3, 6, 12, \)., then \( a^{12} = e \). Thus, \(|a| = 24 \) and \( G = \langle a \rangle \).

**Extra credits**

9. Suppose \( G \) is a set equipped with an associative binary operation \( * \). Furthermore, assume that \( G \) has an left identity \( e \), i.e., \( eg = g \) for all \( g \in G \), and that every \( g \in G \) has an left inverse \( g' \); i.e., \( g' * g = e \). Show that \( G \) is a group.

Solution. Let \( g \in G \). We first show that the left inverse \( g' \) of \( g \) is also the right inverse, i.e., \( g * g' = e \). Note that \( e = (g'')' * g' = (g')' * (e * g') = (g')' * (g' * g') = e * (g * g') = g * g' \).

To show that the left identity is also the right identity, observe that \( g * g' = g' * g = e \) for any \( g \in G \) by the proof in the preceding paragraph. So, we have \( g * e = g * (g' * g) = (g * g') * g = g \).

10. Let \( A \) be a set, and \( \mathcal{P}(A) \) be its power set. Show that there is a group \( G \) with \(|G| = |\mathcal{P}(A)|\).

Proof. Case 1. If \(|A| \) is finite, then \( \mathbb{Z}_N \) with \( N = 2^n \) is a group with \( 2^n \) elements, where \(|\mathbb{Z}_N| = |\mathcal{P}(A)|\).

Case 2. \( A \) is infinite. Let \( S_A \) be the group of bijections (permutations) on \( A \) under function composition. By the Axiom of Choice, we have \(|A \times A| = |A| \) so that \(|\mathcal{P}(A \times A)| = |\mathcal{P}(A)|\).

Clearly, every bijection on \( A \) corresponds to a subset of \( A \times A \). So, there is an injection from \( S_A \) to \( \mathcal{P}(A \times A) \), i.e., \(|S_A| \leq |\mathcal{P}(A \times A)| = |\mathcal{P}(A)|\).

Now, for every subset \( S \) of \( A \), there is a bijection \( f : A \to A \) such that \( f(x) = x \) for all \( x \in S \) and \( f(x) \neq x \) for all \( x \notin S \). Thus, there is an injection from \( \mathcal{P}(A) \) to \( S_A \), i.e., \(|\mathcal{P}(A)| \leq |S_A|\).

By the Schroder-Bernstein Theorem, \(|\mathcal{P}(A)| = |S_A|\).