Problem 1

(5 points) Let $G$ be a group and $a \in G$.

Prove that $|a^{-1}| = |a|$, i.e. the order of $a^{-1}$ equals the order of $a$.

If $|a| = \infty$ then $|a^{-1}| = \infty$ also.

Now, consider $|a| = n \in \mathbb{N}^*$. Then for $i \in \{1, \ldots, n - 1\}$, $a^i \neq e$ and $(a^{-1})^i = a^{-i} = (a^i)^{-1} \neq e^{-1} = e$.

Hence $|a^{-1}| \geq n$.

On the other hand $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$ implies $|a^{-1}| \leq n$.

Thus $|a^{-1}| = n = |a|$.

Alternatively:

$a^{-1} \in < a >$ implies $< a^{-1} > \leq < a >$. Replacing $a$ by $a^{-1}$ it follows analogously that $< (a^{-1})^{-1} > = < a > \leq < a^{-1} >$. Combining these results we get $< a > = < a^{-1} >$ and $|a| = | < a > | = | < a^{-1} > | = |a^{-1}|$.

(10 points) Let $A$ be an Abelian group.

Assume that $a \in A, b \in A$ satisfy $a \neq b$ and $|a| = 2 = |b|$.

Prove that $A$ must have a subgroup of order 4.

Let $c = ab$ so that $c^2 = (ab)^2 = abab = aabb = ee = e$ and $|c| \in \{1, 2\}$.

If $c = ab = e$ then $b = a^{-1} = a$ which contradicts $a \neq b$. Thus $c \neq e$ and $|c| = 2$.

If $c = ab = a$ then $b = e$ which contradicts $|b| = 2$. Thus $c \neq a$.

Similarly $c \neq b$.

Consider the set $H := \{e, a, b, c\}$ where $|H| = 4$ by the above discussion.

$H$ has a Cayley table as follows

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

showing that $H$ is a subgroup of $A$ of order 4 isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. 
Find an example of a noncyclic group, all of whose proper subgroups are cyclic.

Let \( A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \).

The cyclic subgroups of \( A \) are:
\[
\langle (0, 0) \rangle \quad \text{and} \quad \langle (1, 0) \rangle \quad \text{and} \quad \langle (0, 1) \rangle \quad \text{and} \quad \langle (1, 1) \rangle .
\]

which are all proper since their orders are one or two.

Any proper subgroup must have order one or two.

All such subgroups are listed above.

Alternatively:

Let \( G = D_3 \) so that \( |G| = 6 \). If \( H \) is a proper subgroup then its order satisfies \( |H| \in \{1, 2, 3\} \).

It follows that \( H \) is cyclic, since the trivial group and all groups of prime order are cyclic.

\[ \text{ANSWER: } \mathbb{Z}_2 \oplus \mathbb{Z}_2 \text{ or } D_3 \]

Suppose that \( a \in G \) satisfies \( |a| = 24 \).

Find a generator for the subgroup \( \langle a^{10} \rangle \cap \langle a^{21} \rangle \).

Note that \( \gcd(24, 10) = 2 \) and \( \gcd(24, 21) = 3 \).

Then \( \langle a^{10} \rangle = \langle a^2 \rangle \) and \( \langle a^{21} \rangle = \langle a^3 \rangle \)

so that \( \langle a^{10} \rangle \cap \langle a^{21} \rangle = \langle a^2 \rangle \cap \langle a^3 \rangle = \langle a^{\gcd(10,3)} \rangle = \langle a^6 \rangle \).

Alternatively:

\[
\langle a^{10} \rangle = \langle a^2 \rangle = \{a^0, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22}\}
\]
\[
\langle a^{21} \rangle = \langle a^3 \rangle = \{a^0, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}\}
\]

\[
\langle a^{10} \rangle \cap \langle a^{21} \rangle = \langle a^2 \rangle \cap \langle a^3 \rangle = \{a^0, a^6, a^{12}, a^{18}\}
\]

\[
\langle a^{10} \rangle \cap \langle a^{21} \rangle = \langle a^2 \rangle \cap \langle a^3 \rangle = \langle a^6 \rangle
\]

\[ \text{ANSWER: } a^6 \]
What are the orders realized by the elements of $S_7$?
i.e. determine the set \( \{ k \in \mathbb{N}^* \mid \exists (\alpha \in S_7) \ |\alpha| = k \} \).

Let $\alpha \in S_7$ have a disjoint cycle representation in terms of $k \in \mathbb{N}^*$ cycles with cycle lengths $n_1, \ldots, n_k$ arranged in non-increasing order.

Then $|\alpha| = \text{lcm}(n_1, \ldots, n_k)$.

Since $7 = n_1 + \ldots + n_k$ it follows that $n_i \leq 7$ for all $1 \leq i \leq k$.

Listing of possible orders with possible cycle length decompositions for 7:

\[
\begin{align*}
7 & \text{ is the order for the decomposition } \ 7 = 7 \\
6 & \text{ is the order for the decomposition } \ 7 = 6 + 1 \\
10 & \text{ is the order for the decomposition } \ 7 = 5 + 2 \\
5 & \text{ is the order for the decomposition } \ 7 = 5 + 1 + 1 \\
12 & \text{ is the order for the decomposition } \ 7 = 4 + 3 \\
4 & \text{ is the order for the decomposition } \ 7 = 4 + 2 + 1 \\
4 & \text{ is the order for the decomposition } \ 7 = 4 + 1 + 1 + 1 \\
3 & \text{ is the order for the decomposition } \ 7 = 3 + 3 + 1 \\
6 & \text{ is the order for the decomposition } \ 7 = 3 + 2 + 2 \\
6 & \text{ is the order for the decomposition } \ 7 = 3 + 2 + 1 + 1 \\
3 & \text{ is the order for the decomposition } \ 7 = 3 + 1 + 1 + 1 + 1 \\
2 & \text{ is the order for the decomposition } \ 7 = 2 + 2 + 2 + 1 \\
2 & \text{ is the order for the decomposition } \ 7 = 2 + 2 + 1 + 1 + 1 \\
2 & \text{ is the order for the decomposition } \ 7 = 2 + 1 + 1 + 1 + 1 + 1 \\
1 & \text{ is the order for the decomposition } \ 7 = 1 + 1 + 1 + 1 + 1 + 1 + 1 \\
\end{align*}
\]

**ANSWER:** \( \{1, 2, 3, 4, 5, 6, 7, 10, 12\} \)

Consider an element $\beta \in S_7$ such that $\beta^4 = (2, 1, 4, 3, 5, 6, 7)$.

Find $\beta$.

$\beta^4 = (2, 1, 4, 3, 5, 6, 7)$ is cyclic of order 7.

Since $\langle \beta^4 \rangle$ is a subgroup of $\langle \beta \rangle$ the order of $\beta$ is a positive integral multiple of 7.

Since the prime number 7 divides the order $|\beta|$ the analysis of the preceding problem shows that $\beta$ is cyclic of order 7.

Note that $3 \cdot 7 + (-5) \cdot 4 = 21 - 20 = 1 = \gcd(7, 4)$.

Hence $\beta = \beta^1 = \beta^{3 \cdot 7 + (-5) \cdot 4} = (\beta^7)^3 \cdot (\beta^1)^{-5} = (\beta^7)^{-5} = (\beta^4)^2 = (1, 3, 6, 2, 4, 5, 7)$.

Alternatively:

Let $\alpha = \beta^4 = (2, 1, 4, 3, 5, 6, 7)$ so that $|\alpha| = 7$. Since $\langle \alpha \rangle \leq \langle \beta \rangle$ it follows that $|\alpha| = 7$ divides $|\beta|$. By the first part of this problem this implies $|\beta| = 7$.

Hence $\beta = e \cdot \beta = \beta^7 \cdot \beta = \beta^8 = (\beta^4)^2 = \alpha^2 = (1, 3, 6, 2, 4, 5, 7)$.

**ANSWER:** $\beta = (1, 3, 6, 2, 4, 5, 7)$
Suppose that $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{50}$ is a group isomorphism with $\phi(7) = 13$.

Determine $\phi(x)$ for all $x \in \mathbb{Z}_{50}$.

Since $\text{gcd}(50,7) = 1$ it follows that $7 \in U(50) \approx \text{Aut}(\mathbb{Z}_{50})$.

Since $\phi(7) = 7 \cdot \phi(1) = 13$ and $43 \cdot 7 = 1$ in $\mathbb{Z}_{50}$ it follows that $\phi(1) = 7^{-1} \cdot 13 = 43 \cdot 13 = 9$.

Thus, for $x \in \mathbb{Z}_{50}$, $\phi(x) = x \cdot \phi(1) = x \cdot 9 = 9 \cdot x$.

\textbf{Answer:} $\phi(x) = 9 \cdot x$ calculated in $\mathbb{Z}_{50}$

\textbf{(7 points)} Let $a \in G$ satisfy $|a| < \infty$.

Denote by $\phi_a$ the automorphism of $G$ given by $\phi_a(x) := axa^{-1}$.

\textbf{Prove} that $|\phi_a|$ divides $|a|$.

Note that for $i \in \mathbb{N}$, $\phi_a^i(x) = a^i x a^{-i} = (\phi_a)^i(x)$.

Let $n = |a|$ so that $a^n = e$ and $(\phi_a)^n = \phi_{a^n} = \phi_e = i \text{id}_{\text{Aut}(G)}$.

Hence $|\phi_a|$ divides $n = |a|$. 
Suppose that $G$ is a group of odd order $2n + 1$ for some $n \in \mathbb{N}^*$.

(8 points) Given an arbitrary $a \in G$ show that there exists an $x \in G$ with $x^2 = a$.

For the given $a \in G$, $a^{|G|} = a^{2n+1} = e$.
Pick $x = a^{n+1}$.
Then $x^2 = (a^{n+1})^2 = a^{2n+2} = a^{(2n+1)+1} = a^{2n+1}a = ea = a$.

(7 points) Let $x, y$ be elements in the $G$ from above. If $x^2 = y^2$ show that $x = y$.

Let $a = x^2 = y^2$.
Then
\[
\begin{align*}
a^{n+1} &= (x^2)^{n+1} = x^{2n+2} = x^{(2n+1)+1} = x^{2n+1}x^1 = ex = x \\
a^{n+1} &= (y^2)^{n+1} = y^{2n+2} = y^{(2n+1)+1} = y^{2n+1}y^1 = ey = y
\end{align*}
\]
so that $x = a^{n+1} = y$.

Conclusion:
For every element $a \in G$ there exists a unique square root $x \in G$ with $a = x^2$. 

(5 points) Is $\mathbb{Z}_7 \oplus \mathbb{Z}_{49}$ isomorphic to $\mathbb{Z}_{343}$? Why?

$\mathbb{Z}_7 \oplus \mathbb{Z}_{49}$ is not cyclic since $\gcd(7, 49) = 7 \neq 1$.

**ANSWER:** No such isomorphism exists.

---

(10 points) How many elements of order 4 does $\mathbb{Z}_{400,000} \oplus \mathbb{Z}_{8,000,000}$ have?

A finite cyclic groups contains an element of order 4 precisely when the order of the group is a multiple of 4.

Any finite cyclic group with order divisible by 4 contains precisely one subgroup of order 4, which is cyclic and contains precisely 2 elements of order 4.

It follows that $\mathbb{Z}_{400,000}$ and $\mathbb{Z}_{8,000,000}$ each have unique subgroups of order 4.

Similarly, $\mathbb{Z}_{400,000}$ and $\mathbb{Z}_{8,000,000}$ each have unique subgroups of order 2.

An element $(a, b) \in \mathbb{Z}_{400,000} \oplus \mathbb{Z}_{8,000,000}$ has order $|(a, b)| = \text{lcm}(|a|, |b|) = 4$ precisely if $|a|$ and $|b|$ divide 4 and $\max(|a|, |b|) = 4$.

This leaves the following possibilities for the numbers and component orders:

- $2 \times 2 = 4$ if $(|a|, |b|) = (4, 4)$
- $2 \times 1 = 2$ if $(|a|, |b|) = (4, 2)$
- $1 \times 2 = 2$ if $(|a|, |b|) = (2, 4)$
- $2 \times 1 = 2$ if $(|a|, |b|) = (4, 1)$
- $1 \times 2 = 2$ if $(|a|, |b|) = (1, 4)$

Given $m, n$ in $\mathbb{N}^{\ast}$ there are exactly $4 + 2 + 2 + 2 + 2 = 12$ elements of order 4 in any group isomorphic to $\mathbb{Z}_{4n} \oplus \mathbb{Z}_{4n}$.

**ANSWER:** 12