Problem One

1. **Proposition.** The additive group \((\mathbb{R}, +)\) is isomorphic to the multiplicative group \((\mathbb{R}^+, \cdot)\).

   **pf.** Let \(\varphi : \mathbb{R} \to \mathbb{R}^+\) be defined by \(\varphi(x) = e^x\), \(\forall x \in \mathbb{R}\). Then clearly \(\varphi\) is a group homomorphism \((\varphi(xy) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y), \forall x, y \in \mathbb{R}\) and maps \(\mathbb{R}\) bijectively onto \(\mathbb{R}^+\). \(\blacksquare\)

Problem Two

2. **Proposition.** Let \((G, \cdot)\) be a group and \((G^{op}, \ast)\) be the opposite group (meaning \(G^{op} = G\) and \(a \ast b = b \cdot a, \forall a, b \in G^{op}\)). Then \((G, \cdot)\) and \((G^{op}, \ast)\) are isomorphic as groups.

   **pf.** Let \(\varphi : G \to G^{op}\) be defined by \(\varphi(g) = g^{-1}, \forall g \in G\). Then clearly \(\varphi\) maps \(G\) bijectively onto \(G^{op}\).

   Now, suppose that \(g, h \in G\). Then
   \[
   \varphi(a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = a^{-1} \ast b^{-1} = \varphi(a) \ast \varphi(b)
   \]

   so that \(\varphi\) is also a group homomorphism. \(\blacksquare\)

**Remark.** Note that the only non-trivial group axiom that needs to be checked for \((G^{op}, \ast)\) is associativity. Let \(xy, z \in G^{op}\). Then
\[
(a \ast b) \ast c = c \cdot (a \ast b) = c \cdot (b \cdot a) = (c \cdot b) \cdot a = a \ast (c \cdot b) = a \ast (b \ast c)
\]

as desired.
Problem Three

3. Proposition. (a) The automorphism group \( \text{Aut}(C_{12}) \) of the cyclic group \( C_{12} \) of order 12 is isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

(b) The automorphism group \( \text{Aut}(D_8) \) of the dihedral group \( D_8 \) of order 8 is isomorphic to \( D_8 \).

Proof. (a) Denote \( C_{12} = \langle x \mid x^{12} = 1 \rangle \), and define for each \( a \in C_{12} \) the map \( \varphi_a : C_{12} \to C_{12} \) by \( \varphi_a(x) = x^a \). Since \( C_{12} \) is a cyclic group, it is clear that every endomorphism of \( C_{12} \) must have the form \( \varphi_a \) for some \( a \in C_{12} \). Moreover, \( \langle \varphi_a(x) \rangle = \langle x^a \rangle = C_{12} \) only when \( a \in \{1, 5, 7, 11, 3 \} \) since \( x^{12} = 1 \). Thus, defining the product \( \varphi_a \varphi_b = \varphi_{ab} \) on \( \text{Aut}(C_{12}) \), we have that \( \text{Aut}(C_{12}) \) is the group of units in \( C_{12} \), i.e., \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

(b) Denote \( D_8 = \langle x, y \mid x^2 = y^4 = (xy)^2 = 1 \rangle = \langle 1, y, y^2, y^3, x, xy, xy^2, xy^3 \rangle \), and notice that using the relation \( xy = y^{-1}x \) repeatedly,

\[
(xy^2)^2 = xy^2xy^2 = xy^2y^{-1}xy = xyxy = (xy)^2
\]

and \( (xy^3)^2 = xy^3xy^3 = xy^3y^{-1}xy^2 = xy^2y^{-1}xy = (xy)^2 \) similarly.

Thus, \( D_8 \) has 4 noncentral elements of order 2 (namely, \( x, xy, xy^2, \) and \( xy^3 \)) and 2 noncentral elements of order 4 (namely \( y \) and \( y^3 \)), each pair of which satisfies the above relations on \( D_8 \). As such, we can construct exactly 8 automorphisms on \( D_8 \) by mapping \( (x, y) \) to each such pair of elements, and it can then easily be checked that \( \text{Aut}(D_8) \cong D_8 \).
4. Proposition. Let $k \in \mathbb{Z}_{\geq 2}$ and $G$ be a group having a unique element $x \in G$ of order $k$. Then $k = 2$ and $x \in \mathbb{Z}(G)$.

e \iff \text{First note that since } x \text{ and } x^{-1} \text{ must have the same order, } x = x^{-1} \text{ by the uniqueness of the order of } x. \text{ Thus, } x^2 = 1 \text{ so that } k = 2.

For the second part, let $y \in G$. Then notice that

$$(yx^{-1})^2 = yxy^{-1}yxy^{-1} = yx^2y^{-1} = yy^{-1} = 1$$

so that $yx^{-1} = x$ by the uniqueness of the order of $x$. Upon rearranging this, $yx = xy$ so that $x \in \mathbb{Z}(G)$. ■

5. Proposition. Let $G$ be a group with subgroup $H$ and normal subgroup $N$. Define $HN = \{hn \mid h \in H, n \in N\}$.

Then $HN$ is also a subgroup of $G$.

e \iff \text{Clearly } 1 \in HN \text{ so that } HN \neq \emptyset. \text{ Thus, we need only check that } \forall x, y \in HN, xy^{-1} \in HN. \text{ Let } x, y \in HN. \text{ Then } \exists g, h \in H \text{ and } m, n \in N \text{ s.t. } x = hn \text{ and } y = gm. \text{ Denote } a = nm^{-1} \text{ and } b = hg^{-1} \text{ so that } a \in N \text{ and both } b, b^{-1} \in HN, \text{ and notice that } xy = (hn)(gm)^{-1} = hnm^{-1}g^{-1} = hag^{-1}. \text{ Moreover, since } hag^{-1} \cdot b^{-1} = hag^{-1} \cdot g^{-1} = hah^{-1} \in N \subseteq HN \text{ as } N \trianglelefteq G, \text{ it follows that } (hn)(gm)^{-1} = hag^{-1} = hag^{-1}b^{-1} \cdot b \in HN\text{ pg 3/5 as well. ■}
Proposition. Let $G$ be a group for which $G/Z(G)$ is cyclic. Then $G$ is abelian.

pf. Denote $N = Z(G)$. Then since $G/N$ is cyclic, $\exists x \in G$ s.t. $G/N = \langle xN \rangle$, and so $G = \langle x, N \rangle$. Now let $g, h \in G$ so that $g = x^n$ and $h = x^m$ for some $a, b \in \mathbb{Z}_{\geq 0}$ and $n, m \in \mathbb{N}$, and notice that

$$gh = x^n \cdot x^m = x^n x^m = x^{n + m} = x^m x^n = hg,$$

from which $G$ is abelian. $\blacksquare$

Problem Seven

Proposition. Let $G$ be a group, $H$ be a subgroup of $G$, and $K = \bigcap_{a \in G} aHa^{-1}$. Then $[H:K] | ([G:H] - 1)!$.

pf. Denote by $G/H$ the set of left cosets of $H$ in $G$, and let $G \circ G/H$ by left multiplication. Then the kernel $\text{Ker}$ of this action is

$$\text{Ker} = \{ g \in G \mid g \cdot aH = aH, \forall a \in G \} = \{ g \in G \mid (a^{-1}ga)H = H, \forall a \in G \} = \{ g \in G \mid a^{-1}ga \in H, \forall a \in G \} = \{ g \in G \mid g \in aHa^{-1}, \forall a \in G \} = K.$$

Thus, by the First Isomorphism Thm (AKA Fun. Hom. Thm) and Lagrange's Thm,

8 Proposition. Let \( p \) be a prime number.

   (a) Let \( G \) be a group of order \( p^n \) for some \( n \in \mathbb{Z}_+ \).
   Then the center \( Z(G) \) of \( G \) is nontrivial.

   (b) Let \( G \) be a group of order \( p^2 \). Then \( G \) is abelian.

Proof. (a) Let \( g_1, g_2, \ldots, g_k \) be representatives of the distinct noncentral conjugacy classes of \( G \). Note that since \( g_1, \ldots, g_k \) are noncentral elements of \( G \), each centralizer \( C(g_i) = \{ h \in G | h g_i h^{-1} = g_i \} \) must satisfy \( \{1\} \not\subset C(g_i) \not\subset G \). Thus, by Lagrange's Thm., \( p \mid [G : C(g_i)] \) for \( i = 1, \ldots, k \), and so \( p \mid Z(G) \) by the class eq'n:

\[
|G| = |Z(G)| + \sum_{i=1}^{k} [G : C(g_i)].
\]

(b) Note that by Part (a), \( |Z(G)| \in \{p, p^2\} \). If \( |Z(G)| = p \), there is nothing to prove since \( G = Z(G) \) is abelian, so assume that \( |Z(G)| = p \). Then by Lagrange's Thm., \( |G/Z(G)| = p \) so that \( G/Z(G) \) is a cyclic group. Thus, by Problem 6 above, \( G \) is abelian—a contradiction to the assumption that \( Z(G) \not\subset G \). So \( G = Z(G) \).

Problem Nine

9 Proposition. Let \( p \not| q \) be prime numbers and \( G \) be a group of order \( pq \). Then \( G \) is not simple.

Proof. Let \( P \) be a \( p \)-Sylow subgroup of \( G \). By Sylow's 3rd Thm., it's the only \( p \)-Sylow subgroup and so must be self-conjugate. Thus, \( P \) is a normal subgroup of \( G \).