1. (5 points) Define “centralizer”. Use complete sentences.

The centralizer of the element \( a \) in the group \( G \) is the set of all elements in \( G \) which commute with \( a \).

2. (5 points) Define “normal subgroup”. Use complete sentences.

The subgroup \( N \) of the group \( G \) is a normal subgroup if \( gng^{-1} \in N \) for all \( n \in N \) and all \( g \in G \).

3. (6 points) (Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let \( a \) and \( b \) be elements of finite order in the group \( G \). Does \( ab \) have to have finite order?

NO. Let \( G \) be the group of rigid motions of the \( xy \) plane, \( \sigma \) be reflection across the \( x \)-axis, and \( \rho \) be rotation by \( \theta = \frac{2\pi}{\sqrt{2}} \) radians. Let \( a = \sigma \) and \( b = \sigma \rho \). It is clear that \( a \) has order 2. It is not hard to see that \( b \) is reflection across the line through the origin which makes the angle \( \frac{-\theta}{2} \) with the positive \( x \)-axis; thus, \( b \) also has order 2. On the other hand, \( ab = \rho \), which has infinite order; because, if \( \rho^m \) were equal to the identity for some positive integer \( m \), then \( m\theta = \frac{2m\pi}{\sqrt{2}} \) would equal an integer multiple of \( 2\pi \) and \( \sqrt{2} \) would be a rational number.

4. (6 points) Recall that each element of \( \mathbb{C} \) is a point on the complex plane. Notice that \( (\mathbb{R}^{\text{pos}}, \times) \) is a subgroup of \( (\mathbb{C} \setminus \{0\}, \times) \). Give a geometric description of the left cosets of \( (\mathbb{R}^{\text{pos}}, \times) \) in \( (\mathbb{C} \setminus \{0\}, \times) \).

The left cosets of \( (\mathbb{R}^{\text{pos}}, \times) \) in \( (\mathbb{C} \setminus \{0\}, \times) \) are the open rays emanating from the origin. Indeed, the left coset determined by \( e^{i\theta} \) is the ray which forms the angle \( \theta \) with the positive \( x \)-axis.

5. (6 points) (Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let \( a \) be a fixed element of the group \( G \). Consider the function \( \rho_a : G \to G \), which is given by \( \rho_a(g) = ga \), for all \( g \) in \( G \). Is \( \rho_a \) onto?

YES. Take an arbitrary element \( g \) in \( G \). We see that \( ga^{-1} \in G \) with \( \rho_a(ga^{-1}) = g \).
6. (6 points) (Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let $a$ be a fixed element of the group $G$. Consider the function $\rho_a : G \rightarrow G$, which is given by $\rho_a(g) = ga$, for all $g$ in $G$. Is $\rho_a$ a homomorphism?

NO! Let $G$ be $(\mathbb{R}^{\text{pos}}, \times)$ and $a = 2$. We see that $\rho_2(1 \cdot 1) = \rho_2(1) = 2$. On the other hand, $\rho_2(1) \cdot \rho_2(1) = 2 \cdot 2 = 4 \neq 2$.

7. (6 points) (Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Is $\varphi : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_5$, which is given by $\varphi([n]_{10}) = [n]_5$, a function?

YES! If $[n]_{10} = [m]_{10}$, then 10 divides into $n - m$ evenly, so 5 also divides into $n - m$ evenly and $[n]_5 = [m]_5$.

8. (6 points) (Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Is $\varphi : \mathbb{Z}_5 \rightarrow \mathbb{Z}_{10}$, which is given by $\varphi([n]_5) = [n]_{10}$, a function?

NO! Observe that $[0]_5 = [5]_5$, but $[0]_{10} \neq [5]_{10}$.

9. (6 points) Let $N$ be a normal subgroup of the group $G$, and let $G/N$ be the set of left cosets of $N$ in $G$. Prove that $\varphi : G/N \rightarrow G/N$, which is given by

$$\varphi(aN, bN) = abN,$$

is a function.

If $aN = a'N$ and $bN = b'N$, then $a = a'n_1$ and $b = b'n_2$ for some $n_1$ and $n_2$ in $N$. We see that

$$ab = a'n_1b'n_2 = a'b'[(b')^{-1}n_1b']n_2 \in a'b'N,$$

since $(b')^{-1}n_1b'$ is an element of the normal subgroup $N$. It follows that $abN = a'b'N$.

10. (6 points) (Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be a one-to-one and onto function. Suppose $B \subseteq \mathbb{Z}$ with $f(B) \subseteq B$. Is $f(B) = B$?

Let $B$ be the set of positive integers. Notice that the function $f : \mathbb{Z} \rightarrow \mathbb{Z}$, which is given by $f(n) = n + 1$, is a one-to-one and onto function which carries each element of $B$ to another element of $B$. However, $f(B)$ is a proper subset of $B$, because $1 \in B$ and $f(b) \neq 1$ for any $b \in B$.

11. (6 points) What is the order of $( [2]_{6}, [2]_{4} ) + <([3]_{6}, [2]_{4}) >$ in $\mathbb{Z}_6 \times \mathbb{Z}_4$? Explain.

Let $x$ be the element $( [2]_{6}, [2]_{4} ) + <([3]_{6}, [2]_{4}) >$ of the group $G = \mathbb{Z}_6 \times \mathbb{Z}_4$. We show that $x$ has order 6 in $G$. We make our calculation in $\mathbb{Z}_6 \times \mathbb{Z}_4$. Let $N$ be the subgroup

$$<([3]_{6}, [2]_{4}) > = \{([3]_{6}, [2]_{4}), ([0]_{6}, [0]_{4})\}$$
of $\mathbb{Z}_6 \times \mathbb{Z}_4$ and let $a$ be the element $([2]_6, [2]_4)$ of $\mathbb{Z}_6 \times \mathbb{Z}_4$. We show that the least positive integer $n$, with $a + \cdots + a = n$ in $N$ is 6. Notice that none of the elements
\[ a = ([2]_6, [2]_4), \quad a + a = ([4]_6, [0]_4), \]
\[ a + a + a = ([0]_6, [2]_4), \quad a + a + a + a = ([2]_6, [0]_4), \quad a + a + a + a + a = ([4]_6, [2]_4) \]
is in $N$; but
\[ a + a + a + a + a = ([0]_6, [0]_4) \]
and this is in $N$.

12. (6 points) Let $H$ be a non-zero subgroup of $\mathbb{Z}$. Prove that $H$ is cyclic.

The subgroup $H$ contains some element in addition to zero. Either this element or its inverse is positive. Let $h_0$ be the least positive element of $H$. We will show that $H = h_0\mathbb{Z}$. It is clear that $h_0\mathbb{Z} \subset H$. We complete the proof by showing that $H \subset h_0\mathbb{Z}$. Let $h$ be an arbitrary element of $H$. Divide $h_0$ into $h$ in order to obtain integers $n$ and $r$ with $h = nh_0 + r$ with $0 \leq r < h_0$. We see that $r = h - nh_0$ is in $H$. The choice of $h_0$ (as the least positive element of $H$) forces $r$ to be zero. Thus, $h \in h_0\mathbb{Z}$ and the proof is complete.

13. (6 points) Let $d$ be the greatest common divisor of the integers $n$ and $m$. Prove that there exist integers $r$ and $s$ with $rn + sm = d$.

Let $H = \{rn + sm \mid r, s \in \mathbb{Z}\}$. It is clear that $H$ is a subgroup of $\mathbb{Z}$; hence, by the previous problem, $H$ is cyclic and generated by some positive integer $h_0$. We will show that $h_0 = d$. Well, $n$ and $m$ are in $H$; so, $h_0$ is a common divisor of $n$ and $m$. But, $d$ is the greatest common divisor of $n$ and $m$; hence, $h_0 \leq d$. On the other hand, $h_0 \in H$; so, $h_0 = rn + sm$ for some integers $r$ and $s$. We know that $d$ divides $n$ and $m$; so, $d$ divides $h_0$. It follows that $d \leq h_0$. Therefore, $d$ must equal $h_0$.

14. (6 points) List 6 subgroups of the Dihedral group $D_4$. No explanation is needed.

Some of the subgroups of $D_4$ are:
\[ D_4, \quad \{\text{id}\}, \quad \{\text{id}, \sigma, \sigma \rho^2, \rho^2\}, \quad \{\rho^2, \text{id}\}, \quad \{\sigma, \text{id}\}, \quad \{\sigma \rho, \text{id}\}, \quad \{\sigma \rho^2, \text{id}\}. \]

15. (6 points) Prove that $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{\text{pos}}, \times)$.

Define $\varphi : (\mathbb{R}, +) \to (\mathbb{R}_{\text{pos}}, \times)$ by $\varphi(r) = e^r$. We see that $\varphi$ is a homomorphism because, if $r, s \in \mathbb{R}$, then
\[ \varphi(r + s) = e^{r+s} = e^r e^s = \varphi(r)\varphi(s). \]

We see that $\varphi$ is onto. Let $t$ be a positive real number. It follows that $\ln t$ is a real number with $\varphi(\ln t) = e^{\ln t} = t$. We see that $\varphi$ is one-to-one. If $r$ and $s$ are real numbers with $\varphi(r) = \varphi(s)$, then $e^r = e^s$. Apply $\ln$ to both sides to see that $r = s$. 
16. (6 points) Consider \((\mathbb{Z}, *)\), where \(n * m = n + m + 1\) for all integers \(n\) and \(m\). Is \((\mathbb{Z}, *)\) a group? Explain.

YES.

**Closure:** If \(n\) and \(m\) are in \(\mathbb{Z}\), then \(n * m = n + m + 1\) is also in \(\mathbb{Z}\).

**Identity:** We see that \(-1\) is the identity element because \((-1) * a = -1 + a + 1 = a\) for all \(a\) in \(\mathbb{Z}\).

**Inverses:** If \(a\) is in \(\mathbb{Z}\), then the inverse of \(a\) is \(-a - 2\) because \(a * (-a - 2) = a + (-a - 2) + 1 = -1\), which is the identity element.

**Associativity:** If \(a\), \(b\), and \(c\) are in \(\mathbb{Z}\), then

\[
a * (b * c) = a * (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2
\]

and

\[
(a * b) * c = (a * b) * c = (a + b + 1) * c = (a + b + 1) + c + 1 = a + b + c + 2.
\]

These values are equal; therefore, associativity holds.

17. (6 points) \(S\) be a set and let \(B\) be a subset of \(S\). Define

\[H = \{\sigma \in \text{Sym}(S) \mid \sigma(b) \in B \text{ for all } b \in B\}.\]

Suppose \(S = \{1, 2, 3, 4, 5, 6\}\) and \(B = \{1, 3, 5\}\). How many elements does \(H\) have? Explain.

If \(\sigma\) is in \(H\), then \(\sigma = \sigma' \sigma''\), where \(\sigma'\) is a permutation of \(\{2, 4, 6\}\) and \(\sigma''\) is a permutation of \(\{1, 2, 3\}\). There are 6 choices for \(\sigma'\) and there are 6 choices for \(\sigma''\). Thus, the group \(H\) has 36 elements.