1. **[10 pts - 5 each]** State formal definitions of the following.
   (a) equal functions
   (b) permutation

2. **[12 pts - 3 each]** Consider $a = (1562)(137)(25347) \in S_7$.
   (a) Write $a$ as a product of disjoint cycles.
   (b) Write $a^{-1}$ as a product of disjoint cycles.
   (c) Write $a^{-1}$ as a product of transpositions.
   (d) Does either of $a$ or $a^{-1}$ belong to $A_7$?

3. **[10 pts]** Prove that $S_n$ is not abelian if $n \geq 3$.

4. **[8 pts - 4 each]** Consider $D_{12}$; label the vertices of the associated polygon clockwise.
   (a) Write cycle notation for the rotation that sends 1 to 4.
   (b) Write cycle notation for the reflection that doesn't move 1.

5. **[12 pts]** Formally state the Division Algorithm, then apply it to the numbers $-100$ and $17$. (Showing work is optional.)

6. **[8 pts]** Express $gcd(-30, 56)$ as a linear combination. (Showing work is optional.)

7. **[10 pts - 5 each]** State any two definitions of $a \equiv b \mod n$. (You can state the hypothesis just once.)

8. **[10 pts]** Prove that $\odot$ is well-defined on $\mathbb{Z}_n$.

9. **[12 pts - 3 each]** Find the following in $\mathbb{Z}_7$. Write names of classes in “lowest terms.”
   (a) $[6] \oplus ([3] \odot [4])$
   (b) the additive inverse of $[2]$
   (c) the multiplicative inverse of $[2]$
   (d) three elements of $[2]$

10. **[8 pts - 2 each]** You do NOT need to justify below; just answer.
    (a) Name a familiar, proper subset of $\mathbb{R} \setminus \{0\}$ that is a subgroup as well.
    (b) Name a familiar, proper subset of $\mathbb{C}$ that is a subgroup as well.
    (c) Is $D_5 < S_5$?
    (d) Is $Z_5 < Z$?
Solutions

1. a. Two functions $\alpha, \beta$ are equal if they have the same domain, same codomain, and
   \[ \alpha(x) = \beta(x) \text{ for all } x \text{ in the domain.} \]

   OR let $\alpha, \beta$ be functions from $X$ to $Y$. Then
   \[ \alpha = \beta \text{ if } \alpha(x) = \beta(x) \text{ for all } x \in X. \]

   S not addressed

2. a. $a = (1\ 5\ 6\ 2)(1\ 3\ 7)(2\ 5\ 3\ 4\ 7)$
   \[ = (1\ 3\ 4\ 5\ 7)(2\ 6) \]

   b. $a^{-1} = (1\ 7\ 5\ 4\ 3)(2\ 6)$
   (in standard order)

   c. $a^{-1} = (1\ 7)(7\ 5)(5\ 4)(4\ 3)(2\ 6)$
   \[ \text{or } (1\ 3)(1\ 4)(1\ 5)(1\ 7)(2\ 6) \]

   Yes to both

   d. Neither $a$ nor $a^{-1}$ belongs to $A_7$. 

   Yes to one
3. Proof - Because \( n = 3 \), \((1 2)\) and \((1 3)\) belong to \( S_3 \).
\[
\begin{align*}
(1 2)(1 3) &= (1 3 2) \\
\text{but } (1 3)(1 2) &= (1 2 3), \text{ unequal.}
\end{align*}
\]

4. 
\[
\begin{array}{c}
9 \\
8 \\
7 \\
6 \\
5 \\
4 \\
3 \\
2 \\
1
\end{array}
\]

a. \((1 4 7 10)(2 5 8 11)(3 6 9 12)\)
b. \((2 1 2)(3 1 1)(4 1 0)(5 9)(6 8)\)

5. Div. Alg. - Let \( a, b \in \mathbb{Z} \) with \( b > 0 \). There exist unique integers \( q \) and \( r \) with
\[
a = bq + r \quad \text{and} \quad 0 \leq r < b.
\]
When \( a = -100 \) and \( b = 17 \),
\[
-100 = 17 \cdot (-6) + 2
\]
8. \[ \gcd(-30, 560) = 2 \]

\[ 2 = 7 \cdot 560 + 13 \cdot (-30) \]

7. Let \( a, b \in \mathbb{Z} \) and \( n \in \mathbb{Z}^+ \) with \( n \geq 2 \).

\#1 \( \equiv b \mod n \) \iff \( n \mid a-b \)

\#2 \( a \equiv b \mod n \) if \( a = b + kn \) for some \( k \in \mathbb{Z} \).

\#3 \( a \equiv b \mod n \) if \( a \) and \( b \) have the same remainder on division by \( n \).

8. Proof - Let \([a], [b] \in \mathbb{Z}_n\).

Let \( a' \in [a], \ b' \in [b] \).

Then \( a' \equiv a \) and \( b' \equiv b \mod n \), so

\[ a' = a + kn \] and \( b' = b + ln \)

for some \( k, l \in \mathbb{Z} \).

\[ a'b' = (a+kn)(b+ln) \]

\[ = ab + n(bk + al + kln) \]

where \( bk + al + kln \in \mathbb{Z} \).

Thus \( a'b' \equiv ab \mod n \), so \( a'b' \in [ab] \)

and \([a'b'] = [ab] = [a][b] \).
   b. The additive inverse of \([2]\) is \([5]\).
   c. The multiplicative inverse of \([2]\) is \([4]\).
   d. \([2]\) contains \(2, 9, 16, 23, \ldots, -5, -12, \ldots\).

10. a. Various: \(\mathbb{R}^+\) \(\cup \{0, -\infty\}\)
    
    b. Various: \(\mathbb{R}\)
    
    c. Yes - \(\mathbb{D}_5\) is a subset that is a group under \(\mathbb{S}_5\)'s operation.
    
    d. No - \(\mathbb{Z}_5\) is not a subset of \(\mathbb{Z}\) (\(\mathbb{Z}_5\)'s elements are sets) nor does it use \(\mathbb{Z}\)'s operation (\(\oplus\) is not the same as \(+\)).