There are 10 problems on 2 pages of this homework assignment.

Recall that \( i_S \) is the identity function on a nonempty set \( S \).

1. Let \( f : X \to Y \), \( g : Y \to Z \) and \( h : Z \to W \) be functions on nonempty sets \( X \), \( Y \), \( Z \), and \( W \).
   
   (a) Prove that \( h \circ (g \circ f) = h \circ (g \circ f) \).
   
   (b) Prove that \( i_Y \circ f = f \) and \( f \circ i_X = f \).
   
   (c) Prove that if \( f \) and \( g \) are bijective, then so is \( g \circ f \) directly from the definitions.

2. The set of all one-to-one mappings from a nonempty set \( S \) onto itself is denoted \( A(S) \).
   
   (a) Prove that \( A(S) \) is a group under the operation of function composition.
   
   \( \text{For simplicity, write } g \circ f \text{ as } gf \text{ for } f, g \in A(S). \)
   
   (b) Prove that if \( |S| \geq 3 \), then there exists \( f, g \in A(S) \) such that \( fg \neq gf \).

3. Let \( S \) be a nonempty set and \( f : S \to S \) a function.
   
   (a) Prove that if \( S \) is finite and \( f \) is onto, then \( f \) is one-to-one.
   
   (b) Prove that if \( S \) is finite and \( f \) is one-to-one, then \( f \) is onto.
   
   (c) Prove that the first statement is not true if \( S \) is infinite.
   
   (d) Prove that the second statement is not true if \( S \) is infinite.

4. Let \( S \) be a nonempty set and \( f : S \to S \) a bijection. We define \( f^0 = i_S \), \( f^1 = f \), and \( f^n = f \circ f^{n-1} \) for \( n \in \mathbb{N} \) with \( n \geq 2 \). We also define \( f^{-n} = (f^{-1})^n \) for \( n \in \mathbb{N} \). It follows that \( f^n f^m = f^{n+m} \) and \( (f^n)^m = f^{nm} \) for \( n, m \in \mathbb{N} \).
   
   (a) Suppose \( S \) is finite. Prove that there exists an integer \( m > 0 \) such that \( f^m = i_S \).
   
   \( \text{Hint: try contradiction, not construction.} \)
   
   (b) When \( |S| = n < \infty \), then \( A(S) \) is called the symmetric group of degree \( n \), often denoted \( S_n \). The elements of \( S_n \) are called permutations of \( S \). How many elements does \( S_n \) have?
   
   Justify your answer.
   
   (c) Find an \( m \) (in terms of \( n \)) such that \( g^m = i_S \) for all \( g \in S_n \). Justify your answer.

5. Let \( \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\} \). Prove, from the definitions, that \( \mathbb{Z}_n^* \) is a group under multiplication if and only if \( n \geq 2 \) is a prime.

6. Let \( G \) be a finite group with identity \( e \in G \).
   
   (a) Prove that for all \( a \in G \) there exists \( n \in \mathbb{N} \) with \( n > 0 \) such that \( a^n = e \).
   
   (b) Prove that there exists \( m \in \mathbb{N} \) with \( m > 0 \) such that \( a^m = e \) for all \( a \in G \).
7. Let $G$ be a group with identity $e$.

(a) For each $G$ below, how many different product tables can $G$ have? Justify your answer.

i. Let $G = \{ e, a, b \}$.

ii. Let $G = \{ e, a, b, c \}$.

iii. Let $G = \{ e, a, b, c, d \}$.

(b) Give a direct proof that a group of order 5 or less is abelian.

8. Prove by contradiction that a group of order 5 or less is abelian.

9. Let $G$ be a group.

(a) Prove that $G$ is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.

(b) Prove that $G$ is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

(c) Suppose that $a = a^{-1}$ for every $a \in G$. Prove that $G$ is abelian.

10. If $G$ is a finite group of even order, show that there must be an element $a \neq e$ such that $a = a^{-1}$. *Hint: What does $(a^{-1})^{-1}$ equal?*