1. Let \( f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \) be given by \( f(m, n) = m - n \). Discuss whether \( f \) is injective, surjective, bijective.

Solution: Since \( f(m, n) = f(m', n') \) as long as \( m - n = m' - n' \), in particular, \( f(0, 0) = f(1, 1) \), we see the function is not injective.

\( f \) is surjective since \( \forall r \in \mathbb{R}, r = f(r, 0) \).

\( f \) is not bijective since it is not injective.

2. \( S \) is a finite set with cardinality greater than 1. Construct a bijective map

\[ f : S \times \mathbb{Z} \rightarrow \mathbb{Z} \]

and prove it is bijective.

Solution: We denote the elements of \( S \) by \( a_0, ..., a_{n-1} \), where \( n \) is the cardinality of \( S \).

Define

\[ f : S \times \mathbb{Z} \rightarrow \mathbb{Z} \]

\[ (a_i, k) \mapsto kn + i \]

This \( f \) is a bijection, which is proved as follows.

\( f \) is injective: if \( f(a_i, k) = f(a_j, k') \), then \( kn + i = k'n + j \), so \( i - j = (k' - k)n \), which indicates \( i - j \) is a multiple of \( n \). Since \( 0 \leq i \leq n - 1 \) and \( 0 \leq j \leq n - 1 \), \(-n \leq i - j \leq n - 1 \), so the only chance for \( i - j \) to be a multiple of \( n \) is when \( i = j \), then \( k' = k \), so \( (a_i, k) = (a_j, k') \).

\( f \) is surjective: for any \( m \in \mathbb{Z} \), by the division rule of integers, we know there exists integers \( q \) and \( r \) such that \( m = qn + r \), where \( 0 \leq r \leq n - 1 \), so \( m = f(a_r, q) \), hence \( f \) is surjective.

3. Use strong induction to show any integer \( n \geq 2 \) can be written as a product of one or more prime numbers.

Solution: (1). When \( n = 2 \), we know 2 is a prime, so 2 is a product of one prime.

(2). Suppose the statement holds for all \( 2 \leq k \leq n \). If \( n + 1 \) is a prime, then we are done, since it is a product of one prime. If \( n + 1 \) is not a prime, then we
can write \( n + 1 = ab \) where \( 2 \leq a \leq n, \ 2 \leq b \leq n \). By induction hypothesis, both \( a \) and \( b \) can be written as a product of primes, so the product \( ab = n + 1 \) is also a product of primes.

We finish the proof.

4. \( X \) is a nonempty set. Define \( P(X) = \{ f : X \to X | f \text{ is a bijective function} \} \). Define a law of composition

\[
P(X) \times P(X) \to P(X)
\]

\[
(f_1, f_2) \mapsto f_1 \circ f_2
\]

i.e. composition of functions. Prove \( P(X) \) is a group with respect to this law of composition. Is \( P(X) \) a finite group?

**Solution:**

(1). The composition of functions is associative:

\[
(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)
\]

(2). The identity element is the identity function on \( X \), \( id_X : X \to X \) such that \( id_X(x) = x \) for any \( x \in X \). Then we see it satisfies \( f \circ id_X = id_X \circ f = f \) for any \( f \in S(X) \)

(3). Since \( f \in S(X) \) is a bijection, it has an inverse function \( f^{-1} \) such that \( f \circ f^{-1} = f^{-1} \circ f = id_X \), so the inverse function is the inverse element.

We conclude \( S(X) \) with composition of functions is a group.

\( S(X) \) is a finite group if and only if \( X \) is a finite set.

5. Prove the set of nonzero real numbers \( \mathbb{R}^* \) with multiplication of numbers as the law of composition is a group.

**Solution:**

(1). The multiplication of real numbers is associative, i.e. \( (ab)c = a(bc) \) for any \( a, b, c \in \mathbb{R}^* \).

(2). The identity element is the number \( 1 \in \mathbb{R}^* \): \( a \cdot 1 = 1 \cdot a = a \) for any \( a \in \mathbb{R}^* \).

(3). The inverse element of \( a \in \mathbb{R}^* \) is \( \frac{1}{a} \in \mathbb{R}^* \), since \( a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1 \).

So we see \( \mathbb{R}^* \) with real number multiplication is a group.

6. Prove the set of all \( n \times n \) matrices with real entries, \( M_n(\mathbb{R}) \), is an Abelian group if we define the law of composition to be addition of matrices.

**Solution:**

(1). Addition of matrices is associative: \( (A + B) + C = A + (B + C) \) for any \( A, B, C \in M_n(\mathbb{R}) \).
(2). The identity element is the $n \times n$ zero matrix $0_n$: $A + 0_n = 0_n + A = A$ for any $A \in M_n(\mathbb{R})$

(3). The inverse of $A$ is $-A$: $A + (-A) = (-A) + A = 0_n$.

So $M_n(\mathbb{R})$ with matrix addition is a group. It is an Abelian group since the matrix addition is commutative: $A + B = B + A$ for any $A, B \in M_n(\mathbb{R})$

7. Let $G$ be the set of all functions $\mathbb{R} \rightarrow \mathbb{R}$. Given $f_1$ and $f_2$ in $G$, define $f_1 + f_2$ to be the function $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ for any $x \in \mathbb{R}$. Show that $G$ is an Abelian group with the above law of composition.

Solution: (1). The law of composition is associative: for any $f_1, f_2, f_3 \in G$, $((f_1 + f_2) + f_3)(x) = (f_1 + f_2)(x) + f_3(x) = (f_1(x) + f_2(x)) + f_3(x) = f_1(x) + (f_2(x) + f_3(x)) = f_1(x) + (f_2 + f_3)(x) = (f_1 + (f_2 + f_3))(x)$ for any $x \in \mathbb{R}$, so $(f_1 + f_2) + f_3 = f_1 + (f_2 + f_3)$.

(2). The identity element is the zero function $f_0(x) \equiv 0$: for any $f \in G$, $(f + f_0)(x) = f(x) + f_0(x) = f(x) = f_0(x) + f(x) = (f_0 + f)(x)$, so $f + f_0 = f_0 + f = f$.

(3). The inverse of $f \in G$ is the function $-f \in G$ defined by $(-f)(x) = -f(x)$ for any $x \in \mathbb{R}$: $(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-f(x)) = 0$, and similarly $((-f) + f)(x) = 0$, so $f + (-f) = (-f) + f = f_0$.

So $G$ with composition of functions is a group. It is an Abelian group because for any $f_1, f_2 \in G$, $(f_1 + f_2)(x) = f_1(x) + f_2(x) = f_2(x) + f_1(x) = (f_2 + f_1)(x)$, so $f_1 + f_2 = f_2 + f_1$.

8. $G$ is a group. If $x \cdot x = 1$ for any $x \in G$, prove that $G$ is an Abelian group.

Solution: $x \cdot x = 1$ for any $x \in G$ is equivalent to $x = x^{-1}$ for any $x \in G$.

For any $a, b \in G$, $ab$ is also an element in $G$, so $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. So the group is Abelian.