ELEMENTARY SET THEORY

A Brief Review

Definition. $X$ and $Y$ are two sets. A function $f : X \rightarrow Y$ from $X$ to $Y$ is a rule that assigns a unique element $f(x) \in Y$ to each element $x \in X$.

We call $X$ the domain of $f$, and $Y$ the codomain of $f$.

Define the range of $f$ (or image of $f$) to be

$$\text{Range}(f) = \text{Im}(f) = \{ f(x) \mid x \in X \}$$

That is, the set of elements in $Y$ that are assigned to some element in $X$ via the function $f$.

If $y \in Y$, define the preimage of $y$ under the function $f$:

$$f^{-1}(y) = \{ x \in X \mid f(x) = y \}$$

Example. $\mathbb{Z} \xrightarrow{f} \mathbb{Z}$, defined by $f(x) = x^2$.

The domain is $\mathbb{Z}$.

The range is $\text{Range}(f) = \{ n^2 \mid n \in \mathbb{Z} \}$, the set of all perfect squares.

The preimage:

- $f^{-1}(0) = \{ 0 \}$
- $f^{-1}(n^2) = \{ \pm n \}$
- $f^{-1}(k) = \emptyset$ if $k$ is not a perfect square

Example. $X = \{ f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is continuous} \}$.

Define $F : X \rightarrow \mathbb{R}$,

$$f \mapsto f(0)$$

The range of $F$ is $\mathbb{R}$, since for each $f \in X$, we can take the function $f(x) \equiv x$, which is continuous and $F(f) = f(0) = 0$. 

$\Box$
Definition. A function $f : X \to Y$ is injective if
$$f(x_1) = f(x_2) \implies x_1 = x_2.$$ 
Equivalently, $f$ is injective if $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.
We also say $f$ is one-to-one if it's injective.

A function $f : X \to Y$ is surjective if
$$\forall y \in Y, \exists x \in X \text{ such that } y = f(x).$$
In other words, $f$ is surjective if $\text{Range}(f) = Y$.
We also say $f$ is onto if it's surjective.

A function $f : X \to Y$ is bijective if
it's both injective and surjective.

Example. \( \mathbb{Z} \xrightarrow{f} \mathbb{Z} \), $f(x) = x^2$ is not injective, since $f(1) = f(-1)$.
It's not surjective since if $y \in \mathbb{Z}$ is not a perfect square, it has no preimage.
It follows it's not bijective.

Example. \( \mathbb{Z} \xrightarrow{f} \mathbb{Z} \), $f(x) = 2x$ is injective, since $f(x_1) = f(x_2)$ implies $2x_1 = 2x_2$, so $x_1 = x_2$.
It's not surjective since the range is the set of even numbers, not the entire set $\mathbb{Z}$.
It's not bijective.

Example. \( \mathbb{R} \xrightarrow{f} \mathbb{R} \), $f(x) = 2x$ is injective, since $f(x_1) = f(x_2)$ implies $2x_1 = 2x_2$, so $x_1 = x_2$.
It's also surjective since any $y \in \mathbb{R}$, $y = f\left(\frac{y}{2}\right)$
so it's bijective.
Definition. If $X$ is a set, the identity function on $X$ is the function $\text{id}_X: X \rightarrow X$ defined by $\text{id}_X(x) = x \ \forall x \in X$.

Proposition. If $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} X$ are functions, $g \circ f = \text{id}_X$, then $f$ is injective and $g$ is surjective.

Proof. If $g \circ f = \text{id}_X$, $f(x_1) = f(x_2)$, then $g \circ f(x_1) = g \circ f(x_2)$, i.e., $\text{id}_X(x_1) = \text{id}_X(x_2) \Rightarrow x_1 = x_2$, so $f$ is injective.

For any $x \in X$, $x = \text{id}_X(x) = g \circ f(x) = g(f(x))$, so $g$ is surjective.

Definition. $g: Y \rightarrow X$ is the inverse function of $f: X \rightarrow Y$ if $f \circ g = \text{id}_Y$ and $g \circ f = \text{id}_X$.

Proposition. $f: X \rightarrow Y$ has an inverse function if and only if $f$ is bijective.

Proof. If $f: X \rightarrow Y$ has an inverse function $g: Y \rightarrow X$, then $f \circ g = \text{id}_Y \Rightarrow f$ is surjective $\Rightarrow g \circ f = \text{id}_X \Rightarrow f$ is injective.

If $f$ is a bijective function, define $g: Y \rightarrow X$ by $g(y) = x \iff f(x) = y$.

Since $f$ is a bijective function, for each $y \in Y$, there exists a unique $x \in X$ such that $f(x) = y$, so the function $g$ is well-defined. $g$ is the inverse of $f$ since $f \circ g(y) = f(x) = y$ and $g \circ f(x) = g(y) = x$. 
Example. \( R \xrightarrow{f} R, f(x) = 2x \) is bijective since it has inverse function \( f'^{-1} : R \rightarrow R, f'^{-1}(x) = \frac{x}{2} \).

Remark. If \( f : X \rightarrow Y \) has an inverse function \( f'^{-1} : Y \rightarrow X \), then \( f'^{-1} \) is also bijective.

Mathematical Induction.

One powerful tool for proofs is the mathematical induction. It is applied when we want to prove some statement \( S(n) \) is true for all natural number \( n \). There are two steps for mathematical induction.

Step 1. Prove \( S(1) \) is true.

(Based on the specific situation, it may not always be verifying the case \( S(1) \). For example, if \( n \) starts from 0, then we need to verify \( S(0) \) is true instead.)

Step 2. Based on the hypothesis that \( S(k) \) is true, prove \( S(k+1) \) is true.

Example. Show that 8 divides \( 3^{2n} - 1 \) for any positive integer \( n \).

1. When \( n = 1 \), \( 3^{2 \times 1} - 1 = 9 - 1 = 8 \), and we see 8 divides 8.

2. Assume \( 3^{2k} - 1 \) is divisible by 8. Then for \( n = k + 1 \):

\[
3^{2(k+1)} - 1 = 3^{2k+2} - 1 = 9 \cdot 3^{2k} - 1 = 8 \cdot 3^{2k} + (3^{2k} - 1)
\]

Since both \( 8 \cdot 3^{2k} \) and \( 3^{2k} - 1 \) are divisible by 8, we see \( 3^{2(k+1)} - 1 \) is divisible by 8.

We therefore conclude \( 3^{2n} - 1 \) is divisible by 8 for any positive integer \( n \).
Sometimes, mathematical induction is not strong enough to prove some statements. We may try to use the so called strong induction instead.

Strong Mathematical Induction.
This type of induction is also used to prove some statement $S(n)$ is true for all natural number $n$.
There are also two steps:
Step 1. Show that $S(1)$ is true (sometimes need more terms).
Step 2. Based on the assumption that $S(n)$ is true for all $1 \leq n \leq k$, show that $S(k+1)$ is also true.

Example. The Fibonacci Numbers $F_n$ are defined by:
\[
\begin{align*}
F_n &= F_{n-1} + F_{n-2} \\
F_1 &= 1 \\
F_0 &= 0
\end{align*}
\]
Show that if $\phi = \frac{1 + \sqrt{5}}{2}$, then $F_n \geq \phi^{n-2}$ for any $n \geq 2$.
(Note that $\phi$ is the Golden Ratio)

We will prove by strong induction:
1. When $n = 2$, $F_2 = F_1 + F_0 = 1 + 0 = 1$, $\phi^{2-2} = \phi^0 = 1$
   so $F_2 \geq \phi^{2-2}$ is true.
   When $n = 3$, $F_3 = F_2 + F_1 = 2$, $\phi^{3-2} = \phi = \frac{1 + \sqrt{5}}{2} < 2$
   so $F_3 \geq \phi^{3-2}$ is true.
2. Suppose $F_n \geq \phi^{n-2}$ for all $2 \leq n \leq k$ ($k \geq 3$),
then for $n = k+1$:
   $F_{k+1} = F_k + F_{k-1} \geq \phi^{k-2} + \phi^{k-3} = \phi^{k-3}(\phi + 1) = \phi^{k-3} \cdot 2\phi = \phi^{k-1}$
   $= \phi^{(k+1)-2}$

We therefore conclude the statement is true for all $n \geq 2$. ⑤
General Suggestions for Studying This Course

We just had a brief review of some techniques and concepts we may need to use for this course.

From now on, we are going to learn something new, that is, the subject of Abstract Algebra. We are going to study the two concepts: groups and rings. They are abstract concepts, but we can find their applications in many different situations. Similar to Analysis, Algebra is one of the most tools and languages for modern mathematics.

Here are some suggestions:

1. Writing proofs in mathematics is a serious task. Every step should be logically correct. One small mistake may make the whole argument invalid.

2. When meeting with a new definition, think about the motivations and keep in mind some examples. Examples may help when thinking about some problems, but when you write down the formal proof, you should stick to the abstract definitions. Argument by taking example is not logically sufficient.

3. Homework is the minimum amount of exercises that you may need. If you would like to get familiar with the concepts and better understanding, you may need to do more exercises than only the homework.