A set is a collection of elements.

\[ R = \{0, 1, 2\} \]
\[ S = \{n^2, 2^n, n!\} \]
\[ T = \{9, 42, R^2\} \]

We write \(0 \in R\) to say \(R\) contains \(0\) and \(n^2 \notin R\) to say \(R\) does not contain \(n^2\).

We denote the size of a set \(A\) by \(|A|\).

Useful sets

\[ \mathbb{N} = \{1, 2, 3, \ldots\} \] (often contains 0)
\[ \mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\} \]
\[ \mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{N}\} \]
\[ \mathbb{R} = \text{the completion of } \mathbb{Q} \]
\[ \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \]
\[ \emptyset = \{\} \]

Set operations

\[ A \cup B = \{g \mid g \in A \text{ or } g \in B\} \]
\[ A \cap B = \{g \mid g \in A \text{ and } g \in B\} \]
\[ \overline{A} = \{g \mid g \notin A\} \] (complements are relative to some universe)
\[ A \setminus B = \{g \mid g \in A \text{ and } g \notin B\} \]

Note \(\overline{A \cup B} = \overline{A} \cap \overline{B}\) and \(\overline{A \cap B} = \overline{A} \cup \overline{B}\), via De Morgan's laws.

Quantifiers

\(\forall\) = for all
\(\exists\) = there exists
\(\exists!\) = there exists a unique

\(\forall^*\) = for all but finitely many
\(\exists^\infty\) = there exists infinitely many

\(\forall^*\) = \exists n \in \mathbb{N} \, \exists m \geq n
Subsets

$A \subseteq B \iff \forall a \in A, a \in B$

$A \subset B \iff A \subseteq B$ and $\exists b \in B : b \notin A$.

Supersets

As before but with $\supseteq$ and $\supset$.

Power Sets

The power set of a set $S$ is the set of all subsets of $S$.

Ex] $\mathcal{P}(\mathbb{Z}_2) = 2^{\mathbb{Z}_2} = \mathcal{P}[\emptyset, \{0\}, \{1\}, \{0,1\}]$.

The power set produces $2^n$ elements when $|S| = n$.

Tuples

A $k$-tuple is an ordered list of $k$ things.

Ex] $(0, 1, 2)$ is a 3-tuple.

$(a, b)$ is a 2-tuple.

Cartesian Product

The Cartesian product or cross product of two sets $A$ and $B$ is

$A \times B = \{(a, b) | a \in A$ and $b \in B\}$.

Sequences

A sequence is an indexed list of objects (like a tuple).

Ex] $000000\ldots$ is an infinite sequence of 0's.

$1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ is an infinite sequence converging to 0.

$abcd\ldots xyz$ is a finite sequence.
Formal Boolean Logic

There are two literals, true and false, usually denoted as either 1 and 0 or T and F respectively.

Statements or propositions can be either true or false.

Ex) All horses are the same color.
   It is raining.
   \[ \sum_{k=1}^{n} k = \frac{n(n+1)}{2}. \]

Operations

Disjunction (OR): \( P \lor Q \) is true if \( P \) or \( Q \) is true.
Conjunction (AND): \( P \land Q \) is true if both \( P \) and \( Q \) are true.
Negation (NOT): \( \neg P \) is true if \( P \) is false.
Exclusive OR (XOR): \( P \oplus Q \) is true if exactly one of \( P \) or \( Q \) is true.
Implication: \( P \implies Q \) if when \( P \) is true, \( Q \) is true.
Equivalence: \( P \iff Q \) if \( P \implies Q \) and \( Q \implies P \).
   This is often written as "iff" for "if and only if."

If we have to prove the equivalence of 3 statements, how many things do we have to prove?

Functions

A function maps inputs from its domain to its codomain or range.

\[ f: X \to Y \]

The inverse of a function \( f^{-1}: Y \to X \) "undoes" the \( f \) operation.

When does the inverse exist?
Surjections (Onto)
A function \( f: X \to Y \) is onto if \( \forall y \in Y \exists x \in X : f(x) = y \).

Injections (one-to-one)
A function \( f: X \to Y \) is one-to-one if \( \forall x_1, x_2 \in X, f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \).

Bijections
A function \( f: X \to Y \) is a bijection if it is both surjective and injective.
Note that this is precisely when an inverse function exists.

Relations
A binary relation \( R \) between two sets \( X \) and \( Y \) is a subset of \( X \times Y \).
We write \( (x, y) \in R \) or \( x R y \) to denote \( x \) is related to \( y \).

\( \exists x \in X \) is a relation on any set of numbers.
\( \in \) is too.

A relation \( R \) when \( X = Y \) is
- reflexive if \( \forall x \in X : x R x \),
- anti-reflexive if \( \forall x \in X : \neg x R x \),
- symmetric if \( \forall x, y \in X : x R y \Rightarrow y R x \),
- anti-symmetric if \( \forall x, y \in X : x R y \Rightarrow \neg y R x \),
- transitive if \( \forall x, y, z \in X : x R y \land y R z \Rightarrow x R z \).

A relation which is reflexive, symmetric, and transitive is called an equivalence relation.
Types of Proofs

Direct Proofs (do the math)

Prove that the sum of two even numbers is even.

Let $x, y$ be even.

Then $\exists a, b \in \mathbb{Z}$ such that $x = 2a$, $y = 2b$.

Hence $x + y = 2a + 2b = 2(a + b)$.

$\therefore$ $x + y$ is even.

Constructive Proof (show the existence of something)

Prove that $f(x) = x^2$ is not one-to-one.

$f(1) = f(-1) = 1$ (counter example proof)

Contradiction Proof

Prove $|\mathbb{N}| < |\mathbb{R}|$.

Clearly $|\mathbb{R}| \geq |\mathbb{N}|$, since $\mathbb{N} \subseteq \mathbb{R}$.

Now suppose that $|\mathbb{N}| = |\mathbb{R}|$.

Then we can enumerate $\mathbb{R}$ as $\{x_n \mid n \in \mathbb{N}\}$ such that $\mathbb{R} = \{x_n \mid n \in \mathbb{N}\}$.

We can write the fractional part of each $x_n$ as $r_n = d_{1,n} d_{2,n} d_{3,n} d_{4,n} \ldots$

The we can write each $r_n$ together as

$\ldots d_{1,1} d_{1,2} d_{1,3} d_{1,4} d_{1,5} \ldots$

$\ldots d_{2,1} d_{2,2} d_{2,3} d_{2,4} d_{2,5} \ldots$

$\ldots d_{3,1} d_{3,2} d_{3,3} d_{3,4} d_{3,5} \ldots$

$\ldots d_{4,1} d_{4,2} d_{4,3} d_{4,4} d_{4,5} \ldots$

If we define $d_n = 0$ if $d_{n,n} \neq 1$, then $r = d_1, d_2, d_3, d_4, \ldots \in \mathbb{R}$.

But clearly $r \neq r_n$ for any $n$.

$\therefore$ $|\mathbb{N}| < |\mathbb{R}|$. 

Contraposition Proofs

Prove \( \forall x \in \mathbb{Z}, \ x^2 \text{ even } \Rightarrow \ x \text{ even.} \)

Suppose \( x \) is not even. Then \( x \) is odd.
The product of two odd numbers is odd, hence \( x^2 = x \cdot x \) is odd.
Thus \( x^2 \) is not even.

Exhaustion Proofs (proof by cases)

Prove that \( \forall n \in \mathbb{N}, \ n \text{ odd } \Rightarrow \ 2 \not\mid 2n^2 + n + 1 \).

Let \( n \in \mathbb{N} \).

Case \( n \) odd:
\[ n = 2a + 1 \text{ for some } a \in \mathbb{Z} \]
\[ 2(2a+1) + 2a + 1 + 1 = 6a + 4 = 2(3a+2) \]

Case \( n \) even:
\[ n = 2a \text{ for some } a \in \mathbb{Z} \]
\[ 2(2a) + 2a + 1 = 6a + 1 \]

Hence when 2 divides \( 2n^2 + n + 1 \), \( n \) must be odd.

What other way(s) could we have divided the cases?

Nonconstructive Proofs

Prove \( \exists a, b \in \mathbb{R} \setminus \mathbb{Q}; \ a^b \in \mathbb{Q}. \)

Either \( \sqrt{2}^\sqrt{2} \in \mathbb{Q} \) and we're done or \( (\sqrt{2}^\sqrt{2})^\sqrt{2} = \sqrt{2}^2 = 2 \).

Why is this nonconstructive?

We don't ever identify which is correct.
Induction takes the general form for a statement $P$ as follows.

$\forall B \subseteq \mathbb{B}, \ P(b) \text{ where } B \text{ is a set of base cases.} \tag{1}$

$\forall n \in \mathbb{N}, \ P(n) \implies P(n+1), \ (k \text{ is usually } 1)$

**Ex) Prove** $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$

When $n=1$, $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}.$

Now suppose $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$

Then $\sum_{k=1}^{n+1} k = n+1 + \sum_{k=1}^{n} k = n+1 + \frac{n(n+1)}{2} = \frac{(n+2)(n+1)}{2}.$ \hfill $\square$

**Ex) Prove all horses are the same color.**

$P(n) = \text{If there are } n \text{ horses, they all are the same color.}$

When $n=1$, this is trivial.

Now suppose $P(n)$ is true.

Given $n+1$ horses, pick 2. Remove one to get a set $S$ of horses and remove the other to get a set $R$ of horses.

Clearly $|S| = |R| = n$, so the horses in $S$ must be all the same color as must all the horses in $R$. But since $S \cap R \neq \emptyset$, it follows that all $n+1$ horses must have the same color.

$\square$ Where does this proof go wrong?
Ex) Prove every amount of postage of at least 12¢ can be made from 4¢ and 5¢ stamps.

WTS \( \forall n \in \mathbb{N}, n \geq 12 \exists a, b \in \mathbb{N}: n = 4a + 5b. \)

When \( n = 12 \), \( a = 3 \) and \( b = 0 \).
When \( n = 13 \), \( a = 2 \) and \( b = 1 \).
When \( n = 14 \), \( a = 1 \) and \( b = 2 \).
When \( n = 15 \), \( a = 0 \) and \( b = 3 \).

Assume true for \( n \).

What do we know about \( n+1 \)?

Instead assume true for \( k = 12, 13, \ldots, n-1, n \). (Strong induction)

If \( n+1 \leq 16 \), we're done.

Otherwise \( n+1 \geq 16 \) and hence \( (n+1) - 4 \geq 12 \).

Thus \( \exists a', b' \in \mathbb{N}: (n+1) - 4 = 4a' + 5b'. \)

Pick \( a = a' + 1 \) and \( b = b' \).

Then \( n+1 = 4a + 5b. \)

\( \square \)

It suffices to show \( P(n) \Rightarrow P(n+4) \).

For \( n+4 \), we know \( \exists a', b' \in \mathbb{N}: n = 4a' + 5b'. \)

Then \( n+4 = 4a' + 5b' + 4 = 4(a' + 1) + 5b' \), so pick \( a = a' + 1 \) and \( b = b' \).  

\( \square \)
Ex) Prove \( \forall x \in \mathbb{R}, f(x) = x^2 \) is nonnegative.

Define \( S_n = (-\infty, -\frac{1}{n}) \cup [\frac{1}{n}, \infty) \).
Define \( P(n) = \forall x \in S_n, f(x) \geq 0 \).

When \( n = 0 \), \( S_0 = (-1, 1) \). \( x^2 \geq 0 \).

Assume \( P(n) \).

Let \( x \in S_{n+1} \).

If \( x \geq 1 \), then \( x^2 \geq (x-1)^2 \geq 0 \).

If \( x \leq 1 \), then \( x^2 \geq (x+1)^2 \geq 0 \).

Q.E.D.