Principle of Strong Induction
from basis $\ell$ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for $m$ ranging over the natural numbers greater than or equal a fixed natural number $\ell$. If both

$\blacktriangleright$ $P(\ell)$ and

$\blacktriangleright$ $\forall n \geq \ell$ in $\mathbb{N}. \left( \forall k \in [\ell..n]. P(k) \right) \implies P(n + 1)$

hold, then

$\blacktriangleright$ $\forall m \geq \ell$ in $\mathbb{N}. P(m)$ holds.
Fundamental Theorem of Arithmetic

Proposition 95  Every positive integer greater than or equal to 2 is a prime or a product of primes.

Proof:

Base case: Holds because 2 is prime.

Inductive step: Consider \( n \geq 2 \).

Assume for all \( k = 2, 3, \ldots, n \) (\( 2 \leq k \leq n \))

\( k \) is prime or a product of primes.

Hypothesis: \( n+1 \) is prime or a product of primes.
Consider two cases:

1. $n+1$ is prime; then we are done.

2. $n+1$ is composite; then $n+1 = a \cdot b$ with $a, b \geq 2$. Observe $a, b \leq n$.

Then, by (1H), $a$ is a prime or a product of primes and $b$ is a prime or a product of primes. Therefore $n+1 = a \cdot b$ is a product of primes.
Theorem 96 (Fundamental Theorem of Arithmetic) For every positive integer \( n \) there is a unique finite ordered sequence of primes \((p_1 \leq \cdots \leq p_\ell)\) with \( \ell \in \mathbb{N} \) such that

\[
n = \prod(p_1, \ldots, p_\ell) \,.
\]

**Proof:**

\[
\begin{aligned}
\text{notation } & \quad \text{def} \quad \prod(\ldots) = 1 \\
\prod(p_1, \ldots, p_{e+1}) & \quad \text{def} \quad \prod(p_1 - p_e) \cdot p_{e+1}
\end{aligned}
\]
Euclid’s infinitude of primes

Theorem 99  The set of primes is infinite.

Proof: Assume for a contradiction that there are a finite set of primes:

\[ p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n \]  for \( n \in \mathbb{N} \)

Consider \( (\prod_{i=1}^{n} p_i) + 1 \). It is not a prime. So it is a product of primes. So there is \( p_k \) such that \( p_k \mid (\prod_{i=1}^{n} p_i) + 1 \). Also \( p_k \mid \prod_{i=1}^{n} p_i \).

Hence, \( p_k \mid (\prod_{i=1}^{n} p_i + 1) - \prod_{i=1}^{n} p_i = 1 \). \( \square \)
Sets
Objectives

To introduce the basics of the theory of sets and some of its uses.
Abstract sets
It has been said that a set is like a mental “bag of dots”, except of course that the bag has no shape; thus,

\[
\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5)
\end{array}
\]

may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as

\[
\begin{array}{cccccc}
(1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) & (1,4) & (2,4) & (1,5) & (2,5)
\end{array}
\]
or even simply as

\[
\bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet
\]

for other considerations.
We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquitous structures that are available within it.
Set membership

We write $\in$ for the *membership predicate*; so that

$$x \in A$$

stands for $x$ is an element of $A$.

We further write

$$x \notin A$$

for $\neg(x \in A)$.

**Example:** $0 \in \{0, 1\}$ and $1 \notin \{0\}$ are true statements.
Extensionality axiom

Two sets are equal if they have the same elements.

Thus,

\[ \forall \text{ sets } A, B. \ A = B \iff (\forall x. x \in A \iff x \in B) \]

Example:

\[ \{0\} \neq \{0, 1\} = \{1, 0\} \neq \{2\} = \{2, 2\} \]
Proposition 100  For $b, c \in \mathbb{R}$, let

$$A = \{ x \in \mathbb{C} \mid x^2 - 2bc + c = 0 \}$$

$$B = \{ b + \sqrt{b^2 - c}, b - \sqrt{b^2 - c} \}$$

$$C = \{ b \}$$

Then,

1. $A = B$, and

2. $B = C \iff b^2 = c$. 

\[ \forall x. (x \in C \land x^2 - 2bc + c = 0) \iff (x = b + \sqrt{b^2 - c} \lor x = b - \sqrt{b^2 - c}) \]
Subsets and supersets

\[ A = B \iff \forall x. (x \in A \iff x \in B) \]
\[ \iff \forall x. (x \in A \implies x \in B) \land (x \in B \implies x \in A) \]

\[ A \subseteq B \iff \forall x. (x \in A \implies x \in B) \]

\[ A = B \iff (A \subseteq B) \land (B \subseteq A) \]
Lemma 103

1. Reflexivity.

   For all sets $A$, $A \subseteq A$.

2. Transitivity.

   For all sets $A$, $B$, $C$, $(A \subseteq B \land B \subseteq C) \implies A \subseteq C$.

3. Antisymmetry.

   For all sets $A$, $B$, $(A \subseteq B \land B \subseteq A) \implies A = B$. 
Separation principle

For any set $A$ and any definable property $P$, there is a set containing precisely those elements of $A$ for which the property $P$ holds.

$$\{ x \in A \mid P(x) \} \subseteq A$$
Russell’s paradox

\[ U = \{ x \mid R(x) \} \]

For arbitrary \( x \):

\[ x \in U \iff R(x) \iff x \not\in x \]

Then:

\[ U \in U \iff U \not\in U \]
Set theory has an empty set, typically denoted \( \emptyset \) or \{\} , with no elements.
Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set $S$ are $\#S$ or $|S|$.

Example:

$$\#\emptyset = 0$$
Finite sets

The *finite sets* are those with cardinality a natural number.

**Example:** For $n \in \mathbb{N}$,

$$[n] = \{ x \in \mathbb{N} \mid x < n \}$$

is finite of cardinality $n$.  

$$= \{ 0, 1, 2, \ldots, n-1 \}$$
Powerset axiom

For any set, there is a set consisting of all its subsets.

\[ \forall X. X \in \mathcal{P}(U) \iff X \subseteq U. \]
\[ \mathcal{P}(\{x, y, z\}) = \exists \exists \exists, \]

\[ \exists x, \{ y, z \}, \exists z, \]

\[ \exists x, y, z, \{ x, z \}, \{ y, z \}, \]

\[ \{ x, y, z \} \]

\[ \# \mathcal{P}(\{x, y, z\}) = 8 = 2^3 \]