**Exercise Hypothesis:** \( \exists x (P(x) \land TQ(x)) \)
\( \forall x (P(x) \rightarrow R(x)) \)

**Conclusion:** \( \exists x (R(x) \land TQ(x)) \)

1. \( \exists x (P(x) \land TQ(x)) \)  \hspace{1cm} \text{Hypothesis}
2. \( \forall x (P(x) \rightarrow R(x)) \)  \hspace{1cm} \text{Hypothesis}
3. \( P(a) \land TQ(a) \)  \hspace{1cm} \text{Exist. Inst. 1}
4. \( P(a) \)  \hspace{1cm} \text{Simp. 3}
5. \( P(a) \rightarrow R(a) \)  \hspace{1cm} \text{Univ. Inst. 2}
6. \( R(a) \)  \hspace{1cm} \text{Monos. and Simp. 3}
7. \( TQ(a) \)  \hspace{1cm} \text{Conjunction 6, 7}
8. \( R(a) \land TQ(a) \)  \hspace{1cm} \text{Exist. Gen. 8}
9. \( \exists x (R(x) \land TQ(x)) \)

**Note:** Scope of quantifiers

\( \forall x (P(x) \rightarrow Q(x)) \neq \forall x P(x) \rightarrow \forall x Q(x) \)

**Example:**
\( U = \text{All People} \)
\( P(x) = \text{'x has green eyes'} \)
\( Q(x) = \text{'x is so feet tall'} \)

\( \forall x (P(x) \rightarrow Q(x)) \) is **false**
\( \forall x P(x) \rightarrow \forall x Q(x) \) is **true** (why?)
In order to illustrate some methods of proof we first make a few definitions concerning the integers. We denote by \( \mathbb{Z} \) the set of integers.

Given \( a, b \in \mathbb{Z} \) with \( a \neq 0 \), we say \( a \) divides \( b \) iff \( b = ak \) for some \( k \in \mathbb{Z} \). Notation: \( a \mid b \).

\( n \) is called even if \( 2 \mid n \), and odd otherwise. Thus \( n \) is even iff \( \exists k : n = 2k \) and \( n \) is odd iff \( \exists k : n = 2k + 1 \).

**Direct Proof of** \( \quad \Rightarrow \)

**Assume** \( P \) is true. Then use valid rules of inference and previously proved theorems to show \( Q \) is true.

**Ex.** If \( n \) is odd then \( n^2 \) is odd.

**Proof:**

Assume \( n \) is odd. Then \( n = 2k + 1 \) for some integer \( k \). Thus \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \). Since \( 2k^2 + 2k \) is itself an integer, this shows \( n^2 \) is also odd, as claimed.
Indirect Proof of $P \rightarrow q$

Prove the contrapositive statement $\neg q \rightarrow \neg P$, usually directly.

Ex. if $5n+4$ is odd then $n$ is odd.

**Proof**

Assume $n$ is even. Then $n = 2k$ for some integer $k$. Thus $5n + 4 = 5(2k) + 4 = 2(5k + 2)$. Since $5k + 2$ is itself an integer, this shows $5n + 4$ is also even. We've shown that if $n$ is even then $5n + 4$ is even. Hence if $5n + 4$ is odd, then $n$ must be odd.

---

A real number $x$ is called **rational** if $x = a/b$ where $a, b \in \mathbb{Z}$, $b \neq 0$.

A real number which is not rational is called **irrational**.

Let $\mathbb{R}$ denote the set of real numbers, $\mathbb{Q}$ the set of rational numbers, and $\mathbb{R} - \mathbb{Q}$ the set of irrational numbers.
Proof by Contradiction of $P$

Prove the implication $7P \Rightarrow 9$, where $9$ is some contradiction. Since $9$ is necessarily false, the only way $7P \Rightarrow 9$ could be true is if $7P$ were false, i.e., $P$ is true. Often the contradiction $9$ is of the form $9 = \text{RATN}$ for some proposition $R$.

Ex. $\sqrt{2}$ is irrational.

Proof:

Assume that $\sqrt{2}$ is rational. Then there exist $a, b \in \mathbb{Z}$, $b \neq 0$ such that

$$\sqrt{2} = \frac{a}{b}$$

Now if $a$ and $b$ have any common factors, we may cancel them top and bottom. Thus we may assume $a$ and $b$ have no factors in common to begin with.

Thus $2 = \frac{a^2}{b^2}$, $a^2 = 2b^2$, and $a^2$ is even. This implies $a$ is even. (Recall we showed $n$ odd $\Rightarrow n^2$ odd which proves indirectly that $n^2$ even $\Rightarrow n$ even.)
Thus \( a = 2k \) for some \( k \in \mathbb{Z} \) and hence \( 2b^2 = a^2 = (2k)^2 = 4k^2 \), \( b^2 = 2k^2 \). Therefore \( b^2 \) is even and so \( b \) is even.

Now we have that \( a \) and \( b \) have no common factors, and yet they are both even. This contradiction shows that our original assumption was false, i.e. \( \sqrt{2} \) must be irrational.

---

Read: Vacuous and Trivial Proofs P. 64
Proof by Cases P. 67

Often we wish to prove a proposition of the form \( \exists x \ P(x) \) where \( P(x) \) is some propositional function. These are called existence proofs.

**Constructive Existence Proof.** Find, construct, or display an element \( a \) in the universe for which \( P(a) \) is true.

**Non-Constructive Existence Proof.** Usually proceeds by contradiction.
Exercise: There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:
Either $\sqrt{2}$ is rational or it is not. If it is, we are done for then $x = \sqrt{2}$, $y = \sqrt{2}$ are irrational while $x^y$ is rational.

If $\sqrt{2}$ is irrational, take $x = \sqrt{2}$ and $y = \sqrt{2}$. Again we have $x, y$ irrational with

$$x = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$$

which is rational. \[\Box\]

Note: We never produce a pair $x, y$ with $x, y$ irrational and $x^y$ rational. This is a non-constructive existence proof.

Read: Mistakes in Proofs p. 71
1.6) SETS

**Defn**

A **set** is any (unordered) collection of objects. The objects belonging to a set are called its **members** or **elements**.

This intuitively obvious definition leads directly to a paradox. See Problem 30, p. 86.

Write \( x \in S \) to say \( x \) is a member of set \( S \).

We can specify a set by listing its members between braces \( \{ \ldots \} \):

\[
\{1, 2, 3\}, \{1, 2, 3, \ldots, 10\}, \{1, 2, 3, \ldots\}
\]

**Some important sets**:  

\( \mathbb{N} = \{0, 1, 2, \ldots\} \) \quad **Natural numbers**

\( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) \quad **Integers**

\( \mathbb{Z}^+ = \{1, 2, 3, \ldots\} \) \quad **Positive integers**

\( \mathbb{Q} = \{ \text{rational numbers} \} \)

\( \mathbb{R} = \{ \text{real numbers} \} \)

\( \mathbb{C} = \{ \text{complex numbers} \} \)
Two sets are considered equal if they contain the same members. Order and repetition in the listing are irrelevant.

\[ \{1, 2, 3\} = \{3, 1, 2\} = \{1, 1, 2, 2, 3, 3\} \]

We can also specify a set using set builder notation. Let \( P(x) \) be a propositional function with universe \( U \). The set of all \( x \in U \) such that \( P(x) \) is true is denoted:

\[ \{ x \in U \mid P(x) \} \]

or

\[ \{ x \mid P(x) \} \]

if the universe is understood.

\[ \{ x \in \mathbb{R} \mid x \leq 8 \} \]

\[ \{ x \in \mathbb{Z} \mid x \leq 8 \} \]

\( \mathbb{Z}^+ = \{ n \in \mathbb{Z} \mid n > 0 \} \)

\( \mathbb{Q} = \{ x \in \mathbb{R} \mid \exists a, b \in \mathbb{Z} : b \neq 0 \land x = \frac{a}{b} \} \)
DEFINITION: THE EMPTY SET is the set with no members: \( \emptyset = \{ \} \).

DEFINITION: WE say \( A \) is a \textit{subset} of \( B \) if every element of \( A \) is also an element of \( B \).

\[ \forall x \ (x \in A \rightarrow x \in B) \]

\textbf{Notation:} \( A \subseteq B \)

WE say \( A \) is a \textit{proper subset} of \( B \) if \( A \subseteq B \) but \( A \neq B \).

\textbf{Notation:} \( A \subsetneq B \)

\textbf{Remark:} \( \subseteq, \subsetneq, \forall, \subseteq \)

\textbf{Observe that for any set} \( S \):

\( \emptyset \subseteq S \): \( \forall x \ (x \in \emptyset \rightarrow x \in S) \) \( \iff \) \( \text{true} \) \textit{tautology}

\( S \subseteq S \): \( \forall x \ (x \in S \rightarrow x \in S) \) \( \iff \) \( \text{true} \) \textit{tautology}

\textbf{Remark:} 'contains!'
Ex. \( S = \{1, 2\} \)

The subsets of \( S \) are

\[ \emptyset, \{1\}, \{2\}, \{1, 2\} \]

The set of subsets of \( S \) is

\[ \{ \emptyset, \{1\}, \{2\}, \{1, 2\} \} \]

Definition:
The set of all subsets of \( S \) is called the \underline{power set} of \( S \), and is denoted \( \mathcal{P}(S) \).

Definition:
If \( S \) has \( n \) distinct members (\( n \in \mathbb{N} \)) we say \( S \) is \underline{finite}, and that \( n \) is the \underline{cardinality} of \( S \).

Notation: \( |S| = n \)

If \( S \) is not finite it is called \underline{infinite}.

Ex. \( \mathbb{N}, \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are infinite sets.