In this chapter we develop three methods for proving a statement. To start let’s suppose the statement is of the form $P \rightarrow Q$ or if $P$, then $Q$.

- **Direct**: This method typically starts with $P$. Then, using definitions, axioms, mathematical ideas and logic, arrives at $Q$. It does NOT use the English language to argue. The logic is called *modus ponens* or the *law of detachment* and can be summarized by

\[
\begin{align*}
P \\
P \rightarrow Q \\
\therefore Q
\end{align*}
\]

A direct proof of a statement of the form $P \rightarrow (\forall x)Q(x)$ sometimes starts “let $x$...” That is, the arbitrary $x$ is part of the antecedent. We will see many examples of this.

- **Contrapositive**: We recall from Theorem 1.14 that $P \rightarrow Q$ is equivalent to the contrapositive $\neg Q \rightarrow \neg P$. The contrapositive method is a direct proof of $\neg Q \rightarrow \neg P$.

- **Contradiction**: For this method we suppose $P \rightarrow Q$ is false. That is, we assume $P \land \neg Q$ is true (see Theorem 1.14). A *contradiction* is a statement which is always false. For example, let $R$ be any statement. Then $R \land \neg R$ is always false for any statement $R$. To implement a proof by contradiction, we prove the connective statement $(P \land \neg Q) \rightarrow (R \land \neg R)$ is true for some statement $R$ (which we have to supply). This leads to a contradiction and implies $(P \land \neg Q)$ is false. That is, $P \rightarrow Q$ is true. A proof by contradiction has the logical forms

\[
\begin{align*}
P \land \neg Q \\
(P \land \neg Q) \rightarrow (R \land \neg R) \\
\therefore R \land \neg R \\
P \land \neg Q \\
(P \land \neg Q) \rightarrow \neg P \\
\therefore P \land \neg P
\end{align*}
\]
2. Proofs

If the statement to be proved is not in the form $P \rightarrow Q$ but perhaps simply a
statement $P$, then there is no contrapositive. However, the remaining two methods
apply.

- **Direct**: Verify $P$ using mathematical ideas.
- **Contradiction**: For this method we assume $\neg P$ is true. Then we have to
find a statement $R$ so that $\neg P \rightarrow (R \land \neg R)$ - a contradiction. A proof by
contradiction in this case has the logical form

\[
\begin{align*}
\neg P & \rightarrow (R \land \neg R) \\
\therefore R \land \neg R
\end{align*}
\]

2.1. Copious Examples of Proofs

Many examples follow

**Theorem 2.1.** The $\sqrt{2}$ is irrational.

**Proof #1** Suppose $\sqrt{2}$ were rational. Then, $\sqrt{2} = p/q$ for some positive integers
$p$ and $q$. Thus $2q^2 = p^2$. The Fundamental Theorem of Arithmetic shows every
positive integer can be factored in to prime numbers. Thus $2q^2$ has an odd number
of factors while $p^2$ has an even number. Hence $2q^2 \neq p^2$ - a contradiction. \hfill \Box

**Proof #2** Suppose $\sqrt{2}$ were rational. Then $\sqrt{2} = p/q$. Let us suppose $p/q$ is
in reduced form - that is, all of the common factors have been canceled. Then
$2q^2 = p^2$. Thus $p^2$ is even and so $p$ is even. It follows $p = 2r$ for some natural
number $r$. Thus $q^2 = 2r^2$ and we see $q$ is even. This contradicts $p/q$ being in
reduced form and so $\sqrt{2}$ must be irrational. \hfill \Box

When a statement is in the form $P \rightarrow Q$ and $P$ is in the form $P_1 \land P_2...$ we
may use Example 1.18 in the last chapter to make the contrapositive easier to work
with. Our three methods have the form

1. (Direct) If $P_1$ and $P_2$, ..., then $Q$.
2. (Contrapositive) If $\neg Q$, then $\neg P_1$ or $\neg P_2$.
3. (Contradiction) If $P_1$, $P_2$, and $\neg Q$, then $\neg P_1$.

As we saw in the Chapter One, the contrapositive in (2) is equivalent to

(2) (Contrapositive) If $\neg Q$ and $P_1$, then $\neg P_2$.

**Definition 2.2.** The set of even numbers is $\{2k \mid k \in \mathbb{Z}\}$. The set of odd numbers
is $\{2k + 1 \mid k \in \mathbb{Z}\}$.

For now we conjecture that each integer is either even or odd and not both.
We will prove this a bit later on.

**Example 2.3.** Consider the statement

If $n^2$ is even, $n$ is even.
Rewrite it in each of the three forms and prove each.

Solution. The three forms are

1. (Direct) If \( n^2 \) is even, \( n \) is even.
2. (Contrapositive) If \( n \) is odd, \( n^2 \) is odd.
3. (Contradiction) If \( n^2 \) is even and \( n \) is odd, then \( n^2 \) is odd.

Proof. (Direct) If \( n^2 = 0 \), then \( n = 0 \) and \( n \) is even. If \( n^2 \neq 0 \) and \( n^2 \) is even, by the fundamental theorem of arithmetic \( n^2 = n \cdot n = (2 \cdot p_1 \ldots p_k)(2 \cdot p_1 \ldots p_k) \), where \( p_1, \ldots, p_k \) are prime numbers. Dividing by \( n \) we find \( n = 2 \cdot p_1 \ldots p_k \) and \( n \) is even.

Proof. (Contrapositive) Suppose \( n \) is odd. We need to show \( n^2 \) is odd. Since \( n \) is odd, \( n = 2k + 1 \) for some \( k \in \mathbb{Z} \). Then \( n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \). Since \( 2k^2 + 2k \in \mathbb{Z} \), we see \( n^2 \) is odd.

Proof. (Contradiction) Suppose \( n^2 \) is even and \( n \) is odd. Since \( n \) is odd, \( n = 2k + 1 \) for some \( k \in \mathbb{Z} \). Then \( n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \). Since \( 2k^2 + 2k \in \mathbb{Z} \), we see \( n^2 \) is odd - a contradiction.

Example 2.4. Consider the following statement.

Suppose \( x, y \in \mathbb{R} \). Prove that, if \( x^2 y = 2x + y \), then, if \( y \neq 0 \), then \( x \neq 0 \).

Rewrite it in each of the three forms and prove each.

Scratch Work. The statement has the form \((P \rightarrow Q) \rightarrow R\). We saw in Example 1.17 in the previous chapter this is equivalent to \((P \land Q) \rightarrow R\).

Solution. The three forms are

1. (Direct) Suppose \( x, y \in \mathbb{R} \). If \( x^2 y = 2x + y, y \neq 0 \), then \( x \neq 0 \).
2. (Contrapositive) Let \( x, y \in \mathbb{R} \). If \( x = 0 \), then \( x^2 y \neq 2x + y \) or \( y = 0 \).
3. (Contradiction) Let \( x, y \in \mathbb{R} \). If \( x^2 y = 2x + y, y \neq 0 \), and \( x = 0 \), then \( y = 0 \).

Proof. (Direct) Suppose \( y \neq 0 \) and \( x^2 y = 2x + y \). Applying the quadratic formula we find

\[
x = \frac{2 \pm \sqrt{4 + 4y^2}}{2y} = \frac{1 \pm \sqrt{1 + y^2}}{y}.
\]

Since \( y \neq 0 \), \( 1 + y^2 > 1 \). This implies \( \sqrt{1 + y^2} > 1 \) (see HW 2.3 below). Thus \( 1 + \sqrt{1 + y^2} > 2 \) and \( 1 - \sqrt{1 + y^2} < 0 \). That is, \( x \neq 0 \).

Proof. (Contrapositive) Suppose \( x = 0 \) and \( x^2 y = 2x + y \). This immediately implies \( y = 0 \) as required. If \( x^2 y \neq 2x + y \) we again arrive at the conclusion of the contrapositive.

Proof. (Contradiction) Suppose \( x = 0, x^2 y = 2x + y, \) and \( y \neq 0 \). Plugging \( x = 0 \), we find \( y = 0 \) - a contradiction.
Example 2.5. Consider the following statement.

If $a, b, c$ are odd, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Rewrite it in each of the three forms and give a direct prove.

**Scratch Work.** The statement has the form $P \rightarrow Q$. Here

$$Q \equiv \neg(\exists x \in \mathbb{Q})(ax^2 + bx + c = 0)$$

$$\equiv (\forall x \in \mathbb{Q})(ax^2 + bx + c \neq 0).$$

The entire statement has the form

$$(\forall a, b, c \in \mathbb{Z})(a \in \mathcal{O} \land b \in \mathcal{O}) \land c \in \mathcal{O} \rightarrow (\forall x \in \mathbb{Q})(ax^2 + bx + c \neq 0).$$

Here $\mathcal{O}$ represents the set of all odd integers since $Q(x)$ is universally quantified, a direct proof could include $x \in \mathbb{Q}$ in the antecedent.

**Solution.** The three forms are

1. (Direct) If $a, b, c$ are odd, then, for all $x \in \mathbb{Q}$, $ax^2 + bx + c \neq 0$.
2. (Direct) If $a, b, c$ are odd and $x \in \mathbb{Q}$, then $ax^2 + bx + c \neq 0$.
3. (Contrapositive) Suppose $a, b, c \in \mathbb{Z}$. If there exists $x \in \mathbb{Q}$ such that $ax^2 + bx + c = 0$, then at least one of $a, b, c$ is even.
4. (Contradiction) If $a, b, c$ are odd and $x \in \mathbb{Q}$ exists so that $ax^2 + bx + c = 0$, then (some) contradiction.

**Proof.** (Direct) Suppose $a, b, c$ are odd and $x \in \mathbb{Q}$. Then $x = p/q$ (reduced form) for some $p, q \in \mathbb{Z}$ and $q \neq 0$. Note that $p$ and $q$ cannot both be even. We need to consider the quantity $ap^2 + bpq + cq^2$. Specifically, we need to show that this quantity is never zero. If $p$ is even and $q$ odd, then $ap^2$ and $bpq$ are both even while $cq^2$ is odd. Since the sum of an even an odd integer is odd, the quantity $ap^2 + bpq + cq^2$ cannot sum to zero which is even. Similarly, if $p$ is odd and $q$ even, $ap^2$ is odd while the other terms are even. If both $p$ and $q$ are odd, all three terms in $ap^2 + bpq + cq^2$ odd. Thus, in all cases $ax^2 + bx + c \neq 0$.

**Proof.** (Contradiction) Suppose $a, b, c$ are odd and $x \in \mathbb{Q}$ exists so that $ax^2 + bx + c = 0$. Since $x \in \mathbb{Q}$, it may be expressed form $x = p/q$ (reduced form) for some $p, q \in \mathbb{Z}$ and $q \neq 0$. Note both $p$ and $q$ cannot be even. Plugging in our equation, we find $ap^2 + bpq + cq^2 = 0$. If $p$ is even, $cq^2 = 0 - ap^2 - bpq$ is even. Since $c$ is odd, $q^2$ is even. This implies $q$ is even and contradicts our assumption $p/q$ is in reduced form. A similar argument follows if $q$ is assumed even. Thus $p$ and $q$ must be odd. But this would imply 0 is odd - another contradiction.

Example 2.6. Consider the following statement.

If $a$ is less than or equal to every real number greater than $b$, then $a \leq b$.

Rewrite it in each of the three forms and prove the contrapositive and contradiction.
2.1. Copious Examples of Proofs

**Scratch Work.** The statement has the form $P \rightarrow Q$. Here

\[ P \equiv (\forall x > b)(a \leq x) \]

\[ Q \equiv a \leq b. \]

Note the negation of $P$ is $\neg P \equiv (\exists x > b)(a > x)$.

**Solution.** The three forms are

1. (Direct) If $a \leq x$ for all $x > b$, then $a \leq b$.
2. (Contrapositive) If $a > b$, then there exists a $x > b$ such that $a > x$.
3. (Contradiction) If $a > b$ and $a \leq x$ for all $x > b$, then $a \leq b$.

**Proof.** (Contrapositive) Suppose $a > b$. Set $x = \frac{a+b}{2}$. Then

\[ b = \frac{b+b}{2} < \frac{a+b}{2} = x < \frac{a+a}{2} = a. \]

Thus, there exists an $x > b$ such that $a > x$. \hfill $\Box$

**Proof.** (Contradiction) Suppose $a > b$ and $a \leq x$ for all $x > b$. Consider $x = \frac{a+b}{2}$. Then $b = \frac{b+b}{2} < \frac{a+b}{2} = x$. Our assumptions imply $a \leq x$ or $a \leq \frac{a+b}{2}$. This implies $a \leq b$ - a contradiction. \hfill $\Box$

**Definition 2.7.** Suppose $E \subset \mathbb{R}$. We say $M \in \mathbb{R}$ is a maximum element of $E$ iff

1. $x \leq M$ for all $x \in E$,
2. $M \in E$.

**Example 2.8.** Show the set $E = \{x \mid 0 < x < 1\}$ has no maximum element.

**Scratch Work.** This statement is in the form $P$, so there is no contrapositive. If we wish to prove it directly, it might help to know what “no maximum” means. If $E$ has a maximum then

\[ Q \equiv (\exists M \in E)(\forall x \in E)(x \leq M). \]

There is no maximum if

\[ \neg Q \equiv (\forall M \in E)(\exists x \in E)(x \geq M). \]

Since $Q$ is in the form $(\forall M)Q(M)$, a direct proof starts “let $M \in E.$”

**Proof.** (Direct) Let $M \in E$. Set $x = \frac{M+1}{2}$. Then

\[ M = \frac{M+M}{2} < \frac{1+M}{2} = x < \frac{1+1}{2} = 1. \]

Thus for all $M \in E$ there exists $x \in E$ such that $x \geq M$ and the set $E$ does not have a maximum. \hfill $\Box$

**Proof.** (Contradiction) Suppose $E$ has a maximum $M$. Then $x \leq M$ for all $x \in E$ and $M \in E$. However, $y = \frac{M+1}{2}$ is in $E$ and $y < M$. This contradicts $M$ being a maximum of the set $E$. \hfill $\Box$
Example 2.9. Prove the following statement.

Among the numbers \( y_1, y_2, \ldots, y_n \) some number is as large as average \( \frac{1}{n}(y_1 + y_2 + \cdots + y_n) \).

**Scratch Work.** While the \( y_i \) are arbitrary, the statement does not imply they change - they are given fixed numbers. Set \( I = \{i \mid i \in \mathbb{N}, 1 \leq i \leq n\} \). We need to work with the statement

\[
(\exists i \in I) \left( \frac{1}{n}(y_1 + y_2 + \cdots + y_n) \leq y_i \right).
\]

There does not seem to be a contrapositive.

**Solution.** We have

1. (Direct) Let \( y_i \in \mathbb{R} \) for \( 1 \leq i \leq n \) be given and set \( Y = \frac{1}{n} \sum_{i=1}^{n} y_i \). Then there exists \( y_i \) such that \( Y \leq y_i \).

2. (Contradiction) If \( y_i \in \mathbb{R} \) for \( 1 \leq i \leq n \) and \( Y = \frac{1}{n} \sum_{i=1}^{n} y_i \), and, if for all \( 1 \leq i \leq n \), \( y_i < Y \), then \( Y < Y \) - a contradiction.

**Proof.** (Direct) Let \( y_m = \max\{y_1, \ldots, y_n\} \) (we will assume the maximum exists without proof). Then \( y_i \leq y_m \) for all \( 1 \leq i \leq n \). Summing both sides and dividing by \( n \), we find \( Y \leq y_m \). \( \square \)

**Proof.** (Contradiction) Suppose \( Y = \frac{1}{n} \sum_{i=1}^{n} y_i \) and \( y_i < Y \) for all \( 1 \leq i \leq n \). Summing both sides of \( y_i < Y \) and dividing by \( n \) we find \( Y < Y \), a contradiction. \( \square \)

Example 2.10. Prove the following statement.

There is not a largest real number.

**Proof.** Suppose there were a largest real number \( M \). Then \( x \leq M \) for all \( x \in \mathbb{R} \). Since \( M + 1 \in \mathbb{R} \), we have \( M + 1 \leq M \) or \( 1 \leq 0 \), a contradiction. \( \square \)

For problems involving sets, we say \( A = B \) if and only if \( A \subseteq B \) and \( B \subseteq A \).

Example 2.11. Let \( A, B, C \) and \( D \) are sets. Suppose \( A \setminus B \subseteq C \cap D \). Show \( A \setminus D \subseteq B \).

**Scratch Work.** In logic notation the statement is in the form

\[
(A \setminus B \subseteq C \cap D) \rightarrow (\forall x \in A \setminus D)(x \in B).
\]

The consequent is \( Q \equiv (\forall x \in A \setminus D)(x \in B) \). Its negation is \( \neg Q \equiv (\exists x \in A \setminus D)(x \notin B) \).
2.2. Proofs Using Axioms

Solution.
(1) (Direct) If \( A \setminus B \subseteq C \cap D \) and \( x \in A \setminus D \), then \( x \in B \).
(2) (Contrapositive) If there exists \( x \in A \setminus D \) such that \( x \notin B \), then \( A \setminus B \not\subseteq C \cap D \).
(3) (Contradiction) If \( A \setminus B \subseteq C \cap D \) and \( x \in A \setminus D \) exists such that \( x \notin B \), then contradiction.

Proof. (Contrapositive) Suppose \( x \in A \setminus D \) exists such that \( x \notin B \). Since \( x \in A \setminus D \), \( x \in A \). It follows \( x \in A \setminus B \). However, \( x \) cannot be in \( C \cap D \) since \( x \notin D \). Thus, there exists an element in \( A \setminus B \) which is not in \( C \cap D \). That is, \( A \setminus B \not\subseteq C \cap D \). □

2.2. Proofs Using Axioms

We assume the set of real numbers, \( \mathbb{R} \), has two binary operations, denoted + and \( \cdot \) (i.e. a function whose domain is \( \mathbb{R} \times \mathbb{R} \) and range in \( \mathbb{R} \)). The operations are called addition and multiplication respectively. Moreover, they satisfy the following properties:

(A1)
\[
\begin{align*}
    a + b &= b + a \\
    a \cdot b &= b \cdot a
\end{align*}
\]
(commutative laws)

(A2)
\[
\begin{align*}
    a + (b + c) &= (a + b) + c \\
    a \cdot (b \cdot c) &= (a \cdot b) \cdot c
\end{align*}
\]
(associative laws)

(A3)
\[
\begin{align*}
    a \cdot (b + c) &= a \cdot b + a \cdot c
\end{align*}
\]
(distributive law)

(A4) There exists unique, distinct real numbers 0 and 1 such that, for all \( a \in \mathbb{R} \),
\[
\begin{align*}
    a + 0 &= a \\
    a \cdot 1 &= a
\end{align*}
\]
(identity elements)

(A5) For each \( a \in \mathbb{R} \) and \( b \in \mathbb{R} \), \( b \neq 0 \), there exists \(-a \in \mathbb{R} \) and \( b^{-1} := 1/b \in \mathbb{R} \) such that
\[
\begin{align*}
    a + (-a) &= 0 \\
    b \cdot b^{-1} &= 1
\end{align*}
\]
(inverse elements)

The above axioms show that \( (\mathbb{R}, +, \cdot) \) is a “field” in the sense of abstract algebra.

We note that \( (\mathbb{Q}, +, \cdot) \) is a field, where \( \mathbb{Q} \) is the set of rational numbers. This is so since the sum or product of two fractions is again a fraction. That is, the rational numbers are closed under addition and multiplication.

Order Axioms for \( \mathbb{R} \)

We assume the existence of an order property on \( \mathbb{R} \), denoted by \( < \), with the following properties:

(O1) For all \( a, b \in \mathbb{R} \), exactly one of the following holds:
\[
\begin{align*}
    a &= b, a < b, b < a
\end{align*}
\]
(trichotomy)
(O2) For all $a, b, c \in \mathbb{R}$, if $a < b$, then $a + c < b + c$.

(O3) For all $a, b, c \in \mathbb{R}$, if $a < b$ and $0 < c$, then $ac < bc$.

(O4) For all $a, b, c \in \mathbb{R}$, if $a < b$ and $b < c$, then $a < c$ (transitivity).

Note that we did not assume in (A5) that the additive and multiplicative inverses are unique. The uniqueness of these follow from the uniqueness of 1 and 0.

**Theorem 2.12.** Suppose $a \in \mathbb{R}$. Then the additive inverse $-a$ and the multiplicative inverse, $a^{-1}$ ($a \neq 0$) are unique.

**Proof.** Suppose $a, b \in \mathbb{R}$ satisfy $a + (-a) = 0$ and $a + b = 0$. Then, applying the axioms,

$$b = b + 0 = b + (a + -a) = (a + b) + -a = 0 + -a = -a.$$  

Similarly, if $a \neq 0$, $a \cdot a^{-1} = 1$ and $ab = 1$, then

$$b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (a \cdot b) \cdot a^{-1} = 1 \cdot a^{-1} = a^{-1}.$$

\[\square\]

**Theorem 2.13.** Suppose $a, b \in \mathbb{R}$. Then

(a) $0 \cdot a = 0$,

(b) $-a = -1 \cdot a$.

(c) $-1 \cdot -1 = 1$.

**Proof.** Part (a) By (A4), $a = 1 \cdot a = (1 + 0) \cdot a$. Applying (A3) we find $a = 1 \cdot a + 0 \cdot a = a + 0 \cdot a$. Finally, (A4) shows $0 \cdot a = 0$, since 0 is the only real number with this property.

To prove (b), we apply (A4), (A3), (A5) and the previous part, respectively, to find,

$$a + -1 \cdot a = 1 \cdot a + -1 \cdot a$$

$$= (1 + -1) \cdot a$$

$$= 0 \cdot a$$

$$= 0.$$

Part (b) follows from (A5).

To prove (c) we apply (b) with $a = -1$. Then $-(-1) = -1 \cdot -1$. Apply the axioms we find

$$1 = 1 + 0$$

$$= 1 + (-1 + -(-1))$$

$$= (1 + -1) + -(-1)$$

$$= 0 + -(-1)$$

$$= -1 \cdot -1.$$

\[\square\]

**Theorem 2.14.** For all $a, b \in \mathbb{R}$, $a < b$ implies $-b < -a$. 

2.4. One Last Example: $P \rightarrow \forall x Q(x)$

**Proof.** By (O2) $a + (-a) < b + (-a)$. This implies $0 < b - a$. Adding $-b$ to both sides give $-b < -a$ as desired. \(\square\)

**Corollary 2.15.** For all $a, b, c \in \mathbb{R}$, $c < 0$, and $a < b$, implies $cb < ca$.

**Proof.** By the theorem $0 < -c$. By (O3), $-ac < -cb$. Again by the theorem, $cb < ca$. \(\square\)

2.3. Existence and Uniqueness Proofs

Sometimes we need to show a solution exists to a problem and that the solution is unique. The next example illustrates how to do this.

**Example 2.16.** Suppose $x$ is a real number. Then there is a unique real number $y$ such that $x^2 y = x - y$.

**Scratch Work:** Given $x$ we can easily solve for $y$ to find $y = \frac{1}{x^2 + 1}$.

**Proof. Existence:** Set $y = \frac{1}{x^2 + 1}$. Then one checks that $x^2 y = x - y$.

**Uniqueness:** Suppose $y_1$ and $y_2$ solve $x^2 y_1 = x - y_1$ and $x^2 y_2 = x - y_2$ respectively. Subtracting the two, we find $x^2(y_1 - y_2) = -(y_1 - y_2)$. That is, $(x^2 + 1)(y_1 - y_2) = 0$. This implies $y_1 - y_2 = 0$ or $y_1 = y_2$, and so the solution is unique. \(\square\)

2.4. One Last Example: $P \rightarrow \forall x Q(x)$

Theorems of the form $P \rightarrow \forall x Q(x)$ sometimes require special treatment. It may seem counter intuitive, but statements of this form often must start “Let $x$...” Then $P$ is used to help arrive at $Q(x)$. Problems 2.13, 2.17, 2.20, 2.25, 2.31 in the following homework are in this form.

You don’t need to understand the mathematical concepts in the following example to follow the logic.

**Definition 2.17.** We say a set $K \subset \mathbb{R}^n$ is compact if and only if, for all collections of open sets $\{G_\alpha\}$ which cover $K$, that is, $K \subset \cup \alpha G_\alpha$, there exists a finite subcovering. That is, $K \subset \cup_1^N G_i$ - a finite number of the $G_\alpha$ cover $F$.

(It turns out that functions continuous on a compact set have a maximum and a minimum.)

Consider the following statement (a homework problem from MAT 372).

**Theorem 2.18.** Suppose $K \subset \mathbb{R}^n$ is compact and $F$ is a closed subset of $K$. Then $F$ is compact.

The statement is in the form $P \rightarrow Q$. Here $Q \equiv F$ is compact. But compact means for all open coverings of $F$ there exists a finite subcovering. So we **must** start with a collection of open sets covering $F$. If we start with the antecedent “$K$ is compact” and apply the definition of compact to $K$, we get a collection of open sets which have nothing to do with $F$. The theorem is a story about open sets which cover $F$, and somehow $K$ being compact will help us.
2.5. Proof-Writing Guidelines

- Write in complete sentences. While “1+2=3” is a complete sentence it is not possible in a proof since we never start a sentence with a mathematical expression or symbol. Moreover, writing too many equations without words looks more like scratch work. Make all equations part of a sentence. It is fine to display lengthy equations.
- Only use the (subjective) pronoun we - no other.
- Organize sentences into paragraphs. Create a new paragraph when the logic changes or you prove a different part of the theorem.
- If you find yourself making an argument using only words - stop. Look for mathematical ideas to convey your reasoning. Look at many mathematical proofs. Frequently proofs only contain English words like: for all, there exists, since, then, because, therefore, it follows, we see, hence...

A mathematical proof consists of logical arguments starting ONLY from axioms, definitions, or previous results which follow logically from axioms or definitions.
- Do not use a variable without defining it first. Read your proof like a computer would read/compile a program. All quantities must be defined.
- Do not use quantifier logic notation in a proof (∃, ∀, →, ∨, ∧, ¬). Words are better for this.
- Often theorems are of the form $P \rightarrow Q$. A direct proof frequently starts with “Suppose $P$.” Then $P$ is unraveled mathematically and manipulated to arrive at the meaning of $Q$. The exception occurs when $Q$ contains a universal quantifier and/or is itself in the form $P_1 \rightarrow Q$. Then a direct proof starts “Let $x$ be in ..” or “Suppose $P_1$.” For example, if the theorem were in the form $P \rightarrow (\forall x \in A)Q(x)$, then the statement is about something happening when $x \in A$. So the proof starts, suppose $P$ and $x \in A$. It ends with $Q(x)$.
- The proof of an infinite number of statements, $P(n)$, requires induction if the $P(n)$ cannot be directly verified for arbitrary $n \in \mathbb{N}$.
- Read, not for understanding but for style, many, many proofs. Your book is a great source for this activity. Check out your calculus or linear algebra book too.
2.6. Homework

Instructions. When possible restate each problem in each of the following forms. Then choose one and provide a careful, well-written proof.

(1) (Direct) If \( P_1 \) and \( P_2, \ldots \), then \( Q \).
(2) (Contrapositive) If \( \neg Q \), then \( \neg P_1 \) or \( \neg P_2 \).
(3) (Contradiction) If \( P_1, P_2, \) and \( \neg Q \), then (a contradiction).

Then choose a version and prove it. You may have to adapt the logic to the given problem.

Exercise 2.1. Suppose \( a, b \in \mathbb{R} \). Prove the following.

(a) If \( a \neq 0 \), then \( 1/a \neq 0 \) and \( 1/(1/a) = a \).
(b) If \( a \cdot b = 0 \), then \( a = 0 \) or \( b = 0 \).
(c) \( (-a) \cdot (-b) = a \cdot b \).

Exercise 2.2. Suppose \( m, n, p, q \in \mathbb{R} \) are all nonzero. Using only the axioms and the previous theorem, provide proofs of the following equalities (you may find proving them in order useful)

\[
\begin{align*}
\frac{m \cdot p}{n \cdot q} &= \frac{mp}{nq}, \\
\frac{m}{n} + \frac{p}{q} &= \frac{mq + np}{nq}, \\
\frac{-m}{n} &= \frac{-m}{n}, \\
\left(\frac{1}{n}\right)^{-1} &= \frac{1}{n}, \\
\frac{m}{n} &= \frac{mq}{np}.
\end{align*}
\]

Exercise 2.3. Suppose \( a, b \in \mathbb{R} \).

(a) If \( 0 < a < b \), show \( a^2 < b^2 \).
(b) If \( 0 < a < b \), show \( \sqrt{a} < \sqrt{b} \).

Exercise 2.4. A square of an even number is an even number.

Exercise 2.5. An integer \( n \) is odd if and only if \( n^2 \) is odd.

Exercise 2.6. The product of a nonzero rational number and an irrational number is irrational.

Exercise 2.7. The \( \sqrt{n} \) is irrational if \( n \) is a positive integer that is not a perfect square.

Exercise 2.8. If \( x \) and \( y \) are distinct real numbers, then \( (x + 1)^2 = (y + 1)^2 \) if and only if \( x + y = -2 \). How does the conclusion change if we allow \( x = y \)?

Exercise 2.9. Suppose \( x \) and \( y \) are real numbers, \( y + x = 2y - x \), and \( x \) and \( y \) are not both zero. Prove that \( y \neq 0 \).

Exercise 2.10. Suppose that \( x \) and \( y \) are real numbers. Prove that if \( x \neq 0 \), then if \( y = \frac{3x^2 + 2y}{x^2 + 2} \), then \( y = 3 \).
Exercise 2.11. Prove the following theorem: For $x, y \in \mathbb{R}$, $x < 2$ if $0 < y < \frac{1}{3}$ and $2x + \frac{1}{y} < 7$.

Exercise 2.12. Prove or disprove. Suppose $n_1, n_2, n_3,$ and $n_4$ are consecutive positive integers. Then $n_1n_2n_3n_4$ is divisible by four.

Exercise 2.13. Let $A, B, C,$ and $D$ be sets. Suppose that $(A \setminus B) \subseteq (C \setminus D)$. Prove that $A \cap D \subseteq B$.

Exercise 2.14. Using the fact that $\sqrt{k}$, with $k \in \mathbb{N}$ is a rational number if and only if $k$ is a square, prove that $\sqrt{9n^2 + 6n + 4}$ is irrational for all $n \in \mathbb{Z}^+$.

Exercise 2.15. Let $m, n$ be integers. Let $S$ be the assertion "$m+n$ is odd".
   a) Is $S$ a necessary condition for the product $mn$ to be even? Give reasons for your answer.
   b) Is $S$ a sufficient condition for the product $mn$ to be even? Give reasons for your answers.

Exercise 2.16. Suppose $A$ and $B$ are sets. Prove $A \setminus (A \setminus B) = A \cap B$.

Exercise 2.17. Suppose that $A \setminus B$ is disjoint from $C$, and $x \in A$. Prove that if $x \in C$, then $x \in B$.

Exercise 2.18. Prove that $n^2 + n + 1$ is odd for each $n \in \mathbb{N}$.

Exercise 2.19. Prove that for any $x \in \mathbb{R}$ with $x^2 > 9$, if $x > 0$, then $x > 3$.

Exercise 2.20. Prove that if $A$ and $B \setminus C$ are disjoint, then $A \cap B \subseteq C$.

Exercise 2.21. Suppose $n$ is an integer. Show the following are equivalent.
   i) $n$ is even
   ii) $n + 1$ is odd
   iii) $3n + 1$ is odd
   iv) $3n$ is even

Exercise 2.22. Prove the following result. If $a$ and $b$ are even integers, then $(a+b)^2$ is an even integer.

Exercise 2.23. Prove the following result. For every integer $z$, $z + z^2$ is even.

Exercise 2.24. A set $C$ of real numbers is convex if and only if for all elements in $x, y \in C$ and for every real numbers $t$ with $0 \leq t \leq 1$, $tx + (1-t)y \in C$. Suppose $a, b \in \mathbb{R}$. Show that the set $C = \{x \in \mathbb{R} | ax \leq b\}$ is convex.

Exercise 2.25. If $S$ and $T$ are convex sets, then $S \cap T$ is a convex set. Is $S \cup T$ always convex?

Exercise 2.26. A function is strictly increasing if and only if for all real $x, y$ such that $x < y$ implies $f(x) < f(y)$. Prove that $f(x) = x^3$ is strictly increasing.

Exercise 2.27. Suppose $a \in \mathbb{R}$ and that $|a| < \epsilon$ for all $\epsilon > 0$. Show that $a = 0$. 

Exercise 2.28. Suppose $a, b, c \in \mathbb{R}$ with $c \neq 0$. If $cx^2 + bx + a$ has no rational root, then $ax^2 + bx + c$ has no rational root.

Exercise 2.29. Show that a party of $n \geq 2$ people has at least two people who have the same number of friends at the party.

Exercise 2.30. The polynomial $x^4 + 2x^2 + 2x + 2$ cannot be expressed as the product of the two polynomials $x^2 + ax + b$ and $x^2 + cx + d$ in which $a, b, c, d \in \mathbb{Z}$. You may assume two polynomials agree for all $x$ if and only if their coefficients agree.

Exercise 2.31. A set $S$ of real numbers is bounded if and only if there exists a real number $M > 0$ such that $|x| \leq M$ for all $x \in S$. Suppose $S$ and $T$ are sets of real numbers with $S \subseteq T$. If $S$ is not bounded, prove that $T$ is not bounded.

Exercise 2.32. If $c$ is an odd integer, then the equation $n^2 + n - c = 0$ has no integer solution for $n$.

Exercise 2.33. Show that, if $x, y \in \mathbb{R}$ are such that $x \geq 0$, $y \geq 0$, and $x + y = 0$, then $x = 0$ and $y = 0$.

Exercise 2.34. Prove that there is a unique integer $n$ for which $2n^2 - 3n - 2 = 0$.

Exercise 2.35. Prove that for every real number $x$, if $x \neq 0$ and $x \neq 1$, then there is a unique real number $y$ such that $y/x = y - x$.

Exercise 2.36. If $n$ is a positive integer, then either $n$ is prime, or $n$ is a square, or $n$ divides $(n - 1)!$.

Exercise 2.37. Translate the following into quantifier notation:

1. The maximum of a function $f(x)$ on $0 \leq x \leq 1$ is less than some $y$.
2. The minimum of a function $f(x)$ on $0 \leq x \leq 1$ is less than some $y$.

Exercise 2.38. If $S$ is a nonempty subset of a set $T$ of real numbers and $t^*$ is a real number such that for each element $t \in T$, $t \geq t^*$, prove $\min\{s | s \in S\} \geq t^*$. You may assume $S$ has a minimum.