Note. Much of the following discussion is in the nature of a review and does not pretend to be a rigorous derivation of the various results stated. One consequence of this is that I sometimes use concepts before their precise meaning has been discussed. In this I am relying on a certain amount of background knowledge.

1. Unordered Sets

1a) An unordered set is a collection of objects of any sort — numbers, physical objects, names ...

1b) Sets can be defined by a complete listing of members — e.g., \{1, 3, -2\} or \{Fred, Jane, Bob\} — or by specifying the properties which members of a set possess — e.g.,

\[ \{ x \mid x \text{ is an even number and } x > 9 \} \]

Note that a comma between properties means "and", e.g.,

\[ \{ x \mid x^2 = 4, x > 0 \} \]

means

\[ \{ x \mid x^2 = 4 \text{ and } x > 0 \} \]

and thus equals \{2\}.

1c) The number of elements belonging to a set may be finite or infinite. A set with no elements is called the empty set and denoted by \( \emptyset \). Note that \( \emptyset \) and \{0\} are not the same set.

1d) Given a set \( S, x \in S \) denotes "\( x \) belongs to \( S \)". This may be alternatively written as \( S \ni x \), meaning "\( S \) owns \( x \)". If \( x \) does not belong to \( S \), we write \( x \notin S \) or \( S \not\ni x \).

1e) Two sets \( A \) and \( B \) are equal iff\(^2\) both

\[(i) \ x \in A \Rightarrow x \in B \quad \text{and} \quad (ii) \ x \in B \Rightarrow x \in A, \]

i.e., all of the members of each set are also members of the other set.

---

\(^1\) Strictly speaking, there are certain abstract objects which create paradoxes if used as elements of a set — e.g., the set of all sets. Such matters will not concern us.

\(^2\) "Iff" is shorthand for "if and only if".
1f) The sets under discussion are **unordered** in the sense that the order in which the elements of a set are written makes no difference to the definition of the set, e.g.,

\[ \{7, 3\} = \{3, 7\}. \]

This follows directly from the definition of set equality given above.

1g) Repetition in the writing of the elements of a set makes no difference to the definition of an unordered set, e.g.,

\[ \{\text{Ann, Sue}\} = \{\text{Ann, Sue, Ann}\} \quad \text{and} \quad \{1, 2, 1\} = \{1, 2\}. \]

Once again, this follows from the definition of set equality.

1h) A is a **subset** of B — denoted \( A \subset B \) — if \( x \in A \implies x \in B \), i.e., if every element of A is also an element of B. If A is not a subset of B, we write \( A \not\subset B \). Note that \( A \subset A \) for any set A and, by convention, \( \emptyset \subset A \) for any set A. If \( A \subset B \), then we may also write \( B \supset A \), i.e., B is a **superset** of A.

1i) If \( A \subset B \) but \( A \neq B \), then A is a **proper** subset of B. Stated differently, A is a proper subset of B if \( A \subset B \) and there exists \( x_0 \) such that \( x_0 \not\in A \) but \( x_0 \in B \).

1j) Comparing the previous definitions of set equality and of a subset yields the following: \( A = B \) iff both \( A \subset B \) and \( B \subset A \).

1k) The **intersection** of two sets A and B consists of those elements belonging to both. Formally:

\[ A \cap B = \{ x \mid x \in A, x \in B \}. \]

If \( A \cap B = \emptyset \), then A and B are said to be **disjoint**. Note that \( (A \cap B) \subset A \) and \( (A \cap B) \subset B \).

1l) Intersections of more than two sets are similarly defined:

\[ \bigcap_{i=1}^{n} A_i = \{ x \mid x \in A_i \text{ for all } i = 1 \text{ to } n \}. \]

1m) The **union** of two sets A and B consists of those elements belonging to *at least one* of the two sets. Formally:

\[ A \cup B = \{ x \mid x \in A \text{ or } x \in B \}. \]

For more than two sets, we have:

\[ \bigcup_{i=1}^{n} A_i = \{ x \mid x \in A_i \text{ for some } i \}. \]

1n) The **cartesian product** (or simply the product) of A and B is the set of all possible ordered pairs formed by drawing the first element of each pair from A and the second element from B:

\[ A \times B = \{ (x, y) \mid x \in A, y \in B \}. \]

Note that, in general, \( A \times B \neq B \times A \).
For \( n \) sets, the cartesian product is written as:

\[
A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{ (x_1, x_2, \ldots, x_n) \mid x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n \},
\]

where \((x_1, x_2, \ldots, x_n)\) is an ordered set (see next section for a discussion of ordered sets).

1o) The **sum** of \( A \) and \( B \) is the set of all possible sums formed by summing an element of \( A \) and an element of \( B \) (assuming, of course, that the sum operation is defined for those elements):

\[
A + B = \{ (x + y) \mid x \in A, y \in B \}.
\]

For \( n \) sets, the sum is written as:

\[
\sum_{i=1}^{n} A_i = \{ (x_1 + x_2 + \cdots + x_n) \mid x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n \}.
\]

1p) Let \( A \subset B \). Then \( A^c \) (the complement of \( A \) in \( B \)) is the set of elements which do not belong to \( A \) but do belong to \( B \):

\[
A^c = \{ x \mid x \notin A, x \in B \}.
\]

Note that the complement of \( A \) will depend on the set \( B \) as well as on \( A \).

1q) The set difference \( B \setminus A \) is the set of elements belonging to \( B \) but not to \( A \):

\[
B \setminus A = \{ x \mid x \in B, x \notin A \}.
\]

This definition is similar to that of the complement of \( A \) in \( B \), \( A^c \). The difference is that in the case of a set difference it is not required that \( A \subset B \) (should it so happen that \( A \) is a subset of \( B \), then \( A^c \) and \( B \setminus A \) will be the same). The set difference is often written as \( B - A \), but I have not used this notation in order to avoid creating the impression that a set difference is calculated in a similar way to a set sum — it is calculated quite differently.

1r) A multiple of \( A \) is derived by multiplying each element of \( A \) by the same number \( t \) (assuming, of course, that the operation of multiplication by \( t \) is defined for those elements):

\[
tA = \{ y \mid y = tx, x \in A \}.
\]

2. Ordered Sets

2a) **Ordered sets** are sets for which the order (or position or structure) in which elements appear matters for the definition of the set. The most familiar example of an ordered set is the number pair which gives the co-ordinates on a graph with \( x \) and \( y \) axes. These sets take the general form \((x, y)\) — the first element gives the \( x \) co-ordinate and the second element gives the \( y \) co-ordinate; plainly, \((1, 2)\) and \((2, 1)\) are different sets since they correspond to different points.
2b) Two ordered sets containing the same elements appearing in a different order (or position or structure) are different sets. The repetition of elements also changes the set. Thus for an ordered set:

\[(1, 2) \neq (2, 1) \quad \text{and} \quad (1, 2) \neq (1, 2, 1)\].

Two ordered sets \(A\) and \(B\) are equal iff the following conditions are both satisfied: (i) \(A\) and \(B\) have the same number of elements, arranged in the same structure or pattern (ii) the elements in the corresponding positions in sets \(A\) and \(B\) are equal.

In common with unordered sets, the members of ordered sets may be objects of any sort.

2c) Because both ordered and unordered sets can contain objects of any kind, it is possible to have ordered sets whose elements are unordered sets and vice versa, e.g., we could have an unordered set containing ordered pairs:

\[
\{ (1, 2), (3, 5), (4, 1) \}.
\]

It remains an unordered set because, e.g.,

\[
\{ (1, 2), (3, 5), (4, 1) \} = \{ (4, 1), (1, 2), (3, 5) \}.
\]

The Cartesian product of \(n\) sets is another example of an unordered set with ordered sets as its elements.

3. Numbers

3a) The counting numbers or natural numbers are the set:

\[N = \{ 1, 2, 3, 4, \ldots \}.$

3b) Integers consist of the counting numbers and their negative counterparts, \(-1, -2, -3 \ldots\) plus the number 0:

\[Z = \{ \ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots \}.
\]

3c) We say that an integer \(b \neq 0\) is a factor of another integer \(a \neq 0\) iff there exists an integer \(c \neq 0\) such that

\[a = b \cdot c.
\]

An integer \(n > 1\) is said to be a prime number if its only positive factors are 1 and itself. An integer \(n > 1\) that is not a prime is said to be a composite number.\(^3\)

The following unique prime decomposition theorem is of some use:

---

\(^3\) Simon & Blume p. 849 state that the first six prime numbers are 1, 2, 3, 5, 7 and 11. This is contrary to the normal definition which holds that 1 is a special case, being neither prime nor composite. This is for reasons of convenience. There are a lot of theorems about prime numbers, some of which do not hold true for the number 1. Thus, it is more convenient to exclude 1 from the list of prime numbers than to qualify those theorems by saying that they hold “for all prime numbers except 1”.
Every integer \( n > 1 \) is either a prime or a product of primes. Further, the factorisation of an integer into a product of primes is unique, i.e., there is a unique set of primes, \( p_1, \ldots, p_r \), and a unique set of exponents, \( \alpha_1, \ldots, \alpha_r \) (where each \( \alpha_i \) is a positive integer), such that

\[
    n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.
\]

This has two corollaries:

**Corollary 1.** Every factor of \( n \) has the form

\[
    p_1^{\beta_1} \cdots p_r^{\beta_r},
\]

where, for each \( i \), \( \beta_i \) is an integer satisfying \( 0 \leq \beta_i \leq \alpha_i \).

**Corollary 2.** A prime number \( p \) is a factor of a non-zero product of integers \( a \cdot b \) if and only if it is a factor of \( a \) and/or \( b \). More generally, a prime number \( p \) is a factor of a non-zero product of integers \( a_1 \cdot a_2 \cdots a_k \) if and only if it is a factor of at least one \( a_i \) (\( i = 1, \ldots, k \)).

Note that it is essential to Corollary 2 that \( p \) be prime; the result is not true if \( p \) is composite, e.g., the composite number 10 is a factor of \( 5 \cdot 4 \) even though it is not a factor of 5 or 4.

**3d) Rational** numbers consist of all the numbers that can be expressed as the ratio of two integers, i.e., they take the general form

\[
    q = \frac{m}{n},
\]

where \( m \) and \( n \) are integers with \( n \neq 0 \) (integers themselves are therefore special cases of the rational numbers, corresponding to the case of \( n = 1 \)). The set of rational numbers may be formally written as:

\[
    \mathbb{Q} = \{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}\setminus\{0\} \}
\]

(\( \mathbb{Z}\setminus\{0\} \) is the set difference of \( \mathbb{Z} \) and \( \{0\} \), i.e., all of the elements of \( \mathbb{Z} \) except for the element 0).

Equivalently, rational numbers are all the numbers that can be expressed as either a terminating or (eventually) repeating decimal, e.g., \( q = .25 \) or \( q = .3333\ldots \) or \( q = .1325252525\ldots \).

**Note.** The term “rational” is derived from the word “ratio” (as in rational) and has nothing to do with rationality in the sense of consistent or sane behaviour.

**3e) Irrational** numbers consist of all the numbers that \textit{cannot} be expressed as a ratio of integers or, equivalently, \textit{cannot} be expressed as a terminating or repeating decimal. When expressed as a decimal, irrational numbers continue forever without ever falling into a (permanent) repeating pattern (they might repeat a number sequence several times, but the repetition is always broken eventually). The decimal is thus a source of “endless novelty”. Examples are the numbers \( \sqrt{2} \) and \( \pi \) (i.e., the ratio of the circumference of a circle to its diameter).

**3f) Real** numbers consist of the rational and the irrational numbers. Real numbers are often termed the “reals” for short.
3g) The real numbers are dense. This means that, given any two distinct real numbers, \( a \) and \( b \), there always exists a number \( c \) that lies between them, no matter how close \( a \) and \( b \) are to each other. For example, the average of the two numbers \((a + b)/2\) lies between \( a \) and \( b \). This means that, given a real number \( a \), there is no such thing as the “next” real number; for any number \( b \) that is larger than \( a \), there is always a number \( c \) that satisfies \( a < c < b \). In this respect real numbers differ from integers — there is such a thing as a next integer.

The rational numbers are also dense, as are the irrational numbers. Moreover, they are dense relative to each other, i.e., given any two distinct rational numbers, \( a \) and \( b \), there always exists an irrational number \( c \) that lies between them and vice versa.

3h) We denote the set of all real numbers by \( \mathbb{R} \). The set of all non-negative real numbers (those \( \geq 0 \)) is denoted by \( \mathbb{R}_+ \) and the set of all positive real numbers (those \( > 0 \)) is denoted by \( \mathbb{R}^+ \).

3i) In working with sets of numbers, it is important to be clear on the notational conventions that govern them. Suppose, for example, that we have a set

\[ S_1 = \{ x \in \mathbb{R} \mid 0 \leq x \leq 10 \} \]

Then this set is to be interpreted as the set of real numbers between 0 and 10; it is not restricted just to all \( x \) values between 0 and 10. Indeed, the set

\[ S_2 = \{ y \in \mathbb{R} \mid 0 \leq y \leq 10 \} \]

is the same set as \( S_1 \). Moreover, if \( z = 7 \), then that \( z \) value belongs to both sets. In recognition of the fact that the particular choice of letter does not matter, \( x \) in the definition of \( S_1 \) and \( y \) in the definition of \( S_2 \) are referred to as “dummy variables”; their only role is to stand for any number satisfying the conditions that define membership of the set.

3j) Operations with real numbers satisfy various well-known rules, such as the Commutative Law, which states that \( x + y = y + x \) and \( x \cdot y = y \cdot x \) for all \( x, y \in \mathbb{R} \). See Simon & Blume p. 849 for a complete list.

3k) Let \( S \) be a subset of \( \mathbb{R} \). Then \( a \in \mathbb{R} \) is a lower bound of \( S \) if \( a \leq s \) for all \( s \in S \). Similarly \( b \in \mathbb{R} \) is an upper bound of \( S \) if \( s \leq b \) for all \( s \in S \).

If \( a \) is a lower bound of \( S \) and is \( \geq \) all other lower bounds of \( S \), then we say that \( a \) is the greatest lower bound of \( S \). Another name for a greatest lower bound (glb) is an infimum, often abbreviated to \( \text{inf} \).

If \( b \) is an upper bound of \( S \) and is \( \leq \) all other upper bounds of \( S \), then we say that \( b \) is the least upper bound of \( S \). Another name for a least upper bound (lub) is a supremum, often abbreviated to \( \text{sup} \).

We have the following proposition:

For any non-empty \( S \subset \mathbb{R} \), if \( S \) has a lower bound, then it has a greatest lower bound \( a \in \mathbb{R} \). Similarly, if \( S \) has an upper bound, then it has a least upper bound \( b \in \mathbb{R} \).

There are three points to note here. First, we do not assert that \( S \) has a greatest lower bound or least upper bound. We only assert that it has those things if it has a lower bound or upper bound respectively. It may not have a lower bound at all, in which case it won’t have a greatest lower bound. Similarly for upper bounds. The set of real numbers
\( \mathbb{R} \) has neither an upper nor a lower bound. The set of natural numbers has a lower bound but no upper bound.

Second, the glb or lub are guaranteed to belong to \( \mathbb{R} \): they may or may not belong to \( S \), e.g., if
\[
S = \{ x \in \mathbb{R} \mid 5 < x < 9 \},
\]
then \( S \) has a glb of 5 and a lub of 9, neither of which is a member of the set.

Third, given a set of real numbers, if a glb and/or lub exist, then they too are real numbers. By contrast, given a set of rational numbers, if a glb and/or lub exist, then there is no guarantee that they are rational numbers (they are only guaranteed to be real), e.g., the set
\[
S = \{ x \in \mathbb{Q} \mid 0 < x < \sqrt{2} \}
\]
consists entirely of rational numbers but has a least upper bound of \( \sqrt{2} \), which is irrational. Similarly, given a set of irrational numbers, if a glb and/or lub exist, then there is no guarantee that they are irrational numbers, e.g., the set
\[
\{ \pi, \pi/2, \pi/3, \pi/4, \ldots \}
\]
consists entirely of irrational numbers, yet it has a greatest lower bound of 0, which is rational.

The fact that sets of real numbers have greatest lower bounds and least upper bounds that are likewise real — whereas sets of rational numbers and sets of irrational numbers lack the analogous property — gives the set of real numbers a “completeness” property that rational and irrational numbers alone do not possess. It is this “completeness” which makes the set of real numbers a suitable basis for the development of calculus, whereas the rational numbers (by themselves) and the irrational numbers (by themselves) are not suitable. For example, if you tried to develop calculus using only rational numbers, then some derivatives would turn out to be irrational, in the same way that sets of rational numbers can have glbs and lubs that are irrational.

### 4. Absolute Values

4a) The absolute value of a number \( x \) is denoted by \( |x| \). It is defined as follows:
\[
|x| = \begin{cases} 
  x & \text{if } x \geq 0 \\
  -x & \text{if } x < 0 
\end{cases}
\]  
(1)
e.g., \(|4| = 4\), whereas \(|-9| = -(-9) = 9\).

4b) \(|x| < a \) for \( a > 0 \) is equivalent to
\[
-a < x < a.
\]  
(2)
This can be shown by applying the definition given by (1). Using that definition, \(|x| < a \) can be written as:
\[
\begin{align*}
x < a & \quad \text{if } x \geq 0 \\
-x < a & \quad \text{if } x < 0
\end{align*}
\]
Using the property that multiplying both sides of an inequality by a negative number reverses the direction of the inequality, the second of these conditions can be written as $x > -a$ if $x < 0$ or, equivalently, $-a < x$ if $x < 0$. Thus there are two possible intervals for $x$: $0 \leq x < a$ and $-a < x < 0$. Combining them gives (2).

4c) Reasoning in exactly the same way, we may show that $|x - x_0| < a$ is equivalent to $-a < x - x_0 < a$. Adding $x_0$ to all three “sides”, we get $x_0 - a < x < x_0 + a$ as another expression equivalent to $|x - x_0| < a$.

5. Necessary and Sufficient Conditions

5a) When we say that $A$ is necessary for $B$ (where $A$ and $B$ are mathematical properties or some other types of properties), we mean that $A$ is a requirement in order for $B$ to be true. There may, however, be other requirements, so the truth of $A$ does not guarantee that $B$ will be true.

When we say that $A$ is sufficient for $B$, we mean that the truth of $A$ is all that is needed to ensure that $B$ is true. However, other conditions besides $A$ might cause $B$ to be true, so $B$ might still be true even if $A$ is not.

If $A$ is both necessary and sufficient for $B$, then the “howevers” in the preceding sentences may be omitted, i.e., $A$ has to be true in order for $B$ to be true and the truth of $A$ guarantees the truth of $B$.

As examples, consider the following statements:

$A$: $x$ is less than ten
$B$: $x$ is less than eight
$C$: $x$ is an integer
$D$: $x$ is a rational number
$E$: $x$ is a negative number
$F$: $(x + 3)$ is less than eleven

Exercise. For different pairs of propositions from the list above, identify if one proposition is necessary for the other, sufficient for the other, neither, or both.

5b) The following four statements are equivalent:

$A$ is necessary for $B$ (3)
not $B$ is necessary for not $A$ (4)
not $A$ is sufficient for not $B$ (5)
$B$ is sufficient for $A$ (6)

The pattern embodied in the above four statements may be stated as follows: Starting from a given statement, any statement created by making two of the following three changes...
(more generally, an even number of changes) is equivalent to the original statement. The three possible changes are: (i) swapping the positions of \(A\) and \(B\) (with \(A\) and \(B\) retaining their original “not” qualifiers, if present), (ii) changing from necessary to sufficient or vice versa, (iii) changing both \(A\) to not \(A\) and \(B\) to not \(B\) or vice versa (i.e., changing \(A\) to not \(A\) and \(B\) to not \(B\) counts as one change).

One particular set of changes is sufficiently common to have been given a name. If the positions of \(A\) and \(B\) are swapped and the “not switch” is made, then the resulting proposition is known as the **contrapositive** of the original proposition. In the list above, the contrapositive of (3) is (4) and the contrapositive of (5) is (6).

The advantage of knowing these equivalences is simply that it means that if you wish to prove a statement in one of the four forms (e.g., suppose that \(A\) is the statement \(x < 10\) and \(B\) is the statement \(x < 8\) and that you wish to prove that \(A\) is necessary for \(B\)), then you have the option of doing this by proving any of the three equivalent statements — this may be easier than proving the statement in which you are primarily interested.

Note regarding switch (iii) (the “not switch”), that a double “not” gives the original proposition, e.g., if

\[
\text{not } A \text{ is necessary for } B, \tag{7}
\]

then applying switch (iii) gives

\[
A \text{ is necessary for not } B.
\]

To get a statement equivalent to (7), we need a second switch, e.g., we may switch positions to get:

\[
\text{not } B \text{ is necessary for } A.
\]

**Exercise.** Find the other two statements that are equivalent to (7).

**Note.** If only a position switch is made (switch (i)), then we have what is known as the **converse** proposition. This is not equivalent to the original proposition, i.e., if the original proposition is true, then the converse *may or may not* be true, depending on the proposition in question.

5c)  Purely as a matter of notation and terminology, the following are equivalent ways of stating that \(A\) is **necessary** for \(B\) (and hence that \(B\) is **sufficient** for \(A\)):

- \(A\) if \(B\) (or: if \(B\), then \(A\))
- \(A\) is implied by \(B\)
- \(A \Leftarrow B\)

The following are equivalent ways of stating that \(A\) is **sufficient** for \(B\) (and hence that \(B\) is **necessary** for \(A\)):

- \(A\) only if \(B\)
- \(A\) implies \(B\)
- \(A \Rightarrow B\)

The following are equivalent ways of stating that \(A\) is **necessary** and **sufficient** for \(B\):

- \(A\) if and only if \(B\)
- \(A\) implies and is implied by \(B\)
- \(A \iff B\)
6. Methods of Proof

6a) To prove a statement like \( A \) is sufficient for \( B \), it is possible to follow one of three main routes. The first and simplest route is to reason directly from \( A \) to \( B \), e.g., if \( A \) is \( x < 5 \) and \( B \) is \( x < 8 \), then one simply notes that \( x < 5 \) and \( 5 < 8 \) together imply that \( x < 8 \), i.e., \( A \) is sufficient for \( B \).

6b) The second route is to use a proof by contradiction. Note that the distinction between a direct proof and a proof by contradiction is independent of whether one is trying to prove, say, “\( A \) is sufficient for \( B \)” or one of the three statements equivalent to this. The classic example of a proof by contradiction, familiar from high school, is the proof that \( \sqrt{2} \) is irrational (see Simon & Blume, p. 855 for this proof).

The general idea may be illustrated as follows. Suppose we wish to prove some proposition, e.g., that \( A \) implies \( B \). We reason as follows. Either the proposition is true or it is false, i.e., either

(i) \( A \) implies \( B \), or
(ii) \( A \) does not imply \( B \).

There are no other possibilities. Accordingly, if we can disprove (ii), then, by a process of elimination, (i) must be true.

The way we disprove (ii) is to suppose, hypothetically, that (ii) is true, i.e., \( A \) does not imply \( B \). We then show (if we can) that this hypothesis leads to a logical contradiction. On the assumption that mathematics is logically consistent (so that a true proposition cannot lead to a contradiction), we can conclude from this that our hypothesis is false, i.e., that it is false that \( A \) does not imply \( B \). If (ii) is false, then that means that (i) must be true, i.e., \( A \) implies \( B \).

Proofs by contradiction are central to mathematics (and hence to economics). It is worth recording, however, that a minority group of mathematicians (known as the “intuitionists”) regards such proofs as suspect.

As an example of a proof by contradiction, we will prove:

**Theorem.** There is an infinite number of prime numbers.

**Proof.** Assume the contrary, i.e., there is a total of \( n \) prime numbers, where \( n \) is some finite number. Denote these by \( p_1, p_2, \ldots, p_n \). Now form a new number \( A \) which equals the product of these primes plus 1, i.e.,

\[
A = 1 + p_1 \cdot p_2 \cdot p_3 \cdots p_n. \tag{8}
\]

Now, since each prime number is at least 2, the product of all of the primes must be larger than any single prime. Thus \( A \) is larger than any of the primes and hence is not a prime, i.e., it is a composite. Thus, by the unique prime decomposition theorem, it must have a prime number as a factor. Yet we see from (8) that dividing \( A \) by any prime number will leave a remainder of 1, i.e., \( A \) does not have a prime number as a factor. We have thus reached a contradiction, and this contradiction shows that our original hypothesis that there is only a finite number of primes must be false. Accordingly, we may conclude that the number of prime numbers is infinite.

6c) The third method of proof is an induction proof. These are used for certain propositions which involve an integer \( n \) in their statement. The basic approach here involves two steps.
(i) The theorem is shown to be true for \( n = 1 \).

(ii) It is shown that if the theorem is true for some integer \( k \), then it must also be true for \( k + 1 \). Importantly, this demonstration must assume nothing about \( k \) other than that \( k \geq 1 \).

Steps (i) and (ii) together imply that the theorem is true for all integer values \( \geq 1 \). This is for the following reason. The truth of the proposition for \( n = 1 \) and (ii) means that it must be true for \( n = 2 \). The truth of the proposition for \( n = 2 \) and (ii) means that it must be true for \( n = 3 \). By continuing to reason in this way, we can show that the proposition is true for any integer \( n \geq 1 \).

**Note.** While step (i) normally involves \( n = 1 \), it is possible to use \( n = n_0 \) for any integer \( n_0 \) (\( n_0 = 0 \) is fairly common). One then must assume that \( k \) in step (ii) is any integer \( \geq n_0 \).

The proof then establishes the correctness of the theorem for any \( n \geq n_0 \).

An example of an induction proof is the following:

**Theorem.** Consider the following product:

\[
\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \left(1 - \frac{1}{4}\right) \left(1 - \frac{1}{9}\right) \left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{n^2}\right).
\]

Then, for all \( n \geq 2 \):

\[
\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n + 1}{2n}.
\]  \hspace{1cm} (9)

**Proof.** We first show that (9) is true for \( n = 2 \). In that case:

\[
\text{LHS} = \left(1 - \frac{1}{2^2}\right) \quad \text{and} \quad \text{RHS} = \frac{2 + 1}{2 \cdot 2}.
\]

Plainly LHS = RHS, so part (i) of the induction proof is established.

For part (ii), assume that (9) is true for \( n = k \), where \( k \) is some integer \( \geq 2 \), i.e.,

\[
\prod_{i=2}^{k} \left(1 - \frac{1}{i^2}\right) = \frac{k + 1}{2k}.
\]  \hspace{1cm} (10)

We must use this to show that (9) is true for \( n = k + 1 \), i.e.,

\[
\prod_{i=2}^{k+1} \left(1 - \frac{1}{i^2}\right) = \frac{k + 2}{2(k + 1)}.
\]  \hspace{1cm} (11)

Now

\[
\prod_{i=2}^{k+1} \left(1 - \frac{1}{i^2}\right) = \prod_{i=2}^{k} \left(1 - \frac{1}{i^2}\right) \left(1 - \frac{1}{(k+1)^2}\right)
\]

\[
= \frac{k + 1}{2k} \left(1 - \frac{1}{(k+1)^2}\right) \quad \text{from (10)}
\]

\[
= \frac{k + 1}{2k} \cdot \frac{(k+1)^2 - 1}{(k+1)^2}
\]
\[ \frac{1}{2k} \left( \frac{(k+1)^2 - 1}{k+1} \right) = \frac{1}{2k} \cdot \frac{k^2 + 2k}{k+1} = \frac{k+2}{2(k+1)}, \]

i.e.,

\[ \prod_{i=2}^{k+1} \left( 1 - \frac{1}{i^2} \right) = \frac{k+2}{2(k+1)}, \]

which is (11). This completes the proof.

7. Functions

7a) Given two sets \( X \) and \( Y \), a function from \( X \) to \( Y \), written \( f: X \to Y \), is a rule that associates with each element \( x \in X \) a unique element \( f(x) \in Y \). The set \( X \) is called the domain of the function. The set \( Y \) goes under various names including codomain, target and target space. The element \( f(x) \) is called the value of the function at \( x \) or the image of \( x \) under \( f \). The set of all the \( f(x) \) values is called the range of the function, denoted \( f(X) \), i.e., \( f(X) = \{ f(x) \in Y \mid x \in X \} \).

The domain and the codomain can be freely chosen, subject to two restrictions:

(i) \( X \) must be such that \( f(x) \) is meaningful for all \( x \in X \), e.g., if \( f(x) = 1/x \), then \( X \) cannot include the element zero.

(ii) \( Y \) must be large enough to contain the range of \( f \); it can, however, be larger if this is desired, e.g., if \( X = \mathbb{R} \) and \( f(x) = x^2 \), then the range of \( f \) consists of all real numbers greater than or equal to zero (i.e., \( f(X) = \mathbb{R}_+ \)), so the codomain can be any set that contains \( \mathbb{R}_+ \). Thus both \( Y = \mathbb{R}_+ \) and \( Y = \mathbb{R} \) are examples of admissible codomains, but \( Y = \{ y \mid y \geq 2 \} \) is not admissible since it does not contain all of the range of \( f \), i.e., there exist \( x \in X \) such that \( f(x) \notin Y \) (\( x = 0 \), for example).

7b) Subject to the qualifications given above, the domain and codomain can be any sets whatsoever. In particular, there is no need for their elements to be numbers. For example, the domain could consist of the names of different cars (e.g., \( X = \{ \text{Holden}, \text{Daewoo}, \text{Porsche} \} \)) and the codomain could be: \( Y = \{ \text{Australian Made, Foreign Made} \} \). The function rule connecting these two sets would be: \( f(\text{Holden}) = \text{Australian Made}, f(\text{Daewoo}) = \text{Foreign Made} \) and \( f(\text{Porsche}) = \text{Foreign Made} \). Alternatively, the codomain could consist of all real numbers between 100 and 300, i.e., \( Y = \{ y \in \mathbb{R} \mid 100 \leq y \leq 300 \} \). The function rule connecting \( X \) and \( Y \) could involve selecting from \( Y \) the number that corresponds to the maximum speed in kilometres per hour of each car in \( X \), e.g., one could have \( f(\text{Holden}) = 200, f(\text{Daewoo}) = 190 \) and \( f(\text{Porsche}) = 260 \).

7c) The definition of a function consists of its domain, codomain and the rule for associating elements of the domain with elements of the codomain; a change to any one of these three things produces a new function, e.g.,

\[ y = x^2 \quad \text{for all} \ x \in \mathbb{R}_+ \]

and
\[ y = x^2 \quad \text{for all } x \in \mathbb{R} \]

are two different functions.

Domains and codomains are often not specified explicitly and must be inferred from the context and the restrictions listed earlier that must be obeyed when specifying a domain and codomain (that \( f(x) \) be defined for all \( x \in X \) etc.). Sometimes the precise choice of domain and codomain makes a significant practical difference, sometimes it does not.
APPENDIX: Tips on Algebraic Manipulation

A1. Numerical Equations

A1a) An equation containing one or more variables may have no solutions (e.g., \(x + 1 = x\)), a unique solution (e.g., \(x + 1 = 3\)), or multiple solutions (e.g., \(x^2 = 4\)). Another way of putting this is that an equation may be always false (when it has no solution), true for only one value of the equation variables (when there is a unique solution), or true for multiple values of the equation variables (when there are multiple solutions).

An equation containing only constants is either always true or always false, e.g., \(5 = 5\) is always true, whereas \(5 = 7\) is always false.

In what follows I will repeatedly list changes that can be made to an equation that do not change its set of solutions. For equations (initially) containing only constants and hence either always true or always false, an “unchanged solution set” is to be interpreted as meaning that the equation is “still always true” or “still always false”, as appropriate.

A1b) Adding an expression to, or subtracting it from, both sides of an equation always leaves the solution values to the equation unchanged (this is true regardless of whether the expression added or subtracted is a constant or a function).

A1c) Multiplying or dividing both sides of an equation by an expression will leave the set of solution values unchanged if the expression is always non-zero. If, however, the expression is zero for some values of the equation variables, then matters are more complicated. The following cases should be noted:

(i) The set of solution values will change if both sides are multiplied by an expression that is zero for some value of the equation variable(s). For example, \(7 = 3\) is always false, but if both sides are multiplied by \(x\), then we get \(7x = 3x\) which has the solution \(x = 0\) (so that the equation is a true statement for that value of \(x\)). Similarly, \(x + 1 = 6\) has only one solution, \(x = 5\) but, if both sides are multiplied by \((x - 2)\) (which is zero at \(x = 2\)), then we get \((x + 1)(x - 2) = 6(x - 2)\) which has two solutions, \(x = 5\) and \(x = 2\).

(ii) The set of solution values will change both sides are divided by an expression which is zero at a value of the equation variable(s) that solves the original equation. This can happen in two ways. The first occurs where the divisor can be factored out of both sides of the equation. For example, the expression \(3x(x + 5) = 9(x + 5)\) has two solutions, \(x = -5\) and \(x = 3\). Plainly the expression \((x + 5)\) is zero at \(x = -5\) (i.e., at one of the solution values of \(x\)) and can be factored out of both sides of the equation. Hence division of both sides of the equation by \((x + 5)\) yields the equation \(3x = 9\) which has only one solution, \(x = 3\). The second way that the set of solution values can be reduced is when the divisor cannot be factored out of both sides of an equation. For example, the equation \(3^2x = 9x\) has solutions of \(x = 0\) and \(x = 2\). The expression \((x - 2)\) is zero at \(x = 2\) (i.e., at one of the solution values of \(x\)) but cannot be factored out of both sides of the equation. If both sides of the equation are divided by \((x - 2)\), we get:

\[
\frac{3^2x}{x - 2} = \frac{9x}{x - 2}
\]

4 Note that this change may merely be formal, e.g., if \(x = 0\) is multiplied throughout by \(x\) to yield \(x^2 = 0\), then the solution set is increased from a single root of zero to a repeated root of zero.

5 Again, this change may be merely formal as in, e.g., the change from a repeated root to a single root.
This has a single solution of \( x = 0 \) since it is undefined at the second solution of the original equation, \( x = 2 \). Thus the effect on reducing the number of solutions is the same as it would have been if \( (x - 2) \) could be factored out from both sides.\(^6\)

On the other hand, dividing both sides by an expression which is zero at a value of the equation variable(s) that does not solve the original equation leaves the set of solution values unchanged. Consider, for example, the equation \( 3x(x + 5) = 9(x + 5) \) discussed above (with solutions of \(-5\) and \(3\)). If both sides are divided by, say, \((x - 1)\), then we get

\[
\frac{3x(x + 5)}{x - 1} = \frac{9(x + 5)}{x - 1},
\]

which still has solutions of \( x = -5 \) and \( x = 3 \).

\textbf{A1d)} The equality relation is transitive, i.e., if \( a = b \) and \( b = c \) are both true, then \( a = c \) is true.

\textbf{A1e)} When solving simultaneous equations, it is a common solution technique to add an expression to, or subtract it from, both sides, or to multiply or divide both sides by an expression. These techniques are extremely valuable. However, when the procedure involves multiplication or division, the possibility that the expression may be zero should be considered since, as shown above, this can add to or reduce the number of solutions. To guard against the introduction of spurious solutions, the final solution should ideally be tested by substituting it back into the original equations.

\section*{A2. Inequalities}

\textbf{A2a)} Inequalities, like equalities, may or may not have solutions. Examples are:

\[
x < 8 \quad \text{and} \quad x < x - 1,
\]

respectively. Inequalities involving only constants are always true or always false, e.g., \( 5 < 7 \) is always true and \( 5 < 4 \) is always false. As with equalities, for inequalities (initially) containing only constants and hence either always true or always false, an “unchanged solution set” is to be interpreted in what follows as meaning that the inequality is “still always true” or “still always false”, as appropriate.

\textbf{A2b)} As with equations, adding an expression to, or subtracting it from, both sides of an inequality leaves the set of its solution values unchanged.

\textbf{A2c)} Multiplication or division of both sides of an inequality by a positive expression preserves the inequality (i.e., the solution set is the same as before the multiplication/division if we retain the original direction of the inequality) whereas multiplication or division of both sides of an inequality by a negative expression reverses the direction of the inequality (i.e., the solution set is the same as before the multiplication/division if we reverse the original direction of the inequality). For example,

\[
x < 10 \quad \text{and} \quad -3 \cdot x > -3 \cdot 10
\]

\footnote{\(6\) In a way, these cases simply illustrate the rule that “division by zero is not allowed”. However, applying this rule is made complicated by the fact that an expression may be zero for some \( x \) and non-zero for other \( x \).}
have the same solution set.

When an inequality is multiplied by zero, both sides are equal and hence the inequality is not satisfied.

The effect of multiplication or division by expressions with variable sign is difficult to succinctly summarise. It is generally necessary to divide into intervals the possible values that a variable may take and to give separate consideration to each, e.g., if both sides of the inequality \( 2 < 4 \) are multiplied by \( x \), then \( 2x < 4x \) is always true for positive \( x \), \( 2x = 4x \) for zero \( x \), and \( 2x > 4x \) is always true for negative \( x \).

**A2d)** Taking reciprocals of both sides of an inequality reverses the direction of the inequality if both sides have the same sign (i.e., both negative or both positive), but has no effect on the direction of the inequality if the two sides have opposite signs. Examples of reversal are:

\[
5 < 7 \quad \text{and} \quad \frac{1}{5} > \frac{1}{7}, \quad -3 > -8 \quad \text{and} \quad -\frac{1}{3} < -\frac{1}{8}.
\]

An example of non-reversal is

\[
-10 < 5 \quad \text{and} \quad -\frac{1}{10} < \frac{1}{5}.
\]

As before, if the sign of a side can vary, then it is generally necessary to give separate consideration to different intervals of the variables.

**A2e)** The inequality relation is transitive, i.e., if \( a < b \) and \( b < c \) are both true, then \( a < c \) is true.

**A2f)** The weak inequality, "\( a \leq b \)" means "one of \( a < b \) and \( a = b \) holds". Note that it is not necessary that there be any doubt about whether \( a < b \) or \( a = b \) in order for \( a \leq b \) to be used. It is, for example, perfectly correct to write: \( 5 \leq 7 \) and \( 7 \leq 7 \). Put differently, \( a \leq b \) is simply the negation of \( a > b \), i.e., \( a \leq b \) is true if and only if \( a > b \) is not true. Thus \( 5 \leq 7 \) and \( 7 \leq 7 \) are true because \( 5 > 7 \) and \( 7 > 7 \) are not true.

Similarly, "\( a \geq b \)" means "one of \( a > b \) and \( a = b \) holds". Put differently, \( a \geq b \) is the negation of \( a < b \).

**Exercise.** What is the effect of squaring both sides of an inequality?

### A3. Exponents and Logs

Provided all expressions are defined, exponents satisfy the following rules:

(i) \( x^r \cdot x^s = x^{r+s} \).
(ii) \( x^r \cdot y^r = (x \cdot y)^r \).
(iii) \( x^{-r} = \frac{1}{x^r} \).
(iv) \( x^r / x^s = x^{r-s} \).
(v) \( (x^r)^s = x^{rs} \).
(vi) \( x^0 = 1 \).

Provided all expressions are defined, logarithms satisfy the following rules:

(vii) \( \log(x \cdot y) = \log x + \log y \).
(viii) \( \log(1/x) = -\log x \).
(ix) \( \log(x/y) = \log x - \log y \).
(x) \( \log(x^r) = r \log x \).
(xi) \( \log 1 = 0 \).