Chapter One
Sets, Logic, Numbers, Relations, Orderings, Graphs, and Functions

In this chapter we review basic terminology and results concerning sets, logic, numbers, relations, orderings, graphs, and functions. This material is used throughout the book.

1.1 Sets
A set \{x, y, \ldots\} is a collection of elements. A set can include either a finite or infinite number of elements. The set \(X\) is finite if it has a finite number of elements; otherwise, \(X\) is infinite. The set \(X\) is countably infinite if \(X\) is infinite and its elements are in one-to-one correspondence with the positive integers. The set \(X\) is countable if it is either finite or countably infinite.

Let \(X\) be a set. Then,

\[ x \in X \] (1.1.1)

means that \(x\) is an element of \(X\). If \(w\) is not an element of \(X\), then we write

\[ w \notin X. \] (1.1.2)

No set can be an element of itself. Therefore, there does not exist a set that includes every set. The set with no elements, denoted by \(\varnothing\), is the empty set. If \(X \neq \varnothing\), then \(X\) is nonempty.

Let \(X\) and \(Y\) be sets. The intersection of \(X\) and \(Y\) is the set of common elements of \(X\) and \(Y\), which is given by

\[ X \cap Y \triangleq \{x: x \in X \text{ and } x \in Y\} = \{x \in X: x \in Y\} = \{x \in Y: x \in X\} = \varnothing \cap X, \] (1.1.3)

The union of \(X\) and \(Y\) is the set of elements in either \(X\) or \(Y\), which is the set

\[ X \cup Y \triangleq \{x: x \in X \text{ or } x \in Y\} = Y \cup \varnothing. \] (1.1.4)

The complement of \(X\) relative to \(Y\) is

\[ Y \setminus \varnothing \triangleq \{x \in Y: x \not\in X\}. \] (1.1.5)

If \(Y\) is specified, then the complement of \(X\) is

\[ \varnothing \setminus \varnothing \triangleq Y \setminus X. \] (1.1.6)

The symmetric difference of \(X\) and \(Y\) is the set of elements that are in either \(X\) or \(Y\) but not both, which is given by

\[ X \ominus Y \triangleq (X \cup Y)\setminus(X \cap Y). \] (1.1.7)

If \(x \in X\) implies that \(x \in Y\), then \(X\) is a subset of \(Y\) (equivalently, \(Y\) contains \(X\)), which is written as

\[ X \subseteq Y. \] (1.1.8)

Equivalently,

\[ Y \supseteq X. \] (1.1.9)
Note that $\mathcal{X} \subseteq \mathcal{Y}$ if and only if $\mathcal{X} \setminus \mathcal{Y} = \emptyset$. Furthermore, $\mathcal{X} = \mathcal{Y}$ if and only if $\mathcal{X} \subseteq \mathcal{Y}$ and $\mathcal{Y} \subseteq \mathcal{X}$. If $\mathcal{X} \subseteq \mathcal{Y}$ and $\mathcal{X} \neq \mathcal{Y}$, then $\mathcal{X}$ is a proper subset of $\mathcal{Y}$ and we write $\mathcal{X} \subset \mathcal{Y}$. The sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint if $\mathcal{X} \cap \mathcal{Y} = \emptyset$. A partition of $\mathcal{X}$ is a set of pairwise-disjoint and nonempty subsets of $\mathcal{X}$ whose union is equal to $\mathcal{X}$.

The symbols $\mathbb{N}$, $\mathbb{P}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ denote the sets of nonnegative integers, positive integers, integers, rational numbers, and real numbers, respectively.

A set cannot have repeated elements. Therefore, $\{x, x\} = \{x\}$. A multiset is a finite collection of elements that allows for repetition. The multiset consisting of two copies of $x$ is written as $(x, x)_{\text{ms}}$. For example, the roots of the polynomial $p(x) = (x - 1)^2$ are the elements of the multiset $(1, 1)_{\text{ms}}$, while the prime factors of 72 are the elements of the multiset $(2, 2, 2, 3, 3)_{\text{ms}}$.

The operations $\cap$, $\cup$, $\setminus$, $\emptyset$, and $\times$ and the relations $\subseteq$ and $\subset$ extend to multisets. For example,

$$\{x, x\}_{\text{ms}} \cup \{x, x, x\}_{\text{ms}} = \{x, x, x\}_{\text{ms}}.$$  \hspace{1cm} (1.1.10)

By ignoring repetitions, a multiset can be converted to a set, while a set can be viewed as a multiset with distinct elements.

The Cartesian product $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ of sets $\mathcal{X}_1, \ldots, \mathcal{X}_n$ is the set consisting of tuples of the form $(x_1, \ldots, x_n)$, where, for all $i \in \{1, \ldots, n\}$, $x_i \in \mathcal{X}_i$. A tuple with $n$ components is an $n$-tuple. The components of a tuple are ordered but need not be distinct. Therefore, a tuple can be viewed as an ordered multiset. We thus write

$$(x_1, \ldots, x_n) \in \mathcal{X}_1^n \triangleq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n.$$  \hspace{1cm} (1.1.11)

$\mathcal{X}^n$ denotes $\mathcal{X}_1^n \triangleq \mathcal{X}$.

**Definition 1.1.1.** A sequence $(x_i)_{i=1}^\infty = (x_1, x_2, \ldots)$ is a tuple with a countably infinite number of components. Now, let $i_1 < i_2 < \cdots$. Then, $(x_i)_{i=1}^\infty$ is a subsequence of $(x_i)_{i=1}^\infty$.

Let $\mathcal{X}$ be a set, and let $X \triangleq (x_i)_{i=1}^\infty$ be a sequence whose components are elements of $\mathcal{X}$; that is, $\{x_1, x_2, \ldots\} \subseteq \mathcal{X}$. For convenience, we write either $X \subseteq \mathcal{X}$ or $X \subset \mathcal{X}$, where $X$ is viewed as a set and the multiplicity of the components of the sequence is ignored. For sequences $X, Y \subset \mathbb{R}^n$, define $X + Y \triangleq (x_i + y_i)_{i=1}^\infty$ and $X \circ Y \triangleq (x_i \circ y_i)_{i=1}^\infty$, where $\circ$ denotes component-wise multiplication. In the case $n = 1$, we define $XY \triangleq (xy)_{i=1}^\infty$.

### 1.2 Logic

Every statement is either true or false, and no statement is both true and false. A proof is a collection of statements that verify that a statement is true. A conjecture is a statement that is believed to be true but whose proof is not known.

Let $A$ and $B$ be statements. The not of $A$ is the statement (not $A$), the and of $A$ and $B$ is the statement $(A \land B)$, and the or of $A$ and $B$ is the statement $(A \lor B)$. The statement $(A \lor B)$ does not contradict the statement $(A \land B)$; hence, the word “or” is inclusive. The exclusive or of $A$ and $B$ is the statement $(A \Leftrightarrow B)$, which is $[(A \land \neg B) \lor (B \land \neg A)]$. Equivalently, $(A \Leftrightarrow B)$ is the statement $[(A \land B) \lor (\neg A \land \neg B)]$, that is, $A \lor B$, but not both. Note that $(A \land B) = (B \land A)$, $(A \lor B) = (B \lor A)$, and $(A \Leftrightarrow B) = (B \Leftrightarrow A)$.

Let $A$, $B$, and $C$ be statements. Then, the statements $(A \land B \land C)$ and $(A \lor B \lor C)$ are ambiguous. For clarity, we thus write, for example, $(A \land (B \lor C))$ and $(A \lor (B \land C))$. In words, we write “$A$ and either $B$ or $C$” and “$A$ or both $B$ and $C$,” respectively, where “either” and “both” signify parentheses. Furthermore,

$$(A \land B) \lor (A \land C)$$  \hspace{1cm} (1.2.1)

$$(A \lor B) \land (A \lor C).$$  \hspace{1cm} (1.2.2)
Let \( A \) be a statement. To analyze statements involving logic operators, define \( \text{truth}(A) = 1 \) if \( A \) is true, and \( \text{truth}(A) = 0 \) if \( A \) is false. Then,

\[
\text{truth}(\text{not } A) = \text{truth}(A) + 1,
\]

where \( 0 + 0 = 0, 1 + 0 = 0 + 1 = 1, \) and \( 1 + 1 = 0 \). Therefore, \( A \) is true if and only if \( (\text{not } A) \) is false, while \( A \) is false if and only if \( (\text{not } A) \) is true. Note that

\[
\text{truth}(\text{not}(\text{not } A)) = \text{truth}(\text{not } A) + 1
= [\text{truth}(A) + 1] + 1
= \text{truth}(A).
\]

Furthermore, note that \( \text{truth}(A) + \text{truth}(A) = 0 \) and \( \text{truth}(A) \text{truth}(A) = \text{truth}(A) \).

Let \( A \) and \( B \) be statements. Then,

\[
\text{truth}(A \text{ and } B) = \text{truth}(A) \text{truth}(B),
\]

\[
\text{truth}(A \text{ or } B) = \text{truth}(A) \text{truth}(B) + \text{truth}(A) + \text{truth}(B),
\]

\[
\text{truth}(A \text{ xor } B) = \text{truth}(A) + \text{truth}(B).
\]

Hence,

\[
\text{truth}(A \text{ and } B) = \min \{\text{truth}(A), \text{truth}(B)\},
\]

\[
\text{truth}(A \text{ or } B) = \max \{\text{truth}(A), \text{truth}(B)\}.
\]

Consequently, \( \text{truth}(A \text{ and } B) = \text{truth}(B \text{ and } A) \), \( \text{truth}(A \text{ or } B) = \text{truth}(B \text{ or } A) \), and \( \text{truth}(A \text{ xor } B) = \text{truth}(B \text{ xor } A) \). Furthermore, \( \text{truth}(A \text{ and } A) = \text{truth}(A \text{ or } A) = \text{truth}(A) \), and \( \text{truth}(A \text{ xor } A) = 0 \).

Let \( A \) and \( B \) be statements. The \textit{implication} \( (A \implies B) \) is the statement \( [(\text{not } A) \text{ or } B] \). Therefore,

\[
\text{truth}(A \implies B) = \text{truth}(A) \text{truth}(B) + \text{truth}(A) + 1.
\]

The implication \( (A \implies B) \) is read as either “if \( A \), then \( B \),” “if \( A \) holds, then \( B \) holds,” or “\( A \) implies \( B \).” The statement \( A \) is the \textit{hypothesis}, while the statement \( B \) is the \textit{conclusion}. If \( (A \implies B) \), then \( A \) is a \textit{sufficient condition} for \( B \), and \( B \) is a \textit{necessary condition} for \( A \). It follows from (1.2.9) that, if \( A \) and \( B \) are true, then \( (A \implies B) \) is true; if \( A \) is true and \( B \) is false, then \( (A \implies B) \) is false; and, if \( A \) is false, then \( (A \implies B) \) is true whether or not \( B \) is true. For example, both implications \( [(2 + 2 = 5) \implies (3 + 3 = 6)] \) and \( [(2 + 2 = 5) \implies (3 + 3 = 8)] \) are true. Finally, note that \( [(A \implies B) \text{ and } A] = A \text{ and } B \).

A \textit{predicate} is a statement that depends on a variable. Let \( \mathcal{X} \) be a set, let \( x \in \mathcal{X} \), and let \( A(x) \) be a predicate. There are two ways to use a predicate to create a statement. An \textit{existential statement} has the form

\[
\text{there exists } x \in \mathcal{X} \text{ such that } A(x) \text{ holds},
\]

whereas a \textit{universal statement} has the form

\[
\text{for all } x \in \mathcal{X}, A(x) \text{ holds}.
\]

Note that

\[
\text{truth}[\text{there exists } x \in \mathcal{X} \text{ such that } A(x) \text{ holds}] = \max_{x \in \mathcal{X}} \text{truth}[A(x)],
\]

\[
\text{truth}[\text{for all } x \in \mathcal{X}, A(x) \text{ holds}] = \min_{x \in \mathcal{X}} \text{truth}[A(x)].
\]

An \textit{argument} is an implication whose hypothesis and conclusion are predicates that depend on the same variable. In particular, letting \( x \) denote a variable, and letting \( A(x) \) and \( B(x) \) be predicates,
the implication \( A(x) \implies B(x) \) is an argument. For example, for each real number \( x \), the implication \( ((x = 1) \implies (x + 1 = 2)) \) is an argument. Note that the variable \( x \) links the hypothesis and the conclusion, thereby making this implication useful for the purpose of inference. In particular, for all real numbers \( x \), \( \text{truth}((x = 1) \implies (x + 1 = 2)) = 1 \). The statements (for all \( x \), \( A(x) \implies B(x) \)) holds and (there exists \( x \) such that \( A(x) \implies B(x) \)) holds are inferences.

Let \( A \) and \( B \) be statements. The bidirectional implication \( A \iff B \) is the statement \( [(A \implies B) \land (A \iff B)] \), where \( (A \iff B) \) means \( (B \implies A) \). If \( (A \iff B) \), then \( A \) and \( B \) are equivalent. Furthermore,

\[
\text{truth}(A \iff B) = \text{truth}(A) + \text{truth}(B) + 1.
\]

Therefore, \( A \) and \( B \) are equivalent if and only if either both \( A \) and \( B \) are true or both \( A \) and \( B \) are false.

Let \( A \) and \( B \) be statements, and assume that \( (A \iff B) \). Then, \( A \) holds if and only if \( B \) holds. The implication \( A \implies B \) (the “only if” part) is necessity, while \( B \implies A \) (the “if” part) is sufficiency.

Let \( A \) and \( B \) be statements. The converse of \( (A \implies B) \) is \( (B \implies A) \). Note that

\[
(A \implies B) \iff [(\neg A) \lor B] \\
\iff [\neg(\neg A) \lor \neg B] \\
\iff [\neg B \lor \neg A] \\
\iff (\neg B \implies \neg A).
\]

Therefore, the statement \( (A \implies B) \) is equivalent to its contrapositive \( [(\neg B) \implies (\neg A)] \).

Let \( A, B, A' \), and \( B' \) be statements, and assume that \( (A' \implies A \implies B \implies B') \). Then, \( (A' \implies B') \) is a corollary of \( (A \implies B) \).

Let \( A, B, A' \), and \( B' \) be statements, and assume that \( A \implies B \). Then, \( (A \implies B) \) is a strengthening of \( [(A \land A') \implies B] \). If, in addition, \( (A \implies A') \), then the statement \( [(A \land A') \implies B] \) has a redundant assumption.

An interpretation is a feasible assignment of true or false to all statements that comprise a statement. For example, there are four interpretations of the statement \( (A \land B) \), depending on whether \( A \) is assigned to be true or false and \( B \) is assigned to be true or false. Likewise, \( ((x = 1) \land (x = 2)) \) has three interpretations, which depend on the value of \( x \).

Let \( A_1, A_2, \ldots \) be statements, and let \( B \) be a statement that depends on \( A_1, A_2, \ldots \). Then, \( B \) is a tautology if \( B \) is true whether or not \( A_1, A_2, \ldots \) are true. For example, let \( B \) denote the statement \( (A \lor \neg A) \). Then,

\[
\text{truth}(A \lor \neg A) = 1,
\]

and thus the statement \( (A \lor \neg A) \) is true whether or not \( A \) is true. Hence, \( (A \lor \neg A) \) is a tautology. Likewise, \( (A \implies A) \) is a tautology. Furthermore, since

\[
\text{truth}((A \land B) \implies A) = \text{truth}(A)^2 \text{truth}(B) + \text{truth}(A) \text{truth}(B) + 1 = 1,
\]

it follows that \( (A \land B) \implies A \) is a tautology. Likewise, \( \text{truth}[(A \land \neg A) \implies B] = 1 \), and thus \( (A \land \neg A) \implies B \) is a tautology.

Let \( A_1, A_2, \ldots \) be statements, and let \( B \) be a statement that depends on \( A_1, A_2, \ldots \). Then, \( B \) is a contradiction if \( B \) is false whether or not \( A_1, A_2, \ldots \) are true. For example, let \( B \) denote the statement \( (A \land \neg A) \). Then,

\[
\text{truth}(A \land \neg A) = 0,
\]
and thus the statement \((A \text{ and not } A)\) is false whether or not \(A\) is true. Hence, \((A \text{ and not } A)\) is a contradiction.

Let \(A\) and \(B\) be statements. If the implication \((A \implies B)\) is neither a tautology nor a contradiction, then truth\((A \implies B)\) depends on the truth of the statements that comprise \(A\) and \(B\). For example, truth\((A \implies \text{not } A)\) = truth\((A) + 1\), and thus the statement \((A \implies \text{not } A)\) is true if and only if \(A\) is false, and false if and only if \(A\) is true. Hence, \((A \implies \text{not } A)\) is neither a tautology nor a contradiction. A statement that is neither a tautology nor a contradiction is a contingency. For example, the implication \([A \implies (A \text{ and } B)]\) is a contingency. Likewise, for each real number \(x\), truth\([x = 1 \implies (x = 2)]\) = truth\((x \neq 1)\), and thus the statement \([x = 1 \implies (x = 2)]\) is a contingency.

An argument that is a contingency is a theorem, proposition, corollary, or lemma. A theorem is a significant result; a proposition is a theorem of less significance. The primary role of a lemma is to support the proof of a theorem or a proposition. A corollary is a consequence of a theorem or a proposition. A fact is either a theorem, proposition, lemma, or corollary.

In order to visualize logic operations on predicates, it is helpful to replace statements with sets and logic operations by set operations; the truth of a statement can then be visualized in terms of Venn diagrams. To do this, let \(X\) be a set, for all \(x \in X\), let \(A(x)\) and \(B(x)\) be predicates, and define \(A = \{x \in X : \text{truth}(A(x)) = 1\}\) and \(B = \{x \in X : \text{truth}(B(x)) = 1\}\). Then, the logic operations “and,” “or,” “xor,” and “not” are equivalent to “\(\cap\),” “\(\cup\),” “\(\oplus\),” and “\(^\sim\)”, respectively. For example, \(\{x \in X : \text{truth}(\text{not } A(x)) \text{ and } B(x)\} = 1 = A^\sim \cap B\). Furthermore, since \([A(x) \implies B(x)]\) is equivalent to \([\text{not } A(x) \text{ or } B(x)]\), it follows that \(\{x \in X : \text{truth}(A(x) \implies B(x)) = 1\} = A^\sim \cup B\). Similarly, since \([A(x) \iff B(x)]\) is equivalent to \([A(x) \text{ or } B(x)]\) and \([\text{not } A(x)] \text{ or } B(x))\), it follows that \(\{x \in X : A(x) \iff B(x)\} = (A \cup B^\sim) \cap (A^\sim \cup B) = (A \cap B) \cup (A \cup B)^\sim\). Now, define \(X, A(x), B(x), A,\) and \(B\) as in the previous paragraph, and assume that, for all \(x \in X\), \(A(x) \implies B(x)\). Therefore, \(A^\sim \cup B = \{x \in X : \text{truth}(\text{not } A(x)) \text{ or } B(x)\} = 1 = X\), and thus \(A \setminus B = (A^\sim \cup B)^\sim = \{x \in X : \text{truth}(\text{not } A(x)) \text{ or } B(x)\} = 0 = \emptyset\). Consequently, \(A \subseteq B\). This means that the logic operator “\(\implies\)” is represented by “\(\subseteq\).” For example, for all \(x \in X\), let \(C(x)\) be a predicate, and define \(C = \{x \in X : \text{truth}(C(x)) = 1\}\). Then, for all \(x \in X\), truth\([A(x) \text{ and } B(x)] \implies C(x)\) = 1 if and only if \(A \cap B \subseteq C\). Likewise, for all \(x \in X\),

\[
\text{truth}([A(x) \text{ and } (B(x) \text{ or } C(x))] \iff [(A(x) \text{ and } B(x)) \text{ or } (A(x) \text{ and } C(x))]) = 1 \quad (1.2.18)
\]

if and only if

\[
A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \quad (1.2.19)
\]

Note that (1.2.19) represents a tautology.

### 1.3 Relations and Orderings

Let \(X, X_1\), and \(X_2\) be sets. A relation \(R\) on \((X_1, X_2)\) is a subset of \(X_1 \times X_2\). A relation \(R\) on \(X\) is a subset of \(X \times X\). Likewise, a multirelation \(R\) on \((X_1, X_2)\) is a multiset of \(X_1 \times X_2\), while a multirelation \(R\) on \(X\) is a multiset of \(X \times X\).

Let \(X\) be a set, and let \(R_1\) and \(R_2\) be relations on \(X\). Then, the sets \(R_1 \cap R_2, R_1 \cup R_2,\) and \(R_1 \setminus R_2\) are relations on \(X\). Furthermore, if \(R\) is a relation on \(X\) and \(X_0 \subseteq X\), then we define the restricted relation \(R|_{X_0} = R \cap (X_0 \times X_0)\), which is a relation on \(X_0\).

**Definition 1.3.1.** Let \(R\) be a relation on the set \(X\). Then, the following terminology is defined:

- i) \(R\) is reflexive if, for all \(x \in X\), it follows that \((x, x) \in R\).
- ii) \(R\) is symmetric if, for all \((x_1, x_2) \in R\), it follows that \((x_2, x_1) \in R\).
- iii) \(R\) is transitive if, for all \((x_1, x_2) \in R\) and \((x_2, x_3) \in R\), it follows that \((x_1, x_3) \in R\).
- iv) \(R\) is an equivalence relation if \(R\) is reflexive, symmetric, and transitive.
Proposition 1.3.2. Let $R_1$ and $R_2$ be relations on the set $X$. If $R_1$ and $R_2$ are (reflexive, symmetric) relations, then so are $R_1 \cap R_2$ and $R_1 \cup R_2$. If $R_1$ and $R_2$ are (transitive, equivalence) relations, then so is $R_1 \cap R_2$.

**Definition 1.3.3.** Let $R$ be a relation on the set $X$. Then, the following terminology is defined:

i) The *complement* $R^c$ of $R$ is the relation $R^c = (X \times X) \setminus R$.

ii) The *support* $\text{supp}(R)$ of $R$ is the smallest subset $X_0$ of $X$ such that $R$ is a relation on $X_0$.

iii) The *reversal* $\text{rev}(R)$ of $R$ is the relation $\text{rev}(R) = \{(y, x) : (x, y) \in R\}$.

iv) The *shortcut* $\text{shortcut}(R)$ of $R$ is the relation $\text{shortcut}(R) = \{(x, y) \in X \times X : x$ and $y$ are distinct and there exist $k \geq 1$ and $x_1, \ldots, x_k \in X$ such that $(x, x_1), (x_1, x_2), \ldots, (x_k, y) \in R\}$.

v) The *reflexive hull* $\text{ref}(R)$ of $R$ is the smallest reflexive relation on $X$ that contains $R$.

vi) The *symmetric hull* $\text{sym}(R)$ of $R$ is the smallest symmetric relation on $X$ that contains $R$.

vii) The *transitive hull* $\text{trans}(R)$ of $R$ is the smallest transitive relation on $X$ that contains $R$.

viii) The *equivalence hull* $\text{equiv}(R)$ of $R$ is the smallest equivalence relation on $X$ that contains $R$.

**Proposition 1.3.4.** Let $R$ be a relation on the set $X$. Then, the following statements hold:

i) $\text{ref}(R) = R \cup \{(x, x) : x \in X\}$.

ii) $\text{sym}(R) = R \cup \text{rev}(R)$.

iii) $\text{trans}(R) = R \cup \text{shortcut}(R)$.

iv) If $R$ is symmetric, then $\text{trans}(R) = \text{sym}(\text{trans}(R))$.

v) $\text{equiv}(R) = \text{trans}(\text{sym}(\text{ref}(R)))$.

Furthermore, the following statements hold:

vi) $R$ is reflexive if and only if $R = \text{ref}(R)$.

vii) The following statements are equivalent:

a) $R$ is symmetric.

b) $R = \text{sym}(R)$.

c) $R = \text{rev}(R)$.

viii) $R$ is transitive if and only if $R = \text{trans}(R)$.

ix) $R$ is an equivalence relation if and only if $R = \text{equiv}(R)$.

For an equivalence relation $R$ on the set $X$, $(x_1, x_2) \in R$ is denoted by $x_1 \equiv x_2$. If $R$ is an equivalence relation and $x \in X$, then the subset $E_x = \{y \in X : y \equiv x\}$ of $X$ is the *equivalence class of $x$ induced by $R$*.

**Theorem 1.3.5.** Let $R$ be an equivalence relation on a set $X$. Then, the set $\{E_x : x \in X\}$ of equivalence classes induced by $R$ is a partition of $X$.

**Proof.** Since $X = \bigcup_{x \in X} E_x$, it suffices to show that, if $x, y \in X$, then either $E_x = E_y$ or $E_x \cap E_y = \emptyset$. Hence, let $x, y \in X$, and suppose that $E_x$ and $E_y$ are not disjoint so that there exists $z \in E_x \cap E_y$. Thus, $(x, z) \in R$ and $(z, y) \in R$. Now, let $w \in E_x$. Then, $(w, x) \in R$, $(x, z) \in R$, and $(z, y) \in R$ imply that $(w, y) \in R$. Hence, $w \in E_y$, which implies that $E_x \subseteq E_y$. By a similar argument, $E_y \subseteq E_x$. Consequently, $E_x = E_y$. \qed

The following result, which is the converse of Theorem 1.3.5, shows that a partition of a set $X$ defines an equivalence relation on $X$.

**Theorem 1.3.6.** Let $X$ be a set, let $\mathcal{P}$ be a partition of $X$, and define the relation $R$ on $X$ by $(x, y) \in R$ if and only if $x$ and $y$ belong to the same element of $\mathcal{P}$. Then, $R$ is an equivalence relation on $X$.

Theorem 1.3.5 shows that every equivalence relation induces a partition, while Theorem 1.3.6
shows that every partition induces an equivalence relation.

**Definition 1.3.7.** Let $\mathcal{X}$ be a set, let $\mathcal{P}$ be a partition of $\mathcal{X}$, and let $X_0 \subseteq \mathcal{X}$. Then, $X_0$ is a representative subset of $\mathcal{X}$ relative to $\mathcal{P}$ if, for all $X \in \mathcal{P}$, exactly one element of $X_0$ is an element of $X$.

**Definition 1.3.8.** Let $\mathcal{R}$ be a relation on the set $\mathcal{X}$. Then, the following terminology is defined:

i) $\mathcal{R}$ is antisymmetric if $(x_1, x_2) \in \mathcal{R}$ and $(x_2, x_1) \in \mathcal{R}$ imply that $x_1 = x_2$.

ii) $\mathcal{R}$ is a partial ordering if $\mathcal{R}$ is reflexive, antisymmetric, and transitive.

iii) $(\mathcal{X}, \mathcal{R})$ is a partially ordered set if $\mathcal{R}$ is a partial ordering.

Let $(\mathcal{X}, \mathcal{R})$ be a partially ordered set. Then, $(x_1, x_2) \in \mathcal{R}$ is denoted by $x_1 \leq x_2$. If $x_1 \leq x_2$ and $x_2 \leq x_1$, then, since $\mathcal{R}$ is antisymmetric, it follows that $x_1 = x_2$. Furthermore, if $x_1 \leq x_2$ and $x_2 \leq x_3$, then, since $\mathcal{R}$ is transitive, it follows that $x_1 \leq x_3$.

**Definition 1.3.9.** Let $(\mathcal{X}, \mathcal{R})$ be a partially ordered set. Then, the following terminology is defined:

i) Let $S \subseteq \mathcal{X}$. Then, $y \in \mathcal{X}$ is a lower bound for $S$ if, for all $x \in S$, it follows that $y \leq x$.

ii) Let $S \subseteq \mathcal{X}$. Then, $y \in \mathcal{X}$ is an upper bound for $S$ if, for all $x \in S$, it follows that $x \leq y$.

The following result shows that every partially ordered set has at most one lower bound that is “greatest” and at most one upper bound that is “least.”

**Lemma 1.3.10.** Let $(\mathcal{X}, \mathcal{R})$ be a partially ordered set, and let $S \subseteq \mathcal{X}$. Then, there exists at most one lower bound $y \in \mathcal{X}$ for $S$ such that every lower bound $x \in \mathcal{X}$ for $S$ satisfies $x \leq y$. Furthermore, there exists at most one upper bound $y \in \mathcal{X}$ for $S$ such that every upper bound $x \in \mathcal{X}$ for $S$ satisfies $y \leq x$. 

**Proof.** For $i = 1, 2$, let $y_i \in \mathcal{X}$ be such that $y_i$ is a lower bound for $S$ and, for all $x \in \mathcal{X}$, $x \leq y_i$. Therefore, $y_1 \leq y_2$ and $y_2 \leq y_1$. Since “$\leq$” is antisymmetric, it follows that $y_1 = y_2$. □

**Definition 1.3.11.** Let $(\mathcal{X}, \mathcal{R})$ be a partially ordered set. Then, the following terminology is defined:

i) Let $S \subseteq \mathcal{X}$. Then, $y \in \mathcal{X}$ is the greatest lower bound for $S$ if $y$ is a lower bound for $S$ and every lower bound $x \in \mathcal{X}$ for $S$ satisfies $x \leq y$. In this case, we write $y = \text{glb}(S)$.

ii) Let $S \subseteq \mathcal{X}$. Then, $y \in \mathcal{X}$ is the least upper bound for $S$ if $y$ is an upper bound for $S$ and every upper bound $x \in \mathcal{X}$ for $S$ satisfies $y \leq x$. In this case, we write $y = \text{lub}(S)$.

iii) $(\mathcal{X}, \leq)$ is a lattice if, for all distinct $x, y \in \mathcal{X}$, the set $\{x, y\}$ has a least upper bound and a greatest lower bound.

iv) $(\mathcal{X}, \leq)$ is a complete lattice on $\mathcal{X}$ if every subset $S$ of $\mathcal{X}$ has a least upper bound and a greatest lower bound.

**Example 1.3.12.** Consider the partially ordered set $(\mathcal{P}, \leq)$, where $m \leq n$ indicates that $n$ is an integer multiple of $m$. For example, $3 \leq 21$, but it is not true that $2 \leq 3$. Next, note that the greatest lower bound of a subset $S$ of $\mathcal{P}$ is the greatest common divisor of the elements of $S$. For example, $\text{glb}(\{9, 21\}) = 3$. Likewise, the least upper bound of a subset $S$ of $\mathcal{P}$ is the least common multiple of the elements of $S$. For example, $\text{lub}(\{2, 3, 4\}) = 12$. Therefore, $(\mathcal{P}, \leq)$ is a lattice. Next, note that 1 is a lower bound for every subset of $\mathcal{P}$. Since every subset of $\mathcal{P}$ has a smallest element in the usual ordering, it follows that every subset of $\mathcal{P}$ has a greatest lower bound. In particular, $\text{glb}(\mathcal{P}) = 1$. However, no subset of $\mathcal{P}$ that has an infinite number of elements has an upper bound. Therefore, $(\mathcal{P}, \leq)$ is not a complete lattice. Now, consider $(\mathcal{N}, \leq)$. Note that 1 is a lower bound for every subset of $\mathcal{N}$. Since every subset of $\mathcal{N}$ has a smallest element in the usual ordering, it follows that every subset of $\mathcal{N}$ has a greatest lower bound. In particular, $\text{glb}(\mathcal{N}) = 1$. Furthermore, for all $m \in \mathcal{N}$, $0 = m - m$, and thus 0 is an upper bound for every subset of $\mathcal{N}$. In particular, since 0 is the unique upper bound of $\mathcal{N}$, it follows that 0 is the least upper bound of $\mathcal{N}$. Hence, $(\mathcal{N}, \leq)$ is a complete lattice. □
Proposition 1.3.13. Let $(X, \preceq)$ be a lattice, and let $S_1, S_2 \subseteq X$. Then,
\[
\text{glb}(S_1 \cup S_2) = \text{glb}[S_1 \cup \{\text{glb}(S_2)\}], \quad \text{lub}(S_1 \cup S_2) = \text{lub}[S_1 \cup \{\text{lub}(S_2)\}].
\] (1.3.1)

Definition 1.3.14. Let $(X, \preceq)$ be a partially ordered set. Then, $\preceq$ is a total ordering on $X$ if, for all $x, y \in X$, either $(x, y) \in \preceq$ or $(y, x) \in \preceq$.

Let $S \subseteq \mathbb{R}$. Then, it is traditional to write $\inf S$ and $\sup S$ for $\text{glb}(S)$ and $\text{lub}(S)$, respectively, where “inf” and “sup” denote infimum and supremum, respectively. If $S = \emptyset$, then we define $\inf \emptyset \triangleq \infty$ and $\sup \emptyset \triangleq -\infty$. Finally, if $S$ has no lower bound, then we write $\inf S = -\infty$, whereas, if $S$ has no upper bound, then we write $\sup S = \infty$.

The following result uses the fact that “$\subseteq$” is a partial ordering on every collection of sets.

Proposition 1.3.15. Let $S$ be a collection of sets. Then,
\[
\text{glb}(S) = \bigcap_{S \in S} S, \quad \text{lub}(S) = \bigcup_{S \in S} S.
\] (1.3.2)

Hence, for all $S \in S$,
\[
\text{glb}(S) \subseteq S \subseteq \text{lub}(S).
\] (1.3.3)

Let $S = (S_i)_{i=1}^{\infty}$ be a sequence of sets. Then, by viewing $S$ as the collection of sets $\{S_1, S_2, \ldots\}$, it follows that
\[
\text{glb}(S) = \bigcap_{i=1}^{\infty} S_i, \quad \text{lub}(S) = \bigcup_{i=1}^{\infty} S_i.
\] (1.3.4)

Hence, for all $i \geq 1$,
\[
\text{glb}(S) \subseteq S_i \subseteq \text{lub}(S).
\] (1.3.5)

Note that $\text{glb}(S)$ and $\text{lub}(S)$ are independent of the ordering of the sequence $S$.

Proposition 1.3.16. Let $S$ be a collection of sets, let $A$ be a set, let $S_0 = \{S \in S: A \subseteq S\}$, and assume that $S_0 \neq \emptyset$. Then, $A \subseteq \text{glb}(S_0)$. If, in addition, $\text{glb}(S_0) \in S_0$, then $\text{glb}(S_0)$ is the smallest element of $S$ that contains $A$ in the sense that, if $S \in S$ and $A \subseteq S$, then $\text{glb}(S_0) \subseteq S$.

Proposition 1.3.17. Let $S$ be a collection of sets, let $A$ be a set, and let $S_0 = \{S \in S: S \subseteq A\}$. Then, $\text{lub}(S_0) \subseteq A$. If, in addition, $\text{lub}(S_0) \in S_0$, then $\text{lub}(S_0)$ is the largest element of $S$ that is contained in $A$ in the sense that, if $S \in S$ and $S \subseteq A$, then $S \subseteq \text{lub}(S_0)$.

Definition 1.3.18. Let $S = (S_i)_{i=1}^{\infty}$ be a sequence of sets. Then, the essential greatest lower bound of $S$ is defined by
\[
\text{essglb}(S) = \bigcup_{j=1}^{\infty} \bigcap_{i=j}^{\infty} S_i,
\] (1.3.6)

and the essential least upper bound of $S$ is defined by
\[
\text{esslub}(S) = \bigcap_{j=1}^{\infty} \bigcup_{i=j}^{\infty} S_i.
\] (1.3.7)

Let $S = (S_i)_{i=1}^{\infty}$ be a sequence of sets. Then, the set $\text{essglb}(S)$ consists of all elements of $\bigcup_{i=1}^{\infty} S_i$ that belong to all but finitely many of the sets in $S$. Furthermore, the set $\text{esslub}(S)$ consists of all elements of $\bigcup_{i=1}^{\infty} S_i$ that belong to infinitely many of the sets in $S$. Therefore, $\text{essglb}(S)$ and $\text{esslub}(S)$ are independent of the ordering of the sequence $S$, and
\[
\text{glb}(S) \subseteq \text{essglb}(S) \subseteq \text{esslub}(S) \subseteq \text{lub}(S).
\] (1.3.8)
Note that \( \text{lub}(\mathcal{S}) \setminus \text{esslub}(\mathcal{S}) \) is the set of elements of \( \bigcup_{i=1}^{\infty} S_i \) that belong to at most finitely many of the sets in \( \mathcal{S} \).

**Example 1.3.19.** Consider the sequence of sets given by

\[
((1, 4), (1, 2), (1, 2, 3), (1, 2), (1, 2, 3), (1, 2), (1, 2, 3), \ldots).
\]

Then, (1.3.8) becomes \( \{1\} \subseteq \{1, 2\} \subseteq \{1, 2, 3\} \subseteq \{1, 2, 3, 4\} \).

**Definition 1.3.20.** Let \( \mathcal{S} \triangleq (S_i)_{i=1}^{\infty} \) be a sequence of sets, and assume that \( \text{essglb}(\mathcal{S}) = \text{esslub}(\mathcal{S}) \).

Then, the *essential limit* of \( \mathcal{S} \) is defined by

\[
\text{esslim}(\mathcal{S}) \triangleq \text{essglb}(\mathcal{S}) = \text{esslub}(\mathcal{S}).
\]

Let \( \mathcal{S} \triangleq (S_i)_{i=1}^{\infty} \) be a sequence of sets. Then, \( \mathcal{S} \) is *nonincreasing* if, for all \( i \in \mathbb{P} \), \( S_{i+1} \subseteq S_i \).

Furthermore, \( \mathcal{S} \) is *nondecreasing* if, for all \( i \in \mathbb{P} \), \( S_i \subseteq S_{i+1} \).

**Proposition 1.3.21.** Let \( \mathcal{S} \triangleq (S_i)_{i=1}^{\infty} \) be a sequence of sets. If \( \mathcal{S} \) is nonincreasing, then

\[
\text{esslim}(\mathcal{S}) = \text{glb}(\mathcal{S}) = \text{essglb}(\mathcal{S}) = \text{esslub}(\mathcal{S}).
\]

Furthermore, if \( \mathcal{S} \) is nondecreasing, then

\[
\text{esslim}(\mathcal{S}) = \text{essglb}(\mathcal{S}) = \text{esslub}(\mathcal{S}) = \text{lub}(\mathcal{S}).
\]

**Example 1.3.22.** Consider the nonincreasing sequence of sets

\[
(\mathbb{N}, \mathbb{N} \setminus \{1\}, \mathbb{N} \setminus \{1, 2\}, \mathbb{N} \setminus \{1, 2, 3\}, \ldots).
\]

Then, (1.3.8) becomes \( \{0\} = \{0\} = \{0\} \subseteq \mathbb{N} \).

Now, consider the nondecreasing sequence of subsets of \( \mathbb{R} \) given by

\[
((1], [1, 2], [1, 2, 3], [1, 2, 3, 4], \ldots).
\]

Then, (1.3.8) becomes \( \{1\} \subseteq \mathbb{P} = \mathbb{P} = \mathbb{P} \), where \( \mathbb{P} \) is the set of positive integers.

Let \( \mathcal{S} \triangleq (S_i)_{i=1}^{\infty} \) be a sequence of sets. Then, the sequence \( \mathcal{\hat{S}} \triangleq (\cap_{j=1}^{k} [\bigcup_{i=j}^{\infty} S_i])_{k=1}^{\infty} = (\bigcup_{i=k}^{\infty} S_i)_{k=1}^{\infty} = (\hat{S}_k)_{k=1}^{\infty} \) is nonincreasing. Hence,

\[
\text{esslub}(\mathcal{S}) = \text{esslim}(\mathcal{\hat{S}}) = \text{glb}(\mathcal{\hat{S}}) = \text{essglb}(\mathcal{\hat{S}}) = \text{esslub}(\mathcal{\hat{S}}).
\]

Furthermore, the sequence \( \mathcal{\hat{S}} \triangleq (\bigcup_{j=1}^{k} [\cap_{i=j}^{\infty} S_i])_{k=1}^{\infty} = (\cap_{i=k}^{\infty} S_i)_{k=1}^{\infty} = (\hat{S}_k)_{k=1}^{\infty} \) is nondecreasing. Hence,

\[
\text{essglb}(\mathcal{S}) = \text{esslim}(\mathcal{\hat{S}}) = \text{essglb}(\mathcal{\hat{S}}) = \text{esslub}(\mathcal{\hat{S}}) = \text{lub}(\mathcal{\hat{S}}).
\]

### 1.4 Directed and Symmetric Graphs

Let \( X \) be a finite, nonempty set, and let \( R \) be a multirelation on \( X \). Then, the pair \( \mathcal{G} = (X, R) \) is a *directed multigraph*. The elements of \( X \) are the *nodes* of \( \mathcal{G} \), while the elements of \( R \) are the *directed edges* of \( \mathcal{G} \). If \( R \) is a relation on \( X \), then \( \mathcal{G} = (X, R) \) is a *directed graph*. We focus on directed graphs, which have distinct (that is, nonrepeated) directed edges.

The directed graph \( \mathcal{G} = (X, R) \) can be visualized as a set of points in the plane representing the nodes in \( X \) connected by the directed edges in \( R \). Specifically, the directed edge \( (x, y) \in R \) from \( x \) to \( y \) can be visualized as a directed line segment or curve connecting node \( x \) to node \( y \). The direction of a directed edge can be denoted by an arrowhead. A directed edge of the form \((x, x)\) is a *self-directed edge*.

If the relation \( R \) is symmetric, then \( \mathcal{G} \) is a *symmetric graph*. In this case, it is convenient to represent the pair of directed edges \((x, y)\) and \((y, x)\) in \( R \) by a single edge \( \{x, y\} \), which is a subset of \( X \). For the self-directed edge \((x, x)\), the corresponding edge is the single-element self-edge \( \{x\} \). To illustrate these notions, consider a directed graph that represents a city with streets (directed edges).
connecting intersections (nodes). Each directed edge represents a one-way street, while the presence of the one-way street \((x, y)\) and its reverse \((y, x)\) represents a two-way street. A symmetric relation is a street plan consisting entirely of two-way streets (that is, edges) and thus no one-way streets (directed edges), whereas an antisymmetric relation is a street plan consisting entirely of one-way streets (directed edges) and thus no two-way streets (edges).

**Definition 1.4.1.** Let \(G = (X, R)\) be a directed graph. Then, the following terminology is defined:

i) If \(x, y \in X\) are distinct and \((x, y) \in R\), then \(y\) is the head of \((x, y)\) and \(x\) is the tail of \((x, y)\).

ii) If \(x, y \in X\) are distinct and \((x, y) \in R\), then \(x\) is a parent of \(y\), and \(y\) is a child of \(x\).

iii) If \(x, y \in X\) are distinct and either \((x, y) \in R\) or \((y, x) \in R\), then \(x\) and \(y\) are adjacent.

iv) If \(x \in X\) has no parent, then \(x\) is a root.

v) If \(x \in X\) has no child, then \(x\) is a leaf.

**Definition 1.4.2.** Let \(G = (X, R)\) be a directed graph. Then, the following terminology is defined:

i) The reversal of \(G\) is the graph \(\text{rev}(G) \triangleq (X, \text{rev}(R))\).

ii) The complement of \(G\) is the graph \(\bar{G} \triangleq (X, \bar{R})\).

iii) The reflexive hull of \(G\) is the graph \(\text{ref}(G) \triangleq (X, \text{ref}(R))\).

iv) The symmetric hull of \(G\) is the graph \(\text{sym}(G) \triangleq (X, \text{sym}(R))\).

v) The transitive hull of \(G\) is the graph \(\text{trans}(G) \triangleq (X, \text{trans}(R))\).

vi) The equivalence hull of \(G\) is the graph \(\text{equiv}(G) \triangleq (X, \text{equiv}(R))\).

vii) \(G\) is reflexive if \(R\) is reflexive.

viii) \(G\) is transitive if \(R\) is transitive.

ix) \(G\) is an equivalence graph if \(R\) is an equivalence relation.

x) \(G\) is antisymmetric if \(R\) is antisymmetric.

xi) \(G\) is partially ordered if \(R\) is a partial ordering on \(X\).

xii) \(G\) is totally ordered if \(R\) is a total ordering on \(X\).

xiii) \(G\) is a tournament if \(G\) is antisymmetric and \(\text{sym}(R) = X \times X \setminus \{(x, x) : x \in X\}\).

**Definition 1.4.3.** Let \(G = (X, R)\) be a directed graph. Then, the following terminology is defined:

i) The directed graph \(G' = (X', R')\) is a directed subgraph of \(G\) if \(X' \subseteq X\) and \(R' \subseteq R\).

ii) The directed subgraph \(G' = (X', R')\) of \(G\) is a spanning directed subgraph of \(G\) if \(\text{supp}(R) = \text{supp}(R')\).

iii) If \(X_0 \subseteq X\), then \(G|_{X_0} \triangleq (X_0, R|_{X_0})\).

iv) If \(G' = (X', R')\) is a directed graph, then \(G \cup G' \triangleq (X \cup X', R \cup R')\) and \(G \cap G' \triangleq (X \cap X', R \cap R')\).

v) For \(x, y \in X\), a directed walk in \(G\) from \(x\) to \(y\) is an \(n\)-tuple of directed edges of \(G\) of the form \(((x, y_1), (y_1, y_2), \ldots, (y_{n-1}, y)) \in R^n\) for all \(n \geq 2\). The length of the directed walk is \(n\). The nodes \(x, x_1, \ldots, x_{n-1}, y\) are the nodes of the walk. Furthermore, if \(n \geq 2\), then the nodes \(x_1, \ldots, x_{n-1}\) are the intermediate nodes of the walk.

vi) For \(x, y \in X\), a directed trail in \(G\) from \(x\) to \(y\) is a directed walk in \(G\) from \(x\) to \(y\) whose directed edges are distinct.

vii) For \(x, y \in X\), a directed path in \(G\) from \(x\) to \(y\) is a directed trail in \(G\) from \(x\) to \(y\) whose intermediate nodes are distinct and do not include \(x\) and \(y\).
viii) For \( x \in X \), a directed cycle in \( G \) at \( x \) is a directed path in \( G \) from \( x \) to \( x \) whose length is at least 2.

ix) \( G \) is directionally acyclic if \( G \) has no directed cycles.

x) If \( G \) has at least one directed cycle, then the directed period of \( G \) is the greatest common divisor of the lengths of the directed cycles of \( G \).

xi) \( G \) is directionally aperiodic if it has at least one directed cycle and the greatest common divisor of the lengths of the directed cycles in \( G \) is 1.

xii) A directed Hamiltonian path is a directed path whose nodes include all of the nodes of \( X \).

xiv) \( G \) is a directed tree if \( G \) has exactly one root \( x \) and, for all \( y \in X \) such that \( y \neq x \), \( y \) has exactly one parent.

xv) \( G \) is a directed forest if \( G \) is a union of disjoint directed trees.

xvi) \( G \) is a directed chain if \( G \) is a tree and has exactly one leaf.

xvii) \( G \) is directionally connected if, for all distinct \( x, y \in X \), there exist directed walks in \( G \) from \( x \) to \( y \) and from \( y \) to \( x \).

xviii) \( G \) is bipartite if there exist nonempty, disjoint sets \( X_1 \) and \( X_2 \) such that \( X = X_1 \cup X_2 \) and \( \mathcal{R} \cap (X_1 \times X_1) = \mathcal{R} \cap (X_2 \times X_2) = \emptyset \).

xix) The indegree of \( x \in X \) is \( \text{indeg}(x) \triangleq \text{card} \{ y \in X : y \text{ is a parent of } x \} \).

xx) The outdegree of \( x \in X \) is \( \text{outdeg}(x) \triangleq \text{card} \{ y \in X : y \text{ is a child of } x \} \).

xxi) Let \( X = X_1 \cup X_2 \), where \( X_1 \) and \( X_2 \) are nonempty and disjoint, and assume that \( X = \text{supp}(G) \). Then, \((X_1, X_2)\) is a directed cut of \( G \) if, for all \( x_1 \in X_1 \) and \( x_2 \in X_2 \), there does not exist a directed walk from \( x_1 \) to \( x_2 \).

A self-directed edge is a directed path; however, a self-directed edge is not a directed cycle.

A directed Hamiltonian cycle is both a directed Hamiltonian path and a directed cycle, both of which are directed paths.

**Definition 1.4.4.** Let \( G = (X, \mathcal{R}) \) be a symmetric graph. Then, the following terminology is defined:

i) For \( x, y \in X \), a walk in \( G \) connecting \( x \) and \( y \) is an \( n \)-tuple of edges of \( G \) of the form \(( (x, y) ) \in \mathcal{E} \) for \( n = 1 \) and \( \{ (x_1, x_2), \ldots, (x_{n-1}, y) \} \in \mathcal{E}^n \) for \( n \geq 2 \). The length of the walk is \( n \). The nodes \( x, x_1, \ldots, x_{n-1}, y \) are the nodes of the walk. Furthermore, if \( n \geq 2 \), then the nodes \( x_1, \ldots, x_{n-1} \) are the intermediate nodes of the walk.

ii) For \( x, y \in X \), a trail in \( G \) connecting \( x \) and \( y \) is a walk in \( G \) connecting \( x \) to \( y \) whose edges are distinct.

iii) For \( x, y \in X \), a path in \( G \) connecting \( x \) and \( y \) is a trail in \( G \) connecting \( x \) and \( y \) whose intermediate nodes are distinct and do not include \( x \) and \( y \).

iv) For \( x \in X \), a cycle in \( G \) at \( x \) is a path in \( G \) connecting \( x \) and \( x \) whose length is at least 3.

v) \( G \) is acyclic if \( G \) has no cycles.

vi) If \( G \) has at least one cycle, then the period of \( G \) is the greatest common divisor of the lengths of the cycles of \( G \).

vii) \( G \) is aperiodic if the period of \( G \) is 1.

viii) A Hamiltonian path is a path whose nodes include every node in \( X \).

ix) \( G \) is Hamiltonian if \( G \) has a Hamiltonian cycle \( \mathcal{P} \), which is a cycle such that every node in \( X \) is a node of \( \mathcal{P} \).

x) \( G \) is a tree if there exists a directed tree \( G' = (X, \mathcal{R}') \) such that \( G = \text{sym}(G') \).
1.5 Numbers

Let $x$ and $y$ be real numbers. Then, $x$ divides $y$ if there exists an integer $n$ such that $y = nx$. In this case, we write $x \mid y$. For example, $6 \mid 12$, $3 \mid -9$, $\pi \approx -2\pi$, $3 \mid 0$, and $0 \mid 0$. The notation $x \nmid y$ means that $x$ does not divide $y$.

Let $n_1, \ldots, n_k$ be integers, not all of which are zero. Then, the greatest common divisor of the set $\{n_1, \ldots, n_k\}$ is the positive integer defined by

$$\gcd\{n_1, \ldots, n_k\} \triangleq \max\{i \in \mathbb{P} : i \text{ divides } n_1, \ldots, n_k\}.$$  

For example, $\gcd\{5, 10\} = 5$, and $\gcd\{0, 2\} = 2$. The set $\{n_1, \ldots, n_k\}$ is coprime if $\gcd\{n_1, \ldots, n_k\} = 1$. For example, $\gcd\{-3, -7\} = 1$, and thus $-3 \mid -7$ is coprime.

Let $n_1, \ldots, n_k$ be nonzero integers. Then, the least common multiple of the set $\{n_1, \ldots, n_k\}$ is the positive integer defined by

$$\operatorname{lcm}\{n_1, \ldots, n_k\} \triangleq \min\{i \in \mathbb{P} : n_1, \ldots, n_k \text{ divide } i\}.$$  

For example, $\operatorname{lcm}\{-3, -7\} = 21$, and $\operatorname{lcm}\{-2, 3\} = 6$.

Let $m$ be a nonzero integer, and let $n$ be an integer. Then, $m \mid n$ if and only if $\gcd\{m, n\} = |m|$.

Let $n$ be an integer, and let $k$ be a positive integer. Furthermore, let $l$ be an integer, and let $r \in [0, k - 1]$ be an integer satisfying $n = kl + r$. Then, we write

$$r = \operatorname{rem}_k(n).$$  

(1.5.1)

where $r$ is the remainder after dividing $n$ by $k$. For example, $\operatorname{rem}_3(-11) = 1$ and $\operatorname{rem}_3(11) = 2$. Furthermore, $k \mid n$ if and only if $\operatorname{rem}_k(n) = 0$.

**Proposition 1.5.1.** Let $m$ and $n$ be integers, and let $k$ be a positive integer. Then,

$$\operatorname{rem}_k(n - m) = \operatorname{rem}_k(\operatorname{rem}_k(n) - \operatorname{rem}_k(m)).$$  

(1.5.2)

Furthermore, $k \mid n - m$ if and only if $\operatorname{rem}_k(n) = \operatorname{rem}_k(m)$.

**Definition 1.5.2.** Let $n$ and $m$ be integers, and let $k$ be a positive integer. Then, $n$ and $m$ are congruent modulo $k$ if $k$ divides $n - m$. In this case, we write

$$n \equiv m \pmod{k}.$$  

(1.5.3)

Proposition 1.5.1 implies that $n \equiv m$ if and only if the remainders of $n$ and $m$ after dividing by $k$...
differ by a multiple of $k$. For example, $-1 \equiv 3 \equiv 8 \equiv 26 \equiv 39$. Let $n$ be an integer. Then, $n$ is even if 2 divides $n$, whereas $n$ is odd if 2 does not divide $n$. Now, assume that $n \geq 2$. Then, $n$ is prime if, for all integers $m$ such that $2 \leq m < n$, $m$ does not divide $n$. Note that 2 is prime, but 1 is not prime. Letting $p_n$ denote the $n$th prime, it follows that

\[(p_i)_{i=1}^{25} = (2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97).\]

The $n$th harmonic number is denoted by

\[H_n \triangleq \sum_{i=1}^{n} \frac{1}{i}. \tag{1.5.4}\]

Then,

\[(H_i)_{i=0}^{10} = \left(0, 1, \frac{3}{2}, \frac{11}{6}, \frac{25}{12}, \frac{137}{40}, \frac{49}{10}, \frac{363}{70}, \frac{761}{10}, \frac{7129}{70}, \frac{7381}{70}, \frac{83711}{10}, \frac{86021}{10}\right).\]

For all $\alpha \in \mathbb{R}$, the $n$th generalized harmonic number of order $\alpha$ is denoted by

\[H_{n,\alpha} \triangleq \sum_{i=1}^{n} \frac{1}{i^\alpha}. \tag{1.5.5}\]

Define $H_0 \triangleq H_{0,\alpha} \triangleq 0$. Then,

\[(H_{i,2})_{i=0}^{10} = \left(0, 1, \frac{5}{4}, \frac{9}{4}, \frac{49}{36}, \frac{205}{144}, \frac{5269}{5760}, \frac{5369}{5760}, \frac{266681}{3600}, \frac{267749}{3600}, \frac{9777841}{3600}, \frac{9778141}{3600}, \frac{1968329}{176400}, \frac{305600}{176400}, \frac{6350400}{1270080}\right).\]

The symbol $\mathbb{C}$ denotes the set of complex numbers. The elements of $\mathbb{R}$ and $\mathbb{C}$ are scalars. Define

\[j \triangleq \sqrt{-1}. \tag{1.5.6}\]

Let $z \in \mathbb{C}$. Then, $z = x + yj$, where $x, y \in \mathbb{R}$. Define the complex conjugate $\overline{z}$ of $z$ by

\[\overline{z} \triangleq x - yj \tag{1.5.7}\]

and the real part $\text{Re } z$ of $z$ and the imaginary part $\text{Im } z$ of $z$ by

\[\text{Re } z \triangleq \frac{1}{2}(z + \overline{z}) = x, \quad \text{Im } z \triangleq \frac{1}{2i}(z - \overline{z}) = y. \tag{1.5.8}\]

Furthermore, the absolute value $|z|$ of $z$ is defined by

\[|z| \triangleq \sqrt{x^2 + y^2}. \tag{1.5.9}\]

Finally, the argument $\arg z \in (-\pi, \pi]$ of $z$ is defined by

\[\arg z \triangleq \begin{cases} 0, & y = x = 0, \\ \text{atan} \frac{x}{y}, & x > 0, \\ -\frac{\pi}{2}, & y < 0, x = 0, \\ \pi + \text{atan} \frac{x}{y}, & y > 0, x = 0, \\ -\pi + \text{atan} \frac{x}{y}, & y < 0, x < 0, \\ \pi + \text{atan} \frac{x}{y}, & y > 0, x < 0, \end{cases} \tag{1.5.10}\]

where $\text{atan} : \mathbb{R} \mapsto (-\frac{\pi}{2}, \frac{\pi}{2})$.

Let $z$ be a complex number. Then,

\[z = |z|e^{i\arg z}. \tag{1.5.11}\]
$z$ is a nonnegative number if and only if $\arg z = 0$, and $z$ is a negative number if and only if $\arg z = -\pi$. If $z$ is not a nonnegative number, then $\arg z \in (-\pi, 0) \cup (0, \pi]$ is the angle from the positive real axis to the line segment connecting $z$ to the origin in the complex plane, where clockwise angles are negative and confined to the set $(-\pi, 0)$, and counterclockwise angles are positive and confined to the set $(0, \pi]$. Furthermore, if $z$ is nonzero, then

$$\arg \frac{1}{z} = \begin{cases} -\arg z, & \text{if } z \in (-\pi, \pi), \\ \pi, & \text{if } z = \pi. \end{cases} \tag{1.5.12}$$

Let $z_1$ and $z_2$ be nonzero complex numbers. Then, there exists $k \in \{-1, 0, 1\}$ such that

$$\arg z_1 z_2 = \arg z_1 + \arg z_2 + 2k\pi. \tag{1.5.13}$$

Hence, $2\pi |\arg z_1 z_2 - \arg z_1 - \arg z_2$. For example,

$$\arg (-1)(-1) = \arg 1 = 0 = \pi + \pi - 2\pi = \arg 1 + \arg -1 - 2\pi,$$

$$\arg (1)(-1) = \arg -1 = \pi = 0 + \pi = \arg 1 + \arg -1,$$

$$\arg (-j)(-j) = \arg -1 = \pi = \pi/2 - \pi/2 + 2\pi = \arg -j + \arg j + 2\pi.$$

The **closed left half plane** (CLHP), **open left half plane** (OLHP), **closed right half plane** (CRHP), and **open right half plane** (ORHP) are the subsets of $\mathbb{C}$ defined by

$$\text{OLHP} \doteq \{ x \in \mathbb{C}: \text{Re } x < 0 \}, \quad \text{ORHP} \doteq \{ x \in \mathbb{C}: \text{Re } x > 0 \}, \tag{1.5.14}$$

$$\text{CLHP} \doteq \{ x \in \mathbb{C}: \text{Re } x \leq 0 \}, \quad \text{CRHP} \doteq \{ x \in \mathbb{C}: \text{Re } x \geq 0 \}. \tag{1.5.15}$$

The imaginary numbers are represented by $\mathbb{I} \mathbb{A}$ . Note that 0 is a real number, an imaginary number, and a complex number.

Next, we define the **open inside unit disk** (OIUD) and the **closed inside unit disk** (CIUD) by

$$\text{OIUD} \doteq \{ x \in \mathbb{C}: |x| < 1 \}, \quad \text{CIUD} \doteq \{ x \in \mathbb{C}: |x| \leq 1 \}. \tag{1.5.16}$$

The complements of the open inside unit disk and the closed inside unit disk are given, respectively, by the **closed outside unit disk** (COUD) and the **open outside unit disk**, which are defined by

$$\text{COUD} \doteq \{ x \in \mathbb{C}: |x| \geq 1 \}, \quad \text{OOUUD} \doteq \{ x \in \mathbb{C}: |x| > 1 \}. \tag{1.5.17}$$

The unit circle in $\mathbb{C}$ is denoted by $\text{UC}$.

Since $\mathbb{R}$ is a proper subset of $\mathbb{C}$, we state many results for $\mathbb{C}$. In other cases, we treat $\mathbb{R}$ and $\mathbb{C}$ separately. To do this efficiently, we use the symbol $\mathbb{F}$ to consistently denote either $\mathbb{R}$ or $\mathbb{C}$.

Let $n \in \mathbb{N}$. Then,

$$n! \doteq \begin{cases} n(n-1) \cdots (2)(1), & n \geq 1, \\ 1, & n = 0. \end{cases} \tag{1.5.18}$$

Then,

$$(i!)^2_{n=0} = (1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, 39916800, 479001600).$$

Let $z \in \mathbb{C}$ and $k \in \mathbb{Z}$. Then,

$$\binom{z}{k} \doteq \begin{cases} \frac{z(z-1) \cdots (z-k+1)}{k!}, & k \geq 0, \\ 1, & k = 0, \\ 0, & k < 0. \end{cases} \tag{1.5.19}$$
In particular, if \( n, k \in \mathbb{N} \), then
\[
\binom{n}{k} = \begin{cases} 
\frac{n!}{(n-k)!k!}, & n \geq k \geq 0, \\
0, & k > n > 0.
\end{cases} 
\] (1.5.20)
Hence,
\[
\binom{n}{n} = \begin{cases} 
1, & n \geq 0, \\
0, & n < 0.
\end{cases} 
\] (1.5.21)

For example,
\[
\begin{align*}
\binom{-1}{1} &= 0, & \binom{-1}{1} &= -1, & \binom{1}{-1} &= 0, & \binom{-1}{0} &= 1, & \binom{0}{0} &= 1, \\
\binom{-1}{3} &= -1, & \binom{-3}{1} &= -\frac{5}{16}, & \binom{0}{3} &= 0, & \binom{\frac{1}{2}}{3} &= \frac{1}{16}, & \binom{1}{3} &= 0.
\end{align*}
\]

Note that, for all \( n \geq k \geq 1 \), \( \binom{n}{k} \) is the number of \( k \)-element subsets of \( \{1, \ldots, n\} \).

Let \( z, w \in \mathbb{C} \), and assume that \( z \notin \mathbb{P} \), \( w \notin \mathbb{P} \), and \( z - w \notin \mathbb{P} \). Then,
\[
\binom{z}{w} \triangleq \frac{\Gamma(z+1)}{\Gamma(w+1)\Gamma(z-w+1)}. 
\] (1.5.22)

For \( k_1, \ldots, k_l \in \mathbb{N} \), where \( \sum_{i=1}^{l} k_i = n \), we define the multinomial coefficient
\[
\binom{n}{k_1, \ldots, k_l} \triangleq \frac{n!}{k_1! \cdots k_l!}. 
\] (1.5.23)
Note that, if \( 1 \leq m \leq n \), then
\[
\binom{n}{m} = \binom{n}{m, n-m}. 
\]

For \( z \in \mathbb{C} \) and \( k \in \mathbb{N} \), we define the falling factorial
\[
\underline{z}^k \triangleq \begin{cases} 
z(z-1) \cdots (z-k+1), & k \geq 0, \\
1, & k = 0.
\end{cases} 
\] (1.5.24)
In particular, if \( n \in \mathbb{N} \), then \( \underline{n}^0 = n! \). Hence, if \( z \in \mathbb{C} \) and \( k \in \mathbb{Z} \), then
\[
\binom{z}{k} \triangleq \begin{cases} 
\underline{z}^k, & k \geq 0, \\
0, & k < 0.
\end{cases}
\] (1.5.25)
Furthermore, for all \( z \in \mathbb{C} \) and \( k \in \mathbb{N} \), we define the rising factorial
\[
\overline{z}^k \triangleq \begin{cases} 
z(z+1) \cdots (z+k-1), & k \geq 1, \\
1, & k = 0.
\end{cases} 
\] (1.5.26)
In particular, if \( n \in \mathbb{N} \), then \( \overline{1}^n = n! \). Finally, if \( z \in \mathbb{C} \) and \( k \in \mathbb{N} \), then
\[
\underline{z}^k = (z-k+1)\overline{k}, \quad \overline{z}^k = (z+k-1)\underline{k}, \quad \underline{z}^k = (-1)^k\overline{z}^k.
\] (1.5.27)
The double factorial is defined by

\[
\begin{cases}
(n-2)(n-4)\cdots(2) = 2^{\frac{n}{2}}(n/2)!, & \text{n even,} \\
(n-2)(n-4)\cdots(3)(1) = \frac{(n+1)!(n+1)!}{2^{(n+1)/2}[(n+1)/2]!}, & \text{n odd.}
\end{cases}
\]

(1.5.28)

By convention, \((-1)!! = 0!! = 1\). Finally, if \(n \geq 1\), then \((2n-1)!!(2n-1)!! = (2n)!\) and \((2n+1)!!(2n)!! = (2n+1)!\).

### 1.6 Functions and Their Inverses

Let \(X\) and \(Y\) be nonempty sets. Then, a function \(f\) that maps \(X\) into \(Y\) is a rule \(f : X \rightarrow Y\) that assigns a unique element \(f(x)\) (the image of \(x\)) of \(Y\) to each element \(x\) of \(X\). Equivalently, a function \(f : X \rightarrow Y\) can be viewed as a subset \(\mathcal{F}\) of \(X \times Y\) such that, for each \(x \in X\), there exists a unique \(y \in Y\) such that \((x, y) \in \mathcal{F}\). In this case,

\[
\mathcal{F} = \text{Graph}(f) \triangleq \{(x, f(x)) : x \in X\}.
\]

(1.6.1)

The set \(X\) is the domain of \(f\), while the set \(Y\) is the codomain of \(f\). For \(X_1 \subseteq X\), it is convenient to define

\[
f(X_1) \triangleq \{f(x) : x \in X_1\}.
\]

(1.6.2)

The range of \(f\) is the set \(\mathcal{R}(f) \triangleq f(X)\). The function \(f\) is one-to-one if, for all \(x_1, x_2 \in X\) such that \(f(x_1) = f(x_2)\), it follows that \(x_1 = x_2\). The function \(f\) is onto if \(\mathcal{R}(f) = Y\). The function \(I_X : X \rightarrow X\) defined by \(I_X(x) \triangleq x\) for all \(x \in X\) is the identity mapping on \(X\). Finally, if \(S \subseteq X\), \(f_S : S \rightarrow Y\), and, for all \(x \in X\), \(f_S(x) = f(x)\), then \(f_S\) is the restriction of \(f\) to \(S\).

Note that the subset \(\mathcal{F}\) of \(X \times Y\) can be viewed as a relation on \((X, Y)\). Consequently, a function can be viewed as a special case of a relation.

Let \(X\) be a set, and let \(\hat{X}\) be a partition of \(X\). Furthermore, let \(f : \hat{X} \rightarrow X\), where, for all \(S \in \hat{X}\), it follows that \(f(S) \in S\). Then, \(f\) is a canonical mapping, and \(f(S)\) is a canonical form. That is, for each element \(S \subseteq X\) in the partition \(\hat{X}\) of \(X\), the function \(f\) assigns an element of \(S\) to the set \(S\). For example, let \(S \triangleq \{1, 2, 3, 4\}\), \(\hat{X} \triangleq \{\{1, 3\}, \{2, 4\}\}\), \(f(\{1, 3\}) = 1\), and \(f(\{2, 4\}) = 2\).

Let \(X\) and \(Y\) be sets. If \(f : X \rightarrow Y\) is one-to-one and onto, then \(X\) and \(Y\) have the same cardinality, which is written as \(\text{card}(X) = \text{card}(Y)\). Consequently, if \(X\) is finite, then \(\text{card}(X)\) is the number of elements of \(X\). If \(f : X \rightarrow Y\) is one-to-one, then \(\text{card}(X) \leq \text{card}(Y)\). If every function \(f : X \rightarrow Y\) that is one-to-one is not onto, then \(\text{card}(X) < \text{card}(Y)\). If \(\text{card}(X) = \text{card}(Y)\), then \(X\) is countable. Note that \(\text{card}(\mathbb{N}) = \text{card}(\mathbb{P}) = \text{card}(\mathbb{Q}) = \text{card}(\mathbb{Q}^*) = \text{card}(\mathbb{R}) = \text{card}(\mathbb{R}^2)\).

Let \(X\) be a finite multiset. Then, \(\text{card}(X)\) is the number of elements in \(X\). Cardinality is not defined for infinite multisets.

Let \(X\) be a set, and let \(f : X \rightarrow X\). Then, \(f\) is a function on \(X\). The element \(x \in X\) is a fixed point of \(f\) if \(f(x) = x\).

Let \(X\), \(Y\), and \(Z\) be sets, let \(f : X \rightarrow Y\), and let \(g : Y \rightarrow Z\). Then, the composition of \(g\) and \(f\) is the function \(g \circ f : X \rightarrow Z\) defined by \((g \circ f)(x) \triangleq g[f(x)]\). The following result shows that function composition is associative.

**Proposition 1.6.1.** Let \(X, Y, Z,\) and \(W\) be sets, and let \(f : X \rightarrow Y, g : Y \rightarrow Z, h : Z \rightarrow W\). Then,

\[
h \circ (g \circ f) = (h \circ g) \circ f.
\]

(1.6.3)

Hence, we write \(h \circ g \circ f\) for \(h \circ (g \circ f)\) and \((h \circ g) \circ f\).

**Proposition 1.6.2.** Let \(X, Y,\) and \(Z\) be sets, and let \(f : X \rightarrow Y\) and \(g : Y \rightarrow Z\). Then, the
following statements hold:

i) If \( g \circ f \) is onto, then \( g \) is onto.

ii) If \( g \circ f \) is one-to-one, then \( f \) is one-to-one.

**Proof.** To prove i), note that \( Z = g(f(X)) \subseteq g(Y) \subseteq Z \). Hence, \( g(Y) = \emptyset \). To prove ii), suppose that \( f \) is not one-to-one. Then, there exist distinct \( x_1, x_2 \in X \) such that \( f(x_1) = f(x_2) \). Therefore, \( g(f(x_1)) = g(f(x_2)) \), and thus \( g \circ f \) is not one-to-one. □

Let \( f: X \mapsto Y \). Then, \( f \) is left invertible if there exists a function \( f^L: Y \mapsto X \) (a left inverse of \( f \)) such that \( f^L \circ f = I_X \), whereas \( f \) is right invertible if there exists a function \( f^R: Y \mapsto X \) (a right inverse of \( f \)) such that \( f \circ f^R = I_Y \). In addition, the function \( f: X \mapsto Y \) is invertible if there exists a function \( f^{inv}: Y \mapsto X \) (the inverse of \( f \)) such that \( f^{inv} \circ f = I_X \) and \( f \circ f^{inv} = I_Y \); that is, \( f^{inv} \) is both a left inverse of \( f \) and a right inverse of \( f \).

Let \( f: X \mapsto Y \), and let \( \hat{X} \) denote the set of subsets of \( X \). Then, for all \( y \in Y \), the set-valued inverse \( f^{inv}: Y \mapsto \hat{X} \) is defined by \( f^{inv}(y) = \{ x \in X : f(x) = y \} \). If \( f \) is one-to-one, then, for all \( y \in \mathcal{R}(f) \), the set \( f^{inv}(y) \) has a single element, and thus \( f^{inv}: \mathcal{R}(f) \mapsto \hat{X} \) is a function. If \( f \) is invertible, then, for all \( y \in Y \), \( f^{inv}(y) = \{ f^{inv}(y) \} \). The inverse image \( f^{inv}(S) \) of \( S \subseteq Y \) is the set

\[
\text{f}^{\text{inv}}(S) = \bigcup_{y \in S} f^{\text{inv}}(y) = \{ x \in X : f(x) \in S \}.
\]

(1.6.4)

Note that \( f^{inv}(S) \) is defined whether or not \( f \) is invertible. In fact, \( f^{inv}(y) = f^{inv}[f(X)] = X \) and \( f[f^{inv}(y)] = f(X) \).

**Proposition 1.6.3.** Let \( X \) and \( Y \) be sets, let \( f: X \mapsto Y \), and let \( g: Y \mapsto X \). Then, the following statements are equivalent:

i) \( f \) is a left inverse of \( g \).

ii) \( g \) is a right inverse of \( f \).

**Proposition 1.6.4.** Let \( X \) and \( Y \) be sets, let \( f: X \mapsto Y \), and assume that \( f \) is invertible. Then, \( f \) has a unique inverse. Now, let \( g: Y \mapsto X \). Then, the following statements are equivalent:

i) \( g \) is the inverse of \( f \).

ii) \( f \) is the inverse of \( g \).

**Theorem 1.6.5.** Let \( X \) and \( Y \) be sets, and let \( f: X \mapsto Y \). Then, the following statements hold:

i) \( f \) is left invertible if and only if \( f \) is one-to-one.

ii) \( f \) is right invertible if and only if \( f \) is onto.

Furthermore, the following statements are equivalent:

iii) \( f \) is invertible.

iv) \( f \) has a unique inverse.

v) \( f \) is one-to-one and onto.

vi) \( f \) is left invertible and right invertible.

vii) \( f \) has a unique right inverse.

viii) \( f \) has a one-to-one left inverse.

ix) \( f \) has an onto right inverse.

If, in addition, \( \text{card}(X) \geq 2 \), then the following statement is equivalent to iii)–ix):

x) \( f \) has a unique left inverse.

**Proof.** To prove i), suppose that \( f \) is left invertible with left inverse \( g: Y \mapsto X \). Furthermore, suppose that \( x_1, x_2 \in X \) satisfy \( f(x_1) = f(x_2) \). Then, \( x_1 = g(f(x_1)) = g(f(x_2)) = x_2 \), which shows that \( f \) is one-to-one. Conversely, suppose that \( f \) is one-to-one so that, for all \( y \in \mathcal{R}(f) \), there exists a unique \( x \in X \) such that \( f(x) = y \). Hence, define the function \( g: Y \mapsto X \) by \( g(y) \triangleq x \) for all
y = f(x) ∈ R(f) and by g(y) arbitrary for all y ∈ \( \mathcal{Y} \backslash R(f) \). Consequently, \( g[f(x)] = x \) for all \( x \in \mathcal{X} \), which shows that \( g \) is a left inverse of \( f \).

To prove \( ii) \), suppose that \( f \) is right invertible with right inverse \( g: \mathcal{Y} \to \mathcal{X} \). Then, for all \( y \in \mathcal{Y} \), it follows that \( f[g(y)] = y \), which shows that \( f \) is onto. Conversely, suppose that \( f \) is onto so that, for all \( y \in \mathcal{Y} \), there exists at least one \( x \in \mathcal{X} \) such that \( f(x) = y \). Selecting one such \( x \) arbitrarily, define \( g: \mathcal{Y} \to \mathcal{X} \) by \( g(y) = x \). Consequently, \( f[g(y)] = y \) for all \( y \in \mathcal{Y} \), which shows that \( g \) is a right inverse of \( f \).

Let \( f: \mathcal{X} \to \mathcal{Y} \), and assume that \( f \) is one-to-one. Then, the function \( \hat{f}: \mathcal{X} \to \mathcal{R}(f) \) defined by \( \hat{f}(x) \triangleq f(x) \) is one-to-one and onto and thus invertible. For convenience, we write \( \mathcal{f}^{\text{inv}}: \mathcal{R}(f) \to \mathcal{X} \).

The sine and cosine functions \( \sin: \mathcal{R} \to \mathcal{R}, \cos: \mathcal{R} \to \mathcal{R} \) can be defined in an elementary way in terms of ratios of sides of triangles. The additional trigonometric functions \( \tan: \mathcal{R}\{\frac{1}{2} + \mathcal{Z}\} \to \mathcal{R}, \csc: \mathcal{R}\{\mathcal{Z}\} \to \mathcal{R}, \sec: \mathcal{R}\{\frac{1}{2} + \mathcal{Z}\} \to \mathcal{R}, \) and \( \cot: \mathcal{R}\{\mathcal{Z}\} \to \mathcal{R} \) are defined by

\[
\tan x \triangleq \frac{\sin x}{\cos x}, \quad \csc x \triangleq \frac{1}{\sin x}, \quad \sec x \triangleq \frac{1}{\cos x}, \quad \cot x \triangleq \frac{\cos x}{\sin x}. \quad (1.6.5)
\]

The exponential function \( \exp: \mathcal{R} \to (0, \infty) \) is defined by

\[
\exp(x) \triangleq e^x,
\]

where \( e \triangleq \lim_{t \to 0}(1 + 1/t)^t \approx 2.71828 \ldots \). The exponential function can be extended to complex arguments as follows. For all \( x \in \mathcal{R} \), the power series for \( \exp \) is given by

\[
\exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}. \quad (1.6.7)
\]

Hence, for all \( y \in \mathcal{R} \), we define

\[
\exp(y) = e^y \triangleq \sum_{i=0}^{\infty} \frac{(iy)^i}{i!} = \sum_{i=0}^{\infty} (-1)^i \frac{y^{2i}}{(2i)!} + \sum_{i=0}^{\infty} (-1)^{2i+1} \frac{y^{2i+1}}{(2i+1)!} = \cos y + (\sin y)j. \quad (1.6.8)
\]

Thus, for all \( y \in \mathcal{R} \),

\[
\sin y = \frac{1}{2j}(e^y - e^{-y}), \quad \cos y = \frac{1}{2}(e^y + e^{-y}). \quad (1.6.9)
\]

Now, let \( z = x + yj \), where \( x, y \in \mathcal{R} \). Then, \( \exp: \mathcal{C} \to \mathcal{C}\{0\} \) is defined by

\[
\exp(z) = \exp(x + yj) \triangleq e^{x+yj} = e^x e^{yj} = e^x[\cos y + (\sin y)j]. \quad (1.6.10)
\]

In particular, \( e^{yj} = -1 \).

The six trigonometric functions can now be extended to complex arguments. In particular, by replacing \( y \in \mathcal{R} \) in (1.6.9) by \( z \in \mathcal{C} \), we define \( \sin: \mathcal{C} \to \mathcal{C} \) and \( \cos: \mathcal{C} \to \mathcal{C} \) by

\[
\sin z \triangleq \frac{1}{2j}(e^z - e^{-z}), \quad \cos z \triangleq \frac{1}{2}(e^z + e^{-z}). \quad (1.6.11)
\]

Hence,

\[
e^z = \cos z + (\sin z)j, \quad e^{-z} = \cos z - (\sin z)j. \quad (1.6.12)
\]

Likewise, \( \tan: \mathcal{C}\{\frac{1}{2} + \mathcal{Z}\} \to \mathcal{R}, \csc: \mathcal{C}\{\mathcal{Z}\} \to \mathcal{R}, \sec: \mathcal{C}\{\frac{1}{2} + \mathcal{Z}\} \to \mathcal{R}, \) and \( \cot: \mathcal{C}\{\mathcal{Z}\} \to \mathcal{R} \) are defined by

\[
\tan z \triangleq \frac{\sin z}{\cos z}, \quad \csc z \triangleq \frac{1}{\sin z}, \quad \sec z \triangleq \frac{1}{\cos z}, \quad \cot z \triangleq \frac{\cos z}{\sin z}. \quad (1.6.13)
\]
Let \( f : \mathcal{X} \mapsto \mathcal{Y} \). If \( f \) is not one-to-one, then \( f \) is not invertible. This is the case, for example, for a periodic function such as \( \sin : \mathbb{R} \mapsto [-1, 1] \), respectively. In particular, \( \sin^{\text{inv}}(1) = (4k + 1)\pi/2 : k \in \mathbb{Z} \). However, it is convenient to define a principal inverse \( \sin \) by choosing an element of the set \( \sin^{\text{inv}}(y) \) for each \( y \in [-1, 1] \). Although this choice can be made arbitrarily, it is traditional to define

\[
\text{asin}: [-1, 1] \mapsto [-\frac{\pi}{2}, \frac{\pi}{2}].
\] (1.6.14)

Similarly,

\[
\begin{align*}
\text{acos} : [-1, 1] & \mapsto [0, \pi], & \text{atan} : \mathbb{R} & \mapsto (-\frac{\pi}{2}, \frac{\pi}{2}), \\
\text{acsc} : (-\infty, -1) \cup [1, \infty) & \mapsto [-\frac{\pi}{2}, 0) \cup (0, \frac{\pi}{2}], \\
\text{asec} : (-\infty, -1) \cup [1, \infty) & \mapsto [0, \frac{\pi}{2}) \cup \left(\frac{\pi}{2}, \pi\right], \\
\text{acot} : \mathbb{R} & \mapsto (-\frac{\pi}{2}, 0) \cup (0, \frac{\pi}{2}].
\end{align*}
\] (1.6.15 - 1.6.18)

An analogous situation arises for the exponential function \( f(z) = e^z \), which is not one-to-one and thus requires a principal inverse \( \log \) in the form of a logarithm defined on \( \mathbb{C} \setminus \{0\} \). Let \( w \) be a nonzero complex number, and, for all \( i \in \mathbb{Z} \), define

\[
z_i = \log |w| + (\arg w + 2i\pi)j.
\] (1.6.19)

Then, for all \( i \in \mathbb{Z} \),

\[
e^{z_i} = |w|e^{(\arg w)j}e^{2i\pi j} = |w|e^{(\arg w)j} = w.
\] (1.6.20)

Consequently, \( f^{\text{inv}}(w) = \{z_i : i \in \mathbb{Z}\} \). For example, \( f^{\text{inv}}(1) = (2i\pi j : i \in \mathbb{Z}) \), and \( f^{\text{inv}}(-1) = ((2i + 1)\pi j : i \in \mathbb{Z}) \). The principal logarithm \( \log \) of \( w \) is defined by choosing \( z_0 \), which yields

\[
\log w = z_0 = \log |w| + (\arg w)j.
\] (1.6.21)

Therefore,

\[
\log : \mathbb{C} \setminus \{0\} \mapsto \{z : \Re z \neq 0 \text{ and } -\pi < \Im z \leq \pi\}.
\] (1.6.22)

Hence,

\[
\Re \log w = \log |w|, \quad \Im \log w = \arg w.
\] (1.6.23)

Let \( w_1 \) and \( w_2 \) be nonzero complex numbers. Then, with \( f : \mathbb{C} \mapsto \mathbb{C} \setminus \{0\} \) given by (1.6.10),

\[
f^{\text{inv}}(w_1w_2) = f^{\text{inv}}(w_1) + f^{\text{inv}}(w_2).
\] (1.6.24)

However,

\[
\log w_1w_2 = \log w_1 + \log w_2
\] (1.6.25)

if and only if

\[
\arg w_1w_2 = \arg w_1 + \arg w_2.
\] (1.6.26)

For example,

\[
\arg \left(\frac{\sqrt{3}}{2} + \frac{i\sqrt{3}}{2}\right)^2 = \arg j = \frac{\pi}{2} = \frac{\pi}{4} + \frac{\pi}{4} = \arg \left(\frac{\sqrt{3}}{2} + \frac{\sqrt{3}i}{2}\right) + \arg \left(\frac{\sqrt{3}}{2} + \frac{\sqrt{3}i}{2}\right),
\]

and thus

\[
\log \left(\frac{\sqrt{3}}{2} + \frac{\sqrt{3}i}{2}\right)^2 = \log \left(\frac{\sqrt{3}}{2} + \frac{\sqrt{3}i}{2}\right) + \log \left(\frac{\sqrt{3}}{2} + \frac{\sqrt{3}i}{2}\right).
\]

However,

\[
\arg (-1)^2 = \arg 1 = 0 \neq 2\pi = \pi + \pi = \arg(-1) + \arg(-1),
\]
and thus
\[
\log(-1)^2 = \log 1 = 0 \neq 2\pi j = \pi j + \pi j = \log(-1) + \log(-1).
\]

Therefore, there exist nonzero complex numbers \( w_1 \) and \( w_2 \) such that the principal logarithm does not satisfy (1.6.25).

Let \( w \) be a nonzero complex number. Then,
\[
w = e^{\log w}.
\]

Now, let \( z \) be a complex number. Then,
\[
\log e^z = z - \left( \text{round} \frac{\text{Im} z}{2\pi} \right) 2\pi j,
\]
where, for all \( x \in \mathbb{R} \), \( \text{round}(x) \) denotes the closest integer to \( x \) except in the case where \( 2x \) is an integer, in which case \( \text{round}(x) = \lfloor x \rfloor \). Therefore, \( \log e^z = z \) if and only if \( \text{Im} z \in (-\pi, \pi] \).

An analogous situation arises for \( n \)th roots. Consider \( f: \mathbb{R} \to [0, \infty) \) defined by \( f(x) = x^2 \). Then, for all \( y \in [0, \infty) \), it follows that \( f^{\text{inv}}(y) = (-\sqrt[y]{y}, \sqrt[y]{y}) \), where \( \sqrt[y]{y} \) represents the nonnegative square root of \( y \geq 0 \). For complex-valued extensions, let \( n \geq 1 \), and define \( f: \mathbb{C} \to \mathbb{C} \) by \( f(z) = z^n \).

Let \( w \) be a nonzero complex number. Then, \( w = e^{\log w} \). Therefore, there exist nonzero complex numbers, and assume that \( w = e^{\log w} \).

Note that, for all \( z \in \mathbb{C} \), \( \log w \) is defined by choosing \( \log w = \text{log} w + (\arg w)j \), where “log” is the principal log. Furthermore, \( z \) satisfies \( z^n = w \) if and only if there exists an integer \( i \) such that \( n \log z = \log |w| + (\arg w + 2\pi i)j \). Therefore, for all \( i \in \mathbb{Z} \), define
\[
z_i = e^{\frac{1}{n}[\log |w| + (\arg w + 2\pi i)]j},
\]
which satisfies
\[
z_i^n = w.
\]
Note that, for all \( i \in \mathbb{Z} \), \( z_{i+1} = z_i \). Therefore, for all \( i \in \{0, \ldots, n - 1\} \), define the \( n \) distinct numbers
\[
z_i = \sqrt[n]{|w|}e^{\frac{2\pi i}{n}j},
\]
where \( \sqrt[n]{|w|} \) is the nonnegative \( n \)th root of \( |w| \). Consequently, \( f^{\text{inv}}(w) = \{z_0, \ldots, z_{n-1}\} \). The principal \( n \)th root \( w^{1/n} \) of \( w \) is defined by choosing \( z_0 \), which yields
\[
w^{1/n} \triangleq z_0 = \sqrt[n]{|w|}e^{\frac{2\pi i}{n}j}.
\]
In particular, if \( w \) is a positive number, then \( w^{1/n} = \sqrt[n]{w} \), which is the positive \( n \)th root of \( w \). However, for an odd integer \( m \) and a negative number \( a \), a notational conflict arises between the principal \( n \)th root of \( a \) and the negative \( n \)th root of \( a \). For example, \((-1)^{1/3} = e^{\pi i/3} \), whereas, for all odd integers \( n \), it is traditional to interpret \( \sqrt[n]{-1} \) as \(-1 \). In other words, for all \( a < 0 \) and odd \( n \geq 1 \), \( \sqrt[n]{a} \triangleq -\sqrt[n]{|a|} \), and thus
\[
a^{1/n} = \sqrt[n]{|a|}e^{\frac{(n-1)i\pi}{n}} = \sqrt[n]{|a|}e^{\frac{(n-1)i\pi}{n}}.
\]

Let \( z \) and \( \alpha \) be complex numbers, and assume that \( z \) is not zero. As an extension of the functions \( f(z) = z^\alpha \) and \( f(z) = z^{1/n} \), define
\[
z^\alpha \triangleq e^{\alpha \log z},
\]
where \( \log z \) is the principal logarithm of \( z \). For example,
\[
\frac{1}{z^j} = e^{-2j\log z} = e^{-2j(\pi/2)j} = e^\pi.
\]

Next, let \( z_1 \) and \( z_2 \) be complex numbers, and let \( \alpha \) be a real number. Then, \( (z_1z_2)^\alpha = z_1^\alpha z_2^\alpha \). Now, let \( \alpha \) be a complex number. Then, \( \alpha^1 \alpha^{z_1} = \alpha^{z_1 + z_2} \). However, \( (z_1z_2)^\alpha \) and \( z_1^\alpha z_2^\alpha \) are not necessarily
equal. For example, \((-1)^i(-1)^j = e^{-\pi}e^{-\pi} = e^{-2\pi} \neq 1 = 1^i(1^j)\). However,
\[
(z_1z_2)^\alpha = z_1^{\alpha}z_2^{\alpha}e^{2\pi\alpha ij},
\]
where
\[
n = \begin{cases} 1, & -2\pi < \arg z_1 + \arg z_2 \leq -\pi, \\ 0, & -\pi < \arg z_1 + \arg z_2 \leq \pi, \\ -1, & \pi < \arg z_1 + \arg z_2 \leq 2\pi. \end{cases}
\]
Finally,
\[
(a^{z_1})^{z_2} = a^{z_1z_2}e^{2\pi\alpha ij},
\]
where
\[
n = \left\lfloor \frac{1}{2} \left( (\Im z_1) \log |a| + (\Re z_1) \arg \alpha \right) \right\rfloor.
\]
For example, setting \(\alpha = -1\), \(z_1 = -1\), and \(z_2 = \frac{1}{2}\) yields \(n = 1\), and thus \(j = (-1)^{1/2} = \frac{(-1)^{-1}}{2} = (-1)^{-1/2}e^{\pi ij} = (1/j)(-1) = j\). Furthermore,
\[
(e^{z_1})^{z_2} = e^{z_1z_2}e^{2\pi\alpha ij},
\]
where \(n = \left\lfloor \frac{1}{2} - \frac{\Im z_1}{2\pi} \right\rfloor\). See [2216, pp. 108–114] and [2249, pp. 91, 114–119].

Finally, let \(z\), \(\alpha\), and \(\beta\) be complex numbers. Then, \((e^{z\alpha})^\beta\), \((e^{z\beta})^\alpha\), and \((e^{z\alpha})^\beta\) may be different as can be seen from the example \(z = \frac{1}{2}i\), \(\alpha = 2 - j\), and \(\beta = -3 + j\), where \((e^{z\alpha})^\beta \approx 0.03 + 0.04j\), \((e^{z\beta})^\alpha \approx 9104 + 10961j\), and \((e^{z\alpha})^\beta \approx 17 + 20j\). A similar situation can occur in the case where \(z\), \(\alpha\), and \(\beta\) are real. For example, if \(z = -1\), \(\alpha = 1/2\), and \(\beta = 2\), then \((e^{z\alpha})^\beta = e^{z\beta} = -1 \neq 1 = (e^{z\beta})^\alpha\). As a final example, let \(z = e\), \(\alpha = 2\pi ij\), where \(i \geq 1\), and \(\beta = \pi\). Then, \((e^{z\alpha})^\beta = (e^{z\beta})^\alpha = e^{2\pi ij} = e^{2\pi ij} = e^{2\pi ij} = \cos 2\pi^2 i + j \sin 2\pi^2 i\) and \((e^{z\beta})^\alpha = (e^{z\alpha})^\beta = 1^\pi = e^{\pi} = e^{\pi} = 1\). Since, for all \(i \geq 1\), \(\cos 2\pi^2 i + j \sin 2\pi^2 i \neq 1\), it follows that \((e^{z\alpha})^\beta = e^{z\beta} \neq (e^{z\beta})^\alpha\). See [2107, pp. 166, 167].

**Definition 1.6.6.** Let \(J \subset \mathbb{R}\) be a finite or infinite interval, and let \(f: J \mapsto \mathbb{R}\). Then, \(f\) is **convex** if, for all \(\alpha \in [0, 1]\) and \(x, y \in J\),
\[
f(ax + (1 - \alpha)y) \leq \alpha f(x) + (1 - \alpha)f(y).
\]
Furthermore, \(f\) is **strictly convex** if, for all \(\alpha \in (0, 1)\) and distinct \(x, y \in J\),
\[
f(ax + (1 - \alpha)y) < \alpha f(x) + (1 - \alpha)f(y).
\]
Finally, \(f\) is **concave**, **strictly convex** if \(-f\) is (convex, strictly convex).

A more general definition of a convex function is given by Definition 10.6.14.

Let \(\mathcal{X}\) be a set, and let \(\sigma: \mathcal{X} \times \cdots \times \mathcal{X} \mapsto \mathcal{X} \times \cdots \times \mathcal{X}\), where each Cartesian product has \(n\) factors. Then, \(\sigma\) is a **permutation** if, for all \((x_1, \ldots, x_n) \in \mathcal{X} \times \cdots \times \mathcal{X}\) and \(\sigma[(x_1, \ldots, x_n)]\) have the same components with the same multiplicity but possibly in a different order. For convenience, we write \((\sigma(x_1), \ldots, \sigma(x_n))\) for \(\sigma[(x_1, \ldots, x_n)]\). In particular, we write \((\sigma(1), \ldots, \sigma(n))\) for \(\sigma[(1, \ldots, n)]\). The permutation \(\sigma\) is a **transposition** if \((\sigma(x_1), \ldots, \sigma(x_n))\) and \((x_1, \ldots, x_n)\) differ by exactly two distinct interchanged components. Finally, let sign(\(\sigma\)) denote \(-1\) raised to the smallest number of transpositions needed to transform \((\sigma(1), \ldots, \sigma(n))\) to \((1, \ldots, n)\). Note that, if \(\sigma_1\) and \(\sigma_2\) are permutations of \((1, \ldots, n)\), then sign(\(\sigma_1 \circ \sigma_2\)) = sign(\(\sigma_1\)) sign(\(\sigma_2\)).

### 1.7 Facts on Logic

**Fact 1.7.1.** Let \(A\) and \(B\) be statements. Then, the following statements hold:

(i) \([A \land (A \implies B)] \implies B\).
ii) \( \neg(\text{A and B}) \iff (\neg \text{A} \text{ or } \neg \text{B}) \).

iii) \( \neg(\text{A or B}) \iff (\neg \text{A} \text{ and } \neg \text{B}) \).

iv) (A or B) \iff [(\neg \text{A} \implies \text{B}) \iff ((\text{A and B}) \text{ xor } (\text{A xor B}))].

v) (A \implies B) \iff [(\neg \text{A} \text{ or } B) \iff (\neg(\text{A and not B}) \iff ((\text{A and B}) \text{ xor } \neg \text{A})].

vi) not(\text{A and B}) \iff (\text{A implies not B}) \iff (\text{B implies not A}).

vii) [\text{A and not B}] \iff [\neg(\text{A implies B})].

Remark: Each statement is a tautology. Remark: ii) and iii) are De Morgan's laws. See [493, p. 24]. See Fact 1.8.1.

Fact 1.7.2. Let A and B be statements. Then, the following statements are equivalent:

i) A \iff B.

ii) (A or not B) and not(A and not B).

iii) (A or not B) and [(not A) or B].

iv) (A and B) or [(not A) and not B].

v) not(A xor B).

Remark: The equivalence of each pair of statements is a tautology.

Fact 1.7.3. Let A, B, and C be statements. Then,

\[ [(A \implies B) \text{ and } (B \implies C)] \implies (A \implies C). \]

Fact 1.7.4. Let A, B, and C be statements. Then, the following statements are equivalent:

i) A \implies (B \text{ or } C).

ii) [A and (not B)] \implies C.

Remark: The statement that i) and ii) are equivalent is a tautology.

Fact 1.7.5. Let A, B, and C be statements. Then, the following statements are equivalent:

i) (A and B) \implies C.

ii) [B and (not C)] \implies (not A).

iii) [A and (not C)] \implies (not B).

Source: To prove i) \implies ii), note that [(A and B) or (not B)] \implies [C or (not B)], that is, [A or (not B)] \implies [C or (not B)], and thus A \implies [C or (not B)]. Hence, [B and (not C)] \implies (not A). Conversely, to prove ii) \implies i), note that [(B and (not C)) or (not B)] \implies [(not A) or (not B)], that is, [(not C) or (not B)] \implies [(not A) or (not B)], and thus (not C) \implies [(not A) or (not B)]. Hence, (A and B) \implies C.

Fact 1.7.6. Let \( \mathcal{X} \) and \( \mathcal{Y} \) be sets, and let Z be a statement that depends on elements of \( \mathcal{X} \) and \( \mathcal{Y} \). Then, the following statements are equivalent:

i) Not[for all \( x \in \mathcal{X} \), Z holds].

ii) There exists \( x \in \mathcal{X} \) such that Z does not hold.

Furthermore, the following statements are equivalent:

iii) Not[there exists \( y \in \mathcal{Y} \) such that Z holds].

iv) For all \( y \in \mathcal{Y} \), Z does not hold.

Finally, the following statements are equivalent:

v) Not[for all \( x \in \mathcal{X} \), there exists \( y \in \mathcal{Y} \) such that Z holds].

vi) There exists \( x \in \mathcal{X} \) such that, for all \( y \in \mathcal{Y} \), Z does not hold.

1.8 Facts on Sets

Fact 1.8.1. Let A and B be subsets of a set \( \mathcal{X} \). Then, the following statements hold:
i) \( A \cap A = A \cup A = A \).

ii) \( A \setminus B = A \cap B^c \).

iii) \( (A \cup B)^c = A^c \cap B^c \).

iv) \( (A \cap B)^c = A^c \cup B^c \).

v) \( (A \setminus B) \cup (A \cap B) = A \).

vi) \( A \setminus (A \cap B) = A \cap B^c \).

vii) \( A \cap (A^c \cup B) = A \cap B \).

viii) \( (A \cup B) \cap (A \cup B^c) = A \).

ix) \( [A \setminus (A \cap B)] \cup B = A \cup B \).

x) \( (A \cup B) \cap (A^c \cup B^c) = A \cap B \).

xi) \( (A^c \cup B)^c \cap (A \cup B^c) = [A \cup B] \cap (A \cap B)^c = [(A \cup B) \cap (A \cap B)]^c = [(A \cap B^c) \cup (A^c \cap B)]^c \).

Remark: iii) and iv) are De Morgan’s laws. See Fact 1.7.1.

Fact 1.8.2. Let \( A \), \( B \), and \( C \) be subsets of a set \( X \). Then, the following statements hold:

i) \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \).

ii) \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \).

iii) \( (A \setminus B) \cap C = A \setminus (B \cup C) \).

iv) \( (A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C) \).

v) \( (A \setminus B) \cap (C \cap B) = (A \setminus C) \cap B \).

vi) \( (A \cup B) \setminus (C \cup B) = (A \setminus C) \cup (B \setminus C) \).

vii) \( (A \setminus B) \cap (C \cap B) = (A \setminus C) \cup (B \setminus C) \).

viii) \( A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C) \).

ix) \( (A \setminus B) \cap (C \setminus B) = (A \setminus C) \cap (A \setminus B) \).

Fact 1.8.3. Let \( A \), \( B \), and \( C \) be subsets of a set \( X \). Then, the following statements hold:

i) \( A \ominus \emptyset = \emptyset \ominus A = A, A \ominus A = \emptyset \).

ii) \( A \ominus B = B \ominus A \).

iii) \( A \ominus B = (A \cap B^c) \cup (B \cap A^c) = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B) \).

iv) \( A \ominus B = \{x \in X: (x \in A) \xor (x \in B)\} \).

v) \( A \ominus B = \emptyset \) if and only if \( A = B \).

vi) \( A \ominus (B \ominus C) = (A \ominus B) \ominus C \).

vii) \( (A \ominus B) \ominus (C \ominus B) = A \ominus C \).

viii) \( A \ominus (B \ominus C) = (A \ominus B) \ominus (A \ominus C) \).

If, in addition, \( A \) and \( B \) are finite, then

\[
\text{card}(A \ominus B) = \text{card}(A) + \text{card}(B) - 2 \text{card}(A \cap B).
\]

Fact 1.8.4. Let \( A \), \( B \), and \( C \) be finite sets. Then,

\[
\text{card}(A \times B) = \text{card}(A) \cdot \text{card}(B),
\]

\[
\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B),
\]

\[
\text{card}(A \cup B \cup C) = \text{card}(A) + \text{card}(B) + \text{card}(C) - \text{card}(A \cap B) - \text{card}(A \cap C) - \text{card}(B \cap C) + \text{card}(A \cap B \cap C).
\]

Remark: The second and third equalities are versions of the inclusion-exclusion principle. See [411, p. 82], [1372, p. 67], and [2520, pp. 64–67]. Remark: The inclusion-exclusion principle...
CHAPTER 1

holds for multisets $A$ and $B$ with “$A \cup B$” defined as the smallest multiset that contains both $A$ and $B$. For example, $\text{card}(\{1, 1, 2, 2\}) = \text{card}(\{1, 1, 2\} \cup \{1, 2, 2\}) = \text{card}(\{1, 1, 2\}) + \text{card}(\{1, 2, 2\}) - \text{card}(\{1, 1, 2, 2\})$; that is, $4 = 3 + 2 - 2$. See [2879].

**Fact 1.8.5.** Define $A \triangle \{x_1, \ldots, x_n\}$, where, for all $i \in \{1, \ldots, n\}$, $k_i$ is the number of repetitions of $x_i$. Then, the number of multisubsets of $A$ is $\prod_{i=1}^{n} (k_i + 1)$. **Source:** [2460].

**Fact 1.8.6.** Let $A, B \subseteq \mathbb{R}$. Then, the following statements hold:

i) $\sup(-A) = -\inf A$.

ii) $\inf(-A) = -\sup A$.

iii) $\sup(A + B) = \sup A + \sup B$.

iv) $\sup(A - B) = \sup A - \inf B$.

v) $\inf(A + B) = \inf A + \inf B$.

vi) $\inf(A - B) = \inf A - \sup B$.

vii) $\sup(A \cup B) = \max\{\sup A, \sup B\}$.

viii) $\inf(A \cup B) = \min\{\inf A, \inf B\}$.

ix) If $0 \notin A$, then

$$\sup \left\{ \frac{1}{x} : x \in A \right\} = \max \left\{ \frac{1}{\inf[A \cap (-\infty, 0)]}, \frac{1}{\inf[A \cap (0, \infty)]} \right\}.$$  

$x)$ $\sup \{xy : x \in A, y \in B\} = \max \{(\inf A) \inf B, (\inf A) \sup B, (\sup A) \inf B, (\sup A) \sup B\}$.

**Source:** [1566, p. 3].

**Fact 1.8.7.** Let $S_1, \ldots, S_m$ be finite sets, and let $n \triangleq \sum_{i=1}^{m} \text{card}(S_i)$. Then,

$$\left\lfloor \frac{n}{m} \right\rfloor \leq \max_{i \in \{1, \ldots, m\}} \text{card}(S_i).$$

In particular, if $m < n$, then there exists $i \in \{1, \ldots, m\}$ such that $\text{card}(S_i) \geq 2$. **Remark:** This is the pigeonhole principle.

**Fact 1.8.8.** Let $S_1, \ldots, S_m$ be sets, assume that, for all $i \in \{1, \ldots, m\}$, $\text{card}(S_i) = n$, and assume that, for all distinct $i, j \in \{1, \ldots, m\}$, $\text{card}(S_i \cap S_j) \leq k$. Then,

$$\frac{n^m}{n + (m - 1)k} \leq \text{card}\left(\bigcup_{i=1}^{m} S_i\right).$$

**Source:** [1561, p. 23].

**Fact 1.8.9.** Let $X$ be a set, let $n \equiv \text{card}(X)$, let $S_1, \ldots, S_m \subseteq X$, and assume that, for all distinct $i, j \in \{1, \ldots, m\}$, $S_i \setminus S_j$ and $S_j \setminus S_i$ are nonempty. Then, $m \leq \binom{n}{\lfloor n/2 \rfloor}$. **Source:** [1992, p. 57]. **Remark:** This is a Sperner lemma.

**Fact 1.8.10.** Let $X$ be a set, let $n \equiv \text{card}(X)$, let $S_1, \ldots, S_m \subseteq X$, let $k \leq n/2$, assume that, for all $i \in \{1, \ldots, m\}$, $\text{card}(S_i) = k$, and, for all distinct $i, j \in \{1, \ldots, m\}$, $S_i \cap S_j$ is nonempty. Then, $m \leq \binom{n}{k-1}$. **Source:** [1992, p. 57]. **Remark:** This is the Erdős-Ko-Rado theorem.

**Fact 1.8.11.** Let $X$ be a set, let $n \equiv \text{card}(X)$, let $S_1, \ldots, S_m \subseteq X$, assume that, for all $i \in \{1, \ldots, m\}$, $\text{card}(S_i)$ is odd, and, for all distinct $i, j \in \{1, \ldots, m\}$, $\text{card}(S_i \cap S_j)$ is even. Then, $m \leq n$. **Source:** [1992, p. 57]. **Remark:** This is the oddtown theorem.

**Fact 1.8.12.** Let $X$ be a set, let $n \equiv \text{card}(X)$, let $S_1, \ldots, S_m \subseteq X$, let $p \geq 2$ be prime, and assume that, for all $i \in \{1, \ldots, m\}$, $\text{card}(S_i) = 2p - 1$, and, for all distinct $i, j \in \{1, \ldots, m\}$, $\text{card}(S_i \cap S_j) \neq p - 1$. Then, $m \leq \sum_{i=1}^{p-1} \binom{n}{i}$. **Source:** [1992, p. 58]. **Remark:** Excluding intersections of cardinality $p - 1$ restricts the number of possible subsets of $X$.  

For general queries, contact webmaster@press.princeton.edu
**Fact 1.8.13.** Let $X$ be a set, let $S_1, \ldots, S_m, T_1, \ldots, T_m \subseteq X$, let $k \geq 1$ and $l \geq 1$, and assume that, for all $i \in \{1, \ldots, m\}$, card$(S_i) = k$, card$(T_i) = l$, and $S_i \cap T_i = \emptyset$, and, for all $i, j \in \{1, \ldots, m\}$ such that $i < j$, $S_i \cap T_j \neq \emptyset$. Then, $m \leq \binom{k+l}{l}$. **Source:** [1992, pp. 171–173].

**Fact 1.8.14.** Let $S$ be a set, and let $S$ denote the set of all subsets of $S$. Then, “$\subseteq$” and “$\subseteq^*$” are transitive relations on $S$, and “$\subseteq^*$” is a partial ordering on $S$.

**Fact 1.8.15.** Define the relation $\mathcal{R}$ on $\mathbb{R} \times \mathbb{R}$ by
\[
\mathcal{R} \doteq \{((x_1, y_1), (x_2, y_2)) \in (\mathbb{R} \times \mathbb{R}) \times (\mathbb{R} \times \mathbb{R}) : x_1 \leq x_2 \text{ and } y_1 \leq y_2\}.
\]
Then, $\mathcal{R}$ is a partial ordering.

**Fact 1.8.16.** Define the relation $\mathcal{L}$ on $\mathbb{R} \times \mathbb{R}$ by
\[
\mathcal{L} \doteq \{((x_1, y_1), (x_2, y_2)) \in (\mathbb{R} \times \mathbb{R}) \times (\mathbb{R} \times \mathbb{R}) : x_1 \leq x_2 \text{ and, if } x_1 = x_2, \text{ then } y_1 \leq y_2\}.
\]
Then, $\mathcal{L}$ is a total ordering on $\mathbb{R} \times \mathbb{R}$.

**Remark:** Denoting this total ordering by “$\preccurlyeq$”, note that $(1, 4) \preccurlyeq (2, 3)$ and $(1, 4) \preccurlyeq (1, 5)$. **Remark:** This ordering is the **lexicographic ordering** or **dictionary ordering**, where “book” $\preccurlyeq$ “box”. Note that the ordering of words in a dictionary is reflexive, antisymmetric, and transitive, and that every pair of words can be ordered. **Related:** Fact 3.11.23.

**Fact 1.8.17.** Let $n \geq 1$ and $x_1, \ldots, x_{n+1} \in \mathbb{R}$. Then, at least one of the following statements holds:

i) There exist $1 \leq i_1 \leq \cdots \leq i_{n+1} \leq n^2 + 1$ such that $x_{i_1} \leq \cdots \leq x_{i_{n+1}}$.

ii) There exist $1 \leq i_1 \leq \cdots \leq i_{n+1} \leq n^2 + 1$ such that $x_{i_1} \geq \cdots \geq x_{i_{n+1}}$.

**Source:** [2294, p. 53] and [2526]. **Remark:** This is the **Erdős-Szekeres theorem**.

### 1.9 Facts on Graphs

**Fact 1.9.1.** Let $G = (X, R)$ be a directed graph. Then, the following statements hold:

i) $R$ is the graph of a function on $X$ if and only if every node in $X$ has exactly one child.

Furthermore, the following statements are equivalent:

ii) $R$ is the graph of a one-to-one function on $X$.

iii) $R$ is the graph of an onto function on $X$.

iv) $R$ is the graph of a one-to-one and onto function on $X$.

v) Every node in $X$ has exactly one child and not more than one parent.

vi) Every node in $X$ has exactly one child and at least one parent.

vii) Every node in $X$ has exactly one child and exactly one parent.

**Related:** Fact 1.10.1.

**Fact 1.9.2.** Let $G = (X, R)$ be a directed graph, and assume that $R$ is the graph of a function $f : X \mapsto X$. Then, either $f$ is the identity function or $G$ has a directed cycle.

**Fact 1.9.3.** Let $G = (X, R)$ be a directed graph, and assume that $G$ has a directed Hamiltonian cycle. Then, $G$ has no roots and no leaves.

**Fact 1.9.4.** Let $G = (X, R)$ be a directed graph. Then, $G$ has either a root or a directed cycle.

**Fact 1.9.5.** Let $G = (X, R)$ be a directed graph. If $G$ is a directed tree, then it is not transitive.

**Fact 1.9.6.** Let $G = (X, R)$ be a directed graph, and assume that $G$ is directionally acyclic. Furthermore, for all $x, y \in X$, let “$x \preceq y$” denote the existence of directional path from $x$ to $y$. Then, “$\preceq$” is a partial ordering on $X$. **Remark:** This result provides the foundation for the **Hasse diagram**, which illustrates the structure of a partially ordered set. See [2405, 2734].

**Fact 1.9.7.** Let $G = (X, R)$ be a directed graph. If $G$ is a directed forest, then $G$ is directionally acyclic.
**Fact 1.9.8.** Let $G = (X, R)$ be a symmetric graph, and let $n = \text{card}(X)$. Then, the following statements are equivalent:

- $i)$ $G$ is a forest.
- $ii)$ $G$ is acyclic.
- $iii)$ No pair of nodes in $X$ is connected by more than one path.

Furthermore, the following statements are equivalent:

- $iv)$ $G$ is a tree.
- $v)$ $G$ is a connected forest.
- $vi)$ $G$ is connected and has no cycles.
- $vii)$ $G$ is connected and has $n - 1$ edges.
- $viii)$ $G$ has no cycles and has $n - 1$ edges.
- $ix)$ Every pair of nodes in $X$ is connected by exactly one path.

**Fact 1.9.9.** Let $G = (X, R)$ be a tournament. Then, $G$ has a directed Hamiltonian path. If, in addition, $G$ is directionally connected, then $G$ has a directed Hamiltonian cycle. **Remark:** The second statement is Camion’s theorem. See [276, p. 16]. **Remark:** The directed edges in a tournament distinguish winners and losers in a contest where every player (that is, node) encounters every other player exactly once.

**Fact 1.9.10.** Let $G = (X, R)$ be a symmetric graph without self-edges, where $X \subset \mathbb{R}^2$, assume that $v = \text{card}(X) \geq 3$, assume that $G$ is connected, and assume that the edges in $R$ can be represented by line segments that lie in the same plane and that pairwise either are disjoint or intersect at a node. Furthermore, let $e$ denote the number of edges of $G$, and let $f$ denote the number of disjoint regions in $\mathbb{R}^2$ whose boundaries are the edges of $G$. Then,

$$f + v - e = 2, \quad \frac{3}{2} f \leq e \leq 3v - 6, \quad f \leq 2v - 4.$$ 

If, in addition, $G$ has no triangles, then $e \leq 2v - 4$. **Source:** [754, pp. 162–166] and [2735, pp. 97–116]. **Remark:** The equality gives the Euler characteristic for a planar graph. A related result for the surfaces of a convex polyhedron is given by Fact 5.4.8. See [2307].

### 1.10 Facts on Functions

**Fact 1.10.1.** Let $X$ and $Y$ be finite sets, and let $f: X \rightarrow Y$. Then, the following statements hold:

- $i)$ If $\text{card}(X) < \text{card}(Y)$, then $f$ is not onto.
- $ii)$ If $\text{card}(Y) < \text{card}(X)$, then $f$ is not one-to-one.
- $iii)$ If $f$ is one-to-one and onto, then $\text{card}(X) = \text{card}(Y)$.

Now, assume that $\text{card}(X) = \text{card}(Y)$. Then, the following statements are equivalent:

- $iv)$ $f$ is one-to-one.
- $v)$ $f$ is onto.
- $vi)$ $\text{card}(f(X)) = \text{card}(X)$.

**Related:** Fact 1.9.1.

**Fact 1.10.2.** Let $f: X \rightarrow Y$ be invertible. Then, $f^{\text{inv}}$ is invertible, and $(f^{\text{inv}})^{\text{inv}} = f$.

**Fact 1.10.3.** Let $f: X \rightarrow Y$. Then, for all $A, B \subseteq X$, the following statements hold:

- $i)$ $A \subseteq f^{\text{inv}}(f(A)) \subseteq X$.
- $ii)$ $f^{\text{inv}}(f(X)) = X = f^{\text{inv}}(Y)$.
- $iii)$ If $A \subseteq B$, then $f(A) \subseteq f(B)$.
- $iv)$ $f(A \cap B) \subseteq f(A) \cap f(B)$.
Furthermore, the following statements are equivalent:

v) \( f(A \cup B) = f(A) \cup f(B) \).
vi) \( f(A) \setminus f(B) \subseteq f(A \setminus B) \).

\[ \text{Related: Fact 3.12.7.} \]

\[ \text{Fact 1.10.6.} \]

\[ \text{Let } f : \mathcal{X} \to \mathcal{Y} \text{. Then, for all } A, B \subseteq \mathcal{Y}, \text{ the following statements hold:} \]

i) \( f[f^{\text{inv}}(A)] = A \cap f(\mathcal{X}) \subseteq A \).

\[ \text{Related: Fact 3.12.8.} \]

\[ \text{Fact 1.10.5.} \]

\[ \text{Let } f : \mathcal{X} \to \mathcal{Y} \text{. Then, the following statements hold:} \]

i) If \( f \) is invertible, then, for all \( y \in \mathcal{Y} \), \( f[f^{\text{inv}}(y)] = f^{\text{inv}}(y) \).

\[ \text{Related: Fact 3.18.8.} \]

\[ \text{Fact 1.10.6.} \]

\[ \text{Let } g : \mathcal{X} \to \mathcal{Y} \text{ and } f : \mathcal{Y} \to \mathcal{Z} \text{. Then, the following statements hold:} \]

i) \( A \subseteq \mathcal{Z} \), then \( (f \circ g)^{\text{inv}}(A) = g^{\text{inv}}[f^{\text{inv}}(A)] \).

\[ \text{Remark: A matrix version of this result is given by Fact 3.18.9 and Fact 3.18.10.} \]

\[ \text{Fact 1.10.7.} \]

\[ \text{Let } f : \mathcal{X} \to \mathcal{Y} \text{, let } g : \mathcal{Y} \to \mathcal{X} \text{, and assume that } f \text{ and } g \text{ are one-to-one. Then, there exists } h : \mathcal{X} \to \mathcal{Y} \text{ such that } h \text{ is one-to-one and onto.} \text{ Source: } [968, \text{ pp. 311, 312}] \]
pp. 16, 17]. Remark: This is the Schroeder-Bernstein theorem.

Fact 1.10.8. Let $X$ and $Y$ be sets, let $f: X \mapsto Y$, and, for $i \in \{1, 2\}$, let $g_i: X \mapsto \mathbb{F}^0$ and $\alpha_i \in \mathbb{F}$. Then, $(\alpha_1 g_1 + \alpha_2 g_2) \circ f = \alpha_1 (g_1 \circ f) + \alpha_2 (g_2 \circ f)$. Remark: The composition operator $\circ (g, f)$ is linear in its first argument.

1.11 Facts on Integers

Fact 1.11.1. Let $n, m \geq 0$ and $k, l \geq 2$. Then, $\prod_{i=1}^k (n + i) \neq m!$. Source: [997]. Remark: A product of consecutive integers cannot be a power of an integer.

Fact 1.11.2. Let $n$ be an integer. Then, $n(n + 1)(n + 2)(n + 3) + 1 = (n^2 + 3n + 1)^2$. Hence, $n(n + 1)(n + 2)(n + 3) + 1$ is a square. Example: $5(6)(7)(8) + 1 = 41^2$. Related: Fact 2.1.2.

Fact 1.11.3. Let $x$ be a real number, and assume that $x + \frac{1}{2}$ is not an integer. Then, the integer closest to $x$ is $\lfloor x + \frac{1}{2} \rfloor$.

Fact 1.11.4. Let $w, x, y, z$ be real numbers, and let $n$ and $m$ be integers. Then, the following statements hold:

1) If $w|x$ and $y|z$, then $wy|xz$.
2) If $x|y$ and $x|z$, then $x^2|yz$.
3) If $x|y$, then $x|ny$.
4) If $x|y$ and $y|z$, then $x|z$.
5) If $x|y$ and $x|z$, then $x|my + nz$.

Fact 1.11.5. Let $n$ and $m$ be integers, at least one of which is nonzero. Then, the following statements hold:

1) Assume that $m$ is positive. Then, there exist unique integers $q$ and $r \in [0, m - 1]$ such that $n = qm + r$. In particular, $q = \lfloor n/m \rfloor$ and $r = \text{rem}_n(n) = n - qm = n - m\lfloor n/m \rfloor \in [0, m - 1]$.
2) If $m$ is positive, then $\lfloor n/m \rfloor = \lfloor (n + m - 1)/m \rfloor$.
3) If $n|mn$, then $\gcd (n, m) = |n|$.
4) If $k$ is prime and $k|m$, then either $k|n$ or $k|n$.
5) $\gcd (n, m)$ $\gcd (n, m) = \gcd (n, m)$ $\gcd (n, m) = \lfloor nm \rfloor$.
6) If both $n$ and $m$ are prime and $m \neq n$, then $n$ and $m$ are coprime.
7) If $n > 0$ and $m > 0$, then $1 \leq \gcd (n, m) \leq \min(n, m)$. (gcd $\lfloor n, m \rfloor$) $\gcd (n, m) = \lfloor nm \rfloor$.
8) $\lfloor n/m \rfloor \gcd (n, m) = \lfloor nm \rfloor$.
9) There exist integers $k, l$ such that $\gcd (n, m) = kn + lm$.

Now, assume that $n$ and $m$ are coprime, and let $k$ be an integer. Then, the following statements hold:

10) $\gcd (n, m, n + m, nm) = 1$.
11) $\gcd (n^k - m^k, n^k + m^k) \leq 2$.
12) $\gcd (n^k - m^k, n^k + m^k) \leq 2^k$.
13) $\gcd (n^2 - mn + m^2, n + m) \leq 3$.
14) $\gcd (nk, m) = \gcd (k, m)$.

Finally, let $n_1, \ldots, n_6$ and $m_1, \ldots, m_4$ be integers. Then, the following statement holds:

15) $\gcd (n_1 m_1, n_1 m_2, \ldots, n_1 m_4) = (\gcd (n_1, \ldots, n_6)) \gcd (m_1, \ldots, m_4)$.

Source: [2380, p. 12]. (x)–(xiv) are given in [1757, pp. 86, 89, 105]; (xv) is given in [1241, p. 123]. Example: $\gcd (221, 754) = 13 = -17(221) + 5(754)$. See [1757, pp. 86, 87]. Remark: The first set in (xvi) contains $k$ products. Remark: $x$ is the GCD identity. See [79, p. 17].

Fact 1.11.6. Let $l, m, n \geq 1$. Then, the following statements hold:
Furthermore, the following statements are equivalent:

1) \( p \mid (n - m) \).

2) \( k \mid (n - m) \).

Fact 1.11.7. Let \( n \geq 1 \). Then, \( \gcd \{n^2 + 1, (n + 1)^2 + 1\} \in \{1, 5\} \). Furthermore, \( \gcd \{n^2 + 1, (n + 1)^2 + 1\} = 5 \) if and only if \( n \equiv 2 \). Source: [289, pp. 31, 165].

Fact 1.11.8. Let \( k_1, \ldots, k_n \) be positive integers, and assume that \( k_1 < \cdots < k_n \). Then,

\[
\sum_{i=1}^{n-1} \frac{1}{\text{lcm} \{k_i, k_{i+1}\}} \leq 1 - \frac{1}{2^{n-1}}.
\]

Source: [2380, p. 12].

Fact 1.11.9. Let \( m \) and \( n \) be integers. Then, the following statements are equivalent:

1) Either both \( m \) and \( n \) are even or both \( m \) and \( n \) are odd.

2) \( n \equiv m \).

Furthermore, the following statements are equivalent:

3) \( m \mid n \).

4) \( n \equiv 0 \).

5) \( n \equiv m \).

Fact 1.11.10. Let \( k \geq 1 \), and let \( m, n, p, q \) be integers. Then, the following statements hold:

1) If \( n = m \), then \( n \equiv m \).

2) \( n \equiv n \).

Furthermore, the following statements are equivalent:

3) \( k \mid (n - m) \).

4) \( k \equiv m \).

5) \( m \equiv n \).

6) \( -n \equiv -m \).

7) \( n - m \equiv 0 \).

Furthermore, the following statement holds:

8) If \( n \equiv m \) and \( m \equiv p \), then \( n \equiv p \).

Next, if \( p \equiv q \) and \( n \equiv m \), then the following statements hold:

9) \( n + p \equiv m + q \).

10) \( n - p \equiv m - q \).
xi) \( np \equiv mq \).

Finally, the following statements hold:

xii) If \( n \equiv m \) and \( p \) is a positive integer, then \( pn \equiv pm \).

xiii) If \( n \equiv m \) and \( p \) is a positive integer, then \( n^p \equiv m^p \).

xiv) If \( pn \equiv pm \), then \( n^{\gcd(k,p)} \equiv m^{\gcd(k,p)} \).

xv) If \( pn \equiv pm \) and \( \gcd(k,p) = 1 \), then \( n \equiv m \).

xvi) \( k \mid \prod_{i=0}^{k-1}(n + i) \). For example, \( 11(12)(13) = 6(286) \) and \( (22)(23) \cdots (28) = 5040(1184040) \).

xvii) If \( n \equiv n_0 \) and \( m \equiv m_0 \), then \( nm \equiv \text{rem}_k(n_0m_0) \).

**Source:** [2763, pp. 30, 31]. **Remark:** "\( \equiv \)" is an equivalence relation on \( \mathbb{Z} \), which partitions \( \mathbb{Z} \) into residue classes.

**Fact 1.11.11.** Let \( n \geq 1 \), and let \( m \) be the sum of the decimal digits of \( n \). Then, the following statements hold:

i) \( 3|n \) if and only if \( 3|m \).

ii) \( n \equiv m \).

**Source:** [2763, pp. 31, 32].

**Fact 1.11.12.** Let \( n \) be a positive integer. Then, the following statements hold:

i) \( n^3 \equiv 0 \) if and only if \( n \equiv 0 \).

ii) \( n^3 \equiv 1 \) if and only if \( n \equiv 1 \) or \( n \equiv 2 \).

**Source:** [2114]. **Example:** \( 3 \equiv 6 \equiv 9 \equiv 12 \equiv 15 \equiv 0, 9 \equiv 36 \equiv 81 \equiv 144 \equiv 225 \equiv 0, \ 1 \equiv 4 \equiv 7 \equiv 10 \equiv 13 \equiv 1, 2 \equiv 5 \equiv 8 \equiv 11 \equiv 14 \equiv 2, \) and \( 1 \equiv 4 \equiv 16 \equiv 25 \equiv 49 \equiv 64 \equiv 100 \equiv 121 \equiv 169 \equiv 196 \equiv 1 \).

**Fact 1.11.13.** Let \( k, l, m, n \geq 1 \). Then, the following statements hold:

i) If \( m \leq n \) is prime, then \( n \) does not divide \( n! + 1 \). Hence, there exists a prime \( k \in [n+1, n!+1] \) such that \( kn! + 1 \).

ii) None of the integers \( n! + 2, n! + 3, \ldots, n! + m \) are prime.

iii) Assume that \( n \geq 2 \) is not prime, and let \( k \) be the smallest prime such that \( kn \). Then, \( k \leq \sqrt{n} \).

If, in addition, \( \sqrt{n} < k \), then \( nk \equiv k \).

iv) If \( n \) is prime, then \( (2n-1)/n \) is an integer.

v) If \( n \geq 3 \) is odd, then \( n^8 \equiv 1 \).

vi) If \( n \) is prime and \( n \geq 5 \), then either \( n \equiv 1 \) or \( n \equiv 5 \).

vii) If \( n \equiv 7 \), then \( n \) is not the sum of three squares of integers.

viii) If \( n \equiv 4 \), then \( n \) is not the sum of three cubes of integers.

ix) The last digit of \( n^3 \) is neither 2, 3, 7, nor 8.

x) Neither 3 nor 5 divides \( (n+1)^3 - n^3 \).

xi) If \( n \geq 2 \), then \( n^4 + 4^n \) is not prime.

xii) \( 3|n(n^2 - 3n + 8), 6|n^3 + 5n, 8|(n-1)(n^3 - 5n^2 + 18n - 8) \).

xiii) \( 9|4^n + 15n - 1, 30|n^5 - n, 120|n^5 - 5n^4 + 4n \).

xiv) \( 121 \) does not divide \( n^5 + 2 + n \).