Unit 1: Fundamentals

1 Discrete mathematics

Various authors write Discrete mathematics as

- Discrete mathematics is the area fascinating many branch of mathematics[1].
- Discrete mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous. Discrete mathematics excludes topics in continuous mathematics such as calculus and analysis.
- Discrete mathematics is the study of discrete (distinct and disconnected) objects. In other words, it is the study of discrete objects and relationship that bind them[2].

  The sets in discrete mathematics are often finite or countable, whereas those in continuous mathematics are often uncountable. Thus, the terms **discrete** and **continuous** are analogous to the terms **digital** and **analog**.
- Discrete mathematics is the branch of mathematics in which we deal with questions involving finite or countably infinite sets[3].
- Discrete mathematics, also called finite mathematics, is the study of mathematical structures that are fundamentally discrete in the sense that its objects can assume only distinct, separate values, rather than in a range of values[4].

  The author also writes, it is the mathematics of integers and of collections of objects that triggers the operation of digital computer, and is used widely in all fields of computer science for programming and reasoning about data structures algorithms and complexity.

[1]Ralph P Grimaldi, Discrete and combinatorial mathematics
[2]Thomas Koshy, Discrete mathematics with application
[3]N L Biggs, Discrete mathematics, 2002
[4]K H Rosen, Discrete mathematics and its applications with combinatorics and graph theory

2 Sets

A set may be viewed as a well defined collection of objects, called the elements or members of the set.

2.1 Notation

Mathematics has its own universally accepted shorthand. The symbols

$\exists$	means "there exists"
$\exists!$	means "there exists a unique"
$\forall$	means "for all"
$\implies$	means "implies" or "if ... then"
$\iff$	means "implies and implied by" or "if and only if" or "iff"
$\in$	means "belongs to" or "is a member of"
$\notin$	means "does not belong to" or "is not a member of"

The symbols $\forall$ is a *universal* quantifier and $\exists$ is an *existential* quantifier.

Exercise 1 *The well known limit statement that "a function $f(x)$ is said to have a limit L if $\forall \epsilon > 0$ (however small we please) there exists a $\delta > 0$ such that whenever $0 < |x - a| < \delta$, then $|f(x) - L| < \epsilon$".*

This limit statement denoted by

$$\lim_{x \to a} f(x) = L$$

can state using the symbols as:

$$(\forall \epsilon > 0)(\exists \delta > 0)(0 < |x - a| < \delta \implies |f(x) - L| < \epsilon)$$

2.2 Set of numbers

Some sets (or collection) are so basic that they have their own proprietary symbols. Some of these are listed below:

$\mathbb{N} = \mathbb{Z}^+$:	The set of positive integers $= \{1, 2, 3, \ldots\}$
$\mathbb{Z}$:	The set of integers $= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$:	The set of rational numbers $= \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$
$\mathbb{Q}^+$:	The set of all positive rational numbers.
$\mathbb{R}$:	The set of real numbers $=$ rational $\cup$ irrational.
$\mathbb{R}^+$:	The set of all positive real numbers.
$\mathbb{C}$:	The set of complex numbers $= \{a + ib : a, b \in \mathbb{R}\}$.

2.3 Set Operations

Suppose $A, B, C, \ldots$ are sets. We use the standard notation for *intersecton* and *union*.

$$A \cap B = \{x | x \in A \quad \text{and} \quad x \in B\}$$

which is the set of all x which are elements of A and B.

$$A \cup B = \{x | x \in A \quad \text{or} \quad x \in B\}$$

which is the set of all x which are elements of A or B.

Note that the word "or" used in here is different than english literature. Here "or" is a connective. Furthermore note that

$$x \in A \cap B \iff x \in A \quad \text{and} \quad x \in B$$

$$x \in A \cup B \iff x \in A \quad \text{or} \quad x \in B$$

$$x \notin A \cap B \iff x \notin A \quad \text{or} \quad x \notin B$$

$$x \notin A \cup B \iff x \notin A \quad \text{and} \quad x \notin B$$

Definition 1 (Disjoint set) *Let ϕ be the null set. If $A \cap B = \phi$, then A and B are said to be disjoint.*

Definition 2 (Subset) *Suppose A and B are sets. The statement that A is a subset of B ($A \subseteq B$) means that if a is an element of A, then a is an element of B. That is*

$$\forall a \, (a \in A \Rightarrow a \in B)$$

That is,

$$A \subseteq B \iff (\forall a \in A \Rightarrow a \in B)$$

Proper Subset: $A \subset B \iff \forall a (a \in A \Rightarrow a \in B)$ but there exists an element $b \in B$ such that $b \notin A$

Equal sets:

$$A = B \iff A \subseteq B \text{ and } B \subseteq A$$

Exercise 2 *Suppose A and B are sets. The statement that A is not a subset of $B (A \not\subseteq B)$ means .....*

Answer: $A \not\subseteq B \iff \exists a \in A$ *such that* $a \notin B$

Exercise 3 *Complete the following proof that $A \subseteq A \cup B$. Suppose $x \in A$. Then $x \in A \cup B$, because ..... Thus by the definition of subset $A \subseteq A \cup B$.*

Exercise 4 *Complete the following proof that $A \cap B \subseteq A$. Suppose $x \in A \cap B$. Then x belongs to ..... Thus $A \cap B \subseteq A$.*

Definition 3 (Complement set) *Suppose U be a universal set and $A \subset U$. The complement $\overline{A}$ of A is defined by*

$$\bar{A} = \{x \in \mathsf{U} \,|x \notin A\}$$

That is

$$x \in \overline{A} \implies x \notin A$$

Further, if A and B are two sets, we define $A - B$ or $A \backslash B$ the **complement of B with respect to** *A*

$$A - B = \{x | x \in A \; and \, x \notin B\}$$

Definition 4 (Symmetric difference)

$$\begin{aligned} A \oplus B &= \{x \mid x \in A \; and \, x \notin B\} \; or \, \{x \in B \; and \, x \notin A\} \\ &= (A - B) \cup (B - A) \end{aligned}$$

Exercise 5 *Show that $A \oplus B = (A \cup B) - (A \cap B)$.*

Definition 5 (Power set) *For any set S, a collection of family of all subsets of S is called the power set of S and is denoted by $P(S)$.*

Exercise 6 *If S is any set of order n, prove that the order of the power set of S is 2^n.*

Hint: Evaluate $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \, y^{n-i}$ at $x = y = 1$.

Definition 6 (Indexed set) *Any set called an index set (Given a set I we say I serves as an* Index set *for the family $\mathcal{F} = \{A_\alpha\}$ of sets if for every I there exists a set A_α in the family $\mathcal{F}$) is assumed to be non-void. Suppose I is an index set and for each $i \in I, A_\alpha$ is the set.*

$$\bigcup_{i \in I} A_i = \{x | \exists i \in I \; with \, x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x | \forall i \in I, x \in A_i\}$$

2.4 Algebra of sets

Sets under the operation of union, intersection and complement satisfy various laws (identities), which are called algebra of sets. Suppose U be a universal set, $A \subset U$ and $B \subset U$.

1. Idempotent properties

$$A \cup A = A, \qquad A \cap A = A$$

2. Commutative properties

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A$$

3. Associative properties

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

4. Distributive properties

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

5. Identity properties

$$A \cup \phi = A, \quad A \cap U = A$$

6. Domination properties

$$A \cup U = U, \quad A \cap \phi = \phi$$

7. De Morgon's laws

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$$
$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$

8. Complement properties

$$\overline{(\overline{A})} = A, \quad A \cup \overline{A} = U, \quad A \cap \overline{A} = \phi$$

9. Absorption properties

$$A \cup (A \cap B) = A, \qquad A \cap (A \cup B) = A$$

Definition 7 (Cartesian product) *If X and Y are sets.*

$$X \times Y = \{(x, y) | x \in X \, and \, y \in Y\}$$

In otherwords, the Cartesian product of X and Y is defined to be the set of all ordered pairs whose first term is in x and whose second term is in Y.

In general, if each of $X_1, X_2, \cdots X_n$ is a set, then $X_1 \times X_2 \times X_3 \cdots \times X_n = \{(x_1, x_2, \cdots, x_n) | x_i \in X_i \, \text{and} \, 1 \leq i \leq n\}$ = the set of all ordered n-tuples whose ith term is in X.

Exercise 7 *Plane:* $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$

Exercise 8 *Real n-space:* $\underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \, components} = \mathbb{R}^n$

Question: Is $(\mathbb{R} \times \mathbb{R}^2) = (\mathbb{R}^2 \times \mathbb{R}) = \mathbb{R}^3$

2.5 The addition principle

This principle is also known as *principle of inclusion and exclusion.*

Theorem 1 (Addition principle)

(*a*) *If A and B are finite sets, then*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

(*b*) *If A, B and C are finite sets, then*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

(*c*) *In more general, if X_i for $1 \leq i \leq n$ are finite sets, then*

$$\begin{aligned} |X_1 \cup X_2 \cup \cdots \cup X_n| &= \sum_{i=1}^{n} |X_i| - \sum_{1 \leq i < j \leq n} |X_i \cap X_j| + \sum_{1 \leq i < j < k \leq n} |X_i \cap X_j \cap X_k| \\ &\quad + \cdots + (-1)^{n-1} |X_1 \cap \cdots \cap X_n| \end{aligned}$$

The general form can be proved using mathematical induction.

Theorem 2 (Seive formula) *If X_i for $1 \leq i \leq n$ are the subsets of a finite set X, then*

$$\begin{aligned} |\overline{(X_1 \cup X_2 \cup \cdots \cup X_n)}| &= |X| - \left(\sum_{i=1}^{n} |X_i| \right) + \sum_{1 \leq i < j \leq n} |X_i \cap X_j| - \sum_{1 \leq i < j < k \leq n} |X_i \cap X_j \cap X_k| \\ &\quad + \cdots + (-1)^n |X_1 \cap X_2 \cap \cdots \cap X_n| \end{aligned}$$

3 Sequence

A sequence is simply a list of objects arranged in a definite order.

Example 1

(*a*) *The sequence*

$$1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1$$

is a finite sequence with repeated items having eleven terms. The digit zero, for example, occurs as the second, third, fifth, seventh, and eighth elements of the sequence.

(*b*) *The sequence*

$$1, -1, 1, -1, 1, -1, \cdots$$

is infinite with alternative elements as 1 and -1. This sequence can be observed by function

$$f : \mathbb{N} \to \{1, -1\}$$

defined by

$$f(n) = (-1)^{n+1}, \quad \forall n \in \mathbb{N}$$

Definition 8 *A sequence is a function from* $\mathbb{N}$ *or* $\mathbb{N} \cup \{0\}$ *to a set* S.

We use a notation a_n to denote the image of the integer n. We call a_n a term of the sequence, denoted by $\{a_n\}$.

Example 2 *Consider the sequence* $\{a_n\}$, *where* $a_n = \dfrac{1}{n}$. *The list of the terms of this sequence, beginning with* a_1, *namely*

$$a_1, a_2, a_3, \cdots$$

starts with

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots$$

Example 3 *The geometric progression is a sequence of the form*

$$a, ar, ar^2, \cdots, ar^n, \cdots$$

where the initial term a *and the common ratio* r *are real numbers.*

Example 4 *An arithmetic progression is a sequence of the form*

$$a, a + d, a + 2d, \cdots, a + nd, \cdots$$

where the initial term a *and common difference* d *are real numbers.*

3.1 Explicit and recursive formula

Consider a sequence

$$3, 8, 13, 18, 23, \cdots$$

This sequence can be defined by an **explicit formula**

$$a_n = f(n) = 5n - 2, \quad \forall n \in \mathbb{Z}^+$$

If we use a subscript to indicate a term's position in the sequence, we can describe this sequence as

$$a_1 = 3, \quad a_n = a_{n-1} + 5, \quad 2 \leq n < \infty$$

A formula like this one, that refers to a previous terms to define the next term is called a **recursive formula**.

EXERCISES

1. Identify formula as recursive or explicit

   (a) $1, 3, 5, 7, \cdots$ [Ans: Explicit $a_n = 2n - 1$; Recursive $a_1, a_{n+1} = a_n + 2$]

   (b) $0, 3, 8, 15, 24, 35, \cdots$ [Ans: Explicit ; Recursive]

   (c) $0, 2, 0, 2, 0, 2, \cdots$ [Ans: Explicit $a_n = \begin{cases} 0, & \text{if } n = \text{odd} \\ 2, & \text{if } n = \text{even} \end{cases}$]

(d) $1, 4, 7, 10, 13, 16 \cdots$ [Ans: Recursive $a_1, a_n = a_{n-1} + 3, 2 \leq n \leq 6$]

(e) $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16} \cdots$ [Ans: Explicit $a_n = \frac{1}{2^{n-1}}$]

2. Write out the first five terms (beginning with $n = 1$) of the sequence with general term is given

   (a) $a_n = 5^n$

   (b) $a_n = 3n^2 + 2n - 6$

   (c) $a_1 = 2.5, a_n = a_{n-1} + 1.5$

   (d) $a_1 = 1, a_2 = 1, a_n = a_{n-2} + a_{n-1}$

3. Write an explicit formula for the sequence

$$2, 5, 8, 11, 14, 17, \cdots$$

   [Ans: $a_n = 3n - 1 \quad \forall n \in \mathbb{Z}^+$]

4. Write a recursive formula for the sequence

$$2, 5, 7, 12, 19, 31, \cdots$$

   [Ans: $a_1 = 2, a_2 = 5, a_{n+2} = a_n + a_{n+1}$]

5. Let F be a function defined for all nonnegative integers by the following recursive definition

$$F(0) = 0,\ F(1) = 1,\ F(N+2) = 2F(N) + F(N+1), \quad N \geq N$$

   Compute the first six values of F; that i, write the values of $F(N)$ for $N = 0, 1, 2, 3, 4, 5$.

3.2 String

Sequence of the form

$$a_1, a_2, \cdots, a_n$$

are often used in computer science. These finite sequence are also called **string**. A string is also denoted by

$$a_1 a_2 a_3 \cdots a_n$$

The **length** of the string S is the number of terms in this string. The empty string is the string that has no terms. The empty string has length zero.

Example 5 *The string*

$$abcd$$

is a string of length four.

3.3 Countable set

A set is called **countable** if it is the set corresponding to some sequence. A set that is not countable is called **uncountable**.

- All finite sets are countable.
- However, not all infinite sets are countable.

Example 6 *The set of integers $\mathbb{Z}$ is countable.*

Proof: For $z \in \mathbb{Z}$, let us define $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(z) = \begin{cases} 2z, & \text{if } z \geq 0 \\ -(2z+1), & \text{if } z < 0 \end{cases}$$

Clearly, f is one-to-one and onto. Thus, $\mathbb{Z}$ is countable.

Example 7 *The set of rational numbers $\mathbb{Q}$ is countable.*

Example 8 *A set $A = \{x | x = 4m,\ m \in \mathbb{Z}\}$ is countable.*

Example 9 *A set $B = \{x | x$ is a real number and $0 < x < 1\ \}$ is uncountable.*

Example 10 *The set of real numbers $\mathbb{R}$ is uncountable.*

4 Integers and divisibility

Theorem 3 (Division algorithm) *If n and m are integers and $n > 0$, we can write*

$$m = q\,n + r$$

for integers q and r with $0 \leq r < n$.

- n is called a divisor.
- m is called a dividend
- q is called a quotient.
- r is called a remainder.

Example 11

(a) *If $m = 16$ and $n = 3$, then*

$$16 = 5(3) + 1$$

so $q = 5$ and $r = 1$.

(b) *If $m = -11$ and $n = 5$, then*

$$-11 = -3(5) + 4$$

so $q = -3$ and $r = 4$.

In the theorem, if $r = 0$, then $m = n\,q$, and hence m is called a **multiple** of n (in other sense n **divides** m), and it is denoted as

$$n|m$$

which is read as n **divides** m. If m is not a multiple of n, we write

$$n \nmid m$$

which is read as n does not divide m.

Theorem 4 *Let a, b, and c be integers.*

(a) *If $a|b$ and $a|c$, then $a|(b + c)$.*

(b) *If $a|b$ and $a|c$, where $b > c$, then $a|(b - c)$.*

(c) *If $a|b$ or $a|c$, then $a|bc$.*

(d) *If $a|b$ and $b|c$, then $a|c$.*

Proof: (c)
Case 1: If $a|b$ but $a \nmid c$. Then $\exists k \in \mathbb{Z}$ such that $b = ka$. Now

$$bc = (ka)c = (kc)a = K_1 a$$

where $k_1 = kc \in \mathbb{Z}$. So $a|bc$.
Case 2: If $a|c$ but $a \nmid b$. Follow similar to Case 1.
Case 3: If $a|b$ but $a|c$. Then $\exists k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $c = k_2 a$. Now

$$bc = (k_1 a)(k_2 a) = (k_1 a k_2)a = ka$$

where $k = k_1 a k_2 \in \mathbb{Z}$. So $a|bc$. □

4.1 Prime and composite numbers

Definition 9 *A number $p > 1$ in $\mathbb{Z}^+$ is called* **prime** *if the only positive integers that divides p are p and 1.*

Example 12 *The numbers $2, 3, 5, 7, 11, 13, 17$ are prime while $4, 6, 8, 10, 12$ are not prime.*

Definition 10 *A number which is not a prime is called a* **composite number**.

4.1.1 Algorithm

Peter Grossman[5] writes, an algorithm is a finite sequence of steps for performing a task, such that

- each step is clear and unambiguous instruction that can be executed in a finite time.

[5]Peter Grossman, Discrete mathematics for computing, 2002

- the sequence in which the steps are to be executed is clearly defined.
- the process is guaranteed to stop after a finite number of steps have been executed.

Some authors write,

- an algorithm is a process or set of rules to be followed by calculations or other problem-solving operations, especially by computer.
- an algorithm is a finite step-by-step procedures to perform a well defined task.
- an algorithm is a set of instructions used for solving a problem in step-by-step manner.

4.1.2 Algorithm to test an integer $N > 1$ is prime

Step 1: Check whether N is 2. If so, N is a prime. If not, proceed to
Step 2: Check whether $2|N$. If so, N is not prime; otherwise proceed to
Step 3: Compute the largest integer $K \leq \sqrt{N}$. Then
Step 4: Check whether $D|N$, where D is any odd number such that $1 < D \leq K$. If $D|N$, then N is not prime; otherwise, N is prime.

4.1.3 Pseudocode

A pseudocode is used to state an algorithm in an English-like system.

Example 13 *Use the steps in algorithm to test $N = 12$ is not a prime.*

Solution:
Step 1: $N \neq 2$. So we proceed Step 2.
Step 2: $2|12$, so 2 is not a prime.

Example 14 *Use the steps in algorithm to test $N = 13$ is a prime.*

Solution: Since $N \neq 2$ and $2 \not| 13$. Since $\sqrt{N} = \sqrt{13} \approx 3.6056$. So the largest integer K such that $K \leq \sqrt{13}$ is $K = 3$. There does not exist any odd number $D, 1 < D \leq K = 3$ with $D|N$. So 13 is a prime.

Theorem 5 (The Fundamental theorem of arithmetic) *Every positive integer $n > 1$ can be written uniquely as*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

where $p_1 < p_2 < \cdots < p_s$ are distinct primes that divides n and k's are positive integers using the number of times each prime occurs as a factor of n.

Example 15

$$\begin{aligned} 72 &= 2^3 \times 3^2 \\ 315 &= 3^2 \times 5^1 \times 7^1 \\ 7000 &= 2^3 \times 5^3 \times 7 \\ 29400 &= 2^3 \times 3^1 \times 5^2 \times 7^2 \end{aligned}$$

4.2 Greatest common divisor

If a, b and k are in $\mathbb{Z}^+$, and $k|a$ and $k|b$, we say that k is a **common divisor** of a and b. If d is the largest such k, then d is called the **greatest common divisor** or **GCD** of a and b, and we write

$$d = \text{GCD}(a, b)$$

Theorem 6 *If $d = GCD(a, b), a, b \in \mathbb{Z}^+$, then*

(a) *$d = sa + tb$ for some integers s and t (s and t are not necessarily positive).*

(b) *If c is any other common divisor of a and b, then $c|d$.*

Proof:
(a) Omitted
(b) $c|a$ and $c|b$ implies there exist $k_1, k_2 \in \mathbb{Z}^+$ such that $a = k_1 c$ and $b = k_2 c$. From (a)

$$\begin{aligned} d &= sa + tb \\ &= sk_1 c + tk_2 c \\ &= (sk_1 + tk_2)c \\ &= kc \end{aligned}$$

where $k = sk_1 + tk_2 \in \mathbb{Z}^+$, and so this implies $c|d$. □

Based on the above theorem, we can define GCD(a, b) as:

$$d = GCD(a, b) \iff \begin{array}{ll} (a) & d|a \text{ and } d|b \\ (b) & \text{whenever } c|a \text{ and } c|b, \text{then } c|d \end{array}$$

Example 16 *The common divisor of* 12 *and* 30 *are* $1, 2, 3$ *and* 6*, so that $GCD(a, b) =$ 6, and*

$$6 = \underbrace{1}_{s} \cdot 30 + \underbrace{(-2)}_{t} \cdot 12$$

Definition 11 (Relatively prime)
If $GCD(a, b) = 1$, then we say that a and b are relatively prime.

How to compute s and t?
It is based on the **Euclidean algorithm**, and the algorithm is based on division algorithm for finding GCD(a, b).

Suppose $a > b > 0$, then by division algorithm we may write

$$a = k_1\, b + r_1, \quad \text{where } k_1 \in \mathbb{Z}^+ \text{ and } 0 \leq r_1 < b$$

If $n|a$ and $n|b$ then $n|r_1$ because $r_1 = a - k_1 b > 0$. Similarly if $n|b$ and $n|r_1$, then $n|a$. So

$$GCD(a, b) = GCD(b, r_1)$$

We now continue the division algorithm as follows:

$$\begin{aligned}
\text{algorithm as follows:} &: b = k_2 r_1 + r_2, && 0 \le r_2 < r_1 \\
\text{divide } r_1 \text{ by } r_2 &: r_1 = k_3 r_2 + r_3, && 0 \le r_3 < r_2 \\
\text{divide } r_2 \text{ by } r_3 &: r_2 = k_4 r_3 + r_4, && 0 \le r_4 < r_3 \\
&\vdots \ : \ \vdots \\
\text{divide } r_{n-2} \text{ by } r_{n-1} &: r_{n-2} = k_n r_{n-1} + r_n, && 0 \le r_n < r_{n-1} \\
\text{divide } r_{n-1} \text{ by } r_n &: r_{n-1} = k_{n+1} r_n + r_{n+1}, && 0 \le r_{n+1} < r_n
\end{aligned}$$

Since $a > b > r_1 > \cdots$, the remainder will eventually becomes zero, so at some point we have $r_{n+1} = 0$, and then

$$GCD(a, b) = r_n$$

How? Previously we have shown that

$$GCD(a, b) = GCD(b, r_1)$$

Repeating this argument with b and r_1, we see that

$$GCD(b, r_1) = GCD(r_1, r_2)$$

Upon continuing, we have

$$GCD(a, b) = GCD(b, r_1) = GCD(r_1, r_2) = \cdots = GCD(r_{n-1} - r_n)$$

Since $r_{n-1} = k_{n+1}\, r_n$, we see that $GCD(r_{n-1}, r_n) = r_n$. Hence

$$r_n = GCD(a, b)$$

Example 17 *Show* $GCD(12, 30) = 6$ *using Euclidean algorithm.*

Solution:

$$\begin{aligned}
\text{Divide 30 by 12} &: 30 = 2(12) + 6 \\
\text{Divide 12 by 6} &: 12 = 2(6) + 0
\end{aligned}$$

So GCD$(12, 30) = 6$, the last nonzero divisors. By reversing the process

$$GCD(12, 30) = 6 = 1(30) - 2(12) = -2(12) + 1(30)$$

Hence $s = -2$ and $t = 1$.

Theorem 7 *If* a *and* b *are in* $\mathbb{Z}^+, b > a$, *then* $GCD(a, b) = GCD(b, b \pm a)$.

Proof: Let $d = GCD(a, b)$. Then $\exists s, t \in \mathbb{Z}$ such that

$$d = sa + tb$$

Since

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

So

$$\begin{aligned} d &= sb - s(b-a) + tb \\ &= (s+t)b - s(b-a) \\ &= s_1 b - s(b-a) \implies d = GCD(b, b-a) \end{aligned}$$

Likewise

$$\begin{aligned} d &= -sb + s(b+a) + tb \\ &= (t-s)b + s(b+a) \\ &= s_2 b + s(b+a) \implies d = GCD(b, b+a) \end{aligned}$$

Hence

$$GCD(a,b) = GCD(b, b \pm a) \quad \square$$

4.3 Least common multiple

If $a, b, k \in \mathbb{Z}^+$ and $a|k, b|k$, we say k is a **common multiple** of a and b. The smallest such k, call it c, is called the **least common multiple** or LCM of a and b, and we write $c = \text{LCM}(a,b)$.

Theorem 8 *If a and b are two positive integers, then $GCD(a,b) \times LCM(a,b) = ab$.*

Proof: Let $p_1, p_2, \cdots, p_k$ be all prime factors of either of a or b. Then we write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

where some of the a_i and b_i may be zero. It then follows that

$$GCD(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$$

and

$$LCM(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}$$

Hence

$$\begin{aligned} GCD(a,b) \times LCM(a,b) &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k} \\ &= (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) \left(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \right) \\ &= ab \end{aligned}$$

Example 18

Let $a = 540$ and $b = 504$. Factoring a and b into primes, we obtain

$$a = 540 = 2^2 \times 3^3 \times 5 = 2^2 \times 3^3 \times 5^1 \times 7^0$$

and

$$b = 504 = 2^3 \times 3^2 \times 7 = 2^3 \times 3^2 \times 5^0 \times 7^1$$

$$\begin{aligned} GCD(540,504) &= 2^{\min(2,3)} \times 3^{\min(3,2)} \times 5^{\min(1,0)} \times 7^{\min(0,1)} \\ &= 2^2 \times 3^2 \times 5^0 \times 7^0 = 36 \end{aligned}$$

and

$$\begin{aligned} LCM(540,504) &= 2^{\max(2,3)} \times 3^{\max(3,2)} \times 5^{\max(1,0)} \times 7^{\max(0,1)} \\ &= 2^3 \times 3^3 \times 5^1 \times 7^1 = 7560 \end{aligned}$$

Then

$$GCD(540,504) \times LCM(540,504) = 36 \times 7560 = 272160 = 540 \times 504$$

Definition 12 (congruent mod a)
We call b **is congruent to** r **mod** a *denoted by*

$$b \cong r(mod\, a) \iff b = ak + r, \quad k \in \mathbb{Z}^+,\ 0 \leq r < a$$

In other sense

$$b \cong r(mod\, a) \iff a|(b-r)$$

Definition 13 (mod-n function)
For each $n \in \mathbb{Z}$*, we define a function* f_n*, the mod-n function, as follows: If* z *is a nonnegative integers, then*

$$f_n(z) = r$$

where r *is the remainder when* z *is divided by* n*.*

Example 19

(*a*) $f_3(14) = 2$ because $14 = 4(3) + 2$

(*b*) $f_7(17) = 3$ because $17 = 2(7) + 3$

Some more Examples

1. Prove that if $a|b$, then $a|mb$, for any $m \in \mathbb{Z}$.
   Solution: $a|b \implies \exists k \in \mathbb{Z}$ such that $b = ka$. Now

   $$mb = m(ka) = (mk)a = k_1 a,\ k_1 = mk \in \mathbb{Z} \implies a|mb$$

2. Let a and b be integers. If p is a prime and $p|ab$, then $p|a$ or $p|b$.
   Solution: If $p \nmid a$, then the only divisor of a and p is 1, and so GCD$(a,p) = 1$. So

   $$1 = sa + tp$$

   for some integers s and t.

   $$p|ab \implies ab = cp, \quad c \in \mathbb{Z}$$

   Now

   $$b = sab + tbp = scp + tbp = (sc + tb)p \implies p|b$$

   Similarly, we can prove the case for $p \nmid b$.

3. **Generalization of Example 2** We can generalize the above result as, if

$$p|a_1a_2\cdots a_n$$

then

$$p|a_i$$

for some i, where p is a prime number.
Solution: We prove the result by induction on n. If $n = 1$, then the result is clearly true. If $n = 2$, then the result follows from above. Let the result be true for numerals less than n. Suppose

$$p|a_1a_2\cdots a_n \implies p|a_1a_2\cdots a_{n-1} \text{ or } p|a_n$$

If p divides $a_1a_2\cdots a_{n-1}$, then by induction hypothesis, p divides a_i for some i. So the result is true in this case also. By induction result is true for all $n > 1$.

4. Show that if $GCD(a, c) = 1$ and $c|ab$, then $c|b$.
Solution:

$$\begin{aligned} GCD(a,b) = 1 &\implies 1 = sa + tc \text{ for some } s,t \in \mathbb{Z} \\ &\implies b = sab + tbc \\ &\implies b = smc + tbc \quad (\text{since } c|ab \implies ab = mc, m \in \mathbb{Z}) \\ &\implies b = s_1c + t_1c \end{aligned}$$

where $s_1 = sm,\ t_1 = tb \in \mathbb{Z}$. So $b = s_1c + t_1c \implies c|b$.

5. Show that if $GCD(a, b) = 1, a|m$ and $c|m$, then $ac|m$.
Solution: $GCD(a, b) = 1 \implies 1 = sa + tc,\ s, t \in \mathbb{Z}$. Also $a|m$ and $c|m$, so $m = k_1a$ and $m = k_2c$ for some integers k_1 and k_2. Now $m \cdot m = (k_1a)(k_2c) = (k_1k_2)ac$. Also

$$\begin{aligned} 1 = s\left(\frac{m}{k_1}\right) + ts\left(\frac{m}{k_2}\right) &\implies k_1k_2 = sk_2m + tk_1m \\ &\implies \frac{m \cdot m}{ac} = sk_2m + tk_1m \\ &\implies m = (sk_2 + tk_1)ac \\ &\implies ac|m, \quad \text{because } sk_2 + tk_1 \in \mathbb{Z} \end{aligned}$$

6. Show that if $d = GCD(a, b), a|b$ and $c|b$, then $ac|bd$.
Solution: $a|b \implies b = k_1a$ and $c|b \implies b = k_2c$ for some $s, t \in \mathbb{Z}$.

$$\begin{aligned} d = GCD(a,b) &\implies d = sa + tb,\ s,t \in \mathbb{Z} \\ &\implies bd = (sa)b + (tb)b \\ &\implies bd = (sa)k_2c + (tk_2c)b \\ &\implies bd = (sk_2)ac + (tk_2c)(k_1a) \\ &\implies bd = (sk_2 + tk_2k_1)ac \\ &\implies ac|bd \end{aligned}$$

7. Show that $LCM(a, ab) = ab$.
   Solution: Clearly $a|ab$ and $ab|ab$. So ab is the common multiple of a and ab, and no smaller multiple of ab exists. So $LCM(a, ab) = ab$.

8. Show that $LCM(a, b) = 1$, then $LCM(a, b) = ab$.
   Solution: Since

$$\begin{aligned} GCD(a,b) \times LCM(a,b) &= ab \\ 1 \times LCM(a,b) &= ab \\ LCM(a,b) &= ab \end{aligned}$$

9. Let $c = LCM(a, b)$. Show that if $a|k$ and $b|k$, then $c|k$.
   Solution: We know

$$\begin{aligned} GCD(a,b) \times LCm(a,b) &= ab \\ c \times GCD(a,b) &= ab \end{aligned}$$

   Since $a|k$ and $b|k$ so $k = ma$ and $k = nb$ for some $m, n \in \mathbb{Z}$. Let $d = GCD(a, b)$, so $d = sa + tb$ for some $s, t \in \mathbb{Z}$. Now from above

$$\begin{aligned} cd &= ab \\ c(sa+tb) &= ab \\ c\left[s\frac{k}{m} + t\frac{k}{n}\right] &= \frac{k}{m}\frac{k}{n} \\ (sn+tm)c &= k \\ &\implies k|c, \quad sn+tm \in \mathbb{Z} \end{aligned}$$

10. If g is the mod-5 function, solve

    (a) $g(n) = 2$.
    We have to find $n \in \mathbb{Z}^+$ which when divided by 5 leaves remainder 2. So the solution set is

$$\{2, 7, 12, 17, \cdots\}$$

    (b) $g(n) = 1$.

$$\{1, 6, 11, 16, \cdots\}$$

5 Representation of integers

In our daily life, we use numbers on the decimal system. For example, represent the decimal number 4987.

3	2	1	0	$\leftarrow$	position
10^3	10^2	10^1	10^0	$\leftarrow$	place value
4	9	8	7	$\leftarrow$	decimal point
			$\vert$		
				$\longrightarrow$	$7 \times 10^0 = 7$
		$\vert$			
			$\longrightarrow$		$8 \times 10^1 = 80$
	$\vert$				
		$\longrightarrow$			$9 \times 10^2 = 900$
$\vert$					
	$\longrightarrow$				$4 \times 10^3 = 4000$
					Sum = 4987

Thus

$$(4987)_{10} = 4 \times 10^3 + 9 \times 10^2 + 8 \times 10^1 + 7 \times 10^0$$

which is a polynomial in 10. The subscript designated the base of the decimal number.

Theorem 9 *If $b > 1$ is an integer, then every positive integer*

$$n = d_k d_{k-1} \cdots d_1 d_0$$

can be uniquely expressed with base b as

$$(d_k d_{k-1} \cdots d_1 d_0)_b = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_1 b + d_0$$

where $0 \leq d_i < b,\ i = 0, 1, \cdots, k$, and $d_k \neq 0$. $\square$

The most commonly used bases are as shown in table below:

base, b	Number system	Symbols
2	Binary	0, 1
8	Octat	0, 1, 2, 3, 4, 5, 6, 7
10	Decimal	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
16	Hexadecimal	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

There is other base 26 used in **cryptology** (the science of producing and deciphering secret codes).

Example 20 *Find the base* 4 *representation of* 158 *or* $(158)_{10}$.

Solution: We repeatedly divide by 4, and save the remainder

Divisor	Dividend	Remainder
4	158	2
4	39	3
4	9	1
4	2	2
4	0	

Thus

$$158 = (2132)_4$$

Verification This is an expression on base 10:

$$(2132)_4 = 2 \times 4^3 + 1 \times 4^2 + 3 \times 4^1 + 2 \times 4^0 = 128 + 16 + 12 + 2 = 158$$

Example 21 *Find the base* 2 *representation of* 39 *or* $(39)_{10}$.

Solution: We repeatedly divide by 4, and save the remainder

Divisor	Dividend	Remainder
2	39	1
2	19	1
2	9	1
2	4	0
2	2	0
2	1	1
2	0	

Thus

$$39 = (100111)_2$$

Verification This is an expression on base 10:

$$(100111)_2 = 1\times2^5+0\times2^4+0\times2^3+1\times2^2+1\times2^1+1\times2^0 = 32+0+0+4+2+1 = 39$$

Example 22 *Find the base* 5 *representation of* 732 *or* $(732)_{10}$.

Solution: We repeatedly divide by 4, and save the remainder

Divisor	Dividend	Remainder
5	732	2
5	146	1
5	29	4
5	5	0
5	1	1
5	0	

Thus

$$732 = (10412)_5$$

Verification This is an expression on base 10:

$$(10412)_5 = 1 \times 5^4 + 0 \times 5^3 + 4 \times 5^2 + 1 \times 5^1 + 2 \times 5^0 = 625 + 0 + 100 + 5 + 2 = 732$$

EXERCISES

1. Write the expansion in base 10.
   (a) $(144)_5$ (b) $(11231)_5$ (c) $(110111)_2$

6 Boolean matrix

Review
Definition, types of matrices, algebraic operations on matrices, some properties of matrices.

Definition 14 (Boolean matrix)
A Boolean matrix, also called a bit matrix, is an $m \times n$ matrix whose entries are either 0 or 1.

6.1 Operations on Boolean matrices

1. **Join and Meet in Boolean matrices** Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $m \times n$ Boolean matrices. We define

   (*a*) the **join** of A and B, denoted by $A \vee B$ is a Boolean matrix $C = [c_{ij}]$ defined by

   $$c_{ij} = \begin{cases} 1, & \text{if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0, & \text{if } a_{ij} \text{ and } b_{ij} \text{ are both } 0 \end{cases}$$

   (*b*) the **meet** of A and B, denoted by $A \wedge B$ is a Boolean matrix $C = [c_{ij}]$ defined by

   $$c_{ij} = \begin{cases} 0, & \text{if } a_{ij} = 0 \text{ or } b_{ij} = 0 \\ 1, & \text{if } a_{ij} \text{ and } b_{ij} \text{ are both } 1 \end{cases}$$

2. **Boolean product** Let $A = [a_{ij}]$ be an $m \times p$, and $B = [b_{ij}]$ be $p \times n$ Boolean matrices. We define the **Boolean product** of A and B, denoted by $A \odot B$ is the $m \times n$ Boolean matrix $C = [c_{ij}]$ defined by

   $$c_{ij} = \begin{cases} 1, & \text{if } a_{ik} = 1 \text{ and } b_{kj} = 1 \text{ for some } k, 1 \leq k \leq p \\ 0, & \text{otherwise} \end{cases}$$

   The above can be expressed as

   $$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{ip} \wedge b_{pj})$$

Example 23 *Consider the Boolean matrices*

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix};$$

Compute $A \vee B$; $A \wedge B$; $A \odot B$

Solution

$$A \vee B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$A \wedge B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \wedge \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and

$$\begin{aligned} A \odot B &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 1) \vee (0 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) \vee (0 \wedge 0) \\ (0 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) \\ (1 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 1) & (1 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) \end{bmatrix} \\ &= \begin{bmatrix} 1 \vee 0 \vee 0 & 1 \vee 0 \vee 0 & 1 \vee 0 \vee 0 \\ 0 \vee 0 \vee 1 & 0 \vee 0 \vee 0 & 0 \vee 0 \vee 0 \\ 1 \vee 0 \vee 1 & 1 \vee 0 \vee 0 & 1 \vee 0 \vee 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

Theorem 10 *If A, B and C are Boolean matrices of compatible sizes, then*

1. *Commutative law*

$$A \vee B = B \vee A; \qquad A \wedge B = B \wedge A$$

2. *Associate law*

$$(A \vee B) \vee C = A \vee (B \vee C)$$
$$(A \wedge B) \wedge C = A \wedge (B \wedge C)$$

3. *Distributive law*

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$

3. *Associate law of Boolean product*

$$(A \odot B) \odot C = A \odot (B \odot C)$$

Example 24 *Compute the following proofs:*

(*a*) $A \vee A = A$
Proof: *Let $b_{ij} \in A \vee A$. If $b_{ij} = 0$, then $a_{ij} = \underline{0}$, because both a_{ij} and b_{ij} must be $\underline{0}$. If $b_{ij} = 1$, then $a_{ij} = \underline{1}$, because either $a_{ij} = 1$ or $a_{ij} = 1$. Hence $b_{ij} = a_{ij}$ for each i, j pair.*

(*b*) $A \wedge A = A$
Proof: *Let $b_{ij} \in A \wedge A$. If $b_{ij} = 0$, then $a_{ij} = \underline{0}$ or $a_{ij} = \underline{0}$. If $b_{ij} = 1$, then $a_{ij} = \underline{1}$ and $a_{ij} = 1$. Hence $b_{ij} = a_{ij}$ for each i, j pair.*

Example 25 *Show that* $A \vee B = B \vee A$.

Proof: Let $C = [c_{ij}] = A \vee B$, then

$$c_{ij} = \begin{cases} 0, & \text{if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 1, & \text{if } a_{ij} = 0 \text{ and } b_{ij} = 0 \end{cases}$$

Also, $D = [d_{ij}] = B \vee A$, then

$$\begin{aligned} d_{ij} &= \begin{cases} 1, & \text{if } b_{ij} = 1 \text{ or } a_{ij} = 1 \\ 0, & \text{if } b_{ij} = 0 \text{ and } a_{ij} = 0 \end{cases} \\ &= \begin{cases} 1, & \text{if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0, & \text{if } a_{ij} = 0 \text{ and } b_{ij} = 0 \end{cases} \\ &= c_{ij} \text{ for every pair } i, j \end{aligned}$$

So $C = D$. Hence $A \vee B = B \vee A$.

EXERCISES

1. Let $C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ and $D = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$. Compute each of the following:

   (a) $C \oplus D$ (b) $C \vee D$ (c) $C \wedge D$

2. Let $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ and $D = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$. Compute each of the following:

   (a) $C \oplus D$ (b) $C \vee D$ (c) $C \wedge D$

3. Prove the following

   (a) $A \vee (B \vee C) = (A \vee B) \vee C$
   (b) $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
   (c) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

7 Mathematical structures

Definition 15 (Mathematical structure)
A collection of objects with operations defined on them and the accompanying properties form a **mathematical structure** *or* **mathematicsl system**.

Example 26 $(Set\ ,\ \cup,\ \cap,\ -\ )$ *The collection of sets with the operations of union, intersection, complement and their accompanying properties constitute a mathematical structure.*

Definition 16 *A structure is* **closed with respect to an operation** *if that operation always produces another member of the collection of objects.*

Example 27

(*a*) *The structure* $(odd\ integers, +, *)$ *is not closed with respect to addition.*

(*b*) *The structure* $(n \times n\ matrices, +, *, T)$ *is closed with respect to addition of matrices, and multiplication of matrices.*

Definition 17 (Binary operation/Unary operation)
An operation that combines two objects is called a **binary operation**. *An operation that requires only one object is a* **unary operation**.

Example 28

(*a*) *Transpose of matrices is a unary operation.*

(*b*) *Addition operation in* $\mathbb{Z}^+$ *is a binary operation.*

(*c*) *Subtraction operation in* $\mathbb{Z}^+$ *is not a binary operation.*

Properties Let S be a set and consider the mathematical structure $(S, \square, \triangle)$ with operations $\square$ and $\triangle$. Then

(*i*) $\square$ is commutative if

$$a\square b = b\square a, \qquad \forall a, b \in S$$

(*ii*) $\square$ is associative if

$$a\square(b\square c) = (a\square b)\square c, \qquad \forall a, b, c \in S$$

(*ii*) $\triangle$ is distribute over $\square$ if

$$a\triangle(b\square c) = (a\triangle b)\square(a\triangle c), \qquad \forall a, b, c \in S \quad \text{(left distribution)}$$

$$(b\square c)\triangle a = (b\triangle a)\square(b\triangle c), \qquad \forall a, b, c \in S \quad \text{(right distribution)}$$

Example 29 *In the mathematical structure* $(Sets, \cup, \cap)$*, union distributes over intersection, and intersection distributes over union.*

Definition 18 *If the unary operation* $*$ *and the binary operations are* $\square$ *and* $\triangle$*. Then De-Morgon's law states*

$$(x\square y)^* = x^*\triangle y^*$$
$$(x\triangle y)^* = x^*\square y^*$$

For example,

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$
$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$$

Definition 19 (Identity element) *Suppose a structure with binary operation $\triangle$ contains an element e such that*

$$e\triangle x = x\triangle e$$

for all x in that collection of objects. We then call e an identity for $\triangle$.

Example 30 *Consider a structure $(\mathbb{Z}, +)$. Then 0 is the identity for the operation $+$, and is called additive identity for $\mathbb{Z}$.*

Theorem 11 *If e is an identity for a binary operation $\square$, then e is unique.*

Proof: Assume e' is an another identity for $\square$. Then

$$e'\square e = e\square e' = e$$

Also e is an identity for $\square$, then

$$e'\square e = e\square e' = e'$$

Hence $e = e'$. So identity element is unique. $\square$

Definition 20 (Inverse element) *If a binary operation $\square$ has an identity e and x, y be any two elements of the collection of objects of that structure such that*

$$x\square y = y\square x = e$$

then we call y is $\square$-inverse of x. Also x is called $\square$-inverse of y.

Example 31 *Consider a structure $(\mathbb{Z}, +)$. Then $-x \in \mathbb{Z}$ is the inverse element for $x \in \mathbb{Z}$ under the operation addition.*

Theorem 12 *If $\square$ is an associative operation and x has a $\square$-inverse y, then y is unique.*

Proof: Assume that there is another $\square$-inverse for x, say z. Then

$$(z\square x)\square y = e\square y = y$$

and

$$z\square(x\square y) = z\square e = z$$

Since $\square$ is associative, so $(z\square x)\square y = z\square(x\square y)$. This implies $y = z$. Hence unique. $\square$

Example 32 *Let $\square$ be defined for the set $\{0, 1\}$ by the following table*

$\square$	0	1
0	0	1
1	1	0

Show that $(a)\square$ is commutative, and $(b)\square$ is associative.

Solution:
(a) The statement $x\square y = y\square x$ must be true for all choices of x and y. Hence there is only one case to check:

$$\text{Is } 0\square 1 = 1\square 0 \text{ true ?}$$

Since both $0\square 1$ and $1\square 0$ are 1, $\square$ is commutative.
(b) The statement $(x\square y)\square z = x\square(y\square z)$ must be true for all choices of x, y and z. Now the possible cases can be organized in the following table.

x	y	z	$x\square y$	$(x\square y)\square z$	$y\square z$	$x\square(y\square z)$
0	0	0	0	0	0	0
0	0	1	0	1	0	1
0	1	0	1	1	1	1
0	1	1	1	0	0	0
1	0	0	1	1	1	1
1	0	1	1	0	1	0
1	1	0	0	1	1	1
1	1	1	0	1	0	1

From the table, it is clear that the operation $\square$ is associative.

EXERCISES

1. Consider a structure $R = \left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, +, *, {}^T \right)$, where $a \in \mathbb{R}$.
   (a) Show that R is closed with respect to addition.
   (b) Show that R is closed with respect to multiplication.
   (c) Show that R is closed with respect to the transpose operation.
   (d) Does R have an identity for addition? If so, what is it?
   (e) Does R have an identity for multiplication? If so, What is it?

2. Let $R = (\mathbb{Q}, \square)$, where $x\square y = \dfrac{x+y}{2}$. Determine which of the following properties hold for this structure.
   (a) Closure
   (b) Commutative
   (c) Associative
   (d) An identity element
   (e) An inverse element for every element

3. Let $S = (2 \times 2 \text{ Boolean matrices}, \wedge, \vee, \oplus)$ and A be a 2×2 Boolean matrix. Describe the $\wedge$-inverse of A is S.