Lecture Notes on Discrete Mathematics

October 15, 2018

Contents

Chapter 1

Basic Set Theory

We will use the following notation throughout the book.

1. The empty set, denoted $\emptyset$, is the set that has no element.

2. $\mathbb{N} := \{1, 2, \ldots\}$, the set of Natural numbers;

3. $\mathbb{W} := \{0, 1, 2, \ldots\}$, the set of whole numbers

4. $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of Integers;

5. $\mathbb{Q} := \{\frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0\}$, the set of Rational numbers;

6. $\mathbb{R} :=$ the set of Real numbers; and

7. $\mathbb{C} :=$ the set of Complex numbers.

For the sake of convenience, we have assumed that the integer 0, is also a natural number. This chapter will be devoted to understanding set theory, relations, functions and the principle of mathematical induction. We start with basic set theory.

1.1 Basic Set Theory

Mathematicians over the last two centuries have been used to the idea of considering a collection of objects/numbers as a single entity. These entities are what are typically called sets. The technique of using the concept of a set to answer questions is hardly new. It has been in use since ancient times. However, the rigorous treatment that the set received happened only in the 19th century due to the german mathematician Georg Cantor. He was the first person who was responsible in ensuring that the set had a home in mathematics. Cantor developed the concept of the set during his study of the trigonometric series, which is now known as the limit point or the derived set operator. He developed the transfinite numbers of which the ordinals and cardinals are two types. His new and path-breaking ideas were not well received by his contemporaries. Further, from his definition of a set, a number of contradictions and paradoxes arose. One of the most famous paradoxes is the Russell's Paradox, due to Bertrand Russell in 1918. This paradox amongst others, opened the stage for the development of axiomatic set theory. The interested reader may refer to Katz [8]. In this book, we will consider the intuitive or naive view point of sets.

The notion of a set is taken as a primitive and so we will not try to define it explicitly. On the contrary, we will give it an informal description and then go on to establish the properties of a set.

A set can be described intuitively as a collection of distinct objects. The objects are called the elements or members of the set. Here, we will be able to say when an object/element belongs to a set or not.

The objects can be just about anything from real physical things to abstract mathematical objects. The principal, distinguishable and an important feature of a set is that the objects are "distinct" or "uniquely identifiable."

Any object of the collection comprising a set is referred as an element of the set. So, if S is a set and x is an element of S, we denote it by $x \in S$. If x is not an element of S, we denote it by $x \notin S$.

A set is typically denoted by curly braces, $\{ \}$.

Example 1.1.1. 1. $X = \{\text{apple}, \text{tomato}, \text{orange}\}$. Hence, orange $\in X$, but potato $\notin X$.

2. $X = \{a_1, a_2, \ldots, a_{10}\}$. Then, $a_{100} \notin X$.

3. Observe that the sets $\{1, 2, 3\}$, $\{3, 1, 2\}$ and $\{\text{digits in the number12321}\}$ are the same as the order in which the elements appear doesn't matter.

We now address the idea of distinctness of elements of a set, which comes with its own subtleties.

Example 1.1.2. 1. Consider a collection of identical red balls in a basket. Is it a set?

2. Consider the list of digits $1, 2, 1, 4, 2$. Is it a set?

3. Let $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Then X is the set of first 10 natural numbers. Or equivalently, X is the set of integers between 0 and 11.

Definition 1.1.3. **[Empty Set]** The set S that contains no element is called the **empty set** or the **null set** denoted by $\{ \}$ or $\emptyset$.

An object x is an element or a member of a set S, written $x \in S$, if x satisfies the rule that defines the membership for S. With this notation, one has three main ways for specifying a set. They are:

1. Listing all its elements (list notation), *e.g.*, $X = \{2, 4, 6, 8, 10\}$. Then X is the set of even integers between 0 and 12.

2. Stating a property with notation (predicate notation), *e.g.*,

   (a) $X = \{x : x \text{ is a prime number}\}$. This is read as "$X$ is the set of all x such that x is a prime number". Here x is a variable and stands for any object that meets the criteria after the colon.

   (b) The set $X = \{2, 4, 6, 8, 10\}$ in the predicate notation can be written as

      i. $X = \{x : 0 < x \leq 10, x \text{ is an even integer }\}$, or

      ii. $X = \{x : 1 < x < 11, x \text{ is an even integer }\}$, or

      iii. $x = \{x : 2 \leq x \leq 10, x \text{ is an even integer }\}$ etc.

   (c) $X = \{x : x \text{ is a student in IITK and } x \text{ is older than } 30\}$.

   Note that the above expressions are certain rules that help in defining the elements of the set X. In general, one writes $X = \{x : p(x)\}$ or $X = \{x \mid p(x)\}$ to denote the set of all elements x (variable) such that property $p(x)$ holds. In the above note that "colon" is sometimes replaced by "—".

3. Defining a set of rules which generate its members (recursive notation), *e.g.*, let $X = \{x : x \text{ is an even integer greater than } 3\}$. Then, X can also be written as

   (a) $4 \in X$.

   (b) whenever $x \in X$ then $x + 2 \in X$.

   (c) no other element different from those above belongs to X.

Thus, in recursive rule, the first rule is the basis of recursion, the second rule gives a method to generate new element(s) from the elements already determined and the third rule binds or restricts the defined set to the elements generated by the first two rules. The third rule should always be there. But, in practice it is left implicit. At this stage, one should make it explicit.

Definition 1.1.4. [**Subset and Equality**] Let X and Y be two sets.

1. Let Z be a set such that whenever $x \in Z$, $x \in X$ as well, then Z is said to be a **subset** of the set X, denoted $Z \subseteq X$.
2. If $X \subseteq Y$ and $Y \subseteq X$, then X and Y are said to be **equal**, denoted $X = Y$.

Example 1.1.5. 1. Let X be a set. Then $X \subseteq X$. Thus, $\emptyset \subseteq \emptyset$ and hence the empty set is a subset of every set.

2. We know that $\mathbb{N} \subseteq \mathbb{W} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
3. Note that $\emptyset \notin \emptyset$.
4. Let $X = \{a, b, c\}$. Then $a \in X$ but $\{a\} \subseteq X$. Also, $\{\{a\}\} \nsubseteq X$.
5. If $S \subseteq T$ and $S \neq T$ then S is called a **proper subset** of T. That is, there exists an element $a \in T$ such that $a \notin S$.

In the next two subsections, we mention set operations that help us in generating new sets from existing sets.

1.1.1 Union and Intersection of Sets

Definition 1.1.6. [**Set Union and Intersection**] *Let X and Y be two sets.*

1. *The* **union** *of X and Y, denoted by $X \cup Y$, is the set whose elements are the elements of X as well as the elements of Y. Specifically, $X \cup Y = \{x \mid x \in X \text{ or } x \in Y\}$.*
2. *The* **intersection** *of X and Y, denoted by $X \cap Y$, is the set that contains only the common elements of X and Y. Specifically, $X \cap Y = \{x \mid x \in X \text{ and } x \in Y\}$. The set X and Y are said to be* **disjoint** *if $X \cap Y = \emptyset$.*

Example 1.1.7. 1. Let $A = \{1, 2, 4, 18\}$ and $B = \{x : x \text{ is an integer}, 0 < x \leq 5\}$. Then,

$$A \cup B = \{1, 2, 3, 4, 5, 18\} \text{ and } A \cap B = \{1, 2, 4\}.$$

2. Let $S = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ and $T = \{x \in \mathbb{R} : .5 \leq x < 7\}$. Then,

$$S \cup T = \{x \in \mathbb{R} : 0 \leq x < 7\} \text{ and } S \cap T = \{x \in \mathbb{R} : .5 \leq x \leq 1\}.$$

3. Let $A = \{\{b, c\}, \{\{b\}, \{c\}\}, b\}$ and $B = \{a, b, c\}$. Then

$$A \cap B = \{b\} \text{ and } A \cup B = \{a, b, c, \{b, c\}, \{\{b\}, \{c\}\}\ \}.$$

We now state a few properties related to union and intersection of sets. The proof of only the first distributive law is presented. The readers are supposed to provide proofs of the other results.

Lemma 1.1.8. *Let R, S and T be three sets. Then,*

1. *Obvious properties:*
   - (a) *$S \cup T = T \cup S$ and $S \cap T = T \cap S$ (union and intersection are commutative operations).*
   - (b) *$R \cup (S \cup T) = (R \cup S) \cup T$ and $R \cap (S \cap T) = (R \cap S) \cap T$ (union and intersection are associative operations).*

   (c) $S \subseteq S \cup T$, $T \subseteq S \cup T$.

   (d) $S \cap T \subseteq S$, $S \cap T \subseteq T$.

   (e) $S \cup \emptyset = S$, $S \cap \emptyset = \emptyset$.

   (f) $S \cup S = S \cap S = S$.

2. *Distributive laws (combines union and intersection):*

   (a) $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$ *(union distributes over intersection).*

   (b) *and* $R \cap (S \cup T) = (R \cap S) \cup (R \cup T)$ *(intersection distributes over union).*

Proof. Let $x \in R \cup (S \cap T)$. Then, $x \in R$ or $x \in S \cap T$. If $x \in R$ then clearly, $x \in R \cup S$ and $x \in R \cup T$. Thus, $x \in (R \cup S) \cap (R \cup T)$. If $x \notin R$ but $x \in S \cap T$, then $x \in S$ and $x \in T$. Hence, $x \in R \cup S$ and $x \in R \cup T$. Thus, $x \in (R \cup S) \cap (R \cup T)$. Hence, we see that $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$.

Now, let $y \in (R \cup S) \cap (R \cup T)$. Then, $y \in R \cup S$ and $y \in R \cup T$. Now, if $y \in R \cup S$ then either $y \in R$ or $y \in S$ or both.

If $y \in R$ then clearly $y \in R \cup (S \cap T)$. If $y \notin R$ then the conditions $y \in R \cup S$ and $y \in R \cup T$ imply that $y \in S$ and $y \in T$. Thus, $y \in S \cap T$ and hence $y \in R \cup (S \cap T)$. This shows that $(R \cup S) \cap (R \cup T) \subseteq R \cup (S \cap T)$ and hence we get a complete proof of the first distributive law. ∎

EXERCISE **1.1.9.** 1. *Complete the proof of Lemma 1.1.8.*

2. *Proof the following statements:*

   (a) $S \cup (S \cap T) = S \cap (S \cup T) = S$.

   (b) $S \subseteq T$ *if and only if* $S \cup T = T$.

   (c) *If* $R \subseteq T$ *and* $S \subseteq T$ *then* $R \cup S \subseteq T$.

   (d) *If* $R \subseteq S$ *and* $R \subseteq T$ *then* $R \subseteq S \cap T$.

   (e) *If* $S \subseteq T$ *then* $R \cup S \subseteq R \cup T$ *and* $R \cap S \subseteq R \cap T$.

   (f) *If* $S \cup T \neq \emptyset$ *then either* $S \neq \emptyset$ *or* $T \neq \emptyset$.

   (g) *If* $S \cap T \neq \emptyset$ *then both* $S \neq \emptyset$ *and* $T \neq \emptyset$.

   (h) $S = T$ *if and only if* $S \cup T = S \cap T$.

1.1.2 Set Difference, Set Complement and the Power Set

Definition 1.1.10. [**Set Difference, Symmetric Difference**] Let A and B be two sets.

1. The **set difference** of X and Y, denoted by $X \setminus Y$, is defined by $X \setminus Y = \{x \in X : x \notin Y\}$.
2. The **symmetric difference** of X and Y, denoted by $X \Delta Y$, is defined by $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$.

Example 1.1.11. 1. Let $A = \{1, 2, 4, 18\}$ and $B = \{x : x \text{ is an integer}, 0 < x \leq 5\}$. Then,

$$A \setminus B = \{18\}, \; B \setminus A = \{3, 5\} \;\text{ and }\; A \Delta B = \{3, 5, 18\}.$$

2. Let $S = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ and $T = \{x \in \mathbb{R} : .5 \leq x < 7\}$. Then,

$$S \setminus T = \{x \in \mathbb{R} : 0 \leq x < .5\} \;\text{ and }\; T \setminus S = \{x \in \mathbb{R} : 1 < x < 7\}.$$

3. Let $A = \{\{b, c\}, \{\{b\}, \{c\}\}, b\}$ and $B = \{a, b, c\}$. Then

$$A \setminus B = \{\{b, c\}, \{\{b\}, \{c\}\}\}, B \setminus A = \{a, c\} \;\text{ and }\; A \Delta B = \{a, c, \{b, c\}, \{\{b\}, \{c\}\}\}.$$

In many set theory problems, all sets are defined to be subsets of some reference set, referred to as the universal set, denoted mostly by U. We now define the complement of a set.

Definition 1.1.12. [**Set complement**] Let U be the universal set and $X \subseteq U$. Then, the **complement** of X, denoted by X', is defined as $X' = \{x \in U : x \notin X\}$.

We now state a few properties that directly follow from the definition and hence the proofs are omitted.

Lemma 1.1.13. *Let U be the universal set and $S, T \subseteq U$. Then,*

1. $U' = \emptyset$ *and* $\emptyset' = U$.
2. $S \cup S' = U$ *and* $S \cap S' = \emptyset$.
3. $S \cup U = U$ *and* $S \cap U = S$.
4. $(S')' = S$.
5. $S \subseteq S'$ *if and only if* $S = \emptyset$.
6. $S \subseteq T$ *if and only if* $T' \subseteq S'$.
7. $S = T'$ *if and only if* $S \cap T = \emptyset and S \cup T = U$.
8. $S \setminus T = S \cap T'$ *and* $T \setminus S = T \cap S'$.
9. $S \Delta T = (S \cup T) \setminus (S \cap T)$.
10. *De-Morgan's Laws:*
    (a) $(S \cup T)' = S' \cap T'$.
    (b) $(S \cap T)' = S' \cup T'$.

    The De-Morgan's laws help us to convert arbitrary set expressions into those that involve only complements and unions or only complements and intersections.

Definition 1.1.14. [**Power Set**] Let X be a subset of a set Ω. Then the set that contains all subsets of X is called the power set of X and is denoted by $\mathcal{P}(X)$ or 2^X.

Example 1.1.15. 1. Let $X = \emptyset$. Then $\mathcal{P}(\emptyset) = \{\emptyset, X\} = \{\emptyset\}$.

2. Let $X = \{\emptyset\}$. Then $\mathcal{P}(X) = \{\emptyset, X\} = \{\emptyset, \{\emptyset\}\}$.

3. Let $X = \{a, b, c\}$. Then $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

4. Let $X = \{\{b, c\}, \{\{b\}, \{c\}\}\}$. Then $\mathcal{P}(X) = \{\emptyset, \{\{b, c\}\}, \{\{\{b\}, \{c\}\}\}, \{\{b, c\}, \{\{b\}, \{c\}\}\}\ \}$.

1.2 Relations and Functions

We start with the definition of the cartesian product of two sets and use it to define relations. Note that this is another method to construct new sets from given set(s).

Definition 1.2.1. [**Cartesian Product**] Let X and Y be two sets. Then their cartesian product, denoted by $X \times Y$, is defined as $X \times Y = \{(a, b) : a \in X, b \in Y\}$. Thus,

$$(a_1, b_1) = (a_2, b_2) \text{ if and only if } a_1 = a_2 \text{ and } b_1 = b_2.$$

Example 1.2.2. 1. Let $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$. Then

$$\begin{aligned} A \times A &= \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}. \\ A \times B &= \{(a, 1), (a, 2), (a, 3), (a, 4), (b, 1), (b, 2), (b, 3), (b, 4), (c, 1), (c, 2), (c, 3), (c, 4)\}. \end{aligned}$$

2. The Euclidean plane, denoted by $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$.

3. By convention, $\emptyset \times B = A \times \emptyset = \emptyset$. In fact, $A \times B = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$.

4. One can use the product construction several times, *e.g.*, if X, Y and Z are sets then
$$X \times Y \times Z = \{(x, y, z) : x \in X, y \in Y, z \in Z\} = (X \times Y) \times Z = X \times (Y \times Z).$$

EXERCISE **1.2.3.** *Let A, B, C and D be non-empty sets. Then, prove the following statements:*

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

3. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

4. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$. *Give an example to show that the converse need not be true.*

Definition 1.2.4. [**Relation**] Let X and Y be two non-empty sets. A **relation** R from X to Y is a subset of $X \times Y$. We write xRy to mean $(x, y) \in R \subseteq X \times Y$. Thus, for any two sets X and Y, the sets $\emptyset$ and $X \times Y$ are always relations from X to Y. A relation from X to X is called a **relation on** X.

Example 1.2.5. 1. Let X be any non-empty set and consider the set $\mathcal{P}(X)$. Then one can define a relation R on $\mathcal{P}(X)$ by $R = \{(S, T) \in \mathcal{P}(X) \times \mathcal{P}(X) : S \subseteq T\}$.

2. Let $A = \{a, b, c, d\}$. Then, some of the relations R on A are:

(a) $R = A \times A$.

(b) $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (b, c)\}$.

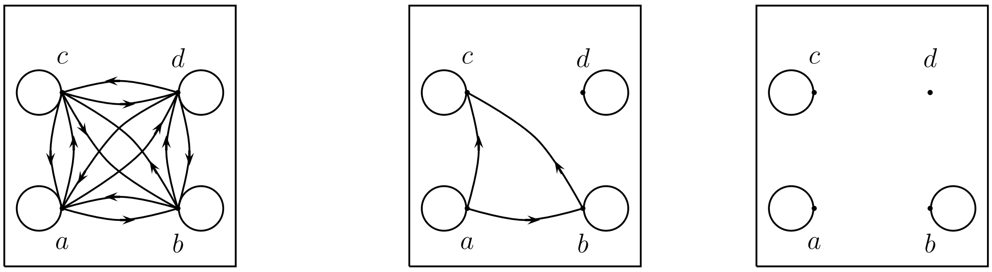
(c) $R = \{(a, a), (b, b), (c, c)\}$.

(d) $R = \{(a, a), (a, b), (b, a), (b, b), (c, d)\}$.

(e) $R = \{(a, a), (a, b), (b, a), (a, c), (c, a), (c, c), (b, b)\}$.

(f) $R = \{(a, b), (b, c), (a, c), (d, d)\}$.

To draw pictures for relations on a set X, we first put a node for each element $x \in X$ and label it x. For each $(x, y) \in R$, we draw a directed line from x to y. If $(x, x) \in R$ then a loop is drawn at x. The figures for some of the relations is given in Figure 1.1.



$A \times A$ Example 2.b Example 2.c

Figure 1.1: Graphic representation of some of the relations in Example 2

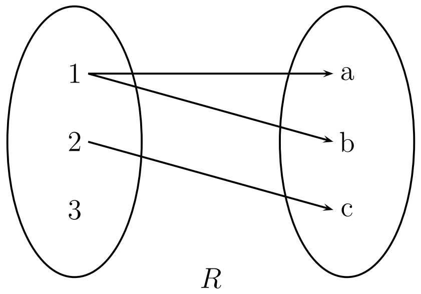


Figure 1.2: Graphic representation of the relation in Example 3

3. Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ and let $R = \{(1, a), (1, b), (2, c)\}$. Figure 1.2 represents the relation R.[1]

4. Let $A = \mathbb{Z}$, the set of integers. Then

$$R = \{(x, y) : x, y \in \mathbb{Z} \text{ and } y = x + 5m, \text{ for some } m \in \mathbb{Z}\}$$

   is a relation on $\mathbb{Z}$. If we try to draw a picture for this relation then there is no arrow among any two elements of $\{1, 2, 3, 4, 5\}$.

5. Let $A = \mathbb{Z}$, the set of integers. For a fixed positive integer n, let

$$R = \{(x, y) : x, y \in \mathbb{Z} \text{ and } y = x + nm, \text{ for some } m \in \mathbb{Z}\}.$$

   Then, R is a relation on $\mathbb{Z}$. A picture for this relation has no arrow among any two elements of $\{1, 2, 3, \ldots, n\}$.

Definition 1.2.6. **[Inverse Relation]** Let X and Y be two non-empty sets and let R be a relation in $X \times Y$. Then, the **inverse relation**, denoted by R^{-1}, is a subset of $Y \times X$ and is defined by $R^{-1} = \{(b, a) \in Y \times X : (a, b) \in R\}$. So, for all $a \in X$ and $b \in Y$

$$aRb \text{ if and only if } bR^{-1}a.$$

Example 1.2.7. 1. If $R = \{1, a), (1, b), (2, c)\}$ then $R^{-1} = \{(a, 1), (b, 1), (c, 2)\}$.

2. Let $R = \{(a, b), (b, c), (a, c)\}$ be a relation on $A = \{a, b, c\}$ then $R^{-1} = \{(b, a), (c, b), (c, a)\}$.

Definition 1.2.8. **[Partial Function, Pre-image, Image]** Let X and Y be two non-empty sets and and let f be a relation in $X \times Y$.

1. Then, f is called a **partial function** from X to Y, denoted by $f : X \to Y$, if for every $a \in X$ and $b, b' \in Y$ the condition $(a, b), (a, b') \in f$ implies that $b = b'$. In such a case, one writes $f(a) = b$, *i.e.*, $f(a) = b$ if there exists a unique $b \in Y$ such that $(a, b) \in f$. Note that it may happen that for a particular choice of $a \in X$, $(a, b) \notin f$, for any $b \in Y$. In this case, one says that $f(a)$ is undefined.

2. Let $f : X \to Y$ be a partial function and let $f(x) = y$. Then, x is called a **pre-image** of y and y is called an **image** of x. Also, for any set Z, one also defines

$$f(Z) := \{b : f(x) = b, \text{ for some } x \in Z\}.$$

   Thus, note that $f(Z) = \emptyset$ if $Z \cap X = \emptyset$.

Example 1.2.9. Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4\}$ and $X = \{3, 4, b, c\}$.

[1] We use pictures to help our understanding and they are not parts of proof.

1. If $R_1 = \{(a,1),(b,1),(c,2)\}$ is a relation in $A \times B$ then
   (a) R_1 is a partial function.
   (b) $R_1(a) = 1$, $R_1(b) = 1$, $R_1(c) = 2$. Also, $R_1(d)$ is undefined. Thus, $R_1(\{d\}) = \emptyset$.
   (c) $R_1(X) = \{1,2\}$.
   (d) $R_1^{-1}(\{1\}) = \{a,b\}$ and $R_1^{-1}(2) = c$ as $R_1^{-1} = \{(1,a),(1,b),(2,c)\}$. For $x \in X$, $R_1^{-1}(x)$ is not defined and hence $R_1^{-1}(X) = \emptyset$.

2. If $R_2 = \{(a,1),(b,4),(c,2),(d,3)\}$ is a relation in $A \times B$ then
   (a) R_2 is a partial function.
   (b) $R_2(a) = 1$, $R_2(b) = 4$, $R_2(c) = 2$ and $R_2(d) = 3$.
   (c) $R_2(X) = \{2,4\}$.
   (d) $R_2^{-1}(1) = a$, $R_2^{-1}(2) = c$, $R_2^{-1}(3) = d$ and $R_2^{-1}(4) = b$. Also, $R_2^{-1}(X) = \{b,d\}$.

Definition 1.2.10. [Domain, Range, Function] Let X and Y be two non-empty sets and let $f : X \to Y$ be a partial function.

1. Then, the **domain** [1] of f, denoted by $\mathsf{dom}\, f := \{a : (a,b) \in f\}$ is the set of all pre-images of f.
2. Then, the **range of** f, denoted by $\mathsf{rng}\, f := \{b : (a,b) \in f\}$ is the collection of images of f.
3. If $\mathsf{dom}\, f = X$ then the partial function f is called a **total function** on X, or a **function** from X to Y.

Convention:

Let $p(x)$ be a polynomial in x with integer coefficients. Then, by writing '$f : \mathbb{Z} \to \mathbb{Z}$ is a function defined by $f(x) = p(x)$', we mean the function $f = \{(a, p(a)) : a \in \mathbb{Z}\}$. For example, the function $f(x) = x^2$ stands for the set $\{(a, a^2) : a \in \mathbb{Z}\}$.

Example 1.2.11. 1. For $A = \{a,b,c,d\}$ and $B = \{1,3,5\}$, let $f = \{(a,5),(b,1),(d,5)\}$ be a relation in $A \times B$. Then, f is a partial function with $\mathsf{dom}\, f = \{a,b,d\}$ and $\mathsf{rng}\, f = \{1,5\}$. Further, we can define a function $g : \{a,b,d\} \to \{1,5\}$ by $g(a) = 5, g(b) = 1$ and $g(d) = 5$. Also, using g, one obtains the relation $g^{-1} = \{(1,b),(5,a),(5,d)\}$.

2. Note that the following relations $f : \mathbb{Z} \to \mathbb{Z}$ are indeed functions.
   (a) $f = \{(x,1) \mid x \text{ is even}\} \cup \{(x,5) \mid x \text{ is odd}\}$.
   (b) $f = \{(x,-1) \mid x \in \mathbb{Z}\}$.
   (c) $f = \{(x, x \pmod{10}) \mid x \in \mathbb{Z}\}$, where $x \pmod{10}$ gives the remainder when 10 divides x.
   (d) $f = \{(x,1) \mid x < 0\} \cup \{(0,0)\} \cup \{(x,-1) \mid x > 0\}$.

Remark 1.2.12. *1. If $X = \emptyset$, then by convention, one assumes that there is a function, called the empty function, from X to Y.*

2. If $Y = \emptyset$, then it can be easily observed that there is no function from X to Y.

3. Individual relations and functions are also sets. Therefore, one can have equality between relations and functions, i.e., they are equal if and only if they contain the same set of pairs. For example, let $A = \{-1,0,1\}$. Then, the functions $f, g, h : A \to A$ defined by $f(x) = x, g(x) = x|x|$ and $h(x) = x^3$ are equal as the three functions correspond to the relation $R = \{(-1,-1),(0,0),(1,1)\}$ on A.

[1] The domain set is the set from which we define our relations but $\mathsf{dom}\, f$ is the domain of the particular partial function f. They are different.

4. *Some books use the word 'map' in place of 'function'. So, both the words are used interchangeably throughout the book.*

5. *Throughout the book, whenever the phrase 'let $f : X \to Y$ be a function' is used, it will be assumed that both X and Y are nonempty sets.*

The following is an immediate consequence of the definition.

Proposition 1.2.13. *Let f be a non-empty relation in $A \times B$ and S be any set. Then,*

1. *$f(S) \neq \emptyset$ if and only if $\mathsf{dom}(f) \cap S \neq \emptyset$.*
2. *$f^{-1}(S) \neq \emptyset$ if and only if $\mathsf{rng}(f) \cap S \neq \emptyset$.*

Proof. We will prove only one way implication. The other way is left for the reader.
Part 1: Since $f(S) \neq \emptyset$, one can find $a \in S \cap A$ and $b \in B$ such that $(a, b) \in f$. This, in turn, implies that $a \in \mathsf{dom}(f) \cap S$ $(a \in S)$.

Part 2: Since $\mathsf{rng}(f) \cap S \neq \emptyset$, one can find $b \in \mathsf{rng}(f) \cap S$ and $a \in A$ such that $(a, b) \in f$. This, in turn, implies that $a \in f^{-1}(b) \subseteq f^{-1}(S)$. ■

Some important functions are now defined.

Definition 1.2.14. [**Identity and Zero functions**] Let X be a non-empty set.

1. Then the relation $\mathbf{Id} := \{(x, x) : x \in X\}$ is called the **identity** relation on X.
2. Then the function $f : X \to X$ defined by $f(x) = x$, for all $x \in X$, is called the **identity** function and is denoted by $\mathbf{Id}$.
3. Then the function $f : X \to \mathbb{R}$ with $f(x) = 0$, for all $x \in X$, is called the **zero** function and is denoted by $\mathbf{0}$.

EXERCISE **1.2.15.** 1. *Do the following relations represent functions? If yes, why?*

(a) *Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by*

i. *$f = \{(x, 1) \mid 2$ divides $x\} \cup \{(x, 5) \mid 3$ divides $x\}$.*

ii. *$f = \{(x, 1) \mid x \in S\} \cup \{(x, -1) \mid x \in S'\}$, where $S = \{n^2 : n \in \mathbb{Z}\}$ and $S' = \mathbb{Z} \setminus S$.*

iii. *$f = \{(x, x^3) \mid x \in \mathbb{Z}\}$.*

(b) *Let $f : \mathbb{R}^+ \to \mathbb{R}$ be defined by $f = \{(x, \pm\sqrt{x}) \mid x \in \mathbb{R}^+\}$.*

(c) *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f = \{(x, \sqrt{x}) \mid x \in \mathbb{R}\}$.*

(d) *Let $f : \mathbb{R} \to \mathbb{C}$ be defined by $f = \{(x, \sqrt{x}) \mid x \in \mathbb{R}\}$.*

(e) *Let $f : \mathbb{R}^* \to \mathbb{R}$ be defined by $f = \{(x, \log_e |x|) \mid x \in \mathbb{R}^*\}$.*

(f) *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f = \{(x, \tan x) \mid x \in \mathbb{R}\}$.*

2. *Let $f : X \to Y$ be a function. Then f^{-1} is a relation in $Y \times X$ and the following results hold for f^{-1}.*

(a) *$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, for each $A, B \subseteq Y$.*

(b) *$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$, for each $A, B \subseteq Y$.*

(c) *$f^{-1}(\emptyset) = \emptyset$.*

(d) *$f^{-1}(Y) = X$.*

(e) *$f^{-1}(B') = \left(f^{-1}(B)\right)'$, for each $B \subseteq Y$, where B' is the complement of B in Y and $\left(f^{-1}(B)\right)'$ is the complement of $f^{-1}(B)$ in X.*

Definition 1.2.16. [**One-one/Injection**] A function $f : X \to Y$ is called **one-one** (also called an **injection**), if $f(x) \neq f(y)$ is true for each pair $x \neq y$ in X. Equivalently, f is one-one if $x = y$ is true for each pair $x, y \in X$ for which $f(x) = f(y)$.

Example 1.2.17.

1. Let A be a non-empty set. Then the identity map, **Id**, is one-one.
2. Let $\emptyset \neq A \subsetneq B$. Then $f(x) = x$ is a one-one map from A to B.
3. The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not one-one as $f(-1) = f(1) = 1$.
4. The function $f : \{1, 2, 3\} \to \{a, b, c, d\}$ defined by $f(1) = c$, $f(2) = b$ and $f(3) = a$, is one-one. It can be checked that there are 24 one-one functions $f : \{1, 2, 3\} \to \{a, b, c, d\}$.
5. There is no one-one function from the set $\{1, 2, 3\}$ to its proper subset $\{1, 2\}$.
6. There are one-one functions from the set $\mathbb{N}$ of natural numbers to its proper subset $\{2, 3, \ldots\}$. One of them is given by $f(1) = 4, f(2) = 3, f(3) = 2$ and $f(n) = n + 1$, for all $n \geq 4$.

Definition 1.2.18. [**Restriction function**] Let $f : X \to Y$ be a function and $A \subseteq X$, $A \neq \emptyset$. Then, by f_A, we denote the function $f_A = \{(x, y) : (x, y) \in f, x \in A\}$, called the **restriction of f to A**.

Example 1.2.19. Define $f : \mathbb{R} \to \mathbb{R}$ as $f(x) = 1$, if x is irrational and $f(x) = 0$, if x is rational. Then, $f_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ is the constant $\mathbf{0}$ function.

Proposition 1.2.20. *Let $f : X \to Y$ be a one-one function and Z be a nonempty subset of X. Then, f_Z is also one-one.*

Proof. Let if possible, $f_Z(x) = f_Z(y)$, for some $x, y \in Z$. Then, by definition of f_Z, we have $f(x) = f(y)$. As f is one-one, we get $x = y$. Thus, f_Z is one-one. ∎

Definition 1.2.21. [**Onto/Surjection**] A function $f : X \to Y$ is called **onto** (also called a **surjection**), if $f^{-1}(b) \neq \emptyset$, for each $b \in Y$. Equivalently, $f : X \to Y$ is onto if 'each $b \in Y$ has some pre-image in X'.

Example 1.2.22.

1. Let A be a non-empty set. Then the identity map, **Id**, is onto.
2. Let $\emptyset \neq A \subsetneq B$. Then $f(x) = x$ is a not onto as $A \subsetneq B$.
3. There are 6 onto functions from $\{1, 2, 3\}$ to $\{1, 2\}$. For example, $f(1) = 1, f(2) = 2$, and $f(3) = 2$ is one such function.
4. Let $\emptyset \neq A \subsetneq B$. Choose $a \in A$. Then $g(y) = \begin{cases} y, & \text{if } y \in A, \\ a, & \text{if } y \in B \setminus A. \end{cases}$ is an onto map from B to A.
5. There is no onto function from the set $\{1, 2\}$ to its proper superset $\{1, 2, 3\}$.
6. There are onto functions from the set $\{2, 3, \ldots\}$ to its proper superset $\mathbb{N}$, the set of natural numbers. One of them is given by $f(n) = n - 1$, for all $n \geq 2$.

Definition 1.2.23. [**Bijection/One-One Correspondence, Equivalent Set**] Let X and Y be two sets. A function $f : X \to Y$ is said to be a **bijection** if f is one-one as well as onto. The sets X and Y are said to be **equivalent** if there exists a bijection $f : X \to Y$.

Example 1.2.24.

1. The function $f : \{1, 2, 3\} \to \{a, b, c\}$ defined by $f(1) = c$, $f(2) = b$ and $f(3) = a$, is a bijection. Thus, the set $\{a, b, c\}$ is equivalent to $\{1, 2, 3\}$.
2. Let A be a non-empty set. Then the identity map, **Id**, is a bijection. Thus, the set A is equivalent to itself.
3. The set $\mathbb{N}$ is equivalent to $\{2, 3, \ldots\}$. Indeed the function $f : \mathbb{N} \to \{2, 3, \ldots\}$ defined by $f(1) = 3, f(2) = 2$ and $f(n) = n + 1$, for all $n \geq 3$ is a bijection.

Exercise **1.2.25.**

1. *Define $f : \mathbb{N} \cup \{0\} \to \mathbb{Z}$ by $f = \{\left(x, \frac{-x}{2}\right) \mid x$ is even$\} \cup \{\left(x, \frac{x+1}{2}\right) \mid x$ is odd$\}$. Is f one-one? Is it onto?*

2. *Define $f : \mathbb{N} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ by $f = \{(x, 2x) \mid x \in \mathbb{N}\}$ and $g = \{\left(x, \frac{x}{2}\right) \mid x$ is even$\} \cup \{(x, 0) \mid x$ is odd$\}$. Are f and g one-one? Are they onto?*

3. *Let A be the class of subsets of $\{1, 2, \ldots, 9\}$ of size 5 and B be the class of 5 digit numbers with strictly increasing digits. For $a \in A$, define $f(a)$ the number obtained by arranging the elements of a in increasing order. Is f one-one and onto?*

1.2.1 Composition of Functions

Definition 1.2.26. **[Composition of relations]** Let f and g be two relations such that $\mathsf{rng}\, f \subseteq \mathsf{dom}\, g$. Then, the **composition** of f and g, denoted by $g \circ f$, is defined as

$$g \circ f = \Big\{(x, z) : (x, y) \in f \text{ and } (y, z) \in g \text{ for some } y \in \mathsf{rng}(f) \subseteq \mathsf{dom}(g)\Big\}.$$

It is a relation. In case, both f and g are functions then $(g \circ f)(x) = g\left(f(x)\right)$ as $(x, z) \in g \circ f$ implies that there exists y such that $y = f(x)$ and $z = g(y)$. Similarly, one defines $f \circ g$ if $\mathsf{rng}\, g \subseteq \mathsf{dom}\, f$.

Example 1.2.27. Take $f = \{(\beta, a), (3, b), (3, c)\}$ and $g = \{(a, 3), (b, \beta), (c, \beta)\}$. Then, $g \circ f = \{(3, \beta), (\beta, 3)\}$ and $f \circ g = \{(a, b), (a, c), (b, a), (c, a)\}$.

The proof of the next result is omitted as it directly follows from definition.

Proposition 1.2.28. **[Algebra of composition of functions]** *Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions.*

1. *Then, $(h \circ g) \circ f : A \to D$ and $h \circ (g \circ f) : A \to D$ are functions. Moreover, $(h \circ g) \circ f = h \circ (g \circ f)$ (associativity holds).*

2. *If f and g are injections then $g \circ f : A \to C$ is an injection.*

3. *If f and g are surjections then $g \circ f : A \to C$ is a surjection.*

4. *If f and g are bijections then $g \circ f : A \to C$ is a bijection.*

5. *[Extension] If $\mathsf{dom}\, f \cap \mathsf{dom}\, h = \emptyset$ and $\mathsf{rng}\, f \cap \mathsf{rng}\, h = \emptyset$ then the function $f \cup h$ from $A \cup C$ to $B \cup D$ defined by $f \cup h = \{(a, f(a)) : a \in A\} \cup \{(c, h(c)) : c \in C\}$ is a bijection.*

6. *Let A and B be sets with at least two elements each and let $f : A \to B$ be a bijection. Then, the number of bijections from A to B is at least 2.*

Theorem 1.2.29. **[Properties of identity function]** *Let A and B be two nonempty sets and $\mathbf{Id} : A \to A$ be the identity function. Then, for any two functions $f : A \to B$ and $g : B \to A$*

1. *the map $f \circ \mathbf{Id} = f$.*

2. *the map $\mathbf{Id} \circ g = g$.*

Proof. Part 1: By definition, $(f \circ \mathbf{Id})(a) = f(\mathbf{Id}(a)) = f(a)$, for all $a \in A$. Hence, $f \circ \mathbf{Id} = f$.

Part 2: The readers are advised to supply the proof. ■

We now give a very important bijection principle.

Theorem 1.2.30. **[bijection principle]** *Let $f : A \to B$ and $g : B \to A$ be functions such that $g \circ f(a) = a$, for each $a \in A$. Then*

1. *f is one-one and*

2. *g is onto.*

Proof. Let $g \circ f(a) = a$, for each $a \in A$. To prove the first part, let us assume that $f(a_1) = f(a_2)$, for some $a_1, a_2 \in A$. Then using the given condition

$$a_1 = g \circ f(a_1) = g\left(f(a_1)\right) = g\left(f(a_2)\right) = g \circ f(a_2) = a_2.$$

Thus, f is one-one and this completes the proof of the first.

For the second part, let $a \in A$. As $g \circ f(a) = a$, we see that for $b = f(a)$, one has $g(b) = g(f(a)) = g \circ f(a) = a$. Thus, we have found $b \in B$ such that $g(b) = a$. Hence, g is onto and this completes the required proof. ■

Exercise **1.2.31.** *1. Let $f, g : \mathbb{N} \to \mathbb{N}$ be defined by $f = \{(x, 2x) \mid x \in \mathbb{N}\}$ and $g = \{\left(x, \frac{x}{2}\right) \mid x \text{ is even}\} \cup \{(x, 0) \mid x \text{ is odd}\}$. Then, verify that $g \circ f$ is the identity map on $\mathbb{N}$, whereas $f \circ g$ maps even numbers to itself and maps odd numbers to 0.*

2. *Let $f : X \to Y$ be a function. Then, prove that $f^{-1} : Y \to X$ is a function if and only if f is a bijection.*

3. *Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m, n) = 2^{m-1}(2n - 1)$. Is f a bijection?*

4. *Let $f : X \to Y$ be a bijection and $A \subseteq X$. Is $f(A') = (f(A))'$?*

5. *Let $f : X \to Y$ and $g : Y \to X$ be two functions such that*

   (a) $(f \circ g)(y) = y$ holds, for each $y \in Y$.

   (b) $(g \circ f)(x) = x$ holds, for each $x \in X$.

   Show that f is a bijection and $g = f^{-1}$. Can we conclude the same without assuming the second condition?

1.2.2 Equivalence Relation

Now that we have seen quite a few examples of relations, let us look at some of the properties that are of interest in mathematics.

Definition 1.2.32. [Relations on Set] Let R be a relation on a non-empty set A. Then R is said to be

1. **reflexive** if $(a, a) \in R$, for all $a \in A$.

2. **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$.

3. **anti-symmetric** if, for all $a, b \in A$ with $(a, b), (b, a) \in R$ implies $a = b$ in A.

4. **transitive** if, for all $a, b, c \in A$ with $(a, b), (b, c) \in R$ implies $(a, c) \in R$.

Exercise **1.2.33.** *For relations defined in Example 1.2.5, determine which of them are*

1. *reflexive.*

2. *symmetric.*

3. *anti-symmetric.*

4. *transitive.*

We are now ready to define a relation that appears quite frequently in mathematics. Before doing so, let us either use the symbol $\sim$ or $\overset{R}{\sim}$ for relation. That is, if $a, b \in A$ then we represent $(a, b) \in R$ by either $a \sim b$ or $a \overset{R}{\sim} b$.

Definition 1.2.34. [Equivalence Relation, Equivalence Class] Let $\sim$ be a relation on a non-empty set A. Then $\sim$ is said to form an **equivalence relation** if $\sim$ is reflexive, symmetric and transitive. The **equivalence class** containing $a \in A$, denoted $[a]$, is defined as $[a] := \{b \in A : b \sim a\}$.

Example 1.2.35. 1. Consider the relations on A that appear in Example 1.2.5. Then,

(a) Example 1.2.5.1 is not an equivalence relation (the relation is not symmetric).

(b) Example 1.2.5.2.2a is an equivalence relation with $[a] = \{a, b, c, d\}$ as the only equivalence class.

(c) Other relations in Example 1.2.5.2 are not equivalence relation.

(d) Example 1.2.5.4 is an equivalence relation with the equivalence classes as

i. $[0] = \{\ldots, -15, -10, -5, 0, 5, 10, \ldots\}$.

ii. $[1] = \{\ldots, -14, -9, -4, 1, 6, 11, \ldots\}$.

iii. $[2] = \{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}$.

iv. $[3] = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}$.

v. $[4] = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}$.

(e) Example 1.2.5.5 is an equivalence relation with the equivalence classes as

i. $[0] = \{\ldots, -3n, -2n, -n, 0, n, 2n, \ldots\}$.

ii. $[1] = \{\ldots, -3n+1, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}$.

iii. $[2] = \{\ldots, -3n+2, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\}$.

iv. $[n-2] = \{\ldots, -2n-2, -n-2, -2, n-2, 2n-2, 3n-2, \ldots\}$.

v. $[n-1] = \{\ldots, -2n-1, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}$.

2. Let $R = \{(a, a), (b, b), (c, c)\}$ be a relation on $A = \{a, b, c\}$. Then, R forms an equivalence relation with three equivalence classes, namely $[a] = \{a\}, [b] = \{b\}$ and $[c] = \{c\}$.

3. Let $R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$ be a relation on $A = \{a, b, c\}$. Then, R forms an equivalence relation with two equivalence classes, namely $[a] = [c] = \{a, c\}$ and $[b] = \{b\}$.

Proposition 1.2.36. [Equivalence relation divides a set into disjoint classes] *Let $\sim$ be an equivalence relation on X.*

1. *Then any two equivalence classes are either disjoint or identical.*

2. *Further, $X = \bigcup\limits_{a \in X} [a]$.*

Thus, an equivalence relation $\sim$ on X divides X into disjoint equivalence classes.

Proof. If the equivalence classes $[a]$ and $[b]$ are disjoint, then there is nothing to prove. So, let us assume that there are two equivalence classes, say $[a]$ and $[b]$, that intersect. Hence, there exists $c \in X$ such that $c \in [a] \cap [b]$. That is, $c \sim a$ and $c \sim b$.

As $\sim$ is symmetric, $a \sim c$ as well. Now, $\sim$ is transitive, with $a \sim c$ and $c \sim b$ and so $a \sim b$. Hence, if $x \sim a$, then the above argument implies that $x \sim b$. Thus, $[a] \subseteq [b]$. A similar argument implies that $[b] \subseteq [a]$ as symmetry with $c \sim b$ implies $b \sim c$ and the transitivity with $b \sim c$ and $c \sim a$ implies $b \sim a$. Thus, whenever two equivalence classes intersect, they are indeed equal.

For the second part, note that for each $x \in X$, $[x]$, the equivalence class containing x is well defined. Thus, if we take the union over all $x \in X$, we get $X = \bigcup\limits_{x \in X} [x]$. ■

EXERCISE **1.2.37.** *Determine the equivalence relation among the relations given below. Further, for each equivalence relation, determine its equivalence classes.*

1. *$R = \{(a, b) \in \mathbb{Z}^2 \mid a \leq b\}$ on $\mathbb{Z}$?*
2. *$R = \{(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^* \mid a$ divides $b\}$, where $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ on $\mathbb{Z}^*$?*
3. *For $\mathbf{x} = (x_1, x_2), \mathbf{y} = (y_1, y_2) \in \mathbb{R}^2$ and $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, let*
   (a) *$R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid \ |\mathbf{x}|^2 = x_1^2 + x_2^2 = y_1^2 + y_2^2 = |\mathbf{y}|^2\}$.*
   (b) *$R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid \mathbf{x} = \alpha\mathbf{y}$ for some $\alpha \in \mathbb{R}^*\}$.*
   (c) *$R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid 4x_1^2 + 9x_2^2 = 4y_1^2 + 9y_2^2\}$.*
   (d) *$R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid \mathbf{x} - \mathbf{y} = \alpha(1, 1)$ for some $\alpha \in \mathbb{R}^*\}$.*
   (e) *Fix $c \in \mathbb{R}$. Now, define $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid y_2 - x_2 = c(y_1 - x_1)\}$.*
   (f) *$R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid |x_1| + |x_2| = \alpha(|y_1| + |y_2|)\}$, for some positive real number α.*
   (g) *$R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x_1x_2 = y_1y_2\}$.*
4. *For $\mathbf{x} = (x_1, x_2), \mathbf{y} = (y_1, y_2) \in \mathbb{R}^2$, let $S = \{\mathbf{x} \in \mathbb{R}^2 \mid x_1^2 + x_2^2 = 1\}$. Then is the relation given below an equivalence relation on S?*
   (a) *$R = \{(\mathbf{x}, \mathbf{y}) \in S \times S \mid x_1 = y_1, x_2 = -y_2\}$.*
   (b) *$R = \{(\mathbf{x}, \mathbf{y}) \in S \times S \mid \mathbf{x} = -\mathbf{y}\}$.*

Definition 1.2.38. [Partition of a set] Let X be a non-empty set. Then a **partition** of X is a collection of disjoint, non-empty subsets of X whose union is X.

Example 1.2.39. Let $X = \{a, b, c, d, e\}$.

1. If R is an equivalence relation on X with
$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (c, e), (e, c)\}$$
then its equivalence classes are $[a] = [b] = \{a, b\}$, $[c] = [e] = \{c, e\}$ and $[d] = \{d\}$.
2. Let $\{a\}, \{b, c, d\}, \{e\}$ be a partition of X. Then verify that
$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (b, c), (c, d), (b, d), (c, b), (d, c), (d, b)\}$$
is an equivalence relation with $[a] = \{a\}$, $[b] = \{b, c, d\}$ and $[e] = \{e\}$.

The next proposition follows directly follows from Proposition 1.2.36 and hence the proof is omitted. It answers the question that "if a partition of a non-empty set X is given then does there exists an equivalence relation on X such that the disjoint equivalence classes are exactly the elements of the partition?"

Proposition 1.2.40. [Constructing equivalence relation from equivalence classes] *Let f be an equivalence relation on $X \neq \emptyset$ whose disjoint equivalence classes are $[a] : a \in A\}$, for some index set A. Then,*
$$f = \left(\bigcup_{x \in X} \{(x, x)\}\right) \bigcup \left(\bigcup_{a \in A} \{(x, y) : x, y \in [a], x \neq y\}\right).$$

EXERCISE **1.2.41.** 1. *Let X and Y be two nonempty sets and $f : X \to Y$ be a relation. Let $\mathbf{Id}_X$ and $\mathbf{Id}_Y$ be the identity relations on X and Y, respectively. Then,*
   (a) *is it necessary that $f^{-1} \circ f \subseteq \mathbf{Id}_X$?*
   (b) *is it necessary that $f^{-1} \circ f \supseteq \mathbf{Id}_X$?*

   (c) *is it necessary that* $f \circ f^{-1} \subseteq \mathbf{Id}_Y$*?*

   (d) *is it necessary that* $f \circ f^{-1} \supseteq \mathbf{Id}_Y$*?*

2. *Suppose now that* f *is a function. Then,*

   (a) *is it necessary that* $f \circ f^{-1} \subseteq \mathbf{Id}_Y$*?*

   (b) *is it necessary that* $\mathbf{Id}_X \subseteq f^{-1} \circ f$*?*

3. *Take* $A \neq \emptyset$*. Is* $A \times A$ *an equivalence relation on* A*? If yes, what are the equivalence classes?*

4. *On a nonempty set* A*, what is the smallest equivalence relation (in the sense that every other equivalence relation will contain this equivalence relation; recall that a relation is a set)?*

EXERCISE **1.2.42. [Optional]**

1. *Let* $X = \{1, 2, 3, 4, 5\}$ *and let* f *be a relation on* X*. By checking whether* f *is reflexive or not, whether* f *is symmetric or not and whether* f *is transitive or not, we see that there are* 8 *types of relations on* X*. Give one example for each type.*

2. *Let* $A = B = \{1, 2, 3\}$*. Then, what is the number of*

   (a) *relations from* A *to* B*?*

   (b) *relations* f *from* $\{1, 2, 3\}$ *to* $\{a, b, c\}$ *such that* $\mathsf{dom}\, f = \{1, 3\}$*?*

   (c) *relations* f *from* $\{1, 2, 3\}$ *to itself such that* $f = f^{-1}$*?*

   (d) *single valued relations from* $\{1, 2, 3\}$ *to itself? How many of them are functions?*

   (e) *equivalence relations on* $\{1, 2, 3, 4, 5\}$*.*

3. *Let* f, g *be two non-equivalence relations on* $\mathbb{R}$*. Then, is it possible to have* $f \circ g$ *as an equivalence relation? Give reasons for your answer.*

4. *Let* f, g *be two equivalence relations on* $\mathbb{R}$*. Then, prove/disprove the following statements.*

   (a) $f \circ g$ *is necessarily an equivalence relation.*

   (b) $f \cap g$ *is necessarily an equivalence relation.*

   (c) $f \cup g$ *is necessarily an equivalence relation.*

   (d) $f \cup g'$ *is necessarily an equivalence relation.*

1.3 Advanced topics in Set Theory and Relations*

1.3.1 Families of Sets

Definition 1.3.1. [Family of sets] Let A be a set. For each $x \in A$, take a new set A_x. Then, the collection

$$\{A_x\}_{x \in A} := \{A_x \mid x \in A\}$$

is a **family of sets** indexed by elements of A (index set). Unless otherwise mentioned, we assume that the index set for a class of sets is nonempty.

Definition 1.3.2. [Union / Intersection of families of sets] Let $\{B_\alpha\}_{\alpha \in S}$ be a nonempty class of sets. We define their

1. **union** as $\bigcup\limits_{\alpha \in S} B_\alpha = \{x \mid x \in B_\alpha, \text{ for some } \alpha\}$, and
2. **intersection** as $\bigcap\limits_{\alpha \in S} B_\alpha = \{x \mid x \in B_\alpha, \text{ for all } \alpha\}$.

[Convention] Union of an empty class is $\emptyset$. The intersection of an empty class of subsets of a set X is X[1].

Example 1.3.3. 1. Take $A = \{1,2,3\}$, $A_1 = \{1,2\}$, $A_2 = \{2,3\}$ and $A_3 = \{4,5\}$. Then,

$$\{A_\alpha \mid \alpha \in A\} = \{A_1, A_2, A_3\} = \Big\{\{1,2\}, \{2,3\}, \{4,5\}\Big\}.$$

Thus, $\underset{\alpha\in A}{\cup} A_\alpha = \{1,2,3,4,5\}$ and $\underset{\alpha\in A}{\cap} A_\alpha = \emptyset$.

2. Take $A = \mathbb{N}$ and $A_n = \{n, n+1, \ldots\}$. Then, the family

$$\{A_\alpha \mid \alpha \in A\} = \{A_1, A_2, \ldots\} = \Big\{\{1,2,\ldots\}, \{2,3,\ldots\}, \ldots\Big\}.$$

Thus, $\underset{\alpha\in A}{\cup} A_\alpha = \mathbb{N}$ and $\underset{\alpha\in A}{\cap} A_\alpha = \emptyset$.

3. Verify that $\bigcap\limits_{n\in\mathbb{N}} [-\frac{1}{n}, \frac{2}{n}] = \{0\}$.

We now give a set of important rules some of whose proofs are left for the reader.

Theorem 1.3.4. **[Algebra of union and intersection]** *Let $\{A_\alpha\}_{\alpha\in L}$ be a nonempty class of subsets of X and B be any set. Then, the following statements are true.*

1. $B \cap \left(\underset{\alpha\in L}{\cup} A_\alpha\right) = \underset{\alpha\in L}{\cup} (B \cap A_\alpha)$.
2. $B \cup \left(\underset{\alpha\in L}{\cap} A_\alpha\right) = \underset{\alpha\in L}{\cap} (B \cup A_\alpha)$.
3. $\big(\underset{\alpha\in L}{\cup} A_\alpha\big)' = \underset{\alpha\in L}{\cap} A'_\alpha$.
4. $\big(\underset{\alpha\in L}{\cap} A_\alpha\big)' = \underset{\alpha\in L}{\cup} A'_\alpha$.

Proof. We give the proofs for Part 1 and 4. For Part 1, we see that

$$x \in B \cap \left(\underset{\alpha\in L}{\cup} A_\alpha\right) \Leftrightarrow x \in B \text{ and } x \in \underset{\alpha\in L}{\cup} A_\alpha \Leftrightarrow x \in B \text{ and } x \in A_\alpha, \text{ for some } \alpha \in L$$
$$\Leftrightarrow x \in B \cap A_\alpha, \text{ for some } \alpha \in L \Leftrightarrow x \in \underset{\alpha\in L}{\cup} (B \cap A_\alpha).$$

For Part 4, we have

$$x \in \big(\underset{\alpha\in L}{\cap} A_\alpha\big)' \Leftrightarrow x \notin \underset{\alpha\in L}{\cap} A_\alpha \Leftrightarrow x \notin A_\alpha, \text{ for some } \alpha \in L \Leftrightarrow x \in A'_\alpha, \text{ for some } \alpha \in L$$
$$\Leftrightarrow x \in \underset{\alpha\in L}{\cup} A'_\alpha.$$

Proceed in similar lines to complete the proofs of the other parts. ■

Exercise **1.3.5.** *1. Consider $\{A_x\}_{x\in\mathbb{R}}$, where $A_x = [x, x+1]$. What is $\underset{x\in\mathbb{R}}{\cup} A_x$ and $\underset{x\in\mathbb{R}}{\cap} A_x$?*

2. *For $x \in [0,1]$ write $\mathbb{Z}x := \{zx \mid z \in \mathbb{Z}\}$ and $A_x = \mathbb{R} \setminus \mathbb{Z}x$. What is $\underset{x\in\mathbb{R}}{\cup} A_x$ and $\underset{x\in\mathbb{R}}{\cap} A_x$?*
3. *Write the closed interval $[1,2] = \underset{n\in\mathbb{N}}{\cap} I_n$, where I_n are open intervals.*
4. *Write $\mathbb{R}$ as a union of infinite number of pairwise disjoint infinite sets.*
5. *Write the set $\{1,2,3,4\}$ as the intersection of infinite number of infinite sets.*
6. *Suppose that $A \Delta B = B$. Is $A = \emptyset$?*
7. *Prove Theorem 1.3.4.*

[1] The way we see this convention is as follows: First we agree that the intersection of an empty class of subsets is a subset of X. Now, let $x \in X$ such that $x \notin \underset{\alpha\in S}{\cap} B_\alpha$. This implies that there exists an $\alpha \in S$ such that $x \notin B_\alpha$. Since S is empty, such an α does not exist.

1.3.2 More on Relations

Proposition 1.3.6. [Properties of union and intersection under a relation] *Let $f : X \to Y$ be a relation and $\{A_\alpha\}_{\alpha \in L} \subseteq \mathcal{P}(X)$. Then, the following statements hold.*

1. $f\big(\underset{\alpha\in L}{\cup} A_\alpha\big) = \underset{\alpha\in L}{\cup} f(A_\alpha)$.
2. $f\big(\underset{\alpha\in L}{\cap} A_\alpha\big) \subseteq \underset{\alpha\in L}{\cap} f(A_\alpha)$. *Give an example where the inclusion is strict.*

Proof. Part 1:

$$y \in f\big(\underset{\alpha\in L}{\cup} A_\alpha\big) \Leftrightarrow (x,y) \in f, \text{ for some } x \in \underset{\alpha\in L}{\cup} A_\alpha \Leftrightarrow (x,y) \in f \text{ with } x \in A_\alpha, \text{ for some } \alpha \in L$$
$$\Leftrightarrow y \in f(A_\alpha), \text{ for some } \alpha \in L \Leftrightarrow y \in \underset{\alpha\in L}{\cup} f(A_\alpha).$$

For Part 2, we assume that $\underset{\alpha\in L}{\cap} A_\alpha \neq \emptyset$. Then,

$$y \in f\big(\underset{\alpha\in L}{\cap} A_\alpha\big) \Leftrightarrow (x,y) \in f, \text{ for some } x \in \underset{\alpha\in L}{\cap} A_\alpha \Leftrightarrow (x,y) \in f \text{ with } x \in A_\alpha, \text{ for all } \alpha \in L$$
$$\Rightarrow y \in f(A_\alpha), \text{ for all } \alpha \in L \Leftrightarrow y \in \underset{\alpha\in L}{\cap} f(A_\alpha).$$

Thus, the required result follows. ■

Remark 1.3.7. *It is important to note the following in the proof of the above theorem: '$y \in f(A_\alpha)$, for all $\alpha \in L$' implies that 'for each $\alpha \in L$, we can find some $x_\alpha \in A_\alpha$ such that $(x_\alpha, y) \in f$'. That is, the x_α's need not be the same. This gives you an idea to construct a counterexample. Define $f : \{1,2,3,4\} \to \{a,b\}$ by $f = \{(1,a),(2,a),(2,b),(3,b),(4,b)\}$. Take $A_1 = \{1,3\}$ and $A_2 = \{1,2,4\}$ and verify that the inclusion in Part 2 of Theorem 1.3.6 is strict. Also, find the x_i's for b.*

EXERCISE **1.3.8. [Important]**

1. *Let $f : X \to Y$ be a single valued relation, $A \subseteq X$, $B \subseteq Y$ and $\{B_\beta\}_{\beta\in I}$ be a nonempty family of subsets of Y. Then, show that*
   (a) $f^{-1}\big(\underset{\beta\in I}{\cap} B_\beta\big) = \underset{\beta\in I}{\cap} f^{-1}(B_\beta)$.
   (b) $f^{-1}\big(\underset{\beta\in I}{\cup} B_\beta\big) = \underset{\beta\in I}{\cup} f^{-1}(B_\beta)$.
   (c) $f^{-1}(B') = \mathsf{dom}\, f \setminus f^{-1}(B)$.
   (d) $f\left(f^{-1}(B) \cap A\right) = B \cap f(A)$. *Note that this equality fails if f is not single valued.*
2. *Let $f : X \to Y$ be one-one and $\{A_\alpha\}_{\alpha\in L}$ be a nonempty family of subsets of X. Is $f\big(\underset{\alpha\in L}{\cap} A_\alpha\big) = \underset{\alpha\in L}{\cap} f(A_\alpha)$?*
3. *Show that each set can be written as a union of finite sets.*
4. *Give an example of an equivalence relation on $\mathbb{N}$ for which there are 7 equivalence classes, out of which exactly 5 are infinite.*
5. *Show that union of finitely many finite sets is a finite set.*

Chapter 2

Peano Axioms and Countability

2.1 Peano Axioms and the set of Natural Numbers

In this section, We are now ready to state the Peano axioms.When these axioms were proposed by Peano and the rest, their goal was to provide the fewest axioms, that would generate the natural numbers that we are familiar with. The intuition here is to first exert the existence of at lest one natural number and define a successor function to determine the rest.

P1. $1 \in \mathbb{N}$, *i.e.*, 1 is a natural number. (One can also consider $0 \in \mathbb{N}$).

At this point, we are guaranteed the existence of exactly one natural number. We now use the successor function to generate other natural numbers. So, we define a function S whose domain is $\mathbb{N}$.

P2. If $x \in \mathbb{N}$ then $S(x) \in \mathbb{N}$, *i.e.*, the successor of a natural number is also a natural number.

Here, $S(x)$ is referred to as the successor of x. Intuitively one can think of $S(x)$ as $x + 1$. However, at this stage we have no formal idea as to what '+' is. Further, we are very far away from establishing $\mathbb{N}$, the way we know it. So far, we can say that $S(1) = 1$. In this case, all the previous conditions are satisfied. Of course, we want to avoid this!!! So, in some sense, we want to ensure that 1 is not the successor of any natural number.

P3. For any $x \in \mathbb{N}, S(x) \neq 1$, *i.e.*, the pre-image of 1 under S is empty. Thus, at this stage $\mathbb{N}$ contains at least two natural numbers $1, S(1)$. If we stop here, we cannot construct $\mathbb{N}$, the way we know it. For example, if $\mathbb{N} = \{1, S(1)\}$ with $S(x) \neq 1$, for all $x \in \mathbb{N}$, forces us to have $S(S(1)) = S(1)$. But we want $\mathbb{N}$, the set of natural numbers, and hence we certainly require that S is injective.

P4. For every $x, y \in \mathbb{N}$, the condition $S(x) = S(y)$ implies that $x = y$.

Remark 2.1.1. **[Consequences of P4]** *As a first step, it eliminates the possibility that* $\mathbb{N} = \{1, S(1)\}$ *as* $S(1) \neq 1$ *from Axiom* **P3**. *Thus,* $S(1) \notin \{1, S(1)\}$. *So, denote* $S(1) = 2$. *A repetition of above argument will imply that* $S(2) \notin \{1, 2\}$. *So, denote* $S(2) = 3$. *Similarly, denote* $S(3) = 4, S(4) = 5, \ldots$. *Continuing this pattern, we get* $\{1, 2, 3, \ldots\} \subseteq \mathbb{N}$. *Hence, these axioms so far have pushed our formal definition of* $\mathbb{N}$ *to include all the usual elements (natural numbers).*

The question arises, what disallows us from having $\{1, 2, 3, \ldots\} \cup \{a, b\} = \mathbb{N}$, *for certain two symbols* a *and* b. *Note that it is possible to define* S *on* $\{1, 2, 3, \ldots\}$ *as above and also to say that* $S(a) = b$ *and* $S(b) = a$. *This clearly satisfies all the axioms defined above.*

So, we need another axiom to exclude versions where $\mathbb{N}$ is 'too large'. Now, taking inspiration from induction, we define the following.

Definition 2.1.2. [**Inductive set**] A set X is said to be **inductive** if

1. either $1 \in X$ or $0 \in X$ or both,
2. $x \in X$ implies that $S(x) \in X$.

The name "inductive" comes from $1 \in X$ (base step) and the second condition being the inductive step. Based on the above definition, the last Peano axiom is the Axiom of Induction.

P5. If X is an inductive set then $\mathbb{N} \subseteq X$.

The previous axioms ensured that $\{1, 2, \ldots\} \subseteq \mathbb{N}$. Also $\{1, 2, \ldots\}$ is an inductive set and hence the last axiom implies that $\mathbb{N} \subseteq \{1, 2, \ldots\}$. Thus, $\mathbb{N} = \{1, 2, \ldots\}$.

Now that we have axiomatically established the set of natural numbers, can we also establish the arithmetic in $\mathbb{N}$, the most important property for which natural numbers are known? The arithmetic in $\mathbb{N}$ that touches every aspect of our lives is clearly addition and multiplication. So, let us carefully define addition and multiplication using the Peano axioms and the successor function.

Using only the Peano axioms, we first prove a small result and then use it to define addition '$+'$ of two natural numbers.

Lemma 2.1.3. *If $n \in \mathbb{N}$ and $n \neq 1$, then there exists $m \in \mathbb{N}$ such that $S(m) = n$.*

Proof. Let $X = \{x \in \mathbb{N} : x = 1 \text{ or } x = S(y) \text{ for some } y \in \mathbb{N}\}$. By definition $1 \in X$. Also, for each $n \in X$, by definition there exists $y \in \mathbb{N}$ such that $n = S(y)$. Further, $y \in \mathbb{N}$ implies that $S(y) \in \mathbb{N}$ and hence $S(S(y)) = S(n) \in X$. Thus, for each $n \in X, S(n) \in X$ and hence by the axiom of induction $X = \mathbb{N}$. ■

2.1.1 Addition, Multiplication and its properties

Now, we use the recursion rule to define addition '+'.

Definition 2.1.4. [**Addition**] We use the following two assignments to define addition.

1. For each $n \in \mathbb{N}$, assign $n + 1 = S(n)$.
2. For each $m, n \in \mathbb{N}$, assign $n + S(m) = S(n + m)$.

Remark 2.1.5.

1. *We have introduced '+' by certain assignments which require justification. Note that 'assign' actually translates into function.*
2. *By Lemma 2.1.3, we know that any natural number $x \neq 1$ is of the form $S(y)$, for some natural number y and hence we have defined addition for all natural numbers.*

On similar lines, we define multiplication '$\cdot$' and again Lemma 2.1.3 will assure us that we have defined multiplication for each natural number.

Definition 2.1.6. [**Multiplication**] We use the following two assignments to define multiplication.

1. For each $n \in \mathbb{N}$, assign $n \cdot 1 = n$.
2. For each $m, n \in \mathbb{N}$, assign $n \cdot S(m) = n \cdot m + n$.

To get a feeling why the above definitions on $\mathbb{N}$ satisfies our existing concept of natural numbers, we shall use only the above axioms to prove some of the familiar properties.

1. **[Associativity of addition]** For every $n, m, k \in \mathbb{N}$, $n + (m + k) = (n + m) + k$.
   Proof. Let $X = \{k \in \mathbb{N} : \text{ for all } m, n \in \mathbb{N}, n + (m + k) = (n + m) + k\}$. To show that $X = \mathbb{N}$.

   By definition, $1 \in X$ as for each $n, m \in \mathbb{N}$, $n + (m + 1) = n + S(m) = S(n + m) = (n + m) + 1$. Now, let $z \in X$ and let us show that $S(z) \in X$. Since $z \in X$

   $$n + (m + z) = (n + m) + z, \text{ for all } n, m \in \mathbb{N}. \tag{2.1}$$

   Thus, by definition and Equation (2.1), we see that

   $$n+(m+S(z)) = n+S(m+z) = S(n+(m+z)) = S((n+m)+z) = (n+m)+S(z), \text{ for all } n, m \in \mathbb{N}.$$

   Hence, $S(z) \in X$ and thus by Axiom **P5**, $X = \mathbb{N}$. ■

2. **[Commutativity of addition]** For every $x, y \in \mathbb{N}$, $x + y = y + x$.
   Proof. Let $X = \{k \in \mathbb{N} : \text{ for all } n \in \mathbb{N}, n + k = k + n\}$. To show that $X = \mathbb{N}$.

   We first show that $1 \in X$. To do so, we define $Y = \{n \in \mathbb{N} : n + 1 = 1 + n, \text{ for all } n \in \mathbb{N}\}$ and prove that $Y = \mathbb{N}$. This in turn will imply that $1 \in X$.

   Firstly, $1 + 1 = 1 + 1$ and hence $1 \in Y$. Now, let $y \in Y$. To show $S(y) \in Y$. But, $y \in Y$ implies that $1 + y = y + 1$ and hence

   $$1 + S(y) = S(1 + y) = S(y + 1) = S(S(y)) = S(y) + 1.$$

   Thus, $S(y) \in Y$ and hence by Axiom **P5**, $Y = \mathbb{N}$. Therefore, we finally conclude that $1 \in X$.

   Now, let $z \in X$. To show $S(z) \in X$. But, $z \in X$ implies that $n + z = z + n$, for all $n \in mN$. Thus, using $1 \in X$, $n + z = z + n$, for all $n \in mN$ and associativity, one has

   $$n + S(z) = n + (z + 1) = (n + z) + 1 = (z + n) + 1 = 1 + (z + n) = (1 + z) + n = S(z) + n,$$

   for all $n \in \mathbb{N}$. Hence, $S(z) \in X$ and thus by Axiom **P5**, $X = \mathbb{N}$. ■

3. **[Distributive Law]** For every $n, m, k \in \mathbb{N}$, $n \cdot (m + k) = n \cdot m + n \cdot k$.
   Proof. Let $X = \{k \in \mathbb{N} : \text{ for all } m, n \in \mathbb{N}, n \cdot (m + k) = n \cdot m + n \cdot k\}$. To show that $X = \mathbb{N}$.

   $1 \in X$ as for each $n, m \in \mathbb{N}$,

   $$n \cdot (m + 1) = n \cdot S(m) = n \cdot m + n = n \cdot m + n \cdot 1.$$

   Now, let $z \in X$ and let us show that $S(z) \in X$. Since $z \in X$

   $$n \cdot (m + z) = n \cdot m + n \cdot z, \text{ for all } n, m \in \mathbb{N}. \tag{2.2}$$

   Thus, by definition and Equation (2.2), we see that

   $$n \cdot (m+S(z)) = n \cdot S(m+z) = n \cdot (m+z)+n = (n \cdot m+n \cdot z)+n = n \cdot m+(n \cdot z+n) = n \cdot m+n \cdot S(z),$$

   for all $n, m \in \mathbb{N}$. Hence, $S(z) \in X$ and thus by Axiom **P5**, $X = \mathbb{N}$. ■

EXERCISE **2.1.7.** *The readers are now required to prove the following using only the above properties:*

1. **[Uniqueness of addition]** *For every $m, n, k \in \mathbb{N}$, whenever $m = n$ then $m + k = n + k$.*

2. [**Cancellation Law**] *For every $x, y \in \mathbb{N}$, if $x+z = y+z$ for some $z \in \mathbb{N}$ then $x = y$.*
3. [**Associative Law for multiplication**] *For every $x, y, z \in \mathbb{N}$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.*
4. [**Multiplication by** 1] *For each $n \in \mathbb{N}, 1 \cdot n = n$.*
5. [**Second Distributive Law**] *For every $n, m, k \in \mathbb{N}$, $(m+n) \cdot k = m \cdot k + n \cdot k$.*

6. [**Commutativity of multiplication**] *For each $m, n \in \mathbb{N}, n \cdot m = m \cdot n$.*
7. [**Uniqueness of multiplication**] *For every $m, n, k \in \mathbb{N}$, whenever $m = n$ then $m \cdot k = n \cdot k$.*
8. [**Multiplicative Cancellation**] *For every $x, y \in \mathbb{N}$, if $x \cdot z = y \cdot z$ for some $z \in \mathbb{N}$ then $x = y$.*

2.1.2 Well Ordering in $\mathbb{N}$

In this subsection, we introduce the ordering on $\mathbb{N}$. So, for any $m, n \in \mathbb{N}$, we need to define what $n < m$ means?

Definition 2.1.8. [**Ordering in** $\mathbb{N}$] Let $m, n \in \mathbb{N}$. Then, we say $n < m$ (in word, n is less than m) if there exists a $k \in \mathbb{N}$ such that $m = n + k$. Further, $n \leq m$ if either $n < m$ or $n = m$.

Lemma 2.1.9. [**Transitivity**] *Let $x, y, z \in \mathbb{N}$ such that $x < y$ and $y < z$. Then $x < z$.*

Proof. Since $x < y$, there exists $k \in \mathbb{N}$ such that $y = x + k$. Similarly, $y < z$ gives the existence of $\ell \in \mathbb{N}$ such that $z = y + \ell$. Hence, $z = y + \ell = (x + k) + \ell = x + (k + \ell) = x + t$, where $t = k + \ell \in \mathbb{N}$ as $k, \ell \in \mathbb{N}$. Thus, by definition $x < z$. ■

EXERCISE **2.1.10.** *Let $x, y, z \in \mathbb{N}$. Then prove that*

1. *whenever $x \leq y$ and $y < z$ then $x < z$.*
2. *whenever $x < y$ and $y \leq z$ then $x < z$.*
3. *whenever $x \leq y$ and $y \leq z$ then $x \leq z$.*
4. *whenever $x < y$ then $x + z < y + z$ and $x \cdot z < y \cdot z$.*

Lemma 2.1.11. *For all $m, n \in \mathbb{N}, m \neq m + n$.*

Proof. Let $X = \{m \in \mathbb{N} : m \neq m + 1\}$. Clearly, $1 \in X$ as $1 \neq 1 + 1 = S(1)$ (Axiom **P3**). Now, let $n \in X$. On the contrary, assume that $S(n) \notin X$. Then, $S(n) = S(n) + 1 = S(S(n))$. As S is injective (Axiom **P4**), we get $n = S(n) = n + 1$, a contradiction to $n \in X$. So, $S(n) \in X$ and hence by Axiom **P5**, $X = \mathbb{N}$. Thus, $n \neq n + 1$ for all $n \in \mathbb{N}$.

Now, define $X = \{k \in \mathbb{N} :$ for all $m \in \mathbb{N}, m \neq m + k\}$. Then, by the previous paragraph, $1 \in X$. So, assume $k \in X$ and try to show that $S(k) \in X$. Or equivalently, need to show that

$$m \neq m + S(k) = S(m + k), \text{ for all } m \in \mathbb{N}.$$

So, let us define $Y = \{m \in \mathbb{N} : m \neq S(m + k)\}$. Clearly, $1 \in Y$ as by Axiom **P3**, $1 \neq S(\ell)$, for any $\ell \in \mathbb{N}$. So, let $m \in Y$. To show, $S(m) \in Y$.

On the contrary, assume that $S(m) \notin Y$. So, by definition of Y, $S(m) = S(S(m) + k)$. As S is injective (Axiom **P4**), the previous step gives $m = S(m) + k = m + 1 + k = m + (1 + k) = m + (k + 1) = (m + k) + 1 = S(m + k)$, a contradiction to $m \in Y$. Thus, by Axiom **P5**, $Y = \mathbb{N}$. ■

Lemma 2.1.12. [**Well ordering in** $\mathbb{N}$] *For all $m, n \in \mathbb{N}$, exactly one of the following is true:*

1. $n < m$,

2. $n = m$,

3. $n > m$.

Proof. As a first step, we show that if one of the above holds then the other two cannot hold. So, let us assume that $n < m$. Then, by definition, there exists $k \in \mathbb{N}$ such that $m = n + k$. Then, by Lemma 2.1.11 $n \neq n + k = m$ and hence $n \neq m$. If $m < n$, then $n = m + \ell$, for some $\ell \in \mathbb{N}$. Thus,

$$n = m + \ell = (n + k) + \ell = n + (k + \ell), \text{ for some } k + \ell \in \mathbb{N},$$

a contradiction.

The readers should prove the other parts of the first step. Now, to complete the proof, let us fix $n \in \mathbb{N}$ and define $X = \{m \in \mathbb{N} : \text{ either } m < n \text{ or } m = n \text{ or } n < m\}$. We now show that $1 \in X$.

If $n = 1$ then $1 = 1$ and hence $1 \in X$. If $n \neq 1$ then there exists $y \in \mathbb{N}$ such that $n = S(y) = y + 1 = 1 + y$ and hence by the definition of order, $1 < n$. Thus, $1 \in X$. Let us now assume that $m \in X$ and prove that $S(m) \in X$. As $m \in X$ then either $m < n$ or $m = n$ or $n < m$. We will consider all three cases and in each case show that $S(m) \in X$.

If $m < n$ then $n = m + k$, for some $k \in \mathbb{N}$. Further, if $k = 1$ then $n = m + 1$ and $S(m) = n$. Thus, $S(m) \in X$. If $k \neq 1$ then there exists $\ell \in \mathbb{N}$ such that $S(\ell) = k$. Then,

$$n = m + k = m + S(\ell) = m + (\ell + 1) = m + (1 + \ell) = (m + 1) + \ell = S(m) + \ell$$

and hence $S(m) < n$. Thus, $S(m) \in X$.

If $m = n$ then $S(m) = m + 1 = n + 1$ and hence $n < S(m)$. Thus $S(m) \in X$.

If $n < m$ then $m = n + \ell$, for some $\ell \in \mathbb{N}$. Thus, $S(m) = S(n + \ell) = (n + \ell) + 1 = n + (\ell + 1)$ and hence $n < S(m)$. Therefore, $S(m) \in X$ and the proof of each case is complete. Thus, by Axiom **P5**, $X = \mathbb{N}$. ■

We are now in a position the state two important principles, namely the Well ordering principle and the principle of mathematical induction.

Theorem 2.1.13. **[Well ordering principle in $\mathbb{N}$ (or $\mathbb{N} \cup \{0\}$)]** *Every non-empty subset X of $\mathbb{N}$ has a least element.*

Proof. We first prove that for each $n \in \mathbb{N}$, the statement "every non-empty subset of $\{1, 2, \ldots, n\}$ has a least element". To prove this let

$$A = \{n \in \mathbb{N} : \text{every non-empty subset of } \{1, 2, \ldots, n\} \text{ has a least element}\}.$$

Clearly $1 \in A$ as 1 itself is the least element of $\{1\}$, the only non-empty subset of $\{1\}$. Let $n \in A$. To show, $S(n) = n + 1 \in A$.

So, let X be a non-empty subset of $\{1, 2, \ldots, n + 1\}$. If $X = \{n + 1\}$ then it has $n + 1$ as its least element. If $X \neq \{n + 1\}$ then $B = \{1, 2, \ldots, n\} \cap X$ is non-empty and is a non-empty subset of $\{1, 2, \ldots, n\}$. As $n \in A$, B has a least element, say k. Then, by the definition of B, k is also the least element of X. Thus, A is an inductive set and by Axiom **P5**, $A = \mathbb{N}$. ■

What is also interesting about the Well ordering principle is that it is logically equivalent to the principle of mathematical induction, which is stated next. One can obtain a direct proof of the principle of mathematical induction by defining an inductive set and then using Axiom **P5**. Here, we use the Well ordering principle to prove the principle of mathematical induction.

Theorem 2.1.14. **[Principle of mathematical induction (PMI)]** *Let $P(n)$ be a statement (proposition) dependent on a natural number $n \in \mathbb{N}$. Assume that*

1. **base step:** *$P(1)$ is true,*
2. **induction step:** *for each $n \in \mathbb{N}$, the statement $P(n)$ is true implies $P(n+1)$ is true.*

Then, $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $X \subseteq \mathbb{N}$ such that $1 \in X$ and if $k \in X$ then $S(k) = k+1 \in X$. To show that $X = \mathbb{N}$.

If $\mathbb{N} \setminus X = \emptyset$ then we are done. So, let us assume that $\mathbb{N} \setminus X \neq \emptyset$. Then, $\mathbb{N} \setminus X$ is a non-empty subset of $\mathbb{N}$ and hence by the Well ordering principle, let $k \neq 1$ $(1 \in X)$ be the least element of $\mathbb{N} \setminus X$. Then, by Lemma 2.1.3, there exists $y \in \mathbb{N}$ such that $k = S(y) = y+1$. Thus, $y < k$. Since k is the least element of $\mathbb{N} \setminus X$, $y \notin \mathbb{N} \setminus X$. So, $y \in X$ and hence by the definition of the set X, $k = S(y) \in X$, a contradiction as $k \in \mathbb{N} \setminus X$. Therefore, $\mathbb{N} \setminus X = \emptyset$, *i.e.*, $X = \mathbb{N}$. ■

We now prove that the principle of mathematical induction implies the Well ordering principle.

Proof: Let $P(n)$ be the statement "Any subset of natural numbers containing an element k, with $k \leq n$, has a least element".

Define $X = \{n \in \mathbb{N} : P(n) \text{ is true}\}$. Clearly, $1 \in X$ as $P(1)$ is trivially true. So, let us assume that $y \in X$ and show that $S(y) = y+1 \in X$.

As $y \in X$, the statement "if there is a subset E of $\mathbb{N}$ containing an element t, with $t \leq y$, then E contains a least element" is true. Now, let $Y \subseteq \mathbb{N}$ with Y containing an element $t \leq S(y) = y+1$. If Y has no element which is less than $y+1$ then $y+1$ is the least element of Y and hence $y+1 \in X$.

If Y has an element $t < y+1$, then $B = Y \cap \{1, 2, \ldots, y\}$ is non-empty and it contains the element $t \leq y$. Thus, B is a subset of $\mathbb{N}$ containing an element t, with $t \leq y$, and hence B contains a least element. Therefore, by definition of B, the least element of B is also the least element of Y and hence Y contains a least element. Thus, $y+1 \in X$.

Thus, by the principle of mathematical induction, $X = \mathbb{N}$. Now, let T be any non-empty subset of $\mathbb{N}$. Since T is non-empty, there exists an $m \in \mathbb{N}$ such that $m \in T$. Thus, T is a subset of $\mathbb{N}$ containing an element t, with $t = m \leq m$. As $P(m)$ is true, the set T has a least element and thus, one has the Well ordering principle. ■

Exercise **2.1.15.** *Prove that for all $m, n \in \mathbb{N}$, $S(m) + n = S(m+n)$.*

2.1.3 Applications

Let us now go back to the definition of addition: $n+1 = S(n), n+S(m) = S(n+m)$, for all $n, m \in \mathbb{N}$. The word 'assign' means that we actually have a function that does the assignment. We will now prove a theorem, commonly known as the recursive theorem, that will help us in actually defining the addition function as an application.

Theorem 2.1.16. **[Recursive Theorem]** *Let α be a fixed natural number and let $f : \mathbb{N} \to \mathbb{N}$ be a function. Then, there exists a unique function $g : \mathbb{N} \to \mathbb{N}$ such that*

$$g(1) = \alpha \text{ and } g(S(x)) = f(g(x)), \text{ for all } x \in \mathbb{N}.$$

Proof. **[Existence of g]** Since we want a function $g : \mathbb{N} \to \mathbb{N}$, we are essentially looking for a subset of $\mathbb{N} \times \mathbb{N}$. By $g(1) = \alpha$, we mean $(1, \alpha) \in g$. Further, $g(S(x)) = f(g(x))$ means if $y = g(x)$, or equivalently, if $(x, y) \in g$ then $(S(x), f(y)) \in g$. Using this understanding, let us construct g. So, let

$$X = \{A \subseteq \mathbb{N} \times \mathbb{N} : (1, \alpha) \in A \text{ and } (x, y) \in A \text{ implies that } (S(x), f(y)) \in A\}.$$

Clearly, $A \neq \emptyset$ as $\mathbb{N} \times \mathbb{N} \in A$. So, define

$$g = \bigcap_{A \in X} A.$$

Then, $(1, \alpha) \in g$ as $(1, \alpha) \in A$, for all $A \in X$. Now, let $(x, y) \in g$. Then, $(x, y) \in A$, for all $A \in X$. Hence, by definition of A, $(S(x), f(y)) \in A$, for all $A \in X$. Thus, whenever $(x, y) \in g$, we see that $(S(x), f(y)) \in g$. Therefore, $g \in X$ and by definition (intersection of all $A \in X$), g is the smallest element of g.

We now claim that $g : \mathbb{N} \to \mathbb{N}$ is a function. So, we show that $\mathsf{dom}(g) = \mathbb{N}$ and each element of the domain has exactly one image under g.

Let $Y = \{n \in \mathbb{N} : \text{ there exists} z \in \mathbb{N} \text{ for which } (n, z) \in g\}$.As $(1, \alpha) \in g$, we get $1 \in Y$. So, let $n \in Y$. To show $S(n) \in Y$. As $n \in X$, there exists $z \in \mathbb{N}$ such that $(n, z) \in g$. Hence, by definition of g, $(S(n), f(z)) \in g$, *i.e.*, $S(n) \in Y$ and therefore by Axiom **P5**, $Y = \mathbb{N}$. In other words, $\mathsf{dom}(g) = \mathbb{N}$.

As a next step, we prove that for each element of the domain, there is exactly one image under g. So, define

$$Z = \{n \in \mathbb{N} : \text{ whenever} (n, y) \in g \text{ and } (n, z) \in g \text{ then } y = z\}.$$

$1 \in Z$ as $1 \notin Z$ implies that there exist $z_1, z_2 \in \mathbb{N}, z_1 \neq z_2$ such that $(1, z_1), (1, z_2) \in g$. Then, the relation $h = g \backslash \{(1, z_2)\} \subsetneq g$ and $h \in X$. This contradicts the minimality of g. Hence, $(1, z_1), (1, z_2) \in g$ implies $z_1 = z_2$.

So, now let us assume that $n \in Z$. We need to show that $S(n) \in Z$. So, let if possible $S(n) \notin Z$. As, $n \in Z$, there exists a unique $m \in \mathbb{N}$ such that $(n, m) \in g$. Hence, by definition, $(S(n), f(m)) \in g$. But, we have assumed that $S(n) \in Z$. Therefore, there exists $z \in \mathbb{N}, z \neq f(m)$ such that $(S(n), z) \in g$. But in this case, we again have $h = g \setminus \{(S(n), z)\} \subsetneq g$ with $h \in X$. This contradicts the minimality of g. Hence, $f(m) = z$. Thus, $S(n) \in Y$ and thus by Axiom **P5**, $Z = \mathbb{N}$.

As a final step in this proof, we show that g is unique. So, let g_1, g_2 be two functions such that $g_1(1) = g_2(1) = \alpha$, $g_1(S(k)) = f(g_1(k))$ and $g_2(S(k)) = f(g_2(k))$. Define $V = \{n \in \mathbb{N} : g_1(n) = g_2(n)\}$. Then, $1 \in V$. Also, $n \in V$ implies that $g_1(n) = g_2(n)$ and hence $g_1(S(n)) = f(g_1(n)) = f(g_2(n)) = g_2(S(n))$. Thus, $S(n) \in V$ and thus by Axiom **P5**, $V = \mathbb{N}$. This completes the proof of the recursive theorem. ■

Example 2.1.17. As an application of the recursion theorem, we re-define addition and multiplication of natural numbers. Note that the uniqueness of the function g helps us in the sense that we can either either guess the function and then verify it or inductively define the function g.

1. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = S(x)$, for all $x \in \mathbb{N}$. Now, fix $m \in \mathbb{N}$. Then, by the recursion theorem, there exists a unique function $g : \mathbb{N} \to \mathbb{N}$ such that

$$g(1) = m \text{ and } g(S(n)) = f(g(n)), \text{ for all } n \in \mathbb{N}.$$

   Thus, $g(n+1) = g(S(n)) = S(g(n)) = g(n) + 1$, for all $n \in \mathbb{N}$. So, let us verify that the unique function g satisfies $g(n+1) = m + n$, for all $n \in \mathbb{N}$.

   Clearly, $g(1) = m$ and by definition of g, $m + S(n) = g(S(n) + 1) = g(S(S(n))) = S(g(S(n))) = S(g(n+1)) = S(m+n)$. Thus, we get the required addition function.

2. Fix $m \in \mathbb{N}$ and define $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = n + m$, for all $n \in \mathbb{N}$. Then, by the recursion theorem, there exists a unique $g : \mathbb{N} \to \mathbb{N}$ such that $g(1) = m$ and $g(S(n)) = f(g(n))$, for all $n \in \mathbb{N}$. Thus, let us verify that the unique function g satisfies $g(n) = m \cdot n$, for all $n \in \mathbb{N}$.

   Clearly, $g(1) = m = m \cdot 1$ and

$$g(S(n)) = f(g(n)) = g(n) + m = m \cdot n + m \cdot 1 = m \cdot (n+1) = m \cdot S(n).$$

Thus, we get the required addition function.

3. Fix $m \in \mathbb{N}$ and define $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = m \cdot n$, for all $n \in \mathbb{N}$. Then, by the recursion theorem, there exists a unique $g : \mathbb{N} \to \mathbb{N}$ such that $g(1) = m$ and $g(S(n)) = f(g(n))$, for all $n \in \mathbb{N}$. Thus, let us verify that the unique function g satisfies $g(n) = m^n$, for all $n \in \mathbb{N}$.

   Clearly, $g(1) = m = m^1$ and

   $$g(S(n)) = f(g(n)) = m \cdot g(n) = m \cdot m^n = m^(n + 1) = m^{S(n)}.$$

   Thus, we get the required addition function.

By now, the readers should have got a glimpse of the work required to axiomatically construct $\mathbb{N}$, the set of natural numbers. Similarly, the construction of integers from natural numbers and the construction of rational numbers from integers require quite a lot of work. These constructions are very helpful in understanding advanced algebra. But, we will skip their constructions for the time being and try to understand the numbers using the well-ordering principle and the principle of mathematical induction.

Theorem 2.1.18. **[Archimedean property for positive integers]** *Let $x, y \in \mathbb{N}$. Then, there exists $n \in \mathbb{N}$ such that $nx \geq y$.*

Proof. On the contrary assume that such an $n \in \mathbb{N}$ does not exist. That is, $nx < y$ for every $n \in \mathbb{N}$. Now, consider the set $S = \{y - nx \mid n \in \mathbb{N} \cup \{0\}\}$. Then $y \in S$ and hence S is a nonempty subset of $\mathbb{N}_0$. Therefore, by the well-ordering principle (Theorem 2.1.13), S contains its least element, say $y - mx$. Then, by assumption the integer $y - (m + 1)x \geq 0$, $y - (m + 1)x \in S$, and $y - (m + 1)x < y - mx$. A contradiction to the minimality of $y - mx$. Thus, our assumption is invalid and hence the required result follows. ■

Theorem 2.1.19. **[Another form of PMI]** *Let $S \subseteq \mathbb{Z}$ be a set which satisfies*

1. *$k_0 \in S$ and*

2. *$k + 1 \in S$ whenever $\{k_0, k_0 + 1, \ldots, k\} \subseteq S$.*

Then $\{k_0, k_0 + 1, \ldots\} \subseteq S$.

Proof. Consider $T = \{x - (k_0 - 1) \mid x \in S, x \geq k_0\}$. Then $1 \in T$ as $k_0 \in S$ and $1 = k_0 - (k_0 - 1)$. Now, let $\{1, 2, \ldots, k\} \subseteq T$. Then, $\{k_0, k_0 + 1, \ldots, k_0 + k - 1\} \subseteq S$. Hence by the hypothesis, $(k_0 + k - 1) + 1 = k_0 + k \in S$. Therefore, by definition of T, we have $k + 1 \in T$ and hence using the strong form of PMI, $T = \mathbb{N}$. Thus, the required result follows. ■

The next result gives the equivalence of the weak form of PMI with the strong form of PMI.

Theorem 2.1.20. **[Equivalence of PMI in weak form and PMI in strong form]** *Fix a natural number k_0 and let $P(n)$ be a statement about a natural number n. Suppose that P means the statement '$P(n)$ is true for each $n \in \mathbb{N}, n \geq k_0$'. Then '$P$ can be proved using the weak form of PMI' if and only if 'P can be proved using the strong form of PMI'.*

Proof. Let us assume that the statement P has been proved using the weak form of PMI. Hence, $P(k_0)$ is true. Further, whenever $P(n)$ is true, we are able to establish that $P(n + 1)$ is true. Therefore, we can establish that $P(n + 1)$ is true if $P(k_0), \ldots, P(n)$ are true. Hence, P can be proved using the strong form of PMI.

So, now let us assume that the statement P has been proved using the strong form of PMI. Now, define $Q(n)$ to mean '$P(\ell)$ holds for $\ell = k_0, k_0+1, \ldots, n$'. Notice that $Q(k_0)$ is true. Suppose that $Q(n)$ is true (this means that $P(\ell)$ is true for $\ell = k_0, k_0+1, \ldots, n$). By hypothesis, we know that P has been proved using the strong form of PMI. That is, $P(n+1)$ is true whenever $P(\ell)$ is true for $\ell = k_0, k_0+1, \ldots, n$. This, in turn, means that $Q(n+1)$ is true. Hence, by the weak form of PMI, $Q(n)$ is true for all $n \geq k_0$. Thus, we are able to prove P using the weak form of PMI. ■

Example 2.1.21. **[Wrong use of PMI: Can you find the error?]** The following is an incorrect proof of 'if a set of n balls contains a green ball then all the balls in the set are green'. Find the error.

Proof. The statement holds trivially for $n = 1$. Assume that the statement is true for $n \leq k$. Take a collection B_{k+1} of $k+1$ balls that contains at least one green ball. From B_{k+1}, pick a collection B_k of k balls that contains at least one green ball. Then by the induction hypothesis, each ball in B_k is green. Now, remove one ball from B_k and put the ball which was left out in the beginning. Call it B'_k. Again by induction hypothesis, each ball in B'_k is green. Thus, each ball in B_{k+1} is green. Hence by PMI, our proof is complete. ■

EXERCISE **2.1.22.** **[Optional]**

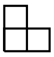
1. *Let $x \in \mathbb{R}$ with $x \neq 1$. Then prove that* $1 + x + x^2 + \cdots + x^n = \sum\limits_{k=0}^{n} x^k = \dfrac{x^{n+1}-1}{x-1}$.
2. *Let $a, a+d, a+2d, \ldots, a+(n-1)d$ be the first n terms of an arithmetic progression. Then,*
$$S = \sum_{i=0}^{n-1} (a+id) = a + (a+d) + \cdots + (a+(n-1)d) = \frac{n}{2}\left(2a + (n-1)d\right).$$
3. *Let $a, ar, ar^2, \ldots, ar^{n-1}$ be the first n terms of a geometric progression, with $r \neq 1$. Then,* $S = a + ar + \cdots + ar^{n-1} = \sum\limits_{i=0}^{n-1} ar^i = a\dfrac{r^n-1}{r-1}$.
4. *Prove that*
   (a) 6 *divides* $n^3 - n$, *for all* $n \in \mathbb{N}$.
   (b) 7 *divides* $n^7 - n$, *for all* $n \in \mathbb{N}$.
   (c) 3 *divides* $2^{2n} - 1$, *for all* $n \in \mathbb{N}$.
   (d) 9 *divides* $2^{2n} - 3n - 1$, *for all* $n \in \mathbb{N}$.
   (e) 10 *divides* $n^9 - n$, *for all* $n \in \mathbb{N}$.
   (f) 12 *divides* $2^{2n+2} - 3n^4 + 3n^2 - 4$, *for all* $n \in \mathbb{N}$.
   (g) $1^3 + 2^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$.
5. *Determine a formula for* $1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + (n-1)\cdot n$ *and prove it.*
6. *Determine a formula for* $1\cdot 2\cdot 3 + 2\cdot 3\cdot 4 + 3\cdot 4\cdot 5 + \cdots + (n-1)\cdot n\cdot (n+1)$ *and prove it.*
7. *Determine a formula for* $1\cdot 3\cdot 5 + 2\cdot 4\cdot 6 + \cdots + n\cdot (n+2)\cdot (n+4)$ *and prove it.*
8. **[Informative]** *For all $n \geq 32$, there exist non-negative integers x and y such that $n = 5x + 9y$. [Hint: Prove it first for the starting 5 numbers.]*
9. **[Informative]** *Prove that, for all $n \geq 40$, there exist non-negative integers x and y such that $n = 5x + 11y$.*

10. *For every positive integer $n \geq 5$ prove that $2^n > n^2 > 2n + 1$.*

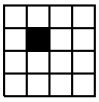
11. **[Informative]** *Prove that for $\mu > 0$,*

$$\prod_{l=1}^{p}(1 + l\mu) \geq 1 + \frac{p(p+1)}{2}\mu + \frac{1}{2}\left(\frac{p^2(p+1)^2}{4} - \frac{p(p+1)(2p+1)}{6}\right)\mu^2.$$

12. **[Informative]** *By an L-shaped piece, we mean a piece of the type shown in the picture. Consider a $2^n \times 2^n$ square with one unit square cut. See the picture given below.*



L-shaped piece



4 × 4 square with a unit square cut

Show that a $2^n \times 2^n$ square with one unit square cut, can be covered with L-shaped pieces.

13. **[Informative]** *Verify that $(k+1)^5 - k^5 = 5k^4 + 10k^3 + 10k^2 + 5k + 1$. Now, put $k = 1, 2, \ldots, n$ and add to get $(n+1)^5 - 1 = 5\sum\limits_{k=1}^{n} k^4 + 10\sum\limits_{k=1}^{n} k^3 + 10\sum\limits_{k=1}^{n} k^2 + 5\sum\limits_{k=1}^{n} k + \sum\limits_{k=1}^{n} 1$. Now, use the formula's for $\sum\limits_{k=1}^{n} k^3$, $\sum\limits_{k=1}^{n} k^2$, $\sum\limits_{k=1}^{n} k$, and $\sum\limits_{k=1}^{n} 1$ to get a expression for $\sum\limits_{k=1}^{n} k^4$.*

14. **[Informative: A general result than AM-GM]**

    (a) *Let $a_1, \ldots, a_9$ be non-negative real numbers such that the sum $a_1 + \cdots + a_9 = 5$. Assume that $a_1 \neq a_2$. Consider $\frac{a_1+a_2}{2}, \frac{a_1+a_2}{2}, a_3, \ldots, a_9$ and argue that*

    $$a_1 \cdots a_9 \leq \left(\frac{a_1 + a_2}{2}\right)^2 a_3 \cdots a_9.$$

    (b) *Let $a_1, \ldots, a_n$ be any non-negative real numbers such that the sum $a_1 + \cdots + a_n = r_0$. Argue that the highest value of $a_1 \cdots a_n$ is obtained when $a_1 = \cdots = a_n = r_0/n$.*

    (c) *Let $a_1, \ldots, a_n$ be fixed non-negative real numbers such that the sum $a_1 + \cdots + a_n = r_0$. Conclude from the previous item that $(r_0/n)^n \geq a_1 \cdots a_n$, the AM-GM inequality.*

2.2 Finite and Infinite Sets

We now discuss the size of sets. A useful way to compare two sets is through their size. In particular, we will be concerned about those sets whose size exceeds the size of the set $\mathbb{N}$, the set of natural numbers.

To start with, for a fixed positive integers n, let us write $\{1, 2, \ldots, n\} = \{1, 2, \ldots, n\}$. We are now ready to prove a few results which will be quite useful in this section.

Lemma 2.2.1. **[One-One order preserving map from a one-one map]** *Fix a positive integer n and let $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ be a one-one function. Let $\mathsf{rng}\, f = \{f(x) : x \in \{1, 2, \ldots, n\}\}$, the image of f in $\mathbb{N}$. Then, there exists a function $g : \{1, 2, \ldots, n\} \to \mathsf{rng}\, f$ such that g is one-one and g preserves order, i.e., $x < y$ implies that $g(x) < g(y)$, for all $x, y \in \{1, 2, \ldots, n\}$.*

Proof. We use induction to prove this result. The result is clearly true for $n = 1$ as $g : [1] \to \{f(1)\}$ given by $g(1) = f(1)$ is a one-one and order preserving map. So, let the result be true for $n = k$ and suppose we have been given a one-one map $f : [k+1] \to \mathbb{N}$. We need to construct the function g which is one-one and preserves order.

As $\mathsf{rng}\, f$ is a non-empty subset of $\mathbb{N}$, by the well-ordering principle, $\mathsf{rng}\, f$ contains a least element, say $\alpha \in \mathbb{N}$ such that $f(x) = \alpha$, for some $x \in [k+1]$. Now, define $h : \{1, 2, \ldots, k\} \to \mathsf{rng}\, f \setminus \{\alpha\}$ by

$$h(y) = \begin{cases} f(y) & \text{if } y < x \\ f(y+1) & \text{if } y \geq x \end{cases}.$$

Then, h is one-one as f is one-one and by definition, h is onto. But, by induction step, there exists a map $g_1 : \{1, 2, \ldots, k\} \to \mathsf{rng}\, h = \mathsf{rng}\, f \setminus \{\alpha\}$ such that g_1 is one-one and order preserving. Thus, the required map $g : [k+1] \to \mathsf{rng}\, f$ is given by

$$g(y) = \begin{cases} \alpha & \text{if } y = 1 \\ g_1(y-1) & \text{if } y \geq 2 \end{cases}.$$

Verify that g is indeed one-one and order preserving and hence the required result follows. ■

As an application of Lemma 2.2.1, we prove the following result.

Lemma 2.2.2. **[Injection]** *Let $f : [m] \to \{1, 2, \ldots, n\}$ be a one-one function for some $m, n \in \mathbb{N}$. Then $m \leq n$.*

Proof. As $\{1, 2, \ldots, n\} \subseteq \mathbb{N}$, by Lemma 2.2.1 there exists a function $g : [m] \to \mathsf{rng}\, f \subseteq \{1, 2, \ldots, n\}$ which is one-one and order preserving. We claim that $g(x) \geq x$, for all $x \in [m]$.

Suppose the claim is false. Then, the set $S = \{\ell \in [m] : g(\ell) < \ell\}$ is non-empty subset of $\mathbb{N}$. Hence by the well ordering principle, S contains a least element, say $k \in [m]$ such that $g(k) < k$. Clearly $k \neq 1$ as $g(1) \geq 1$. So, we see that $g(k-1) \geq k-1$ and $g(k) < k$. But, g is order preserving and hence

$$g(k) > g(k-1) \geq k-1,$$

a contradiction to $g(k) < k$. Thus, the claim is true.

As g is order preserving and $g(x) \in \{1, 2, \ldots, n\}$, one has $n \geq g(m) \geq m$. Thus, $n \geq m$ and hence the required result follows. ■

As an immediate corollary one has the following result. The proof is left for the reader.

Lemma 2.2.3. **[Bijection]** *Let $f : [m] \to \{1, 2, \ldots, n\}$ be a bijection for some $m, n \in \mathbb{N}$. Then $m = n$.*

The following remark helps us to define cardinality of a finite set.

Remark 2.2.4. **[Cardinality of a finite set]** *Let X be a finite set and suppose there exist $m, n \in \mathbb{N}$ and bijections $f : [m] \to X$ and $g : \{1, 2, \ldots, n\} \to X$. As g is a bijection, $g^{-1} : X \to \{1, 2, \ldots, n\}$ is also a bijection and hence the map $g^{-1} \circ f : [m] \to \{1, 2, \ldots, n\}$ is a bijection. Thus, by Lemma 2.2.3 $m = n$. Thus we see that if X is a finite set then the number m for which there is a bijection $f : [m] \to X$ is unique. This number m is called the* **cardinality** *of X and is generally denoted by $|X|$. Hence, for any positive integer m, $|[m]| = m$.*

We now assemble a few important facts on cardinality.

Fact 2.2.5.

1. Let X and Y be two disjoint sets and let $f : X \to \{1, 2, \ldots, n\}$ and $g : Y \to [m]$ be two bijections. Then, the function $h : X \cup Y \to [m+n]$ defined by

$$h(x) = \begin{cases} f(x) & \text{if } x \in X \\ g(x) + n & \text{if } x \in Y \end{cases}$$

is a bijection.

2. Fix $n \geq 2$ and let $f : X \to \{1, 2, \ldots, n\}$ be a bijection such that for a fixed element $a \in X$, one has $f(a) = k$. Then $g : X \setminus \{a\} \to \{1, 2, \ldots, n-1\}$, defined by
$$g(x) = \begin{cases} f(x) & \text{if } f(x) \leq k-1 \\ f(x)-1 & \text{if } f(x) \geq k+1 \end{cases}$$
is a bijection.

3. For any positive integer n and k, there is no bijection from $\{1, 2, \ldots, n\}$ to $[n+k]$.

   Proof. Use Lemma 2.2.3. ■

4. Any subset of $\{1, 2, \ldots, n\}$ is finite.

   Proof. We use PMI to prove this. It is true for $n = 1$. Let the result be true for $\{1, 2, \ldots, n-1\}$,. Now, let $S \subseteq \{1, 2, \ldots, n\}$. If $n \notin S$, then $S \subseteq \{1, 2, \ldots, n-1\}$, and hence using PMI the result follows. If $n \in S$, let $T = S \setminus \{n\}$. Then by PMI, T is finite, and hence by Fact 2.2.5.1, S is finite as S is disjoint union of T and $\{n\}$. ■

5. Any subset of a finite set is finite.

   Proof. Let $|S| = n$, for some $n \in \mathbb{N}$. Then, there is a bijection $f : S \to \{1, 2, \ldots, n\}$. Let $T \subseteq S$. If T is empty then there is nothing to prove. Else, consider the map $f_T : T \to f(T)$. This map is a bijection. By Fact 2.2.5.4, $f(T) \subseteq \{1, 2, \ldots, n\}$ is finite. Hence, Lemma 2.2.3 gives T is finite. ■

6. The set $\mathbb{N}$ is not finite.

   Proof. Assume that the set $\mathbb{N}$ is finite and $|\mathbb{N}| = n$, for some natural number n. But, $\{1, 2, \ldots, n, n+1\} \subseteq \mathbb{N}$ and therefore the identity map $\mathbf{Id} : \{1, 2, \ldots, n, n+1\} \to \mathbb{N}$ is one-one. Thus, by Lemma 2.2.2, $n + 1 = |\{1, 2, \ldots, n, n+1\}| \leq n$, a contradiction. ■

Exercise **2.2.6.** *1. Let X and Y be two disjoint sets with $|X| = m$ and $|Y| = n$. Then $|X \cup Y| = m + n$.*

2. Let X be a nonempty finite set and let $Y \subseteq X$. Then $|Y| \leq |X|$. In particular, if $Y \subsetneq X$ then $|Y| < |X|$.

3. Let X be a finite nonempty set and α be a fixed symbol. Now, consider the set $Y = \{(\alpha, a) \mid a \in X\}$. Then $|X| = |Y|$.

4. Let X be a nonempty finite set. Then, for any set Y, $|X| = |X \setminus Y| + |X \cap Y|$.

5. Let X and Y be two finite sets then $|X \cup Y| = |X| + |Y| - |X \cap Y|$.

Proof. We know $X \cup Y = (X \setminus Y) \cup (X \cap Y) \cup (Y \setminus X)$. As the sets $X \setminus Y$, $X \cap Y$, and $Y \setminus X$ are finite and pairwise disjoint, the result follows from Exercise 2.2.6.1. ■

To proceed with the next definition, recall that the sets X and Y are said to be equivalent if there exists a bijection between X and Y.

Definition 2.2.7. [Finite/Countably finite and Infinite/Countably infinite sets]

1. A set X is said to be **finite** or **countably finite** if either X is empty or X is equivalent to $[m]$, for some $m \in \mathbb{N}$. A set which is not finite is called an **infinite** set.

2. A set which is either finite or is equivalent to $\mathbb{N}$ is called a **countable** set. In particular, a set which is equivalent to $\mathbb{N}$ is called a **countably infinite** set.

We now give a few useful criteria to determine whether a set is finite or infinite.

Fact 2.2.8. 1. Let X be an infinite set and Y be a finite set. Then $X \setminus Y$ is also infinite. In particular, if $a \in X$, then $X \setminus \{a\}$ is also infinite.

2. A set X is infinite if and only if there is a one-one function $f : \mathbb{N} \to X$.

   Proof. Let X be infinite. So $X \neq \emptyset$. Let $a_1 \in X$. Put $f(1) = a_1$ and $X_1 = X \setminus \{a_1\}$. By Fact 2.2.8.1, X_1 is infinite. Assume that we have defined $f(1), \ldots, f(k)$ and obtained $X_k = X_{k-1} \setminus \{a_k\}$. As X_{k-1} was infinite, by Fact 2.2.8.1, X_k is also infinite. Hence $X_k \neq \emptyset$. Let $a_{k+1} \in X_k$. Define $f(k+1) = a_{k+1}$ and $X_{k+1} = X_k \setminus \{a_{k+1}\}$. By applying induction, f gets defined on $\mathbb{N}$. Notice that by construction $a_{k+1} \notin \{a_1, \ldots, a_k\}$. Hence f is one-one.

   Conversely, let $f : \mathbb{N} \to X$ be one-one. Then $f : \mathbb{N} \to f(\mathbb{N})$ is a bijection. Thus, $\mathbb{N}$ is equivalent to $f(\mathbb{N})$. So, X contains $f(\mathbb{N})$, a countably infinite set. Thus, using Fact 2.2.5.5, X is infinite as well. ∎

3. A set is infinite if and only if it is equivalent to a proper subset of itself.

   Proof. Let S be an infinite set. Then, by Fact 2.2.8.2, there is a one-one function $f : \mathbb{N} \to S$. Now define a map $g : S \to S \setminus \{f(1)\}$ by

$$g(x) = \begin{cases} x, & \text{if } x \notin f(\mathbb{N}) \\ f(k+1), & \text{if } x = f(k) \end{cases}.$$

   Then, g is indeed a bijection. Thus, S is equivalent to its proper subset $S \setminus \{f(1)\}$.

   Conversely, let T be a proper subset of a set S such that S and T are equivalent. Suppose S is finite. Then, by Fact 2.2.5.5, T is finite with $|T| < |S|$. But, by Remark 2.2.4 $|S| = |T|$, a contradiction. ∎

EXERCISE **2.2.9.** *1. Let X be a infinite set and let $Y \supseteq X$. Then Y is also infinite.*

2. Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(x) = \begin{cases} \frac{-x}{2} & \text{if } x \text{ is even} \\ \frac{x-1}{2} & \text{if } x \text{ is odd} \end{cases}.$$

Prove that f gives an equivalence between $\mathbb{N}$ and $\mathbb{Z}$. Thus, $\mathbb{Z}$ is countably infinite set.

2.3 Countable and Uncountable sets

In the previous section we learnt that $\mathbb{N}$ is a countably infinite set. We now show that the set $\mathbb{N} \times \mathbb{N}$ is also countably infinite.

Lemma 2.3.1. *The set $\mathbb{N} \times \mathbb{N}$ is countably infinite.*

Proof. Verify that $\mathbb{N} \times \mathbb{N}$ is equivalent to the set $A = \{(x, y) \in \mathbb{N} \times \mathbb{N} : y \leq x\}$ by using the map $g : \mathbb{N} \times \mathbb{N} \to A$ defined by $g(x, y) = (x + y - 1, y)$. Further, use he map $f : A \to \mathbb{N}$ defined by $f(x, y) = \dfrac{x(x-1)}{2} + y$ to show that A is equivalent to $\mathbb{N}$. ∎

We now present another proof using the even and odd numbers. Note that this idea can be suitably generalized to replace 2 by any prime number.

Alternate. Define a map $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $h(x, y) = 2^{x-1}(2y - 1)$. Then, h is one-one as $h(x, y) = h(m, n)$ if and only if $2^{x-1}(2y-1) = 2^{m-1}(2n-1)$. Now, if $x = m$ then $2y - 1 = 2n - 1$ and hence $y = n$. Therefore $(x, y) = (m, n)$. If $x > m$ then $2^{x-m}(2y - 1) = 2n - 1$, a contradiction as the left hand side is an even number whereas the right hand side is an odd number.

h is onto as every $x \in \mathbb{N}$ can be uniquely written as $x = 2^{r-1}(2n - 1)$, for some $r, n \geq 1$. ■

EXERCISE **2.3.2.** *Let* $\mathbb{Q}^+ = \left\{\frac{m}{n} : m, n \in \mathbb{N}, \gcd(m, n) = 1\right\}$ *and* $\mathbb{Q}^- = \{-x : x \in \mathbb{Q}^+\}$.

1. *Then prove that* $\mathbb{Q}^+$ *is countably infinite.*
2. *Thus conclude that* $\mathbb{Q}^-$ *is countably infinite as well.*
3. *Therefore, prove that* $\mathbb{Q}$ *is countably infinite.*

2.3.1 Cantor's Lemma

To proceed further, we present Cantor's experiment. To do so, recall that for any set X, $\mathcal{P}(X)$ denotes the power set of X, *i.e.*, $\mathcal{P}(X)$ is the set containing all subsets of X.

Cantor's Experiment for the student: Why does it happen?

Take a plain paper.

1. On the left draw an oval (of vertical length) and write the elements of $\{1, 2, 3, 4\}$ inside it, one below the other. On the right draw a similar but large oval and write the elements of $\mathcal{P}(\{1, 2, 3, 4\})$ inside it, one below the other.
2. Now draw a directed line from 1 (on the left) to any element on the right. Repeat this for $2, 3$ and 4. We have drawn a function. Call it f.
3. Notice that $f(1), f(2), f(3)$ and $f(4)$ are sets. Find out the set $X = \{i : i \notin f(i)\}$. Locate this set on the right.
4. It is guaranteed that you do not have a directed line touching X. Why?

Lemma 2.3.3. [**Cantor**] *Let S be a set and $f : S \to \mathcal{P}(S)$ be a function. Then, there exists $A \in \mathcal{P}(S)$ which does not have a pre-image. That is, there is no surjection from S to $\mathcal{P}(S)$.*

Proof. On the contrary assume that there exists $f : S \to \mathcal{P}(S)$ such that f is a surjection. Now, consider the set $A = \{x : x \notin f(x)\} \in \mathcal{P}(S)$. As f is a surjection, there exists $s \in S$ with $f(s) = A$. So, $A = f(s) = \{x : x \notin f(x)\}$. We now show that s neither belongs to A nor to A'.

If $s \in A$, then by definition of A, $s \notin f(s) = A$. Similarly, if $s \notin A$ means that $s \in f(s) = A$. Thus, $s \notin A \cup A' = S$, a contradiction. ■

Remark 2.3.4. [**Uncountable set**] *Cantor's Lemma states that one cannot have a bijection between a set and its power set. So, the sets $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ cannot be equivalent. Thus, the set $\mathcal{P}(\mathbb{N})$ is infinite but cannot be countably infinite. The sets that are not countable are called* **uncountable** *sets.*

Definition 2.3.5.

1. [**Enumeration**] Let A be a countably infinite set. Then, by definition, there is a bijection $f : \mathbb{N} \to A$. So, we can list all the elements of A as $f(1), f(2), \ldots$. This list is called an **enumeration** of the elements of A.
2. [**Sequence**] An infinite **sequence** of a non-empty set X is a function $f : \mathbb{N} \to X$ and is represented by $\{f_i\}_{i \in \mathbb{N}} = \{f_1, f_2, \ldots\}$.

Example 2.3.6. 1. Let S be the set of all 0-1-sequences, *i.e.*, S is the collection of all functions $x : \mathbb{N} \to \{0, 1\}$. Or equivalently,

$$S = \big\{x : x = \{x_1, x_2, \ldots\} \text{ where for each } i \in \mathbb{N}, x_i \in \{0, 1\}\big\}.$$

Define $f : S \to \mathcal{P}(\mathbb{N})$ as

$$f(x) = f\big(\{x_1, x_2, \ldots\}\big) = \{n : x_n = 1\}.$$

Then f is a bijection. Hence, S is uncountable by Cantor's lemma.

2. Let $T = \{x \in (0, 1) \mid x \text{ has a decimal expansion containing the digits 0 and 1 only}\}$. Then T is uncountable.

Proof. One proof follows by the previous idea.

Alternate. [Cantor's diagonalization] If T is countably infinite, let $x_1, x_2, \cdots$ be an enumeration of T. Let $x_n = .x_{n1}x_{n2}\cdots$, where $x_{ni} \in \{0, 1\}$. Put $y_{nn} = 1$, if $x_{nn} = 0$ and $y_{nn} = 0$, otherwise. Consider the number $y = .y_{11}y_{22}\cdots \in T$. Notice that for each n, $y \neq x_n$. That is, $y \in T$ but it is not in the enumeration list. This is a contradiction.

2.3.2 Creating Bijections

Experiment 1:

Make a horizontal list of the elements of $\mathbb{N}$ using '$\cdots$' only once. Now, horizontally list the elements of $\mathbb{Z}$ just below the list of $\mathbb{N}$ using '$\cdots$' once. Draw vertical lines to supply a bijection from $\mathbb{N}$ to $\mathbb{Z}$. Can you supply another by changing the second list a little bit?

Experiment 2:

Suppose that you have an open interval (a, b). Its center is $c = \frac{a+b}{2}$ and the distance of the center from one end is $\frac{l}{2} = \frac{b-a}{2}$. View this as a line segment on the real line. Stretch (a, b) uniformly without disturbing the center and make its length equal to L.

Where is c now (in $\mathbb{R}$)? Where is $c - \frac{l}{2}$? Where is $c + \frac{l}{2}$? Where is $c - \alpha \times \frac{l}{2}$, for a fixed $\alpha \in (-1, 1)$?

Now, use the above idea to find a bijection from (a, b) to (s, t)? [Hint: Fix the center first.]

EXERCISE **2.3.7.** *1. Supply two bijections from $(1, \infty)$ to $(5, \infty)$, one by 'scaling' and the other by 'translating'.*

2. Take reciprocal to supply a bijection from $(0, 1)$ to $(1, \infty)$. You can also use the exponential function to get this.

3. Supply a bijection from $(-1, 1)$ to $(-\infty, \infty)$.

4. Supply a bijection from $(0, 1)$ to $\mathbb{R}$.

5. Supply a bijection from $(0, 1) \times (0, 1)$ to $\mathbb{R} \times \mathbb{R}$.

Train-Seat argument to find a bijection

Let $f : P = (0,1) \to T = (3,5)$ be a bijection. Imagine elements of P as PERSONS and elements of T as seats in a TRAIN. So, f assign a seat to each person and the train is full.

1. Now suppose a new person 0 is arriving. He wants a seat. To manage it, let us un-seat two persons $\frac{1}{2}, \frac{1}{3}$. So, two seats $f(\frac{1}{2}), f(\frac{1}{3})$ are vacant. But we have 3 persons to take those seats. Giving each person a seat is not possible.
2. Suppose that we un-seat $\frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{30}$? Can we manage it?
3. Suppose that we un-seat $\frac{1}{2}, \frac{1}{3}, \cdots$? Can we manage it now?
4. What do we do if we had two new persons arriving? Fifty new persons arriving? A set $\{a_1, a_2, \cdots\}$ of new persons arriving?

The readers are required to prove the next theorem.

Theorem 2.3.8. *Let A be a set containing the set $\{a_1, a_2, \ldots, \}$ and let $f : A \to B$ be a bijection. Then, prove that, for any collection*

1. *$\{c_1, \ldots, c_k\}$ of elements that are outside A, the function*

$$h(x) = \begin{cases} f(x) & \text{if } x \in A \setminus \{a_1, a_2, \ldots\} \\ f(a_{i+k}) & \text{if } x = a_i, i \in \mathbb{N} \\ f(a_i) & \text{if } x = c_i, i = 1, 2, \ldots, k. \end{cases}$$

is a bijection from $A \cup \{c_1, \ldots, c_k\}$ to B.

2. *$\{c_1, c_2, \ldots\}$ of elements that are outside A, the function*

$$h(x) = \begin{cases} f(x) & \text{if } x \in A \setminus \{a_1, a_2, \ldots\} \\ f(a_{2n-1}) & \text{if } x = a_n, n \in \mathbb{N} \\ f(a_{2n}) & \text{if } x = c_n, n \in \mathbb{N} \end{cases}$$

is a bijection from $A \cup \{c_1, c_2, \ldots\}$ to B.

Exercise **2.3.9.** *Use Theorem 2.3.8 to give bijections from A to B, where*

1. *$A = [0,1)$ and $B = (0,1)$.*
2. *$A = (0,1) \cup \{1,2,3,4\}$ and $B = (0,1)$.*
3. *$(0,1) \cup \mathbb{N}$ to $(0,1)$.*
4. *$A = [0,1]$ and $B = [0,1] \setminus \{\frac{1}{1}, \frac{1}{3}, \frac{1}{5}, \cdots\}$.*
5. *$A = \mathbb{R}$ and $B = \mathbb{R} \setminus \mathbb{N}$.*
6. *$A = (0,1)$ and $B = \mathbb{R} \setminus \mathbb{N}$.*
7. *$A = [0,1]$ and $B = \mathbb{R} \setminus \mathbb{N}$.*
8. *$A = (0,1)$ and $B = (1,2) \cup (3,4)$.*
9. *$A = \mathbb{R} \setminus \mathbb{Z}$ and $B = \mathbb{R} \setminus \mathbb{N}$.*

2.3.3 Schröder-Bernstein Theorem

Creating bijections from injections

Let $X = Y = \mathbb{N}$. Take injections $f : X \to Y$ and $g : Y \to X$ defined as $f(x) = x + 2$ and $g(x) = x + 1$. In the picture, we have X on the left and Y on the right. If $(x, y) \in f$, we draw a solid line joining x and y. If $(y, x) \in g$, we draw a dotted line joining y and x.

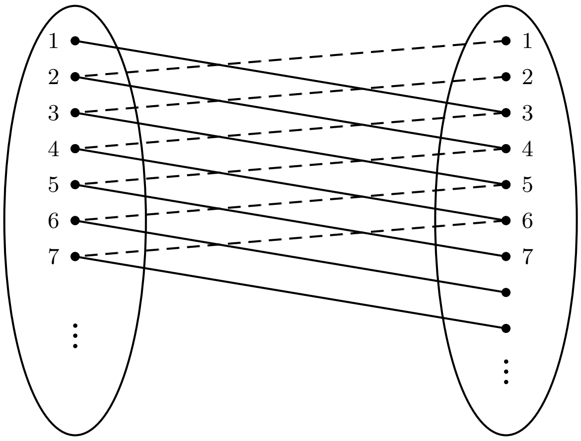


Figure 2.1: Graphic representation of functions f and g

We want to create a bijection h from X to Y by erasing some of these lines.

1. Thus, $h(1)$ must be 3. So, the dotted line $(3, 4)$ cannot be used for h.
2. So, $h(4)$ must be 6. So, the dotted line $(6, 7)$ cannot be used for h.
3. So, $h(7)$ must be 9. Continue two more steps to realize what is happening.

Thus, the bijection $h : X \to Y$ is given by $h(x) = \begin{cases} f(x), & \text{if } x = 3n - 2, n \in \mathbb{N} \\ g^{-1}(x), & \text{otherwise.} \end{cases}$

Exercise **2.3.10.** *Take $X = Y = \mathbb{N}$. Supply bijections using the given injections $f : X \to Y$ and $g : Y \to X$.*

1. *$f(x) = x + 1$ and $g(x) = x + 2$.*
2. *$f(x) = x + 1$ and $g(x) = x + 3$.*
3. *$f(x) = x + 1$ and $g(x) = 2x$.*

Theorem 2.3.11. [**Schröder-Bernstein: Creating a bijection**] *Let A and B be two non-empty sets and let $f : A \to B$ and $g : B \to A$ be injections. Then, there exists a bijection from A to B.*

Proof. If g is onto, we have nothing to prove. So, assume that g is not onto. Put $O = A \setminus g(B)$, $\phi = g \circ f$ and $E = O \cup \phi(O) \cup \phi^2(O) \cup \cdots$. Use $\phi^0(O)$ to denote O. Notice that

$$g\Big(f(E)\Big) = \phi(E) = \phi\Big(\mathop{\cup}_{n=0}^{\infty} \phi^n(O)\Big) = \mathop{\cup}_{n=1}^{\infty} \phi^n(O) = E \setminus O,$$

as g does not map to O. Hence, g maps $f(E)$ to $E \setminus O$ bijectively. Recall that O is the set of points in A that are not mapped by g, $O \subseteq E$ and g has already mapped $f(E)$ onto $E \setminus O$. Hence, g must map $f(E)'$ to E' bijectively. So, the function

$$h(x) = \begin{cases} g^{-1}(x) & \text{if } x \in E', \\ f(x) & \text{if } x \in E, \end{cases}$$

is a bijection from A to B.

Alternate. If g is onto, we have nothing to prove. So, assume that g is not onto. Put $O = A\backslash g(B)$, $\phi = g\circ f$ and $E = O\cup\phi(O)\cup\phi^2(O)\cup\cdots$. Use $\phi^0(O)$ to denote O. Notice that

$$\phi(E) = g\Big(f(E)\Big) = \phi(E) = \phi\Big(\bigcup_{n=0}^{\infty}\phi^n(O)\Big) = \bigcup_{n=1}^{\infty}\phi^n(O) = E\setminus O,$$

as g does not map to O. Observe that $\phi : E\to E\setminus O$ is a bijection. Define $h : A\to A\setminus O$ as

$$h(x) = \begin{cases} x, & \text{if } x\in A\setminus E,\\ \phi(x), & \text{if } x\in E.\end{cases}$$

Then, note that h is a bijection and hence $h^{-1}\circ g$ is a bijection from B to A.

Alternate. Let $F = \{T\subseteq A \mid g\left(f(T)'\right)\subseteq T'\}$.

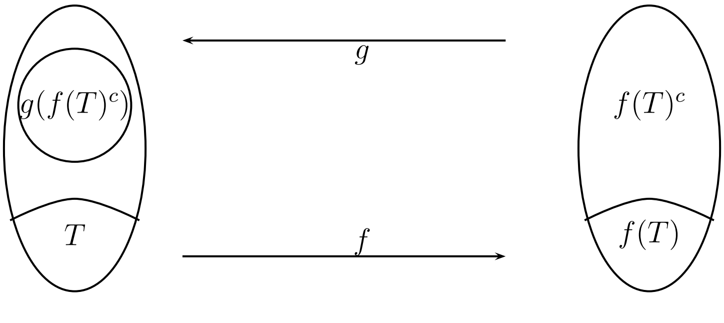


Figure 2.2: Depiction of Schrӧder-Bernstein Theorem

Note that $\emptyset\in F$. Put $U = \bigcup\limits_{T\in F} T$. Then, $U\in F$, as

$$g\big(f(U)'\big) = g\Big(\big[f\big(\bigcup_{T\in F} T\big)\big]'\Big) = g\Big(\big[\bigcup_{T\in F} f(T)\big]'\Big) = g\Big(\bigcap_{T\in F} f\left(T\right)'\Big) = \bigcap_{T\in F} g\left(f\left(T\right)'\right) \subseteq \bigcap_{T\in F} T' = U'.$$

Thus, U is the maximal element of F. We claim that $U'\subseteq g\left(f(U)'\right)$. To see this, take $x\in U'\setminus g\left(f(U)'\right)$ and put $V = U\cup\{x\}$. Then, $f(U)\subseteq f(V)$ and so $f(V)'\subseteq f(U)'$. Thus

$$g\big(f(V)'\big)\subseteq g\big(f(U)'\big)\subseteq U'\cap\{x\}' = V',$$

a contradiction to the maximality of U in F. So, $g\big(f(U)'\big) = U'$. Now, define $h : A\to B$ as

$$h(x) = \begin{cases} f(x) & \text{if } x\in U,\\ g^{-1}(x) & \text{else.}\end{cases}$$

It is easy to see that h is a bijection. ∎

The next two results are applications of Schrӧder-Bernstein theorem.

Lemma 2.3.12. [Infinite iff countably infinite subset]

1. *Let X be an infinite subset of $\mathbb{N}$. Then, X is countably infinite.*

2. *Let $X = \{a_1, a_2, \ldots\}$ be countably infinite and $Y\subseteq X$. Then Y is countable.*

3. *A set X is infinite if and only if X has a countably infinite subset.*

Proof. **Part 1.** Since X is infinite, by Fact 2.2.8.2 there is a one-one function $f : \mathbb{N}\to X$. Also, $X\subseteq\mathbb{N}$ and hence $\mathbf{Id} : X\to\mathbb{N}$ is a one-one function. Hence, by Schrӧder-Bernstein theorem, there exists a bijection from X to $\mathbb{N}$ and the required result follows.

Part 2. Since X is countably infinite , by definition, there exists a bijection $f : X\to\mathbb{N}$. If Y is finite then by definition, it is countable. So, assume that Y is infinite. As f is one-one, $f(Y)$ is an infinite subset of $\mathbb{N}$ and hence by the first part, $f(Y)$ is countably infinite. So, let $g : f(Y) \to \mathbb{N}$ be a bijection. Then the map $g \circ f$ gives a bijection from Y to $\mathbb{N}$ and hence the required result follows.

Part 3. Since X is infinite, by Fact 2.2.8.2 there is a one-one function $f : \mathbb{N} \to X$. Thus, $f(\mathbb{N})$ is a countably infinite subset of X. Conversely, assume that X is finite. Then, by Fact 2.2.5.5, every subset of X is finite, a contradiction to the assumption that X has a countably infinite subset. Thus, the required result follows. ■

As a corollary, we have the following result.

Corollary 2.3.13. *Let X be uncountable and $X \subseteq Y$. Then Y is uncountable.*

Proof. If Y is countable, then by Lemma 2.3.12, X must be countable, a contradiction. ■

Theorem 2.3.14. **[Power set and uncountability]** *If S is infinite, then $\mathcal{P}(S)$ is uncountable.*

Proof. As S is infinite, by Fact 2.2.8.2, there is a one-one map, say $f : \mathbb{N} \to S$. Now, define a map $g : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(S)$ as $g(A) = f(A)$, for all $A \in \mathcal{P}(\mathbb{N})$. Then, g is clearly one-one and hence $g\big(\mathcal{P}(\mathbb{N})\big)$ is uncountable (as $\mathcal{P}(\mathbb{N})$ is uncountable). Hence $\mathcal{P}(S)$, being a superset of $g\big(\mathcal{P}(\mathbb{N})\big)$, is uncountable, by Corollary 2.3.13. ■

Theorem 2.3.15. **[Countable union of countable sets]** *Countable union of countable sets (union of a countable class of countable sets) is countable.*

Proof. Let $\{A_i\}_{i\in\mathbb{N}}$ be a countable class of countable sets and put $X = \underset{i}{\cup} A_i$. If X is finite then we are done. So, let X be infinite. Hence, by Fact 2.2.8.2, there is a one-one map $f : \mathbb{N} \to X$. Define $g : X \to \mathbb{N}$ as $g(x) = 2^i 3^k$, if i is the smallest positive integer for which $x \in A_i$ and x appears at the k-th position in the enumeration of A_i. Then g is one-one. Now, by Schröder-Bernstein theorem A is equivalent to $\mathbb{N}$. ■

Theorem 2.3.16. **[Powet set of $\mathbb{N}$ equivalent to $\mathbb{R}$]** *The set $\mathcal{P}(\mathbb{N})$ is equivalent to $[0, 1)$. Furthermore, $\mathcal{P}(\mathbb{N})$ is equivalent to $\mathbb{R}$.*

Proof. We already know a one-one map $f : \mathcal{P}(\mathbb{N}) \to [0, 1)$ (see Examples 2.3.6.1 and 2.3.6.2). Let $r \in (0, 1)$. Consider the nonterminating binary representation of r. Denote by F_r the set of positions of 1 in this representation. Now, define $g : [0, 1) \to \mathcal{P}(\mathbb{N})$ by $g(r) = F_r$, if $r \neq 0$ and $g(0) = \emptyset$. Then g is one-one. Now, by Schröder-Bernstein theorem $\mathcal{P}(\mathbb{N})$ is equivalent to $[0, 1)$.

The next statement follows as $[0, 1)$ is equivalent to $(0, 1)$ (see Exercise 2.3.17.5) and $(0, 1)$ is equivalent to $\mathbb{R}$. ■

EXERCISE **2.3.17.**

1. *Give a one-one function from $\mathbb{N}$ to $\mathbb{Q}$. Define f from $\mathbb{Q}$ to $\mathbb{N}$ as*

$$f(x) = \begin{cases} 2^r 3^s & \text{if } x = \frac{r}{s}, \gcd(r, s) = 1, r > 0, s > 0, \\ 5^r 3^s & \text{if } x = \frac{-r}{s}, \gcd(r, s) = 1, r > 0, s > 0, \\ 1 & \text{if } x = 0 \end{cases}$$

   Argue that f is one-one. Apply Schröder-Bernstein theorem to prove that $\mathbb{Q}$ is equivalent to $\mathbb{N}$.

2. *Give a one-one map from $(0, 1) \to (0, 1) \times (0, 1)$. For each $x \in (0, 1)$, let $.x_1x_2\cdots$ be the nonterminating decimal representations*[1] *of x. For $x = .x_1x_2x_3\cdots$, $y = .y_1y_2y_3\cdots$, define $f(x, y) = .x_1y_1x_2y_2x_3y_3\cdots$. Argue that f is an injection from $(0, 1) \times (0, 1)$ to $(0, 1)$. Hence, show that $(0, 1)$ is equivalent to $(0, 1) \times (0, 1)$. Hence, show that $\mathbb{R} \times \mathbb{R}$ is equivalent to $\mathbb{R}$.*

[1] Recall that every real number has a unique nonterminating decimal representation.

3. *Fix $k \in \mathbb{N}$. Supply a one-one map from $\mathbb{N}$ to $\mathbb{N}^k$, the k-fold cartesian product of $\mathbb{N}$. Now, use k distinct primes to supply a one-one map from $\mathbb{N}^k$ to $\mathbb{N}$. Hence, conclude that $\mathbb{N}^k$ is equivalent to $\mathbb{N}$.*

4. *Supply a bijection from $(0,1)$ to $(1,2) \cup (3,4) \cup (5,6) \cup (7,8) \cup \cdots$.*

5. *Show using Schröder-Bernstein that $(0,1)$ is equivalent to $(0,1]$.*

6. *Let X be a set such that $f : \mathbb{N} \to X$ is an onto function. Then, either X is a finite set or X is countably infinite.*

7. *Let $X = \{a_1, a_2, \ldots\}$ be a countably infinite set and let $Y \subseteq X$. Then, Y is countable.*

8. **[Cardinal numbers in brief]**

   (a) **Cardinal numbers** *are symbols which are associated with sets such that equivalent sets get the same symbol. By $\overline{\overline{A}}$ we denote the cardinal number associated with A.*

   i. *If there is an injection $f : A \to B$, then we write $\overline{\overline{A}} \le \overline{\overline{B}}$. By $\overline{\overline{A}} \ge \overline{\overline{B}}$, we mean that $\overline{\overline{B}} \le \overline{\overline{A}}$.*

   ii. *If there is a bijection $f : A \to B$, then we write $\overline{\overline{A}} = \overline{\overline{B}}$.*

   iii. *We write $\overline{\overline{\{1,2,\ldots,n\}}}$ as n and $\overline{\overline{\emptyset}}$ as 0. Thus, for a finite set A, we have $\overline{\overline{A}} = |A|$.*

   iv. *We use $\aleph_0$ to denote $\overline{\overline{\mathbb{N}}}$. If $x = \overline{\overline{A}}$ is a cardinal number by 2^x we mean $\overline{\overline{\mathcal{P}(A)}}$.*

   (b) *Facts about cardinal numbers:*

   i. *If x, y, z are cardinal numbers such that $x \le y$ and $y \le z$, then $x \le z$. In other words it says, if there is a one-one map from A to B and a one-one map from B to C, then there is a one-one map from A to C.*

   ii. *Let x be any cardinal number. Then $x \lneq 2^x$. This is Cantor's lemma.*

   iii. *The cardinal numbers we know till now are $0, 1, 2, 3, \ldots, \aleph_0 = \overline{\overline{\mathbb{N}}}, 2^{\aleph_0} = \overline{\overline{\mathbb{R}}}, 2^{2^{\aleph_0}}, \ldots$.*

   iv. *The cardinal numbers $\aleph_0 = \overline{\overline{\mathbb{N}}}, 2^{\aleph_0} = \overline{\overline{\mathbb{R}}}, 2^{2^{\aleph_0}}, \ldots$ are called the* **infinite cardinal numbers**.

   v. *The 'generalized continuum hypothesis' says that there is no cardinal number between an infinite cardinal number x and 2^x.*

9. *Let A be the set of all infinite sequences formed using $0, 1$ and B be the set of all infinite sequences formed using $0, 1, 2$. Which one has larger cardinality and why?*

10. *Write $\mathbb{R}$ as a union of pairwise disjoint sets of size 5.*

11. *Let S be a countable set of points on the unit circle in $\mathbb{R}^2$. Consider the line segments L_s with one end at the origin and the other end at a point $s \in S$. Fix these lines. We are allowed to rotate the circle anticlockwise (the lines do not move). Let T be another countable set of points on the unit circle. Can we rotate the circle by an angle θ so that no line L_s touches any of the points of T?*

12. *A complex number is* **algebraic** *if it is a root of a polynomial equation with integer coefficients. All other numbers are* **transcendental**. *Show that the set of algebraic numbers is countable.*

13. *Give a bijection from $\mathbb{R}$ to $\mathbb{R} \setminus \mathbb{Q}$.*

2.4 Integers and Modular Arithmetic

In this section, we study some properties of integers. We start with the 'division algorithm'.

Lemma 2.4.1. [Division algorithm] *Let a and b be two integers with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$, where $0 \le r < b$. The integer q is called the* **quotient** *and r, the* **remainder**.

Proof. Existence: Take $S = \{a + bx \mid x \in \mathbb{Z}\} \cap \mathbb{N}_0$. Then $a + |a|b \in S$. Hence, S is a nonempty subset of $\mathbb{N}_0$. Therefore, by Well-Ordering Principle, S contains its minimum, say s_0. So, $s_0 = a + bx_0$, for some $x_0 \in \mathbb{Z}$. Notice that $s_0 \geq 0$. We claim that $s_0 < b$.

If $s_0 \geq b$ then $s_0 - b \geq 0$ and hence $s_0 - b = a + b(x_0 - 1) \in S$, a contradiction to s_0 being the minimum element of S. Put $q = -x_0$ and $r = s_0$. Thus, we have obtained q and r such that $a = qb+r$ with $0 \leq r < b$.

Uniqueness: Assume that there exist integers q_1, q_2, r_1 and r_2 satisfying $a = q_1b + r_1$, $0 \leq r_1 < b$, $a = q_2b + r_2$, and $0 \leq r_2 < b$. Without loss of generality, we assume $r_1 \leq r_2$. Then, $0 \leq r_2 - r_1 < b$. Notice that $r_2 - r_1 = (q_1 - q_2)b$. So, $0 \leq (q_1 - q_2)b < b$. But the only integer multiple of b which lies in $[0, b)$ is 0. Hence, $q_1 - q_2 = 0$. Thus, $r_1 = r_2$ as well. This completes the proof. ■

Definition 2.4.2. [**Divisibility**]

1. [**Divisor**] Let $a, b \in \mathbb{Z}$ with $b \neq 0$. If $a = bc$, for some $c \in \mathbb{Z}$ then b is said to **divide** (be a **divisor** of) a and is denoted $b \mid a$.

   Discussion: If a is a nonzero integer then the set of positive divisors of a is always nonempty (as $1 \mid a$) and finite (as a positive divisor of a is less than or equal to $|a|$).

2. [**Greatest common divisor/Highest common factor**] Let a and b be two nonzero integers. Then the set S of their common positive divisors is nonempty and finite. Thus, S contains its greatest element. This element is called the **greatest common divisor** of a and b and is denoted $\gcd(a, b)$. In some books, the gcd is also called the **highest common factor**.

3. [**Relatively prime/Co-prime integers**] An integer a is said to be **relatively prime** to an integer b if $\gcd(a, b) = 1$. Or, two integers a and b are said to be **co-prime** if $\gcd(a, b) = 1$.

The next remark follows directly from the definition and the division algorithm.

Remark 2.4.3. *Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $d = \gcd(a, b)$. Then, for any positive common divisor c of a and b, one has $c \mid d$.*

The next result is often stated as 'the $\gcd(a, b)$ is a linear combination of a and b'.

Theorem 2.4.4. [**Bézout's identity**] *Let a and b be two nonzero integers. Then, there exist integers x_0, y_0 such that $d = ax_0 + by_0$, where $d = \gcd(a, b)$.*

Proof. Consider the set $S = \{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Then, either $a \in S$ or $-a \in S$. Thus, S is a nonempty subset of $\mathbb{N}$. Hence, by Well-ordering principle, S contains its least element, say d. As $d \in S$, we have $d = ax_0 + by_0$, for some $x_0, y_0 \in \mathbb{Z}$. We claim that $d = \gcd(a, b)$.

Note that d is positive. Let c be any positive common divisor of a and b. Then $c \mid ax_0 + by_0 = d$ as $x_0, y_0 \in \mathbb{Z}$. We now show that $d \mid a$ and $d \mid b$.

By division algorithm, there exist integers q and r such that $a = dq + r$, with $0 \leq r < d$. Thus, we need to show that $r = 0$.

On the contrary, assume that $r > 0$. Then

$$r = a - dq = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) \in \{ax + by \mid x, y \in \mathbb{Z}\}.$$

Hence, r is a positive integer in S which is strictly less than d. This contradicts the fact that d is the least element of S. Thus, $r = 0$ and hence $d|a$. Similarly, $d|b$. ■

The division algorithm gives us an idea to algorithmically compute the greatest common divisor of two integers, commonly known as the Euclid's algorithm.

Discussion 2.4.5. 1. Let $a, b \in \mathbb{Z} \setminus \{0\}$. By division algorithm, $a = |b|q + r$, for some integers $q, r \in \mathbb{Z}$ with $0 \le r < |b|$. Then,

$$\gcd(a, b) = \gcd(a, |b|) = \gcd(|b|, r).$$

To show the second equality, note that $r = a - |b|q$ and hence $\gcd(a, |b|) \mid r$. Thus, $\gcd(a, |b|) \mid \gcd(|b|, r)$. Similarly, $\gcd(|b|, r) \mid \gcd(a, |b|)$ as $a = |b|q + r$.

2. We can now apply the above idea repeatedly to find the greatest common divisor of two given nonzero integers. This is called the **Euclid's algorithm**. For example, to find $\gcd(155, -275)$, we proceed as follows

$$\begin{array}{rll} -275 = (-2) \cdot 155 + 35 & \qquad & (\text{so, } \gcd(-275, 155) = \gcd(155, 35)) \\ 155 = 4 \cdot 35 + 15 & & (\text{so, } \gcd(155, 35) = \gcd(35, 15)) \\ 35 = 2 \cdot 15 + 5 & & (\text{so, } \gcd(35, 15) = \gcd(15, 5)) \\ 15 = 3 \cdot 5 & & (\text{so, } \gcd(15, 5) = 5). \end{array}$$

To write $5 = \gcd(155, -275)$ in the form $155x_0 + (-275)y_0$, notice that

$$5 = 35 - 2\cdot 15 = 35 - 2(155 - 4\cdot 35) = 9\cdot 35 - 2\cdot 155 = 9(-275 + 2\cdot 155) - 2\cdot 155 = 9\cdot(-275) + 16\cdot 155.$$

Also, note that $275 = 5 \cdot 55$ and $155 = 5 \cdot 31$ and thus, $5 = (9 + 31x) \cdot (-275) + (16 + 55x) \cdot 155$, for all $x \in \mathbb{Z}$. Therefore, we see that there are infinite number of choices for the pair $(x, y) \in \mathbb{Z}^2$, for which $d = ax + by$.

3. [**Euclid's algorithm**] In general, given two nonzero integers a and b, the algorithm proceeds as follows:

$$\begin{array}{rcll} a & = & bq_0 + r_0 \text{ with } 0 \le r_0 < b, & \qquad b = r_0 q_1 + r_1 \text{ with } 0 \le r_1 < r_0, \\ r_0 & = & r_1 q_2 + r_2 \text{ with } 0 \le r_2 < r_1, & \qquad r_1 = r_2 q_3 + r_3 \text{ with } 0 \le r_3 < r_2, \\ \vdots & = & \vdots & \\ r_{\ell-1} & = & r_\ell q_{\ell+1} + r_{\ell+1} \text{ with } 0 \le r_{\ell+1} < r_\ell, & \qquad r_\ell = r_{\ell+1} q_{\ell+2}. \end{array}$$

The process will take at most $b - 1$ steps as $0 \le r_0 < b$. Also, note that $\gcd(a, b) = r_{\ell+1}$ and $r_{\ell+1}$ can be recursively obtained, using backtracking. That is,

$$r_{\ell+1} = r_{\ell-1} - r_\ell q_{\ell+1} = r_{\ell-1} - q_{\ell+1}\left(r_{\ell-2} - r_{\ell-1}q_\ell\right) = r_{\ell-1}\left(1 + q_{\ell+1}q_\ell\right) - q_{\ell+1}r_{\ell-2} = \cdots.$$

EXERCISE **2.4.6.** *1. Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = d$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

2. Prove that the system $15x + 12y = b$ has a solution for $x, y \in \mathbb{Z}$ if and only if 3 divides b.

3. [**Linear Diophantine Equation**] *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$. Then the linear system $ax + by = c$, in the unknowns $x, y \in \mathbb{Z}$ has a solution if and only if $\gcd(a, b)$ divides c. Furthermore, determine all pairs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $ax + by$ is indeed c.*

4. Prove that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, for any three nonzero integers a, b and c.

5. Euclid's algorithm can sometimes be applied to check whether two numbers which are functions of an unknown integer n, are relatively prime or not? For example, we can use the algorithm to prove that $\gcd(2n + 3, 5n + 7) = 1$ for every $n \in \mathbb{Z}$.

6. **[Informative]** *Suppose a milkman has only 3 cans of sizes $7, 9$ and 16 liters. What is the minimum number of operations required to deliver 1 liter of milk to a customer? Explain.*

To proceed further, we need the following definitions.

Definition 2.4.7. [Prime/Composite numbers]

1. **[Unity]** The positive integer 1 is called the **unity** (or the **unit** element) of $\mathbb{Z}$.

2. **[Prime]** A positive integer p is said to be a **prime**, if p has exactly two positive divisors, namely, 1 and p.

3. **[Composite]** A positive integer r is called **composite** if $r \neq 1$ and is not a prime.

We are now ready to prove an important result that helps us in proving the fundamental theorem of arithmetic.

Lemma 2.4.8. [Euclid's lemma] *Let p be a prime and let $a, b \in \mathbb{Z}$. If $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, we are done. So, assume that $p \nmid a$. As p is a prime, $\gcd(p, a) = 1$. Thus, we can find integers x, y such that $1 = ax + py$. As $p \mid ab$, we have

$$p \mid abx + pby = b(ax + py) = b \cdot 1 = b.$$

Thus, if $p|ab$ then either $p|a$ or $p|b$. ■

One also has the following result.

Corollary 2.4.9. *Let n be an integer such that $n \mid ab$ and $\gcd(n, a) = 1$. Then $n \mid b$.*

Proof. As $\gcd(n, a) = 1$, there exists $x_0, y_0 \in \mathbb{Z}$ such that $nx_0 + ay_0 = 1$. Hence, $b = aby_0 + nbx_0$. As n divides ab, n divides $aby_0 + n(bx_0) = b$. Thus, the required result follows. ■

Now, we are ready to prove the fundamental theorem of arithmetic that states that 'every positive integer greater than 1 is either a prime or is a product of primes. This product is unique, except for the order in which the prime factors appear'.

Theorem 2.4.10. [Fundamental theorem of arithmetic] *Let $n \in \mathbb{N}$ with $n \geq 2$. Then there exist prime numbers $p_1 > p_2 > \cdots > p_k$ and positive integers $s_1, s_2, \ldots, s_k$ such that $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, for some $k \geq 1$. Moreover, if n also equals $q_1^{t_1} q_2^{t_2} \cdots q_\ell^{t_\ell}$, for distinct primes $q_1 > q_2 > \cdots > q_\ell$ and positive integers $t_1, t_2, \ldots, t_\ell$ then $k = \ell$ and for each i, $1 \leq i \leq k$, $p_i = q_i$ and $s_i = t_i$.*

Proof. We prove the result using the strong form of the principle of mathematical induction. The result is clearly true for $n = 2$. So, let the result be true for all $m, 2 \leq m \leq n - 1$. If n is a prime, then we have nothing to prove. Else, n has a prime divisor p. Then apply induction on $\frac{n}{p}$ to get the required result. ■

Theorem 2.4.11. [Euclid: Infinitude of primes] *The number of primes is infinite.*

Proof. On the contrary assume that the number of primes is finite, say $p_1 = 2, p_2 = 3, \ldots, p_k$. Now, consider the positive integer $N = p_1 p_2 \cdots p_k + 1$. Then, we see that none of the primes $p_1, p_2, \ldots, p_k$ divides N which contradicts Theorem 2.4.10. Thus, the result follows. ■

Proposition 2.4.12. **[Primality testing]** *Let $n \in \mathbb{N}$ with $n \geq 2$. Suppose that for any prime $p \leq \sqrt{n}$, p does not divide n then, n is prime.*

Proof. Suppose $n = xy$, for $2 \leq x, y < n$. Then, either $x \leq \sqrt{n}$ or $y \leq \sqrt{n}$. Without loss of generality, assume $x \leq \sqrt{n}$. If x is a prime, we are done. Else, take a prime divisor of x to get a contradiction. ∎

Exercise **2.4.13.** **[Informative]** *Prove that there are infinitely many primes of the form $4n - 1$.*

Definition 2.4.14. **[Least common multiple]** Let $a, b \in \mathbb{Z}$. Then the **least common multiple** of a and b, denoted $\mathsf{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

Theorem 2.4.15. *Let $a, b \in \mathbb{N}$. Then, $\gcd(a, b) \cdot \mathsf{lcm}(a, b) = ab$. Thus, $\mathsf{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.*

Proof. Let $d = \gcd(a, b)$. Then $d = as + bt$, for some $s, t \in \mathbb{Z}$, $a = a_1 d$, $b = b_2 d$, for some $a_1, b_1 \in \mathbb{N}$. We need to show that $\mathsf{lcm}(a, b) = a_1 b_1 d = ab_1 = a_1 b$, which is clearly a multiple of both a and b. Let $c \in \mathbb{N}$ be any common multiple of a and b. To show, $a_1 b_1 d$ divides c. Note that

$$\frac{c}{a_1 b_1 d} = \frac{cd}{(a_1 d) \cdot (b_1 d)} = \frac{c(as + bt)}{ab} = \frac{c}{b} s + \frac{c}{a} t \in \mathbb{Z}$$

as $\frac{c}{a}, \frac{c}{b} \in \mathbb{Z}$ and $s, t \in \mathbb{Z}$. Thus, $a_1 b_1 d = \mathsf{lcm}(a, b)$ divides c and hence $\mathsf{lcm}(a, b)$ is indeed the smallest. Thus, the required result follows. ∎

Definition 2.4.16. **[Modular Arithmetic]** Fix a positive integer n. Then, 'an integer a is said to be **congruent** to an integer b modulo n', denoted $a \equiv b \pmod{n}$, if n divides $a - b$.

Example 2.4.17.

1. It can be easily verified that any two even (odd) integers are equivalent modulo 2 as $2 \mid 2(l - m) = 2l - 2m$ ($2 \mid 2(l - m) = ((2l + 1) - (2m + 1))$).
2. The numbers ± 10 and 22 are equivalent modulo 4 as $4 \mid 12 = 22 - 10$ and $4 \mid 32 = 22 - (-10)$.
3. Let n be a fixed positive integer and let $S = \{0, 1, 2, \ldots, n - 1\}$.
    - (a) Then, by division algorithm, for any $a \in \mathbb{Z}$ there exists a unique $b \in S$ such that $a \equiv b \pmod{n}$. The number b is called the **residue** of a modulo n.
    - (b) Thus, the set of integers, $\mathbb{Z} = \bigcup\limits_{a=0}^{n-1} \{a + kn : k \in \mathbb{Z}\}$, *i.e.*, every integer is congruent to an element of S. The set S is taken as the **standard representative** for the set of residue classes modulo n.

Theorem 2.4.18. *Let n be a positive integer. Then, the following results hold.*

1. *Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, for some $a, b, c \in \mathbb{Z}$. Then, $a \equiv c \pmod{n}$.*
2. *Let $a \equiv b \pmod{n}$, for some $a, b \in \mathbb{Z}$. Then, $a \pm c \equiv b \pm c \pmod{n}$ and $ac \equiv bc \pmod{n}$, for all $c \in \mathbb{Z}$.*
3. *Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, for some $a, b, c, d \in \mathbb{Z}$. Then, $a \pm c \equiv b \pm d \pmod{n}$ and $ac \equiv bd \pmod{n}$. In particular, $a^m \equiv b^m \pmod{n}$, for all $m \in \mathbb{N}$.*
4. *Let $ac \equiv bc \pmod{n}$, for some non-zero $a, b, c \in \mathbb{Z}$. Then, $a \equiv b \pmod{n}$, whenever $\gcd(c, n) = 1$. In general, $a \equiv b \pmod{\frac{n}{\gcd(c, n)}}$.*

Proof. We will only prove two parts. The readers should supply the proof of other parts.

Part 3: Note that $ac - bd \equiv ac - bc + bc - bd \equiv c(a-b) + b(c-d)$. Thus, $n \mid ac - bd$, whenever $n \mid a - b$ and $n \mid c - d$.

In particular, taking $c = a$ and $d = b$ and repeatedly applying the above result, one has $a^m \equiv b^m \pmod{n}$, for all $m \in \mathbb{N}$.

Part 4: Let $\gcd(c, n) = d$. Then, there exist non-zero $c_1, n_1 \in \mathbb{Z}$ and $c = c_1 d, n = n_1 d$. Thus, $n \mid ac - bc$ means that $n_1 d \mid c_1 d(a - b)$. This, in turn implies that $n_1 \mid c_1(a - b)$. Hence, by Corollary 2.4.9, we get $\dfrac{n}{\gcd(c,n)} = n_1 \mid a - b$. ■

Before coming to the next result, we look at the following examples.

Example 2.4.19. 1. Note that $3 \cdot 9 + 13 \cdot (-2) \equiv 1 \pmod{13}$. So, the system $9x \equiv 4 \pmod{13}$ has the solution

$$x \equiv x \cdot 1 \equiv x \cdot (3 \cdot 9 + 13 \cdot (-2)) \equiv 3 \cdot 9x \equiv 3 \cdot 4 \equiv 12 \pmod{13}.$$

2. Verify that $9 \cdot (-5) + 23 \cdot (2) = 1$. Hence, the system $9x \equiv 1 \pmod{23}$ has the solution

$$x \equiv x \cdot 1 \equiv x\,(9 \cdot (-5) + 23 \cdot (2)) \equiv (-5) \cdot (9x) \equiv -5 \equiv 18 \pmod{23}.$$

3. The system $3x \equiv 15 \pmod{30}$ has solutions $x = 5, 15, 25$, whereas the system $7x = 15$ has only the solution $x = 15$. Also, verify that the system $3x \equiv 5 \pmod{30}$ has no solution.

Theorem 2.4.20. **[Linear Congruence]** *Let n be a positive integer and let a and b be non-zero integers. Then, the system $ax \equiv b \pmod{n}$ has at least one solution if and only if $\gcd(a, n) \mid b$. Moreover, if $d = \gcd(a, n)$ then $ax \equiv b \pmod{n}$ has exactly d solutions in $\{0, 1, 2, \ldots, n-1\}$.*

Proof. Let x_0 be a solution of $ax \equiv b \pmod{n}$. Then, by definition, $ax_0 - b = nq$, for some $q \in \mathbb{Z}$. Thus, $b = ax_0 - nq$. But, $\gcd(a, n) \mid a, n$ and hence $\gcd(a, n) \mid ax_0 - nq = b$.

Suppose $d = \gcd(a, n) \mid b$. Then, $b = b_1 d$, for some $b_1 \in \mathbb{Z}$. Also, by Euclidean algorithm, there exists $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + ny_0 = d$. Hence,

$$a(x_0 b_1) \equiv b_1(ax_0) \equiv b_1(ax_0 + ny_0) \equiv b_1 d \equiv b \pmod{n}.$$

This completes the proof of the first part.

To proceed further, assume that x_1, x_2 are two solutions. Then, $ax_1 \equiv ax_2 \pmod{n}$ and hence, by Theorem 2.4.18.4, $x_1 \equiv x_2 \pmod{\frac{n}{d}}$. Thus, we can find $x_2 \in \{0, 1, \ldots, \frac{n}{d}\}$ such that $x = x_2 + k\frac{n}{d}$ is a solution of $ax \equiv b \pmod{n}$, for $0 \le k \le d - 1$. Verify that these x's are distinct and lie between 0 and $n - 1$. Hence, the required result follows. ■

Exercise **2.4.21.** *1. Prove Theorem 2.4.18.*

2. *Determine the solutions of the system* $3x \equiv 5 \pmod{65}$.

3. *Determine the solutions of the system* $5x \equiv 95 \pmod{100}$.

4. *Prove that the system* $3x \equiv 4 \pmod{28}$ *is equivalent to the system* $x \equiv 20 \pmod{28}$.

5. *Prove that the pair of systems* $3x \equiv 4 \pmod{28}$ *and* $4x \equiv 2 \pmod{27}$ *is equivalent to the pair* $x \equiv 20 \pmod{28}$ *and* $x \equiv 14 \pmod{27}$. *Hence, prove that the above system is equivalent to solving either* $20 + 28k \equiv 14 \pmod{27}$ *or* $14 + 27k \equiv 20 \pmod{28}$ *for the unknown quantity* k. *Thus, verify that* $k = 21$ *is the solution for the first case and* $k = 22$ *for the other. Hence* $x = 20 + 28 \cdot 21 = 608 = 14 + 22 \cdot 27$ *is a solution of the above pair.*

6. *Let p be a prime. Then, prove that* $p \mid \binom{p}{k} = \dfrac{p!}{k!(p-k)!}$*, for* $1 \leq k \leq p-1$.

7. **[Informative]** *Let p be a prime. Then, the set*

   (a) $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ *has the following properties:*

   i. *for every* $a, b \in \mathbb{Z}_p$, $a + b \pmod{p} \in \mathbb{Z}_p$.

   ii. *for every* $a, b \in \mathbb{Z}_p$, $a + b = b + a \pmod{p}$.

   iii. *for every* $a, b, c \in \mathbb{Z}_p$, $a + (b + c) \equiv (a + b) + c \pmod{p}$.

   iv. *for every* $a \in \mathbb{Z}_p$, $a + 0 \equiv a \pmod{p}$.

   v. *for every* $a \in \mathbb{Z}_p$, $a + (p - a) \equiv 0 \pmod{p}$.

   (b) $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ *has the following properties:*

   i. *for every* $a, b \in \mathbb{Z}_p$, $a \cdot b \pmod{p} \in \mathbb{Z}_p^*$.

   ii. *for every* $a, b \in \mathbb{Z}_p^*$, $a \cdot b = b \cdot a \pmod{p}$.

   iii. *for every* $a, b, c \in \mathbb{Z}_p^*$, $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{p}$.

   iv. *for every* $a \in \mathbb{Z}_p^*$, $a \cdot 1 \equiv a \pmod{p}$.

   v. *for every* $a \in \mathbb{Z}_p^*$, $a \cdot b \equiv 1 \pmod{p}$. *To see this, note that* $\gcd(a, p) = 1$. *Hence, by Euclid's algorithm, there exists* $x, y \in \mathbb{Z}$ *such that* $ax + py = 1$. *Define* $b \equiv x \pmod{p}$. *Then,*

   $$a \cdot b \equiv a \cdot x \equiv a \cdot x + p \cdot y \equiv 1 \pmod{p}.$$

   In algebra, any set, say $\mathbb{F}$, in which 'addition' and 'multiplication' can be defined in such a way that the above properties are satisfied then $\mathbb{F}$ is called a **field**. *So,* $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ *is an example of a field. In general, the well known examples of fields are:*

   i. $\mathbb{Q}$, *the set of rational numbers.*

   ii. $\mathbb{R}$, *the set of real numbers.*

   iii. $\mathbb{C}$, *the set of complex numbers.*

   (c) *From now on let p be an odd prime.*

   i. *Then, the equation* $x^2 \equiv 1 \pmod{p}$. *Since, p is a prime, the only solutions in* $\mathbb{Z}_p$ *are* $x = 1, p-1$.

   ii. *Then, for* $a \in \{2, 3, \ldots, p-2\}$, *the number* $b \in \mathbb{Z}_p^*$ *that satisfies* $a \cdot b \equiv 1 \pmod{p}$ *also satisfies* $b \in \{2, 3, \ldots, p-2\}$ *and* $b \neq a$.

   iii. *Thus, for* $1 \leq i \leq \frac{p-1}{2}$, *we have pairs* $\{a_i, b_i\}$ *that are pairwise disjoint and satisfy* $a_i \cdot b_i \equiv 1 \pmod{p}$. *Moreover,* $\bigcup\limits_{i=1}^{\frac{p-1}{2}} \{a_i, b_i\} = \{2, 3, \ldots, p-2\}$.

   iv. *Hence,* $2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}$.

   v. *We thus have the following famous theorem called the* **Wilson's Theorem***: Let p be a prime. Then* $(p-1)! \equiv -1 \pmod{p}$. *Proof. Note that from the previous step, we have*

   $$(p-1)! \equiv 1 \cdot (p-1) \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv -1 \cdot 1 \equiv -1 \pmod{p}.$$

   ■

   vi. *(Primality Testing) Let n be a positive integer. Then,* $(n-1)! \equiv -1 \pmod{n}$ *if and only if n is a prime.*

Theorem 2.4.22. **[Chinese remainder theorem]** *Fix a positive integer m and let* $n_1, n_, \ldots, n_m$ *be pairwise co-prime positive integers. Then, the linear system*

$$\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
&\vdots \\
x &\equiv a_m \pmod{n_m}
\end{aligned}$$

has a unique solution modulo $M = n_1 n_2 \cdots n_m$.

Proof. For $1 \leq k \leq m$, define $M_k = \dfrac{M}{n_k}$. Then, $\gcd(M_k, n_k) = 1$ and hence there exist integers x_k, y_k such that $M_k x_k + n_k y_k = 1$ for $1 \leq k \leq m$. Then

$$M_k x_k \equiv 1 \pmod{n_k} \text{ and } M_k x_k \equiv 0 \pmod{n_\ell} \text{ for } \ell \neq k.$$

Define $x_0 = \sum\limits_{k=1}^{m} M_k x_k a_k$. Then, it can be easily verified that x_0 satisfies the required congruence relations. ∎

Example 2.4.23. Let us come back to Exercise 2.4.21.5. In this case, $M = 28 \cdot 27 = 756, M_1 = 27$ and $M_2 = 28$. Therefore, $x_1 = -1$ and $x_2 = 1$. Thus,

$$x_0 = 27 \cdot -1 \cdot 20 + 28 \cdot 1 \cdot 14 \equiv -540 + 392 \equiv -148 \equiv 608 \pmod{756}.$$

EXERCISE **2.4.24.**

1. *Find the smallest positive integer which when divided by* 4 *leaves a remained* 1 *and when divided by* 9 *leaves a remainder* 2.
2. *Find the smallest positive integer which when divided by* 8 *leaves a remained* 4 *and when divided by* 15 *leaves a remainder* 10.
3. *Does there exist a positive integer* n *such that*

$$n \equiv 4 \pmod{14}, \quad n \equiv 6 \pmod{18}?$$

Give reasons for your answer. What if we replace 6 *or* 4 *with an odd number?*

4. **[Informative]** *Let* n *be a positive integer. Then, the set*

(a) $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ *has the following properties:*

i. *for every* $a, b \in \mathbb{Z}_n$, $a + b \pmod{n} \in \mathbb{Z}_n$.
ii. *for every* $a, b \in \mathbb{Z}_n$, $a + b = b + a \pmod{n}$.
iii. *for every* $a, b, c \in \mathbb{Z}_n$, $a + (b + c) \equiv (a + b) + c \pmod{n}$.
iv. *for every* $a \in \mathbb{Z}_n$, $a + 0 \equiv a \pmod{n}$.
v. *for every* $a \in \mathbb{Z}_n$, $a + (p - a) \equiv 0 \pmod{n}$.
vi. *for every* $a, b \in \mathbb{Z}_n$, $a \cdot b \pmod{n} \in \mathbb{Z}_n$.
vii. *for every* $a, b \in \mathbb{Z}_n$, $a \cdot b = b \cdot a \pmod{n}$.
viii. *for every* $a, b, c \in \mathbb{Z}_n$, $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{n}$.
ix. *for every* $a \in \mathbb{Z}_n$, $a \cdot 1 \equiv a \pmod{n}$.

In algebra, any set, say $\mathcal{R}$, *in which 'addition' and 'multiplication' can be defined in such a way that the above properties are satisfied then* $\mathcal{R}$ *is called a* **commutative ring with unity**. *So,* $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ *is an example of a commutative ring with unity. In general, the well known examples of commutative ring with unity are:*

i. $\mathbb{Z}$, *the set of integers.*
ii. $\mathbb{Q}$, *the set of rational numbers.*
iii. $\mathbb{R}$, *the set of real numbers.*
iv. $\mathbb{C}$, *the set of complex numbers.*

(b) *Now, let* m *and* n *be two co-prime positive integers. Then, by the above, the sets* $\mathbb{Z}_m, \mathbb{Z}_n$, *and* $\mathbb{Z}_{mn}$ *are commutative rings with unity. In the following, we show that there is a one-to-one correspondence (ring isomorphism) between* $\mathbb{Z}_m \times \mathbb{Z}_n$ *and* $\mathbb{Z}_{mn}$. *To do so, define*

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \text{ by } f(x) = (x \pmod{m}, \ x \pmod{n}) \text{ for all } x \in \mathbb{Z}_{mn}.$$

Then, defining 'addition' and 'multiplication' in $\mathbb{Z}_m \times \mathbb{Z}_n$ *component-wise and using Theorem 2.4.18, we have the following:*

i. $f(x+y) = f(x) + f(y)$, *for all* $x, y \in \mathbb{Z}_{mn}$.

ii. $f(x \cdot y) = f(x) \cdot f(y)$, *for all* $x, y \in \mathbb{Z}_{mn}$.

iii. *for every* $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, *by CRT, there exists a unique* $x \in \mathbb{Z}_{mn}$ *such that*

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}.$$

iv. *also,* $\mid \mathbb{Z}_m \times \mathbb{Z}_n \mid = \mid \mathbb{Z}_{mn} \mid = mn$..

Hence, we have obtained the required one-one correspondence, commonly known as the ring isomorphism. That is, the two rings $\mathbb{Z}_m \times \mathbb{Z}_n$ *and* $\mathbb{Z}_{mn}$ *are isomorphic.*

2.5 Construction of Integers and Rationals*

This section contains two subsections. In the first subsection, we construct integers from natural numbers and prove a few properties, such as addition, multiplication and subtraction. The second subsection generalizes the ideas in the first subsection to construct rationals and then study a few properties of rationals.

2.5.1 Construction of Integers

To start with let $X = \mathbb{N} \times \mathbb{N}$. We define a relation '$\sim$' on X by

$$(a, b) \sim (c, d) \text{ if } a + d = b + c \text{ for all } a, b, c, d \in \mathbb{N}.$$

Then, verify that $\sim$ is indeed an equivalence relation on X. Let $\mathbb{Z}$ denote the collection of all equivalence classes under this relation. So, if $[\mathbf{x}], [\mathbf{y}] \in \mathbb{Z}$ then $[\mathbf{x}]$ is an equivalence class containing $\mathbf{x} = (x_1, x_2)$, for some $x_1, x_2 \in \mathbb{N}$ and $[\mathbf{y}]$ is an equivalence class containing $\mathbf{y} = (y_1, y_2)$, for some $y_1, y_2 \in \mathbb{N}$. Now, using the successor function S defined in Axiom **P2**, observe that $\mathbb{Z}$ consists of all equivalence classes of the form

1. $[(1, 1)] = \{(n, n) : \text{ for all } n \in \mathbb{N}\}$,
2. for a fixed element $m \in \mathbb{N}$, $[(1, S(m))] = \{(n, m + n) : \text{ for all } n \in \mathbb{N}\}$, and
3. for a fixed element $m \in \mathbb{N}$, $[(S(m), 1)] = \{(m + n, n) : \text{ for all } n \in \mathbb{N}\}$.

Definition 2.5.1. **[Addition in $\mathbb{Z}$]** Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Z}$, for some $x_1, x_2, y_1, y_2 \in \mathbb{N}$. Then, one defines **addition** in $\mathbb{Z}$, denoted by $\oplus$, as

$$[\mathbf{x}] \oplus [\mathbf{y}] = (x_1, x_2) \oplus (y_1, y_2) = [(x_1 + y_1, x_2 + y_2)]. \tag{2.3}$$

Note that basically we have defined a map $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ which takes two non-empty sets, say $[(x_1, x_2)]$ and $[(y_1, y_2)]$ and gives a set $[(x_1 + y_1, x_2 + y_2)]$"namely the addition of the two" as the image. Thus, we need to verify that the addition of two different representatives of the domain, give rise to the same set on the range. This process of defining a map using representatives and then verifying that the image is independent of the representatives chosen is characterized by saying that "the map is well-defined". So, let us now prove that $\oplus$ is well-defined.

Lemma 2.5.2. *The map* $\oplus$ *defined in Equation (2.3) is well-defined.*

Proof. Let $[(u_1, u_2)] = [(v_1, v_2)]$ and $[(x_1, x_2)] = [(y_1, y_2)]$ be two equivalence classes in $\mathbb{Z}$. Then, by definition

$$[(u_1, u_2)] \oplus [(x_1, x_2)] = [(u_1 + x_1, u_2 + x_2)] \text{ and } [(v_1, v_2)] \oplus [(y_1, y_2)] = [(v_1 + y_1, v_2 + y_2)].$$

For well-definedness, we need to show that $[(u_1+x_1, u_2+x_2)] = [(v_1+y_1, v_2+y_2)]$. Or equivalently, we need to show that $u_1+x_1+v_2+y_2 = u_2+x_2+v_1+y_1$.

But, the equality of the equivalence classes $[(u_1,u_2)] = [(v_1,v_2)]$ and $[(x_1,x_2)] = [(y_1,y_2)]$ implies

$$u_1+v_2 = u_2+v_1 \text{ and } x_1+y_2 = x_2+y_1.$$

Thus, adding the two and using the commutativity of addition in $\mathbb{N}$, we get $u_1+x_1+v_2+y_2 = u_2+x_2+v_1+y_1$. Thus, the required result follows. ∎

In this particular case, one can also check the following statements to verify the well-definedness of $\oplus$, *i.e.*, one needs to show that for all $\ell, m, n, r \in \mathbb{N}$ the following statements hold.

1. $[(1,1)] \oplus [(n,n)] = [(m,m)] + [(n,n)]$.
2. $[(1,S(m))] \oplus [(1,S(\ell))] = [(r,m+r)] \oplus [(n,\ell+n)]$.
3. $[(S(m),1)] \oplus [(S(\ell),1)] = [(m+r,r)] \oplus [(\ell+n,n)]$.
4. $[(1,1)] \oplus [(1,S(m))] = [(n,n)] \oplus [(r,m+r)] = [(1,1)] \oplus [(r,m+r)] = [(r,r)] \oplus [(1,S(m))]$.
5. $[(1,1)] \oplus [(S(m),1)] = [(n,n)] \oplus [(m+r,m)] = [(1,1)] \oplus [(m+r,m)] = [(r,r)] \oplus [(S(m),1)]?$.
6. $[(1,S(m))] \oplus [(S(\ell),1)] = [(r,m+r)] \oplus [(\ell+n,n)]$ and so on.

We give the argument for the fourth statement. The readers are supposed to provide arguments for other statements.

1. $[(1,1)] \oplus [(1,S(m))] = [(2,S(m)+1)] = [(n+r,m+n+r)]$ as using commutativity and associativity of addition of natural numbers, one has
$$2+m+n+r = m+2+n+r = (m+1)+1+n+r = S(m)+1+n+r.$$
Hence, $[(1,1)] \oplus [(1,S(m))] = [(n+r,m+n+r)] = [(n,n)] \oplus [(r,m+r)]$.
2. $[(1,1)] \oplus [(r,m+r)] = [(r+1,m+r+1)] = [(r+1,r+S(m))] = [(r,r)] \oplus [(1,S(m))]$.

On similar lines, we now define multiplication among elements of $\mathbb{Z}$.

Definition 2.5.3. [Multiplication of Integers] Let $[\mathbf{x}] = [(x_1,x_2)], [\mathbf{y}] = [(y_1,y_2)] \in \mathbb{Z}$, for some $x_1,x_2,y_1,y_2 \in \mathbb{N}$. Then, one defines **multiplication** in $\mathbb{Z}$, denoted by $\odot$, as

$$[\mathbf{x}] \odot [\mathbf{y}] = [(x_1,x_2)] \odot [(y_1,y_2)] = [(x_1y_1+x_2y_2, x_1y_2+x_2y_1)]. \tag{2.4}$$

Since we are talking about multiplication between two sets using their representatives, we need to verify that the multiplication is indeed well-defined. So, the readers are required to prove "well-definedness" of multiplication. The readers can now prove all the properties of addition and multiplication in $\mathbb{Z}$ by using the corresponding properties of natural numbers.

EXERCISE **2.5.4.** *Let* $[\mathbf{x}], [\mathbf{y}], [\mathbf{z}] \in \mathbb{Z}$ *and let us denote* $[\mathbf{0}] = [(1,1)]$. *Then, prove that*

1. **[Associativity of addition]** $([\mathbf{x}]+[\mathbf{y}])+[\mathbf{z}] = [\mathbf{x}]+([\mathbf{y}]+[\mathbf{z}])$.
2. **[Commutativity of addition]** $[\mathbf{x}]+[\mathbf{y}] = [\mathbf{y}]+[\mathbf{x}]$.
3. **[Existence of the zero element]** $[\mathbf{x}]+[\mathbf{0}] = [\mathbf{x}]$.
4. **[Cancellation property holds]** *If* $[\mathbf{x}]+[\mathbf{y}] = [\mathbf{x}]+[\mathbf{z}]$ *then* $[\mathbf{y}] = [\mathbf{z}]$. *This implies that the zero element is unique.*
5. **[Existence of additive inverse]** *for every* $[\mathbf{x}] = [(x_1,x_2)]$, *the equivalence class* $[(x_2,x_1)]$, *denoted by* $-[\mathbf{x}]$, *satisfies* $[\mathbf{x}] \oplus (-[\mathbf{x}]) = [\mathbf{0}]$. *Now, use the cancellation property in* $\mathbb{Z}$ *to show that the additive inverse is unique.*

6. **[Distributive laws]** $([\mathbf{x}] + [\mathbf{y}]) \odot [\mathbf{z}] = [\mathbf{x}] \odot [\mathbf{z}] \oplus [\mathbf{y}] \odot [\mathbf{z}]$.
7. **[Associativity of multiplication]** $([\mathbf{x}] \odot [\mathbf{y}]) \odot [\mathbf{z}] = [\mathbf{x}] \odot ([\mathbf{y}] \odot [\mathbf{z}])$.
8. **[Commutativity of multiplication]** $[\mathbf{x}] \odot [\mathbf{y}] = [\mathbf{y}] \odot [\mathbf{x}]$.
9. **[Existence of the identity element]** $[\mathbf{x}] \odot [\mathbf{1}] = [\mathbf{x}]$, *where* $[\mathbf{1}] = [(S(1), 1)]$.
10. **[Cancellation property holds]** *If* $[\mathbf{x}] \odot [\mathbf{y}] = [\mathbf{x}] \odot [\mathbf{z}]$ *with* $[\mathbf{x}] \neq [\mathbf{0}]$ *then* $[\mathbf{y}] = [\mathbf{z}]$. *This implies that the identity element is unique.*
11. $[\mathbf{x}] \odot [\mathbf{0}] = [\mathbf{0}]$.

As a last property, we show that a copy of $\mathbb{N}$ naturally seats inside $\mathbb{Z}$.

Lemma 2.5.5. *Consider the map $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(n) = [(S(n), 1)]$, for all $n \in \mathbb{N}$. Then, for all $a, b \in \mathbb{N}$*

1. *f is one-one,*
2. *$f(a + b) = f(a) \oplus f(b)$, and*
3. *$f(a \cdot b) = f(a) \odot f(b)$.*

Proof. **Part** 1.**:** Suppose $f(a) = f(b)$ for some $a, b \in \mathbb{N}$. Then, by definition, $[(S(a), 1)] = [(S(b), 1)]$, or equivalently, $S(a) + 1 = S(b) + 1$. Now, use cancellation in $\mathbb{N}$ to get $S(a) = S(b)$. Thus, $a = b$ as S is an injective map.

Part 2.**:** By definition, $f(a + b) = [(S(a + b), 1)]$ and

$$\begin{aligned} f(a) \oplus f(b) &= [(S(a), 1)] \oplus [(S(b), 1)] = [(S(a) + S(b), 1 + 1)] = [(S(a) + b + 1, 1 + 1)] \\ &= [(S(a + b) + 1, 1 + 1)] = [(S(a + b), 1)] = f(a + b). \end{aligned}$$

Part 3.**:** By definition, $f(a \cdot b) = [(S(a \cdot b), 1)]$ and

$$\begin{aligned} f(a) \odot f(b) &= [(S(a), 1)] \odot [(S(b), 1)] = [(S(a) \cdot S(b) + 1 \cdot 1, S(a) \cdot 1 + 1 \cdot S(b))] \\ &= [(S(a) \cdot S(b) + 1, S(a) + S(b))] = [(S(a \cdot b), 1)] = f(a \odot b) \end{aligned}$$

as $S(a) \cdot S(b) + 1 + 1 = S(a) \cdot b + S(a) \cdot 1 + 1 + 1 = a \cdot b + 1 \cdot b + S(a) + 1 + 1 = S(a \cdot b) + S(b) + S(a)$. ■

Thus, we have indeed shown that $\mathbb{N}$ is seating inside $\mathbb{Z}$ as $f(\mathbb{N})$ and the addition and multiplication operations are satisfied by f (the map f commutes with the addition operation and the multiplication operation). So, from now on, the symbols $+$ and $\cdot$ will be used for addition and multiplication in integers. Further, as $n \in \mathbb{N}$ is identified with $f(n) = [(S(n), 1)]$, we would like to associate the symbol '$-$' as $n = S(n) - 1$ and $-n = 1 - S(n)$. We proceed to do this in the next few paragraphs.

Definition 2.5.6. [Order in $\mathbb{Z}$] Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Z}$, for some $x_1, x_2, y_1, y_2 \in \mathbb{N}$. Then, the **order** in $\mathbb{Z}$ is defined by saying that $[\mathbf{x}] < [\mathbf{y}]$ if $x_1 + y_2 < y_1 + x_2$. Further, $[\mathbf{x}] \leq [\mathbf{y}]$ if either $[\mathbf{x}] = [\mathbf{y}]$ or $[\mathbf{x}] < [\mathbf{y}]$.

We again need to check for well-definedness. So, let $[(u_1, u_2)] = [(v_1, v_2)]$ and $[(x_1, x_2)] = [(y_1, y_2)]$ be two equivalence classes in $\mathbb{Z}$ with $[(u_1, u_2)] < [(x_1, x_2)]$. We need to show that $[(v_1, v_2)] < [y_1, y_2)]$. Or equivalently, $v_1 + y_2 < y_1 + v_2$ whenever $u_1 + v_2 = v_1 + u_2, x_1 + y_2 = y_1 + x_2$ and $u_1 + x_2 < x_1 + u_2$. Thus,

$$\begin{aligned} v_1 + y_2 + x_1 + u_2 &= v_1 + u_2 + x_1 + y_2 = u_1 + v_2 + y_1 + x_2 = y_1 + v_2 + u_1 + x_2 \\ &< y_1 + v_2 + x_1 + u_2. \end{aligned}$$

Hence, by the order property in $\mathbb{N}$ (see Exercise 2.1.10), $v_1 + y_2 < y_1 + v_2$. Thus, the above definition is well-defined. At this stage, one would like to verify that the function f defined in Lemma 2.5.5 preserves the order as well.

Lemma 2.5.7. *Consider the map $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(n) = [(S(n), 1)]$, for all $n \in \mathbb{N}$. Then, for all $a, b \in \mathbb{N}$, $a < b$ if and only if $f(a) < f(b)$.*

Proof. Using Exercise 2.1.10 $a < b$ if and only if $a + 1 + 1 < b + 1 + 1$, or equivalently, $a < b$ if and only if $S(a) + 1 < S(b) + 1$. Thus, $a < b$ if and only if $f(a) = [(S(a), 1)] < [(S(b), 1)] = f(b)$. ■

Definition 2.5.8. [Positive elements in $\mathbb{Z}$] Let $[\mathbf{x}] = [(x_1, x_2)] \in \mathbb{Z}$. Then, $[\mathbf{x}]$ is said to be **positive** if $[\mathbf{0}] < [\mathbf{x}]$ and is said to be **non-negative** if $[\mathbf{0}] \leq [\mathbf{x}]$. In general, we write $[\mathbf{x}] > [\mathbf{0}]$ to mean $[\mathbf{x}]$ is positive and $[\mathbf{x}] \geq [\mathbf{0}]$ for $[\mathbf{x}]$ being non-negative.

Lemma 2.5.9. *Let $[\mathbf{x}] = [(x_1, x_2)] \in \mathbb{Z}$. Then, $[\mathbf{x}] > [\mathbf{0}]$ if and only if $x_1 > x_2$.*

Proof. By definition, $[(x_1, x_2)] > [\mathbf{0}] = [(1, 1)]$ if and only if $x_1 + 1 > x_2 + 1$. Or equivalently, using Exercise 2.1.10, one obtains $[(x_1, x_2)] > [(1, 1)]$ if and only if $x_1 > x_2$. ■

EXERCISE **2.5.10.** 1. *Prove the following results for any $[\mathbf{x}] \in \mathbb{Z}$.*
   (a) $[\mathbf{x}] > 0$ if and only if $[\mathbf{x}] = [(S(n), 1)] = f(n)$, for some $n \in \mathbb{N}$.
   (b) $[\mathbf{x}] > 0$ if and only if $-[\mathbf{x}] < 0$.

2. *$[\mathbf{y}] > [\mathbf{z}]$, for some $[\mathbf{y}], [\mathbf{z}] \in \mathbb{Z}$ if and only if $[\mathbf{y}] + [\mathbf{x}] > [\mathbf{z}] + [\mathbf{x}]$.*
3. *If $[\mathbf{y}] > [\mathbf{z}]$, for some $[\mathbf{y}], [\mathbf{z}] \in \mathbb{Z}$ then $[\mathbf{y}] \cdot [\mathbf{x}] > [\mathbf{z}] \cdot [\mathbf{x}]$, whenever $[\mathbf{x}] > 0$.*

Thus, $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ and hence from now on, in place of using equivalence class to represent the elements of $\mathbb{Z}$, we will just use natural numbers, their negatives and the zero element to represent $\mathbb{Z}$, the set of integers. Thus, whenever we define functions or operations on $\mathbb{Z}$ then we don't have to worry about well-definedness. Let us now discuss the "absolute value function", namely the modulus function.

Definition 2.5.11. A function $g : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is called as **absolute/modulus** function if

1. $g(n) = n$ if $n \geq 0$,
2. $g(n) = -n$, if $n < 0$.

This function is denoted by $|\cdot|$. Thus, $|m| = m$, if $m \geq 0$ and $-m$, if $m < 0$. Further, by Exercise 2.5.10.1, observe that $|m| \geq 0$ for all $m \in \mathbb{Z}$.

For a better understanding of this function, we prove the following two results.

Lemma 2.5.12. *For any $x \in \mathbb{Z}$, $-|x| \leq x \leq |x|$. Further, if $x \geq 0$ and $-x \leq y \leq x$ for some $y \in \mathbb{Z}$ then $|y| \leq x$.*

Proof. Let $x \geq 0$. Then, by definition $|x| = x$ and hence $x \leq |x|$. As $|x| = x$, the other inequality $-|x| \leq x$ reduces to $-x \leq x$. Or equivalently, we need to show that $0 = x + (-x) \leq x + x = 2x$, which is indeed true. If $x < 0$ then we see that $|x| > 0 > x$ and hence $x \leq |x|$. Note that the condition $-|x| \leq x$ is equivalent to the condition $|x| + x \geq 0$ (use Exercise 2.5.10.2) which is indeed true as by definition $x + |x| = x + (-x) = 0$.

For the second part, we again consider two cases, namely, $y \geq 0$ and $y < 0$. If $y \geq 0$ then $|y| = y$ and hence the condition $y \leq x$ implies $|y| \leq x$. In case $y < 0$ implies $|y| = -y$. Further, using Exercise 2.5.10.2, the condition $-x \leq y$ is equivalent to the condition $0 \leq y + x$ which in turn is equivalent to $-y \leq x$. Hence $|y| = -y \leq x$. Thus, the required result follows. ■

As a direct application of Lemma 2.5.12, one obtains the triangle inequality.

Lemma 2.5.13. [Triangle inequality in $\mathbb{Z}$] *Let $x, y \in \mathbb{Z}$. Then $|x+y| \le |x| + |y|$.*

Proof. Using Lemma 2.5.12, one has $-|x| \le x \le |x|$ and $-|y| \le y \le |y|$. Hence,

$$-|x| + (-|y|) \le x + y \le |x| + |y|.$$

Now, use the associativity and commutativity of addition to get

$$0 = -|x| + (-|y|) + |x| + |y| = -(|x| + |y|) + (|x| + |y|)$$

and hence the uniqueness of the additive inverse implies $-|x| + (-|y|) = -(|x| + |y|)$. Thus, the required result follows from the second part of Lemma 2.5.12. ∎

This finishes most of the results on the basic operations related with integers.

2.5.2 Construction of Rational Numbers

In this subsection, we will describe the construction of rational numbers and prove a few properties, such as addition, multiplication, subtraction and division by non-zero element.

So, let us start with denoting $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ and defining an equivalence relation on $X = \mathbb{Z} \times \mathbb{Z}^*$ and then doing everything afresh as was done for the set of integers. Define a relation '$\sim$' on X by

$$(a, b) \sim (c, d) \text{ if } a \cdot d = b \cdot c \text{ for all } a, c \in \mathbb{Z}, b, d \in \mathbb{Z}^*.$$

Then, verify that $\sim$ is indeed an equivalence relation on X. Let $\mathbb{Q}$ denote the collection of all equivalence classes under this relation. This set is called the "set of rational numbers". In this set, we define addition and multiplication, using the addition and multiplication in $\mathbb{Z}$, as follows:

1. **[Addition in $\mathbb{Q}$]** Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$. Then, one defines **addition** in $\mathbb{Q}$, denoted by $\oplus$, as

$$[\mathbf{x}] \oplus [\mathbf{y}] = (x_1, x_2) \oplus (y_1, y_2) = [(x_1 \cdot y_2 + x_2 \cdot y_1, x_2 \cdot y_2)].$$

2. **[Multiplication in $\mathbb{Q}$]** Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$. Then, one defines **multiplication** in $\mathbb{Q}$, denoted by $\odot$, as

$$[\mathbf{x}] \odot [\mathbf{y}] = (x_1, x_2) \odot (y_1, y_2) = [(x_1 \cdot y_1, x_2 \cdot y_2)].$$

The readers are advised to verify the well-definedness of the above operations in $\mathbb{Q}$. Further, if we define the map $f : \mathbb{Z} \to \mathbb{Q}$ by $f(a) = [(a, 1)]$ then it can be easily verified that the map f is one-one and it preserves addition and multiplication. Thus, $\mathbb{Z}$ is seating inside $\mathbb{Q}$ as $f(\mathbb{Z})$. So, again one replaces the symbols '$\oplus$' and '$\odot$' by '+' and '$\cdot$'. Sometimes, even '$\cdot$' is not used for multiplication. We also note that the element $0 \in \mathbb{Z}$ corresponds to $[(0, 1)] = [(0, x)]$, for all $x \in \mathbb{Z}^*$. Hence, an element $[(x_1, x_2)] \in \mathbb{Q}$ with $[(x_1, x_2)] \ne 0$ implies that $x_1 \ne 0$. Thus, verify that for each $[(x_1, x_2)] \in \mathbb{Q}$ with $x_1 \ne 0$, the element $[(x_2, x_1)] \in \mathbb{Q}$ satisfies $[(x_1, x_2)] \cdot [(x_2, x_1)] = 1$. As the next operation, one defines division in $\mathbb{Q}$ as follows.

Definition 2.5.14. [Division in $\mathbb{Q}$] Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$ with $y_1 \ne 0$. Then, one defines **division** in $\mathbb{Q}$, denoted by $/$, as

$$[\mathbf{x}]/[\mathbf{y}] = [(x_1, x_2)]/[(y_1, y_2)] = [(x_1 y_2, x_2 y_1)].$$

Note that $x_2 y_1 \in \mathbb{Z}^*$ as $x_2, y_1 \ne 0$.

The readers are advised to verify the well-definedness of division defined above. Before proceeding further with other important properties of rational numbers, the readers should verify all the properties related with addition, subtract, multiplication and division by a non-zero element. The next result, even though it doesn't seem important, helps us to define order in rational numbers.

Lemma 2.5.15. **[Representation of an element of $\mathbb{Q}$]** *Let* $[\mathbf{x}] \in \mathbb{Q}$. *Then* $[\mathbf{x}] = [(y_1, y_2)]$, *for some* $y_1, y_2 \in \mathbb{Z}$ *such that* $y_2 > 0$.

Proof. Let $[\mathbf{x}] = [(x_1, x_2)]$, for some $x_1, x_2 \in \mathbb{Z}$. If $x_2 > 0$, we are done. Else, using Exercise 2.5.10.1, we know that $-x_2 > 0$. Then, by the definition of equivalence class $[\mathbf{x}] = [(x_1, x_2)] = [(-x_1, -x_2)]$. Hence, the required result follows. ■

So, now we proceed with the definition of order in $\mathbb{Q}$.

Definition 2.5.16. **[Order in $\mathbb{Q}$]** Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$, for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ with $x_2, y_2 > 0$. Then the **order** in $\mathbb{Q}$ is defined by $[\mathbf{x}] > [\mathbf{y}]$ if $x_1 y_2 > x_2 y_1$.

We again need to verify the well-definedness of order in $\mathbb{Q}$. Also, as before, $[\mathbf{x}] \geq [\mathbf{y}]$ means either $[\mathbf{x}] = [\mathbf{y}]$ or $[\mathbf{x}] > [\mathbf{y}]$. As a final result of this section, we prove the following result.

Lemma 2.5.17. **[Existence of rational between two rational]** *Let* $[\mathbf{x}], [\mathbf{y}] \in \mathbb{Q}$ *with* $[\mathbf{x}] < [\mathbf{y}]$. *Then, there exists a rational number* $[\mathbf{z}]$ *such that* $[\mathbf{x}] < [\mathbf{z}] < [\mathbf{y}]$.

Proof. Let $[\mathbf{x}] = [(x_1, x_2)]$ and $[\mathbf{y}] = [(y_1, y_2)]$, for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ with $x_2, y_2 > 0$. Since $[\mathbf{x}] < [\mathbf{y}]$, $x_1 y_2 < x_2 y_1$, one has $2x_1 y_2 < x_1 y_2 + x_2 y_1 < 2x_2 y_1$. Further, $2x_2 y_2 > 0$ and hence let us take $[\mathbf{z}] = [(x_1 y_2 + x_2 y_1, 2x_2 y_2)]$. Then, it can be easily verified that $[\mathbf{x}] < [\mathbf{z}] < [\mathbf{y}]$ as $x_2, y_2 \in \mathbb{Z}$ and the cancellation property with respect to multiplication holds in $\mathbb{Z}$. ■

Chapter 3

Partial Orders, Lattices and Boolean Algebra

3.1 Partial Orders

Let X be a non-empty set and let f be a relation on X. Then, recall from Definition 1.2.32 that f is **anti-symmetric** if $(x, y) \in f$ and $x \neq y$ implies $(y, x) \notin f$. That is, both (x, y) and (y, x) cannot be in f, whenever x and y are distinct.

Definition 3.1.1. [**Partial order**] Let X be a non-empty set. A relation f on X is called a **partial order** if f is reflexive, transitive and anti-symmetric. Further, two elements, namely $a, b \in X$, are said to be **comparable** if either $(a, b) \in f$ or $(b, a) \in f$.

Example 3.1.2.

1. Let $X = \{1, 2, 3, 4, 5\}$.
    (a) The identity relation **Id** is reflexive, transitive and anti-symmetric. So, it is a partial order. But, none of the elements of X are comparable.
    (b) The relation $\mathbf{Id} \cup \{(1, 2)\}$ is also a partial order. Here 1 and 2 are comparable.
    (c) The relation $\mathbf{Id} \cup \{(1, 2), (2, 1)\}$ is reflexive, transitive. But it is not anti-symmetric, as $(1, 2)$ and $(2, 1)$ are both in the given relation.
    (d) The relation $\mathbf{Id} \cup \{(1, 2), (3, 4)\}$ is also a partial order. Here, $1, 2$ are comparable and $3, 4$ are comparable.
2. Let $X = \mathbb{N}$. Then $f = \{(a, b) : a \text{ divides } b\}$ is a partial order.
3. Let X be a nonempty collection of sets. Then $f = \{(A, B) \mid A, B \in X, A \subseteq B\}$ is a partial order on X.
4. On $\mathbb{R}$ the set $f = \{(a, b) : a - b \leq 0\}$ is a partial order. It is called the **usual partial order** on $\mathbb{R}$. List 5 elements of f. Usual partial order on a subset of $\mathbb{R}$ is defined similarly.

EXERCISE **3.1.3.** *Give a partial order on* $\{1, 2, 3, 4, 5\}$ *with the*

1. *maximum number of elements in it.*
2. *minimum number of elements in it.*

Definition 3.1.4. Let X be a non-empty set.

1. [**Partially ordered set (poset)**] The tuple (X, f) is called a **partially ordered set** (in short, **poset**) if f is a partial order on X. It is common to use $\leq$ instead of f. We say $x \leq y$ to mean that $(x, y) \in f$ or x and y are related or x and y are comparable. We say $x < y$ to mean that $x \leq y$ and $x \neq y$.

2. **[Linear/Total/Complete order]** A partial order f on X is called a **linear/complete/total order** if either $(x, y) \in f$ or $(y, x) \in f$, for each pair $x, y \in X$, *i.e.*, each pair of elements of X are comparable.

3. **[Linearly ordered set]** The poset (X, f) is said to be a **linearly ordered set** if f is a linear order on X. You may imagine the elements of a linearly ordered set as points on a line.

4. **[Chain and its height]** A linearly ordered subset of a poset is called a **chain**. The maximum size of a chain is called the **height** of a poset.

5. **[Anti-chain and its width]** Let (X, f) be a poset and $A \subseteq X$. Suppose that no two elements in A are comparable. Then A is called an **anti-chain**. The maximum size of an anti-chain is called the **width** of the poset.

6. **[Strictly ordered set]** Then (X, f) be a (**strictly**) ordered set if f is anti-symmetric and transitive.

Example 3.1.5. 1. The poset in Example 3.1.2.1a has height 1 (resp. chain is $\{1\}$) and width 5 (respectively, anti-chain is $\{1, 2, 3, 4, 5\}$).

2. The poset in Example 3.1.2.1b has height 2 (resp. chain is $\{1, 2\}$) and width 4 (resp. anti-chain is $\{2, 3, 4, 5\}$ or $\{1, 3, 4, 5\}$).

3. The poset in Example 3.1.2.1d has height 2 (resp. chain is $\{1, 2\}$ or $\{3, 4\}$) and width 3 (resp. anti-chain is $\{1, 3, 5\}$). Find other anti-chains?

4. The set $\mathbb{N}$ with the usual order is a linearly ordered set.

5. If (X, f) is a nonempty linearly ordered set, then the height of X is $\overline{\overline{X}}$ and the width of X is 1.

6. The set $\mathbb{N}$ with $a \leq b$ if a divides b, is not linearly ordered. However, the set $\{1, 2, 4, 8, 16\}$ is a chain. This is just a completely ordered subset of the poset. There are larger chains, for example, $\{2^k \mid k = 0, 1, 2, \ldots\}$. It has height $\overline{\overline{N}}$ and width $\overline{\overline{N}}$.

7. The poset $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \subseteq)$ is not linearly ordered. However, $\{\emptyset, \{1, 2\}, \{1, 2, 3, 4, 5\}\}$ is a chain in it. So, is $\{\emptyset, \{2\}, \{2, 3\}, \{2, 3, 4\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$. Its height is 6. What is its width?

Definition 3.1.6. [Lexicographic/Dictionary ordering] Let $(\Sigma, \leq)$ be a nonempty finite linearly ordered set (like the English alphabets with $a \leq b \leq c \leq \cdots \leq z$) and Σ^* be the collection of all words formed using the elements of Σ. For $a \equiv a_1 a_2 \cdots a_n$, $b \equiv b_1 b_2 \cdots b_m \in \Sigma^*$, for some $m, n \in \mathbb{N}$, define $a \leq b$ if

(a) $a_1 < b_1$ or

(b) $a_i = b_i$ for $i = 1, \ldots, k$ for some $k < \min\{m, n\}$ and $a_{k+1} < b_{k+1}$ or

(c) $a_i = b_i$ for $i = 1, \ldots, n = \min\{m, n\}$.

Then $(\Sigma^*, \leq)$ is a linearly ordered set. This ordering is called the **lexicographic** or **dictionary** ordering. Sometimes Σ is called the 'alphabet set' and Σ^* is called the 'dictionary'.

EXERCISE **3.1.7.** *Let D_1 be the dictionary of words made from a, b, c and D_2 be the dictionary of words made from a, b, d. Are these two sets equivalent?*

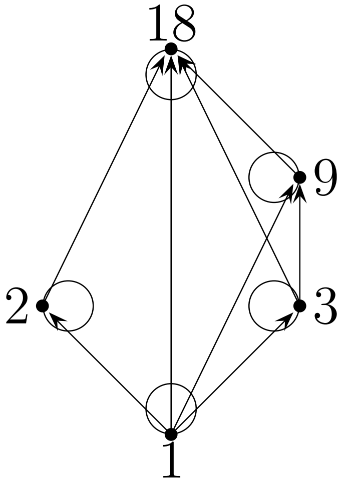
Discussion 3.1.8. [Directed graph representation of a finite poset] Often we represent a nonempty finite poset $(X, \leq)$ by a picture. The process is described below.

(a) Put a dot/node for each element of X and label it.

(b) If $a \leq b$, then join the dot/node for a and the dot/node for b by an arrow (a directed line).

(c) Put a loop at the dot/node of a, for each $a \in X$.

1. A directed graph representation of $A = \{1, 2, 3, 9, 18\}$ with the 'divides' relation ($a \leq b$ if $a \mid b$) is given below.

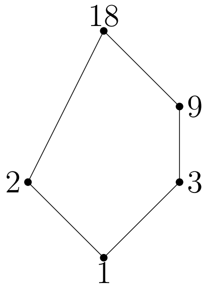


Definition 3.1.9. [**Hasse diagram**] The **Hasse diagram** of a nonempty finite poset $(X, \leq)$ is a picture drawn in the following way.

1. Each element of X is represented by a point and is labeled with the element.
2. If $a \leq b$ then the point representing a must appear at a lower height than the point representing b and further the two points are joined by a line.
3. If $a \leq b$ and $b \leq c$ then the line between a and c is removed.

Later, we shall show that for every nonempty finite poset $(X, \leq)$, a Hasse diagram can be drawn.

Example 3.1.10. Hasse diagram for $A = \{1, 2, 3, 9, 18\}$ with the relation as 'division'.



EXERCISE **3.1.11.** *Draw the Hasse diagram for* $\{1, 2, 3\} \times \{1, 2, 3, 4\}$ *under lexicographic order.*

Proposition 3.1.12. *Let $\mathcal{F}$ be a nonempty family of single valued relations such that either $f \subseteq g$ or $g \subseteq f$, that is, $\mathcal{F}$ is linearly ordered. Let $h = \bigcup\limits_{f \in \mathcal{F}} f$. Then the following are true.*

1. *h is single valued.*
2. $\mathsf{dom}(h) = \bigcup\limits_{f \in \mathcal{F}} \mathsf{dom}(f)$.
3. $\mathsf{rng}(h) = \bigcup\limits_{f \in \mathcal{F}} \mathsf{rng}(f)$.
4. *If every element of $\mathcal{F}$ is one-one (from its domain to its range) then h is also one-one.*

Proof. We shall only prove the first two items.

1. Let $x \in \mathsf{dom}(h)$ and $(x, y), (x, z) \in h$. Then there are $f, g \in \mathcal{F}$, such that $(x, y) \in f$ and $(x, z) \in g$. As $\mathcal{F}$ is a chain, either $f \subseteq g$ or $g \subseteq f$, say $f \subseteq g$. Then, g is not single valued, a contradiction.

2. Note that $x \in \mathsf{dom}(h)$ means $(x, y) \in h$ for some y. This means $(x, y) \in f$ for some f. That is, $x \in \mathsf{dom}(f)$, for a function f. This means $x \in \underset{f \in \mathcal{F}}{\cup} \mathsf{dom}(f)$. ■

Definition 3.1.13. 1. [**Bounds**] Let (X, f) be a poset and $A \subseteq X$. We say $x \in X$ is an **upper bound** of A if for each $z \in A, (z, x) \in f$. In words, it means 'each element of A is $\leq x$'. The term **lower bound** is defined analogously.

2. [**Maximal**] An element $x \in A$ is **maximal** element in A, if 'whenever there exists a $z \in A$ with $(x, z) \in f$ then $x = z$. In other words, it means 'no element in A is strictly larger than x'. The term **minimal** is defined analogously.

3. [**Maximum**] An element $x \in A$ is called the **maximum** of A, if x is an upper bound of A. In other words, it means 'an upper bound of A which is contained in A'. Such an element, when it exists, is unique. The term **minimum** is defined analogously.

4. [**Least upper bound**] An element $x \in X$ is called the **least upper bound (lub)** of A if x is an upper bound of A and for each upper bound y of A, we have $(x, y) \in f$. In other words 'x is the minimum/least of the set of all upper bounds of A. The term **greatest lower bound (glb)** is defined analogously.

Example 3.1.14. Consider the two posets described by the following picture.

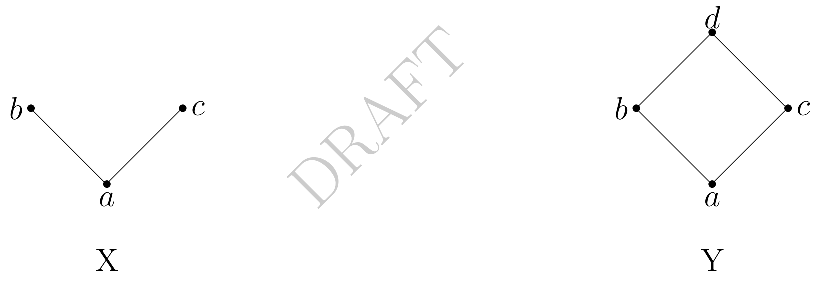


Figure 3.1: Posets X and Y

1. Consider the poset $X = \{a, b, c\}$ in Figure 3.1. If $A = X$ then

   (a) the maximal elements of A are b and c,

   (b) the only minimal element of A is a,

   (c) a is the lower bound of A in X,

   (d) A has no upper bound in X,

   (e) A has no maximum element,

   (f) a is the minimum element of A,

   (g) no element of X is the lub of A and

   (h) a is the glb of A in X.

2. Consider the posets in Figure 3.1. Then, the following table illustrates different definitions. Note that $X = \{a, b, c\}$ and $Y = \{a, b, c, d\}$.

	$A=\{b,c\} \subseteq X$	$A=\{a,c\} \subseteq X$	$A=\{b,c\} \subseteq Y$
Maximal element(s) of A	b, c	c	b, c
Minimal element(s) of A	b, c	a	b, c
Lower bound(s) of A in X/Y	a	a	a
Upper bound(s) of A in X/Y	doesn't exist	c	d
Maximum element of A	doesn't exist	c	doesn't exist
Minimum element of A	doesn't exist	a	doesn't exist
lub of A in X/Y	doesn't exist	c	d
glb of A in X/Y	a	a	a

Exercise **3.1.15.** *Determine the maximal elements, minimal elements, lower bounds, upper bounds, maximum, minimum, lub and glb of A in the following posets (X, f).*

1. *Take $X = \mathbb{Z}$ with usual order and $A = \mathbb{Z}$.*

2. *Take $X = \mathbb{N}$, $f = \{(i, i) \, : \, i \in \mathbb{N}\}$ and $A = \{4, 5, 6, 7\}$.*

Discussion 3.1.16. [**Bounds of empty set**] Let (X, f) be a nonempty poset. Then each $x \in X$ is an upper bound for $\emptyset$ as well as a lower bound for $\emptyset$. So, an lub for $\emptyset$ may or may not exist. For example, if $X = \{1, 2, 3\}$ and f is the usual order, then $\mathsf{lub}\,\emptyset = 1$. Whereas, if $X = \mathbb{Z}$ and f is the usual order, then an lub for $\emptyset$ does not exist. Similar statements hold for glb.

Definition 3.1.17. [**Well order**] A linear order f on X is said to be a **well order** if each nonempty subset A of X has a minimal element (in A). We call (X, f) a well ordered set to mean that f is a well order on X. Note that 'a minimal element', if it exists, is 'a minimum' in this case.

Example 3.1.18.

1. The set $\mathbb{Z}$ with usual ordering is not well ordered, as $\{-1, -2, \dots, \}$ is a nonempty subset with no minimal element.

2. The ordering $0 \leq 1 \leq -1 \leq 2 \leq -2 \leq 3 \leq -3 \leq \cdots$ describes a well order on $\mathbb{Z}$.

3. The set $\mathbb{N}$ with the usual ordering is well ordered.

4. The set $\mathbb{R}$ with the usual ordering is not well ordered as the set $(0, 1)$ doesn't have its minimal element in $(0, 1)$.

Exercise **3.1.19.** *Consider the dictionary order on $\mathbb{N}^2$. Show that this is a well order.*

Definition 3.1.20. [**Initial segment**] Let $(W, \leq)$ be well ordered and $a \in W$. The **initial segment of** a is defined as $I(a) := \{x \mid x \in W, x < a\}$.

Example 3.1.21. Take $\mathbb{N}$ with the usual order. Then $I(5) = \{1, 2, 3, 4\}$ and $I(1) = \emptyset$.

Theorem 3.1.22. [**Principle of transfinite induction**] *Let $(W, \leq)$ be a nonempty well ordered set. Let $A \subseteq W$ which satisfies 'whenever $I(w) \subseteq A$ then $w \in A$'. Then $A = W$.*

Proof. If $A \neq W$, then $A^c \neq \emptyset$. As W is well ordered, let s be the minimal element of A^c. So, any element $x < s$ is in A. That is, $I(s) \subseteq A$. By the hypothesis $s \in A$, a contradiction. ∎

Fact 3.1.23. The principle of transfinite induction is the principle of mathematical induction when $W = \mathbb{N}$.

Proof. To see this, let $p(n)$ be a statement which needs to be proved by mathematical induction. Put $A = \{n \in \mathbb{N} \mid p(n) \text{ is true}\}$. Assume that we have been able to show that '$I(n) \subseteq A \Rightarrow n \in A$'. It means, we have shown that $1 \in A$, as $\emptyset = I(1) \subseteq A$. Also we have shown that for $n \geq 2$, if $\{p(1), \ldots, p(n-1)\}$ are true then $p(n)$ is true as well, as $I(n) = \{1, 2, \ldots, n-1\}$. ■

Definition 3.1.24. **[Product of sets]** Recall that the product $A_1 \times A_2 = \{(x_1, x_2) \mid x_i \in A_i\}$ may be written as

$$\big\{\big(f(1), f(2)\big) \big| f : \{1,2\} \to A_1 \cup A_2 \text{ is a function with } f(1) \in A_1, f(2) \in A_2\big\}.$$

Moreover, if A_1 and A_2 are finite sets then $|A_1 \times A_2| = |A_1| \cdot |A_2|$. In general, we define the **product** of the sets in $\{A_\alpha\}_{\alpha \in L}$, $L \neq \emptyset$, as

$$\prod_{\alpha \in L} A_\alpha = \big\{f \mid f : L \to \underset{\alpha \in L}{\cup} A_\alpha \text{ is a function with } f(\alpha) \in A_\alpha, \text{ for each } \alpha \in L\big\}.$$

Example 3.1.25.

1. Take $L = \mathbb{N}$ and $A_n = \{0, 1\}$. Then $\prod\limits_{\alpha \in L} A_\alpha$ is the class of functions $f : L \to \{0, 1\}$. That is, it is the class of all 0-1-sequences.
2. By definition, product of a class of sets among which one of them is $\emptyset$ is empty.

What about product of a class of sets in which no set is empty? Is it nonempty? This could not be proved using the standard set theory. In fact, it is now proved that this question cannot be answered using the standard set theory. So, a new axiom, called the **axiom of choice**, was introduced.

Axiom 3.1.26. **[Axiom of Choice]** *The product of a nonempty class of nonempty sets is nonempty.*

Proposition 3.1.27. **[Injection-Surjection]** *Let A and B be nonempty sets. Then, there is a surjection $g : A \to B$ if and only if there is an injection $f : B \to A$.*

Proof. Let $g : A \to B$ be onto. We shall find an injection from B to A. To start with, notice that for each $b \in B$, the set $g^{-1}(b) \neq \emptyset$. Then, by axiom of choice $\prod\limits_{b \in B} g^{-1}(b) \neq \emptyset$. Let $f \in \prod\limits_{b \in B} g^{-1}(b)$. Then, by Definition 3.1.24, $f : B \to A$ is a function. As g is a function, $g^{-1}(b)$'s are disjoint and hence f is one-one.

Conversely, let $f : B \to A$ be one-one. Fix an element $b \in B$. Define $g : A \to B$ as

$$g(x) = \begin{cases} f^{-1}(x), & \text{if } x \in f(B), \\ b, & \text{if } x \in A \setminus f(B). \end{cases}$$

Observe that g is onto. ■

Definition 3.1.28. **[Family of finite character]** A class F of sets is called a **family of finite character** if it satisfies: '$A \in F$ if and only if each finite subset of A is also in F'.

Example 3.1.29.

1. $\{\ \}$ is a family of finite character.
2. Power sets are families of finite character.
3. $\{\emptyset, \{1\}, \{2\}\}$ is a family of finite character.
4. If $A \cap B = \emptyset$, then $\mathcal{P}(A) \cup \mathcal{P}(B)$ is a family of finite character.
5. The set $\{\emptyset\} \cup \{\{a\} \mid a \neq 0, a \in \mathbb{R}\}$ is a family of finite character. This is the class of linearly independent sets in $\mathbb{R}$.

6. Let $\mathbb{V}$ be a non trivial vector space and F be the class of linearly independent subsets of $\mathbb{V}$. Then F is a family of finite character.

EXERCISE **3.1.30.** *1. Let* $L = A_1 = A_2 = A_3 = \{1, 2, 3\}$. *Is the set* $\prod\limits_{\alpha \in L} A_\alpha$ *equal to the class of functions* $f : \{1, 2, 3\} \to \{1, 2, 3\}$*? Give reasons for your answer.*

2. Give sets A_n*,* $n \in \mathbb{N}$ *such that* $\prod\limits_{n \in \mathbb{N}} A_n$ *has* 6 *elements. Give another.*[1]

Some equivalent axioms of axiom of choice

[**Axiom of choice**] Cartesian product of a nonempty collection of nonempty sets is nonempty.

[**Zorn's lemma**] A partially ordered set in which every chain has an upper bound, has a maximal element.

[**Zermelo's well ordering principle**] Every set can be well ordered.

[**Hausdorff's maximality principle**] Every nonempty partially ordered set contains a maximal chain.

[**Tukey's lemma**] Every nonempty family of finite character has a maximal element.

EXERCISE **3.1.31.** *1. Does there exist a poset with exactly* 5 *maximal chains of size (number of elements in it)* 2, 3, 4, 5, 6*, respectively and* 2 *maximal elements? If yes, draw the Hasse diagram. If no, argue it.*

2. Let (X, f) *be a nonempty poset and* $\emptyset \neq Y \subseteq X$*. Define* $f_Y = \{(a, b) \in f \mid a, b \in Y\}$*. Show that* f_Y *is a partial order on* Y*. This is the* **induced partial order** *on* Y*.*

3. Apply induction to show that a nonempty finite poset has a maximal element and a minimal element.

Discussion 3.1.32. [**Drawing the Hasse diagram of a finite poset** (X, f)] Let $x_1, \ldots, x_k$ be the minimal elements of X. Draw k points on the same horizontal line and label them $x_1, \ldots, x_k$. Now consider $Y = X \setminus \{x_1, \ldots, x_k\}$ and f_Y. By induction, the picture of (Y, f_Y) can be drawn. Put it above those k dots. Let $y_1, \ldots, y_m$ be the minimal elements of Y. Now, draw the lines (x_i, y_j) if $(x_i, y_j) \in f$. This is the Hasse diagram of (X, f).

Discussion 3.1.33. [**Existence of Hamel basis**] Let $\mathbb{V}$ be a vector space with at least two elements. Recall that the collection $\mathcal{F}$ of linearly independent subsets of $\mathbb{V}$ is a family of finite character. Recall that a basis or a **Hamel basis** is a maximal linearly independent subset of $\mathbb{V}$. As $\mathbb{V}$ has at least 2 elements, it has a nonzero element, say a. Then $\{a\} \in \mathcal{F}$. Hence, $\mathcal{F} \neq \emptyset$. Thus, by Tukey's lemma, the set $\mathcal{F}$ has a maximal element. This maximal set is the required basis. Hence, we have proved that *every vector space with at least* 2 *elements has a Hamel basis.*

EXERCISE **3.1.34.** *1. Let* $n \in \mathbb{N}$*. Define* $P_n = \{k \in \mathbb{N} \mid k \text{ divides } n\}$*. Define a relation* $\leq_n$ *on* P_n *as* $\leq_n = \{(a, b) \mid a \text{ divides } b\}$*. Show that* $(P_n, \leq_n)$ *is a poset, for each* $n \in \mathbb{N}$*. Give a necessary and sufficient condition on* n *so that* $(P_n, \leq_n)$ *is a completely ordered set.*

2. Take $X = \Big\{(1, 1), (1, 2), (1, 3), \ldots\Big\} \cup \Big\{(2, 1)(3, 1), (4, 1), \ldots\Big\}$*. The ordering defined is*

$$f = \underset{\substack{m, n \in \mathbb{N} \\ m \leq n}}{\cup} \Big\{((1, m), (1, n))\Big\} \bigcup \underset{\substack{m, n \in \mathbb{N} \\ m \leq n}}{\cup} \Big\{((m, 1), (n, 1))\Big\}.$$

Does X *have any maximal or minimal elements? Is* X *linearly ordered? Is it true that every nonempty set has a minimal element? Is it true that every nonempty set has a minimum? What type of nonempty sets always have a minimum?*

[1] When we ask for more than one example, we encourage the reader to get examples of different types, if possible.

3. *Prove or disprove:*

   (a) *There are at least* 5 *functions* $f : \mathbb{R} \to \mathbb{R}$ *which are partial orders.*

   (b) *Let* S *be the set of sequences* (x_n), *with* $x_n \in \{0, 1, \ldots, 9\}$, *for each* $n \in \mathbb{N}$, *such that ‘if* $x_k < x_{k+1}$, *then* $x_{k+1} = x_{k+2} = \cdots \}$*‘. Then* S *is countable.*

   (c) *Take* $\mathbb{N}$ *with usual order. Then the dictionary order on* $\mathbb{N}^2$ *is a well order.*

   (d) *Let* S *be the set of all non-increasing sequences made with natural numbers. Then* S *is countable.*

   (e) *Let* S *be the set of all non-decreasing sequences made with natural numbers. Then* S *is countable.*

   (f) *Take* $\mathbb{N}$ *with usual order and* $\mathbb{N}^2$ *with the dictionary order. Then any nonempty subset of* $\mathbb{N}^2$ *which is bounded above has a lub.*

   (g) *Every nonempty countable linearly ordered set is well ordered with respect to the same ordering.*

   (h) *Every nonempty countable chain which is bounded below, in a partially ordered set, is well ordered with respect to the same ordering.*

   (i) *The set* $\mathbb{Q}$ *can be well ordered.*

   (j) *For a fixed* $n \in \mathbb{N}$, *let* A_n *and* B_n *be non-empty sets and let* R_n *be a one-one relation from* A_n *to* B_n. *Then,* $\bigcap\limits_n R_n$ *is a one-one relation.*

   (k) *Let* S *be the set of words with length at most* 8 *using letters from* $\{3, A, a, b, C, c\}$. *We want to define a lexicographic order on* S *to make it a dictionary. There are more than* 500 *ways to do that.*

   (l) *An infinite poset in which each nonempty finite set has a minimum, must be linearly ordered.*

   (m) *A nonempty finite poset in which each nonempty finite set has a minimum, must be well ordered.*

   (n) *An infinite poset in which each nonempty finite set has a minimum, must be well ordered.*

4. *Let* $S = \{(x, y) : x^2 + y^2 = 1, x \geq 0\}$. *It is a relation from* $\mathbb{R}$ *to* $\mathbb{R}$. *Draw a picture of the inverse of this relation.*

5. *Construct the Hasse diagram for the* $\subseteq$ *relation on* $\mathcal{P}(\{a, b, c\})$.

6. *Draw the Hasse diagram for the partial order describing the ‘divides’ relations on the set* $\{2, 3, 4, 5, 6, 7, 8\}$.

7. *Draw the Hasse diagram of* $\{1, 2, 3, 6, 9, 18\}$ *with ‘divides’ relation.*

   (a) *What is its height? What is its width.*

   (b) *Let* $A = \{2, 3, 6\}$. *What are the maximal elements, minimal elements, maximum, minimum, lower bounds, upper bounds, glb and lub of* A.

EXERCISE **3.1.35.** *

1. *Show that the following three definitions are equivalent.*

   (a) *A set* X *is finite if either* $X = \emptyset$ *or* $\overline{\overline{X}} = \overline{\overline{\{1, 2, \ldots, n\}}}$, *for some* $n \in \mathbb{N}$.

   (b) **[Tarski]** *A set* X *is finite if and only if every nonempty family of subsets of* X *has a minimal element.*

   (c) **[Dedekind]** *A set is infinite if it is equivalent to a proper subset of itself. A set is finite if it is not infinite.*

2. *Let* (X, f) *be a nonempty poset. Show that there exists a linear order* g *on* X *such that* $f \subseteq g$.

3. *Let G be a non-Abelian group and H be an Abelian subgroup of G. Show that there is a maximal Abelian subgroup J of G such that $H \subseteq J$.*

4. *Let F be a family of finite character and B be a chain in F. Show that $\underset{A\in B}{\cup} A \in F$.*

5. *Let $A \neq \emptyset$ and $\mathbb{F}$ be a field. Let $\mathbb{F}^A := \{f \,:\, f$ is a function from A to $\mathbb{F}\}$. Let $\Gamma := \{f \in \mathbb{F}^A \,:\, \{a \in A \,:\, f(a) \neq 0\}$ is finite$\}$. Show that Γ is a vector space over $\mathbb{F}$ with respect to point-wise addition of functions and point-wise scalar multiplication. Also show that every vector space $\mathbb{V}$ is isomorphic to Γ for some suitable choice of A.*

6. *Let X be a vector space and A be a nonempty linearly independent subset of X. Let $S \subseteq X$ satisfy span$(S) = X$. Show that $\exists$ a Hamel basis B such that $A \subseteq B \subseteq S$.*

7. *Let $(L, \leq)$ be a nonempty linearly ordered set. Prove that $\exists\, W \subseteq L$ such that $\leq$ well orders W and such that for each $x \in L$, there is a $y \in W$ satisfying $x \leq y$. For example, for $L = \mathbb{R}$, we can take $W = \mathbb{N}$.*

8. *Show that $\mathbb{R}$ is not a finite dimensional vector space over $\mathbb{Q}$. Hint: Assume that $\mathbb{R}$ as a vector space over $\mathbb{Q}$ has dimension k. Argue that $\mathbb{R}$ is isomorphic to $\mathbb{Q}^k$ and so it is countable, a contradiction.*

9. *Let A be a nonempty set. Then there is an element a which is not in A.*

10. *Let A be a nonempty set. Then there exists B such that $A \cap B = \emptyset$ and $\overline{\overline{A}} = \overline{\overline{B}}$.*

11. *Let A and B be two nonempty sets. Show that there is a set C such that $C \cap A = \emptyset$ and $\overline{\overline{C}} = \overline{\overline{B}}$.*

12. *Let A and B be nonempty sets. Put $a = \overline{\overline{A}}$ and $b = \overline{\overline{B}}$. Then show that either $a \leq b$ or $b \leq a$.*

13. *Let $a = \overline{\overline{A}}$ and $b = \overline{\overline{B}}$, where $A \cap B = \emptyset$. Then we define $a + b$ as $\overline{\overline{A \cup B}}$ and ab as $\overline{\overline{A \times B}}$.*

    (a) Let a be an infinite cardinal number. Show that $a + a = a$ and $aa = a$.

    (b) Let a, b, c be cardinal numbers. Show that $a \leq b \Rightarrow \{a + c \leq b + c, ac \leq bc\}$.

14. *Suppose that $u \leq v$ are two infinite cardinal numbers. Then show that $u + v = v$ and $uv = v$.*

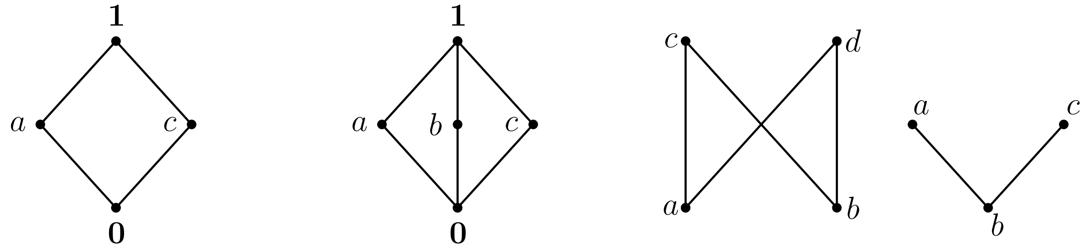
3.2 Lattices

Discussion 3.2.1. In a poset, is it necessary that two elements x, y should have a common upper bound?

Ans: No. Take $\{1, 2, \ldots, 6\}$ with 'divides' partial order. The elements 5 and 3 have no common upper bound.

In a poset, if a pair $\{x, y\}$ has at least one upper bound, is it necessary that $\{x, y\}$ should have a lub?

Ans: No. Consider the third poset described by it's Hasse diagram in Figure 3.2. Then, the pair $\{a, b\}$ has c, d as upper bounds, but there is no lub of $\{a, b\}$.



A distributive lattice A non-distributive lattice Both are non-lattices

Figure 3.2: Hasse diagrams

Definition 3.2.2. [Lattice]

1. A poset $(L, \leq)$ is called a **lattice** if each pair $x, y \in L$ has a lub denoted '$x \vee y$' and a glb denoted '$x \wedge y$'.
2. A lattice is called a **distributive lattice** if it satisfies the following two properties.

$$\left.\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z). \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z). \end{aligned}\right\} \text{distributive laws}$$

Example 3.2.3. 1. Let $L = \{0, 1\} \subseteq \mathbb{Z}$ and define $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$. Then, L is a chain as well as a distributive lattice.

2. The set $\mathbb{N}$ with usual order and $\vee := \max$ and $\wedge := \min$ is a distributive lattice. We consider two cases to verify that $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. The second distributive identity is left as an exercise for the reader.

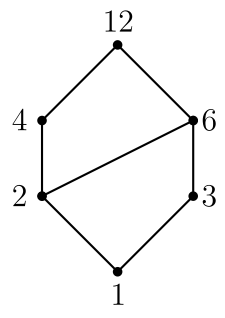
   (a) **Case 1:** $a \geq \min\{b, c\}$. Then, either $a \geq b$ or $a \geq c$, say $a \geq b$. Hence,

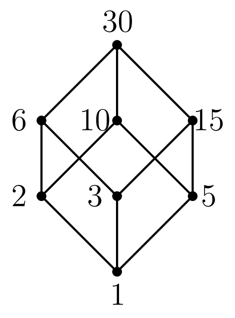
$$\begin{aligned} a \vee (b \wedge c) &= \max\{a, \min\{b, c\}\} \\ &= a = \min\{\max\{a, b\} = a, \max\{a, c\} \geq a\} = (a \vee b) \wedge (a \vee c). \end{aligned}$$

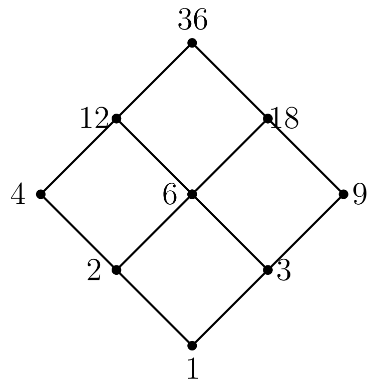
   (b) **Case 2:** $a < \min\{b, c\}$. Then, $a < b$ and $a < c$. Hence,

$$\begin{aligned} a \vee (b \wedge c) &= \max\{a, \min\{b, c\}\} \\ &= \min\{b, c\} = \min\{\max\{a, b\} = b, \max\{a, c\} = c\} = (a \vee b) \wedge (a \vee c). \end{aligned}$$

3. Prove that the first figure in Figure 3.2 is a distributive lattice.
4. Prove that the second figure in Figure 3.2 is a lattice but not a distributive lattice.
5. Let $S = \{a, b, c\}$. On $\mathcal{P}(S)$, we define $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. Then, it can be easily verified that $\mathcal{P}(S)$ is a lattice.
6. Fix a positive integer n and let $D(n)$ denote the poset obtained using the 'divides' partial order with $\vee := \mathsf{lcm}$ and $\wedge := \gcd$. Then, prove that $D(n)$ is a distributive lattice. For example, for $n = 12, 30$ and 36, the corresponding lattices are shown below.







EXERCISE **3.2.4.** *1. Fix a prime p and a positive integer n. Draw the Hasse diagram of $D(p^n)$. Does this correspond to a chain? Give reasons for your answer.*

2. Let n be a positive integer. Then, prove that $D(n)$ is a chain if and only if $n = p^m$, for some prime p and a positive integer m.

3. Let (X, f) be a nonempty chain with $\vee := \mathsf{lub}$ and $\wedge := \mathsf{glb}$. Is it a distributive lattice?

Proposition 3.2.5. [**properties of a lattice**] *Let $(L, \leq)$ be a lattice. Then, the following statements are true.*

(a) The operations $\vee$ and $\wedge$ are idempotent, i.e., ‘$\mathsf{lub}\{a, a\} = a$ and $\mathsf{glb}\{a, a\} = a$’.

(b) $\vee$ commutative (so is $\wedge$).

(c) $\vee$ is associative (so is $\wedge$).

(d) $a \wedge (a \vee b) = a = a \vee (a \wedge b)$ [**absorption**] *, i.e., ‘$\mathsf{glb}\{a, \mathsf{lub}\{a, b\}\} = a = \mathsf{lub}\{a, \mathsf{glb}\{a, b\}\}'$.*

(e) $a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$.

(f) $b \leq c \Rightarrow \{a \vee b \leq a \vee c, a \wedge b \leq a \wedge c\}$ [**isotonicity**] *.*

(f1) $\{a \leq b, c \leq d\} \Rightarrow \{a \vee c \leq b \vee d, a \wedge c \leq b \wedge d\}$.

(g) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$ [**distributive inequalities**] *.*

(h) $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$ [**modular inequality**] *.*

Proof. We prove only a few parts. The rest are left for the reader.

(c) Let $d = a \vee (b \vee c)$. Then, d is the lub of $\{a, b \vee c\}$. Thus, d is an upper bound of both $\{a, b\}$ and $\{a, c\}$. So, $d \geq a \vee b$ and $d \geq a \vee c$. Therefore, $d \geq a \vee b$ and $d \geq c$ and hence d an upper bound of $\{a \vee b, c\}$. So, d is greater or equals to the lub of $\{a \vee b, c\}$, *i.e.*, $d \geq (a \vee b) \vee c$. Thus, the first part of the result follows.

(e) Let $a \leq b$. As b is an upper bound of $\{a, b\}$, we have $a \vee b = \mathsf{lub}\{a, b\} \leq b$. Also, $a \vee b$ is an upper bound of $\{a, b\}$ and hence $a \vee b \geq b$. So, we get $a \vee b = b$. Conversely, let $a \vee b = b$. As $a \vee b$ is an upper bound of $\{a, b\}$, we have $a \leq a \vee b = b$. Thus, the first part of the result follows.

(f) Let $b \leq c$. Note that $a \vee c \geq a$ and $a \vee c \geq c \geq b$. So, $a \vee c$ is an upper bound for $\{a, b\}$. Thus, $a \vee c \geq \mathsf{lub}\{a, b\} = a \vee b$ and hence the prove of the first part is over.

(f1) Using isotonicity, we have $a \vee c \leq b \vee c \leq b \vee d$. Similarly, using isotonicity again, we have $a \wedge c \leq b \wedge c \leq b \wedge d$.

(g) Note that $a \leq a \vee b$ and $a \leq a \vee c$. Thus, $a = a \wedge a \leq (a \vee b) \wedge (a \vee c)$. As $b \leq a \vee b$ and $c \leq a \vee c$, we get $b \wedge c \leq (a \vee b) \wedge (a \vee c)$. Now using (f1), we obtain the required result, *i.e.*, $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

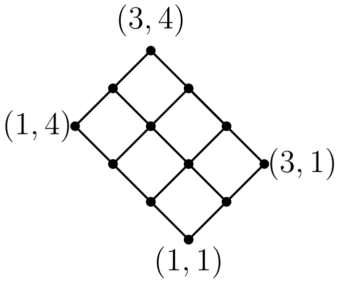
(h) Let $a \leq c$. Then, $a \vee c = c$ and hence by the ‘distributive inequality’, we have $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$. Conversely, let $a \vee (b \wedge c) \leq (a \vee b) \wedge c$. Then, $a \leq a \vee (b \wedge c) \leq (a \vee b) \wedge c \leq c$ and the required result follows. ■

PRACTICE **3.2.6.** *Show that in a lattice one distributive equality implies the other.*

Definition 3.2.7. If $(L_i, \leq_i)$, $i = 1, 2$ are lattices with $\vee := \mathsf{lub}$ and $\wedge := \mathsf{glb}$. Then, $(L_1 \times L_2, \leq)$ is a poset with $a = (a_1, a_2) \leq (b_1, b_2) = b$ if $a_1 \leq_1 b_1$ and $a_2 \leq_2 b_2$, that is, if b dominates a entry-wise. In this case, we see that $a \vee b = (a_1 \vee_1 b_1, a_2 \vee_2 b_2)$ and $a \wedge b = (a_1 \wedge_1 b_1, a_2 \wedge_2 b_2)$. Thus $(L_1 \times L_2, \leq)$ is a lattice, called the **direct product** of $(L_i, \leq_i)$, for $i = 1, 2$.

Example 3.2.8. 1. Consider $L = \{0, 1\}$ with usual order. The set of all binary strings L^n of length n is a poset with the order $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ if $a_i \leq b_i$, $\forall i$. This is the n-fold direct product of L. It is called the **lattice of n-tuples of 0 and 1**.

2. Consider the lattices $\{1, 2, 3\}$ and $\{1, 2, 3, 4\}$ with usual orders. Hasse diagram of the direct product $\{1, 2, 3\} \times \{1, 2, 3, 4\}$ is given below.



PRACTICE **3.2.9.** *Consider $\mathbb{N}$ with the usual order. The lattice order defined on $\mathbb{N}^2$ as a direct product is different from the lexicographic order on $\mathbb{N}^2$. Draw pictures for all $(a,b) \le (5,6)$ in both the orders to see the argument.*

Proposition 3.2.10. *The direct product of two distributive lattices is a distributive lattice.*

Proof. The direct product of two lattices is a lattice by definition. Note that

$$\begin{aligned}
[(a_1,b_1)\vee(a_2,b_2)]\wedge(a_3,b_3) &= (a_1\vee a_2, b_1\vee b_2)\wedge(a_3,b_3)\\
&= \Big((a_1\vee a_2)\wedge a_3, (b_1\vee b_2)\wedge b_3\Big)\\
&= \Big((a_1\wedge a_3)\vee(a_2\wedge a_3), (b_1\wedge b_3)\vee(b_2\wedge b_3)\Big)\\
&= \Big((a_1\wedge a_3),(b_1\wedge b_3)\Big)\vee\Big((a_2\wedge a_3),(b_2\wedge b_3)\Big)\\
&= \Big((a_1,b_1)\wedge(a_3,b_3)\Big)\vee\Big((a_2,b_2)\wedge(a_3,b_3)\Big).\blacksquare
\end{aligned}$$

Definition 3.2.11. Let $(L_i, \le_i)$, $i = 1,2$ be two lattices. A function $f : L_1 \to L_2$ satisfying $f(a \vee_1 b) = f(a) \vee_2 f(b)$ and $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$ is called a **lattice homomorphism**. Furthermore, if f is a bijection, then it is called a **lattice isomorphism**.

Example 3.2.12. 1. Let D be the set of all words in our English dictionary with 'dictionary ordering'. Then, prove that D is a lattice. Now, consider the set S of all words in D which are of length at most six or first-part-words of length six. Note that S is a lattice again. Define $f : D \to S$ as $f(d) = d$ if d has length at most six, otherwise $f(d)$ is the first-part-word of length 6 of d. Then, f is a homomorphism. It is not an isomorphism as $f(\text{stupid}) = f(\text{stupidity})$.

2. Consider the lattice $\mathbb{N}$ with usual order. Let $S = \{0,1,2\}$ with usual order. Let $f : \mathbb{N} \to S$ be a homomorphism. If $f(m) = 0$ and $f(n) = 1$, then $m \le n$, or else, we have

$$0 = f(m) = f(m \vee n) \ne f(m) \vee f(n) = 0 \vee 1 = 1.$$

Thus, the map f must have one of the following forms. Draw pictures to understand this.

(a) $f^{-1}(0) = \mathbb{N}$.

(b) $f^{-1}(0) = \{1,2,\ldots,k\}$ and $f^{-1}(1) = \{k+1,\ldots\}$, for some $k \in \mathbb{N}$.

(c) $f^{-1}(0) = \{1,2,\ldots,k\}$, $f^{-1}(1) = \{1,2,\ldots,r\} \setminus \{1,2,\ldots,k\}$ and $f^{-1}(2) = \mathbb{N} \setminus \{1,2,\ldots,r\}$, for some $k, r \in \mathbb{N}$ with $k < r$.

Definition 3.2.13. **[Complete lattice]** A lattice $(L, \le)$ is **complete** if $\vee A$ (lub of A) and $\wedge A$ (glb of A) exist in L, for each nonempty subset A of L.

Example 3.2.14. 1. Verify that the lattices in Figure 3.3 are complete.

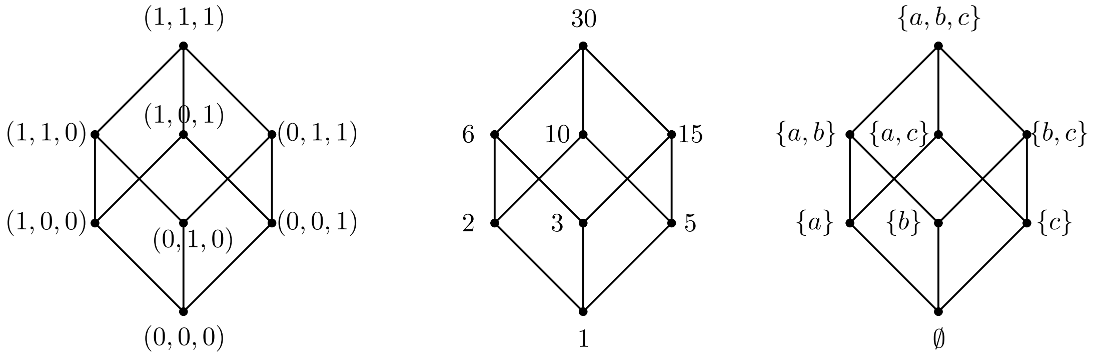


Figure 3.3: Complete lattices

2. Verify that every finite lattice is complete.

3. [**Bounded lattice**] Every complete lattice has a least element **0** and a greatest element **1**. Any lattice with these two elements is called a **bounded lattice**.

4. The set $[0, 5]$ with usual order is a bounded and complete lattice. So, is the set $[0, 1) \cup [2, 3]$.

5. The set $(0, 5]$ is a lattice which is neither bounded nor complete.

6. The set $[0, 1) \cup (2, 3]$ is a bounded lattice, though not complete.

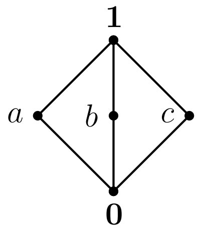
7. The set $\mathbb{R}$ with usual order is a lattice. It is not complete in the lattice 'sense'. It is 'conditionally complete', that is, for every bounded nonempty subset glb and lub exist. Can you think of a reason which implies the importance of the condition 'non-emptiness'?

8. Fix $n \in \mathbb{N}$ and let $p_1, p_2, \ldots, p_n$ be n distinct primes. Prove that the lattice $D(N)$, for $N = p_1 p_2 \cdots p_n$ is isomorphic to the lattice L^n (the lattice of n-tuples of 0 and 1) and to the lattice $\mathcal{P}(S)$, where $S = \{1, 2, \ldots, n\}$. The Hasse diagram for $n = 3$ is shown above.

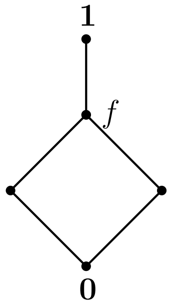
Definition 3.2.15. [**Lattice Complement**] Let $(L, \leq)$ be a bounded lattice. Then, a **complement** of $b \in L$ is an element (if it exists) $c \in L$ such that $b \vee c = \mathbf{1}$ and $b \wedge c = \mathbf{0}$. The lattice is called **complemented** if every element has at least one complement. We shall use $\neg b$ to denote $\overline{b}$, a complement of b.

Example 3.2.16. 1. The interval $[0,\ 1]$ with usual ordering is a distributive lattice but is not complemented.

2. Verify the captions of the two figures given below. Also, compute $\neg 0, \neg a, \neg b, \neg c$, and $\neg 1$.



Complemented but NOT distributive



Distributive but NOT complemented

Discussion 3.2.17. [**The comparison table**] Let $(L, \leq)$ be a lattice and let $a, b, c \in L$. Then, the following table lists the properties that hold (make sense) in the specified type of lattices.

Properties	**Lattice type**
$\vee$, $\wedge$ are idempotent	any lattice
$\vee$, $\wedge$ are commutative	any lattice
$\vee$, $\wedge$ are associative	any lattice
[absorption] $a \wedge (a \vee b) = a = a \vee (a \wedge b)$	any lattice
$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$	any lattice
[isotonicity] $b \leq c \Rightarrow \{a \vee b \leq a \vee c, a \wedge b \leq a \wedge c\}$	any lattice
[distributive inequalities] $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$	any lattice
[modular inequality] $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$	any lattice
$\mathbf{0}$ is unique; $\mathbf{1}$ is unique	bounded lattice ‼
if a is a complement of b, then b is also a complement of a	bounded lattice ‼
$\neg\mathbf{0}$ is unique and it is $\mathbf{1}$; $\neg\mathbf{1}$ is unique and it is $\mathbf{0}$	bounded lattice ‼
an element a has a unique complement	distributive complemented lattice ‼
[cancellation] $\left\{a \vee c = b \vee c,\ a \vee \neg c = b \vee \neg c\right\} \Rightarrow a = b$ $\left\{a \wedge c = b \wedge c,\ a \wedge \neg c = b \wedge \neg c\right\} \Rightarrow a = b$	distributive complemented lattice
[De-Morgan] $\neg(a \vee b) = \neg a \wedge \neg b$ $\neg(a \wedge b) = \neg a \vee \neg b$	distributive complemented lattice
$a \vee \neg b = \mathbf{1} \Leftrightarrow a \vee b = a$ $a \wedge \neg b = \mathbf{0} \Leftrightarrow a \wedge b = a$	distributive complemented lattice

Proof. We will only prove the properties that appear in the last three rows. The other properties are left as an exercise for the reader. To prove the cancellation property, note that

$$b = b \vee \mathbf{0} = b \vee (c \wedge \neg c) = (b \vee c) \wedge (b \vee \neg c) = (a \vee c) \wedge (a \vee \neg c) = a \vee (c \wedge \neq c) = a \vee \mathbf{0} = a$$

and

$$b = b \wedge \mathbf{1} = b \wedge (c \vee \neg c) = (b \wedge c) \vee (b \wedge \neg c) = (a \wedge c) \vee (a \wedge \neg c) = a \wedge (c \vee \neg c) = a \wedge \mathbf{1} = a.$$

To prove the De-Morgan's property, note that

$$(a \vee b) \vee (\neg a \wedge \neg b) = (a \vee b \vee \neg a) \wedge (a \vee b \vee \neg b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1},$$

and

$$(a \vee b) \wedge (\neg a \wedge \neg b) = (a \wedge \neg a \wedge \neg b) \vee (b \wedge \neg a \wedge \neg b) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}.$$

Hence, by Definition 3.2.15, we get $\neg(a \vee b) = \neg a \wedge \neg b$. Similarly, note that $(a \wedge b) \vee (\neg a \vee \neg b) = (a \vee \neg a \vee \neg b) \wedge (b \vee \neg a \vee \neg b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$ and $(a \wedge b) \wedge (\neg a \vee \neg b) = (a \wedge b \wedge \neg a) \vee (a \wedge b \wedge \neg b) = \mathbf{0} \wedge \mathbf{0} = \mathbf{0}$. Thus, by Definition 3.2.15, we again get $\neg(a \wedge b) = (\neg a \vee \neg b)$. To prove the next assertion, note that if $a \vee \neg b = \mathbf{1}$, then

$$a = a \vee (b \wedge \neg b) = (a \vee b) \wedge (a \vee \neg b) = (a \vee b) \wedge \mathbf{1} = a \vee b.$$

Conversely, if $a = a \vee b$, then $a \vee \neg b = (a \vee b) \vee \neg b = \mathbf{1}$. On similar lines, one completes the proof of the second part and is left as an exercise for the reader. ∎

Exercise **3.2.18.** *1. Prove that every linearly ordered set is distributive.*

2. *Draw the Hasse diagrams of* $\{1,2,3\} \times \{1,2,3,4\}$ *with dictionary order and the lattice order* $((m,n) \leq (p,q)$ *if* $m \leq p$ *and* $n \leq q)$*.*
3. *Give a partial order on* $\mathbb{N}$ *to make it a bounded lattice. You may draw Hasse diagram representing it.*
4. *Does there exist a partial order on* $\mathbb{N}$ *for which each nonempty subset has finitely many (at least one) upper bounds and finitely many (at least one) lower bounds?*
5. *Consider the lattice* $\mathbb{N}^2$ *with lexicographic order. Is it isomorphic to the direct product of* $(\mathbb{N}, \leq)$ *with itself, where* $\leq$ *is the usual order?*
6. *Show that* $\{0,1,2,\ldots\}$ *is a complete lattice under divisibility relation (allow* $(0,0)$ *in the relation). Characterize those sets* A *for which* $\vee A = 0$*.*
7. *Is the lattice* $\{1,2\} \times \{1,2\} \times \{1,2\} \times \{1,2\}$ *isomorphic to* $\{1,2,3,4\} \times \{1,2,3,4\}$*?*
8. *Prove/Disprove: If* L *is a lattice which is not complete, then* $\overline{\overline{L}} \geq \overline{\overline{N}}$*.*
9. *Draw the Hasse diagram of a finite complemented lattice which is not distributive.*
10. *How many lattice homomorphisms are there from* $\{1,2\}$ *to* $\{1,2,\ldots,9\}$*?*
11. *Draw as many Hasse diagrams of non-isomorphic lattices of size* 6 *as you can.*

3.3 Boolean Algebras

Definition 3.3.1. [**Boolean algebra**] A **Boolean algebra** is a set S which is closed under the binary operations $\vee$ (called the **join**) and $\wedge$ (called the **meet**) and for each $x, y, z \in S$, satisfies the following properties.

1. $x \vee y = y \vee x$, $x \wedge y = y \wedge x$ [**commutative**] .
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ [**distributive**] .
3. $\exists\ \mathbf{0}, \mathbf{1} \in S$ such that $x \vee \mathbf{0} = x$, $x \wedge \mathbf{1} = x$ [**identity elements**] .
4. For each $x \in S$, $\exists\ y \in S$ such that $x \vee y = \mathbf{1}$ and $x \wedge y = \mathbf{0}$ [**inverse**] .

Proposition 3.3.2. *Let* S *be a Boolean algebra. Then, the following statements are true.*

1. *Elements* $\mathbf{0}$ *and* $\mathbf{1}$ *are unique.*
2. *For each* $s \in S$*,* $\neg s$ *is unique. Therefore, for each* $x \in S$*,* $\neg x$ *is called the* **inverse** *of* x*.*
3. *If* y *is the inverse of* x*, then* x *is the inverse of* y*. That is,* $x = \neg(\neg x)$*.*

Proof.

1. Let $\mathbf{0}_1$ and $\mathbf{0}_2$ be two such elements. Then, $\mathbf{0}_1 \vee x = x$ and $x = x \vee \mathbf{0}_2$, for all $x \in S$. Hence, $\mathbf{0}_1 = \mathbf{0}_1 \vee \mathbf{0}_2 = \mathbf{0}_2$. Thus, the required result follows. A similar argument implies that $\mathbf{1}$ is unique.
2. Suppose there exists $t, r \in S$ such that $s \vee t = \mathbf{1}, s \wedge t = \mathbf{0}, s \vee r = \mathbf{1}$ and $s \wedge r = \mathbf{0}$. Then,
$$t = t \wedge \mathbf{1} = t \wedge (s \vee r) = (t \wedge s) \vee (t \wedge r) = \mathbf{0} \vee (t \wedge r) = (s \wedge r) \vee (t \wedge r) = (s \vee t) \wedge r = \mathbf{1} \wedge r = r.$$
3. It directly follows from the definition of 'inverse'. ■

Example 3.3.3. 1. Let $S \neq \emptyset$. Then, $P(S)$ is a Boolean algebra with $\vee = \cup$, $\wedge = \cap$, $\neg A = A^c$, $\mathbf{0} = \emptyset$ and $\mathbf{1} = S$. So, we have Boolean algebras of finite size as well as of uncountable size.

2. Take $S = \{n \in \mathbb{N} : n|30\}$ with $a \vee b = \mathsf{lcm}(a, b)$, $a \wedge b = \gcd(a, b)$, $\neg a = \frac{30}{a}$, $\mathbf{0} = 1$ and $\mathbf{1} = 30$. It is a Boolean algebra.
3. Let $B = \{T, F\}$ with $\mathbf{0} = F$, $\mathbf{1} = T$ and with usual $\vee, \wedge, \neg$. It is a Boolean algebra.
4. Let B be the set of all truth functions involving the variables $p_1, \ldots, p_n$, with usual $\vee, \wedge, \neg$. Take $\mathbf{0} = \mathbf{F}$ and $\mathbf{1} = \mathbf{T}$. This is the **free Boolean algebra** on the generators $p_1, \ldots, p_n$.
5. The class of finite length formulae involving variables $p_1, p_2, \ldots$ is a countable infinite Boolean algebra with usual operations.

Observation.

The rules of Boolean algebra treat $(\vee, \mathbf{0})$ and $(\wedge, \mathbf{1})$ equally. Notice that the second part of the rules in Definition 3.3.1 can be obtained by replacing $\vee$ with $\wedge$ and $\mathbf{0}$ with $\mathbf{1}$. Thus, any statement that one can derive from these rules has a dual version which is derivable from the rules. This is called the **principle of duality**.

Theorem 3.3.4. [**Rules**] *Let $(S, \vee, \wedge, \neg)$ be a Boolean algebra. Then, the following rules, as well as their dual, hold true.*

1. $\neg\mathbf{0} = \mathbf{1}$.
2. *For each $s \in S$, $s \vee s = s$* [**idempotence**] .
3. *For each $s \in S$, $s \vee \mathbf{1} = \mathbf{1}$.*
4. *For each $s, t \in S$, $s \vee (s \wedge t) = s$* [**absorption**] .
5. *If $s \vee t = r \vee t$ and $s \vee \neg t = r \vee \neg t$, then $s = r$* [**cancellation**] .
6. $(s \vee t) \vee r = s \vee (t \vee r)$ [**associative**] .

Proof. We give the proof of the first part of each item and that of its dual is left for the reader.

1. $\mathbf{1} = \mathbf{0} \vee (\neg\mathbf{0}) = \neg\mathbf{0}$.
2. $s = s \vee \mathbf{0} = s \vee (s \wedge \neg s) = (s \vee s) \wedge (s \vee \neg s) = (s \vee s) \wedge \mathbf{1} = (s \vee s)$.
3. $\mathbf{1} = s \vee \neg s = s \vee (\neg s \wedge \mathbf{1}) = (s \vee \neg s) \wedge (s \vee \mathbf{1}) = \mathbf{1} \wedge (s \vee \mathbf{1}) = s \vee \mathbf{1}$.
4. $s \vee (s \wedge t) = (s \wedge \mathbf{1}) \vee (s \wedge t) = s \wedge (\mathbf{1} \vee t) = s \wedge \mathbf{1} = s$.
5. $s = s \vee \mathbf{0} = s \vee (t \wedge \neg t) = (s \vee t) \wedge (s \vee \neg t) = (r \vee t) \wedge (r \vee \neg t) = r \vee (t \wedge \neg t) = r \vee \mathbf{0} = r$.
6. We will prove it using absorption and cancellation. Using absorption, $(s \vee t) \wedge s = s$ and $s \vee (r \wedge s) = s$. Thus, $\big((s \vee t) \vee r\big) \wedge s = \big((s \vee t) \wedge s\big) \vee (r \wedge s) = s \vee (r \wedge s) = s$. Using absorption, we also have $\big(s \vee (t \vee r)\big) \wedge s = s$ and hence
$$\big(s \vee (t \vee r)\big) \wedge s = \big((s \vee t) \vee r\big) \wedge s.$$
Now, we see that $[s \vee (t \vee r)] \wedge \neg s = \mathbf{0} \vee [(t \vee r) \wedge \neg s] = (t \wedge \neg s) \vee (r \wedge \neg s)$ and on similar lines, $[(s \vee t) \vee r] \wedge \neg s = (t \wedge \neg s) \vee (r \wedge \neg s)$. Thus, we again have
$$\big(s \vee (t \vee r)\big) \wedge \neg s = \big((s \vee t) \vee r\big) \wedge \neg s.$$
Hence, applying the cancellation property, the required result follows. ■

Example 3.3.5. Let $(L, \leq)$ be a distributive complemented lattice. Then, by Definition 3.2.2, L has two binary operations $\vee$ and $\wedge$ and by Definition 3.2.15, the operation $\neg x$. It can be easily verified that $(L, \vee, \wedge, \neg)$ is a indeed a Boolean algebra.

Now, let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. Then, for any two elements $a, b \in B$, we define $a \leq b$ if $a \wedge b = a$. The next result shows that $\leq$ is a partial order in B. This partial order is generally called the **induced partial order**. Thus, we see that the Boolean algebra B, with the induced partial order, is a distributive complemented lattice.

Theorem 3.3.6. *Let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. Define, $a \leq b$ if $a \wedge b = a$. Then, $\leq$ is a partial order on B. Furthermore, $a \vee b = \mathsf{lub}\{a, b\}$ and $a \wedge b = \mathsf{glb}\{a, b\}$.*

Proof. We first verify that $(B, \leq)$ is indeed a partial order.
Reflexive: By idempotence, $s \leq s$ and hence $\leq$ is reflexive.
Antisymmetry: Let $s \leq t$ and $t \leq s$. Then, we have $s = s \wedge t = t$.
Transitive: Let $s \leq t$ and $t \leq r$. Then, using associativity, $s \wedge r = (s \wedge t) \wedge r = s \wedge (t \wedge r) = s \wedge t = s$ and thus, $s \leq r$.

Now, we show that $a \vee b = \mathsf{lub}\{a, b\}$. Since B is a Boolean algebra, using absorption, we get $(a \vee b) \wedge a = a$ and hence $a \leq a \vee b$. Similarly, $b \leq a \vee b$. So, $a \vee b$ is an upper bound for $\{a, b\}$.

Now, let x be any upper bound for $\{a, b\}$. Then, by distributive property, $(a \vee b) \wedge x = (a \wedge x) \vee (b \wedge x) = a \vee b$. So, $a \vee b \leq x$. Thus, $a \vee b$ is the lub of $\{a, b\}$. The rest of the proof is similar and hence is left for the reader. ■

Thus, we observe that there is one-to-one correspondence between the set of Boolean Algebras and the set of distributive complemented lattice.

Definition 3.3.7. [**Atom**] Let B be a Boolean algebra. If there exists a $b \in B, b \neq \mathbf{0}$ such that b is a minimal element in B, then b is called an **atom**.

Example 3.3.8.

1. In the powerset Boolean algebra, singleton sets are the only atoms.
2. Atoms of the 'divides 30' Boolean algebra are $2, 3$ and 5.
3. The $\{F, T\}$ Boolean algebra has only one atom, namely T.

EXERCISE **3.3.9.**

1. *Determine the atoms of the free Boolean algebra with generators $p_1, \ldots, p_n$?*
2. *Is it necessary that every Boolean algebra has at least one atom?*

Definition 3.3.10. [**Boolean homomorphism**] Let B_1 and B_2 be two Boolean algebras. A function $f : B_1 \to B_2$ is a **Boolean homomorphism** if it preserves $\mathbf{0}$, $\mathbf{1}$, $\vee$, $\wedge$, and $\neg$. That is,

$$f(\mathbf{0}_1) = \mathbf{0}_2, \;\; f(\mathbf{1}_1) = \mathbf{1}_2, \;\; f(a \vee b) = f(a) \vee f(b), \;\; f(a \wedge b) = f(a) \wedge f(b), \text{and } f(\neg a) = \neg f(a).$$

A **Boolean isomorphism** is a Boolean homomorphism which is a bijection.

EXERCISE **3.3.11.** *Let B_1 and B_2 be two Boolean algebras and let $f : B_1 \to B_2$ be a function that satisfies the four conditions $f(\mathbf{0}_1) = \mathbf{0}_2$, $f(\mathbf{1}_1) = \mathbf{1}_2$, $f(a \vee b) = f(a) \vee f(b)$ and $f(a \wedge b) = f(a) \wedge f(b)$. Then, prove that f also satisfies the fifth condition, namely $f(\neg a) = \neg f(a)$.*

Example 3.3.12. The function $f : P(J_4) \to P(J_3)$ defined as $f(S) = S \setminus \{4\}$ is a Boolean homomorphism. We check just two properties and the rest is left as an exercise.

$$f(A \vee B) = f(A \cup B) = (A \cup B) \setminus \{4\} = (A \setminus \{4\}) \cup (B \setminus \{4\}) = f(A) \vee f(B).$$

$$f(\mathbf{1}_1) = f(J_4) = J_4 \setminus \{4\} = J_3 = \mathbf{1}_2.$$

Proposition 3.3.13. *Let B be a Boolean algebra and p, q be two distinct atoms. Then, $p \wedge q = \mathbf{0}$.*

Proof. Suppose that $p \wedge q \neq \mathbf{0}$. As $p \wedge q \leq p$ and p is an atom, we must have $p \wedge q = p$, *i.e.*, $q \leq p$. As $p \neq q$ and q is an atom, it follows that p cannot be an atom. ■

Proposition 3.3.14. *Let B be a Boolean algebra with three distinct atoms p, q and r. Then, $p \vee q \neq p \vee q \vee r$.*

Proof. Let if possible $p \vee q = p \vee q \vee r$. Then, we have

$$r = r \vee \mathbf{0} = r \vee [(p \vee q) \wedge \neg(p \vee q)] = [r \vee p \vee q] \wedge [r \vee \neg(p \vee q)] = [p \vee q] \wedge [r \vee \neg(p \vee q)]$$

$$= [(p \vee q) \wedge r] \vee [(p \vee q) \wedge \neg(p \vee q)] = (p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r) = \mathbf{0} \vee \mathbf{0} = \mathbf{0},$$

a contradiction to r being an atom, *i.e.*, r is nonzero. ■

Example 3.3.15. Let B be a Boolean algebra having distinct atoms $A = \{p, q, r\}$. Then, B has at least 2^3 elements.

To show this, we define $f : \mathcal{P}(A) \to B$ by $f(\emptyset) = \mathbf{0}$ and for $S \subseteq A$, $f(S) = \bigvee\limits_{x \in S} x$ and claim that f is a one-one function.

Suppose $f(S) = f(T)$. Then, $f(S) = f(S) \vee f(T) = f(S \cup T)$. In view of Proposition 3.3.14, we have $S = S \cup T$, *i.e.*, $T \subseteq S$. Similarly, as $f(T) = f(T \cup S)$, we have $S \subseteq T$ and hence $S = T$. Thus, f is a one-one function. Therefore, $f(S)$ is distinct, for each subset of A and thus B has at least 2^3 elements.

Theorem 3.3.16. *Let B be a Boolean algebra having distinct atoms $A = \{p, q, r, s\}$. Let $b \in B$, $b \neq \mathbf{0}$. Suppose that $S = \{\text{atoms } x : x \leq b\} = \{p, q, r\}$. Then, $b = p \vee q \vee r$.*

Proof. It is clear that $p \vee q \vee r \leq b$. Suppose that $p \vee q \vee r < b$. Then,

$$b = b \wedge [(p \vee q \vee r) \vee \neg(p \vee q \vee r)] = [b \wedge (p \vee q \vee r)] \vee [b \wedge \neg(p \vee q \vee r)] = (p \vee q \vee r) \vee [b \wedge \neg(p \vee q \vee r)].$$

Therefore, the above equality implies that $[b \wedge \neg(p \vee q \vee r)] \neq \mathbf{0}$. So, there is an atom, say x, such that $x \leq b \wedge \neg(p \vee q \vee r)$. Thus, we have $x \leq b$ and $x \leq \neg(p \vee q \vee r)$.

Notice that if $x \leq (p \vee q \vee r)$, then $x \leq \mathbf{0}$, which is not possible. So, $x \neq p, q, r$ is an atom in S, a contradiction. ■

Theorem 3.3.17. **[Representation]** *Let B be a finite Boolean algebra. Then, there exists a set X such that B is isomorphic to $\mathcal{P}(X)$.*

Proof. Put $X = \{\text{atoms of } B\}$. Note that $X \neq \emptyset$. Define $f : B \to \mathcal{P}(X)$ by $f(b) = \{\text{atoms} \leq b\}$. We show that f is the required Boolean isomorphism.

Injection: Let $b_1 \neq b_2$. Then, either $b_1 \not\leq b_2$ or $b_2 \not\leq b_1$. Without loss of generality, let $b_1 \not\leq b_2$. [Now imagine the power set Boolean algebra. Saying $b_1 \not\leq b_2$ is the same as $b_1 \not\subseteq b_2$. In that case, we have an element in b_1 which is not in b_2. That is, $b_1 \cap b_2^c \neq \emptyset$. That is, there is a singleton subset of $b_1 \cap b_2^c$. This is exactly what we are aiming for, *i.e.*, to prove that $b_1 \wedge \neg b_2 \neq \mathbf{0}$.] Note that $b_1 = b_1 \wedge (b_2 \vee \neg b_2) = (b_1 \wedge b_2) \vee (b_1 \wedge \neg b_2)$. Also, the assumption $b_1 \not\leq b_2$ implies $b_1 \wedge b_2 \neq b_1$ and hence $b_1 \wedge \neg b_2 \neq \mathbf{0}$. So, there exists an atom $x \leq (b_1 \wedge \neg b_2)$ and hence $x = x \wedge b_1 \wedge \neg b_2$. Therefore,

$$x \wedge b_1 = (x \wedge b_1 \wedge \neg b_2) \wedge b_1 = x \wedge b_1 \wedge \neg b_2 = x.$$

Thus, $x \leq b_1$. Similarly, $x \leq \neg b_2$. As $x \neq \mathbf{0}$, we cannot have $x \leq b_2$ (the condition $x \leq \neg b_2$ and $x \leq b_2$ implies $x \leq b_2 \wedge \neg b_2 = \mathbf{0}$). Thus, $f(b_1) \neq f(b_2)$.

Surjection: Let $A = \{x_1, \ldots, x_k\} \subseteq X$ and put $b = x_1 \vee \cdots \vee x_k$ (if $k = 0$, then $b = \mathbf{0}$). Clearly, $A \subseteq f(b)$. Need to show: $A = f(b)$. So, let $y \in f(b)$, *i.e.*, y is an atom in B and

$$y = y \wedge b = y \wedge (x_1 \vee \cdots \vee x_k) = (y \wedge x_1) \vee \cdots \vee (y \wedge x_k).$$

Since $y \neq \mathbf{0}$, by Proposition 3.3.13, it follows that $y \wedge x_{i_0} \neq \mathbf{0}$, for some $i_0 \in \{1, 2, \ldots, k\}$. As x_{i_0} and y are atoms, we have $y = y \wedge x_i = x_i$ and hence $y \in A$. Thus, f is a surjection.
Preserving $\mathbf{0}, \mathbf{1}$: Clearly $f(\mathbf{0}) = \emptyset$ and $f(\mathbf{1}) = X$.
Preserving $\vee, \wedge$: By definition,

$$\begin{aligned} x \in f(b_1 \wedge b_2) &\Leftrightarrow x \leq b_1 \wedge b_2 \Leftrightarrow x \leq b_1 \text{ and } x \leq b_2 \\ &\Leftrightarrow x \in f(b_1) \text{ and } x \in f(b_2) \Leftrightarrow x \in f(b_1) \cap f(b_2). \end{aligned}$$

Now, let $x \in f(b_1 \vee b_2)$. Then, by definition, $x = x \wedge (b_1 \vee b_2) = (x \wedge b_1) \vee (x \wedge b_2)$. So, there exists i such that $x \wedge b_i \neq \mathbf{0}$ (say, $x \wedge b_1$). As, x is an atom, $x \leq b_1$ and hence $x \in f(b_1) \subseteq f(b_1) \cup f(b_2)$. Conversely, let $x \in f(b_1) \cup f(b_2)$. Without loss of generality, let $x \in f(b_1)$. Thus, $x \leq b_1$ and hence $x \leq b_1 \vee b_2$ which in turn implies that $x \in f(b_1 \vee b_2)$. ■

As a direct corollary, we have the following result.

Corollary 3.3.18. *Let B be a finite Boolean algebra having exactly k atoms. Then, B is isomorphic to $\mathcal{P}(\{1, 2, \ldots, k\})$ and hence has exactly 2^k elements.*

EXERCISE **3.3.19.** *1. Determine the number of elements in a finite Boolean algebra.*

2. *Supply a Boolean homomorphism f from $P(J_4)$ to $P(J_3)$ such that the image of $P(J_4)$ has 4 elements.*

3. *Prove/Disprove: The number of Boolean homomorphisms from $P(J_4)$ to $P(J_3)$ is less than the number of lattice homomorphisms from $P(J_4)$ to $P(J_3)$.*

4. *Show that a lattice homomorphism on a Boolean algebra which preserves $\mathbf{0}$ and $\mathbf{1}$ is a Boolean homomorphism.*

5. *Consider the class of all functions $f : \mathbb{R} \to \{\pi, e\}$. Can we define some operations on this class to make it a Boolean algebra?*

6. *Show that a finite Boolean algebra must have at least one atom. Is 'finite' necessary?*

7. *A positive integer is called* **square-free** *if it is not divisible by the square of a prime. Let $B_n = \{k \in \mathbb{N} : k|n\}$. For $a, b \in B_n$ take the operations $a \vee b = \mathsf{lcm}(a, b)$, $a \wedge b = \gcd(a, b)$ and $\neg a = n/a$. Show that B_n is a Boolean algebra if and only if $n > 1$ is square-free.*

8. *Show that the set of subsets of $\mathbb{N}$ which are either finite or have a finite complement is a countable infinite Boolean algebra. Find the atoms. Is it isomorphic to the Boolean algebra of all finite length formulae involving variables $p_1, p_2, \cdots$?*

9. *Let B be a Boolean algebra and $x_i \in B$, $i = 1, 2, \ldots$. We know that, for each $n \in \mathbb{N}$, the expression '$\bigvee\limits_{i=1}^{n} x_i$' is meaningful in each Boolean algebra due to associativity. Is '$\bigvee\limits_{i=1}^{\infty} x_i$' necessarily a meaningful expression?*

10. *Prove/Disprove: Let $f : B_1 \to B_2$ be a Boolean homomorphism and $a \in B_1$ be an atom. Then, $f(a)$ is an atom of B_2.*

11. *Fill in the blank: The number of Boolean homomorphisms from $P(J_4)$ to $P(J_3)$ is _____.*

12. *Fill in the blank: The number of Boolean homomorphisms from $P(J_4)$ onto $P(J_3)$ is _____.*

13. *How many atoms does "divides* 30030 *Boolean algebra" has? How many elements does it have?*

14. *If B_1 and B_2 are Boolean algebras of size k ($k > 100$), then they must be isomorphic and there must be more than k isomorphisms between them.*

15. *Give examples of two countably infinite non-isomorphic Boolean algebras.*

16. *Give examples of two uncountably infinite non-isomorphic Boolean algebras.*

Chapter 4

Basic Counting

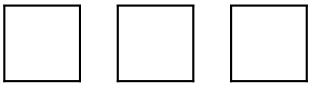
Discussion 4.0.1. In the previous chapters, we had learnt that two sets, say A and B, have the same cardinality if there exists a one-one and onto function $f : A \to B$. We also learnt the following two rules of counting which play a basic role in the development of this subject.

1. [**Multiplication rule**] If a task has n compulsory parts, say $A_1, A_2, \ldots, A_n$ and the i-th part can be completed in $m_i = |A_i|$ ways, $i = 1, \ldots, n$, then the task can be completed in $m_1 m_2 \cdots m_n$ ways. In mathematical terms,
$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|.$$

2. [**Addition rule**] If a task consists of n alternative parts, say $A_1, A_2, \ldots, A_n$, and the ith part can be done in $|A_i| = m_i$ ways, $i = 1, \ldots, n$, then the task can be completed in $m_1 + m_2 + \cdots + m_n$ ways. In mathematical terms,
$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|, \text{ whenever } A_i \cap A_j \neq \emptyset, 1 \leq i < j \leq n.$$

Example 4.0.2. 1. How many three digit natural numbers can be formed using digits $0, 1, \cdots, 9$? Identify the number of parts in the task and the type of the parts (compulsory or alternative). Which rule applies here?

Ans: The task has three compulsory parts. Part 1: choose a digit for the leftmost place. Part 2: choose a digit for the middle place. Part 3: choose a digit for the rightmost place.



Multiplication rule applies. **Ans:** 900.

2. How many three digit natural numbers with distinct digits can be formed using digits $1, \cdots, 9$ such that each digit is odd or each digit is even? Identify the number of parts in the task and the type of the parts (compulsory or alternative). Which rule applies here?

Ans: The task has two alternative parts. Part 1: form a three digit number with distinct numbers from $\{1, 3, 5, 7, 9\}$ using the odd digits. Part 2: form a three digit number with distinct numbers from $\{2, 4, 6, 8\}$ using the even digits. Observe that Part 1 is a task having three compulsory subparts. In view of 4.0.2, we see that Part 1 can be done in 60 ways. Part 2 is a task having three compulsory subparts. In view of 4.0.2, we see that Part 2 can be done in 24 ways. Since our task has alternative parts, addition rule applies. **Ans:** 84.

Definition 4.0.3. We use the notation $n! = 1 \cdot 2 \cdot \cdots \cdot n$. By convention, we take $0! = 1$.

4.1 Permutations and Combinations

Definition 4.1.1. An r**-sequence** of elements of X is a sequence of length r with elements from X. This may be viewed as a word of length r with alphabets from X or as a function $f : \{1, 2, \ldots, r\} \to X$. We write 'an r-sequence of X' to mean 'an r-sequence of elements of X'.

Theorem 4.1.2. *The number of r-sequences of $\{1, 2, \ldots, n\}$ is n^r.*

Proof. Here the task has r compulsory parts. Choose the first element of the sequence, the second element and so on. ■

EXERCISE **4.1.3.** 1. *In how many ways can r* **distinguishable/distinct** *balls be put into n* **distinguishable/distinct** *boxes?*

2. *How many distinct ways are there to make a 5 letter word using the ENGLISH alphabet*

   (a) *with no restriction?*

   (b) *with ONLY consonants?*

   (c) *with ONLY vowels?*

   (d) *with a consonant as the first letter and a vowel as the second letter?*

   (e) *if the vowels appear only at odd positions?*

3. *Determine the total number of possible outcomes if*

   (a) *two coins are tossed?*

   (b) *a coin and a die are tossed?*

   (c) *two dice are tossed?*

   (d) *three dice are tossed?*

   (e) *k dice are tossed, where $k \in \mathbb{N}$?*

   (f) *five coins are tossed?*

4. *How many 5-letter words using only A's, B's, C's, and D's are there that do not contain the word "CAD"?*

Definition 4.1.4. [r**-permutation,** n**-set**] By an n**-set**, we mean a set containing n elements. An r**-permutation** of an n-set S is an arrangement of r distinct elements of S in a row. An r-permutation may be viewed as a one-one mapping $f : \{1, 2, \ldots, r\} \to S$. An n-permutation of an n-set is simply called a **permutation**.

Example 4.1.5. How many one-one maps $f : \{1, 2, 3, 4\} \to \mathcal{A} = \{A, B, \ldots, Z\}$ are there?

Ans: The task has 4 compulsory parts: select $f(1)$, select $f(2)$, select $f(3)$ and select $f(4)$. Note that $f(2)$ cannot be $f(1)$, $f(3)$ cannot be $f(1)$ or $f(2)$ and so on. Now apply the multiplication rule. **Ans:** $26 \cdot 25 \cdot 24 \cdot 23 = \frac{26!}{22!}$.

Theorem 4.1.6. [Number of r**-permutations]** *The number of r-permutation of an n-set S is $P(n, r) = \frac{n!}{(n-r)!}$.*

Proof. Let us view an r-permutation as a one-one map from $f : \{1, 2, \ldots, r\} \to S$. Here the task has r compulsory tasks: select $f(1)$, select $f(2)$, $\ldots$, select $f(r)$ with the condition, for $2 \le k \le r$, $f(k) \notin \{f(1), f(2), \ldots, f(k-1)\}$. Multiplication rule applies. Hence, the number of r-permutations equals $n(n-1) \cdots (n-r+1) = \frac{n!}{(n-r)!}$. ■

Definition 4.1.7. By $P(n, r)$, we denote the number of r-permutations of $\{1, 2, \ldots, n\}$. By convention, $P(n, 0) = 1$. Some books use the notation $n_{(r)}$ and call it the **falling factorial** of n. Thus, if $r > n$ then $P(n, r) = n_{(r)} = 0$ and if $n = r$ then $P(n, r) = n_{(r)} = n!$.

EXERCISE **4.1.8.**

1. *How many distinct ways are there to make 5 letter words using the ENGLISH alphabet if the letters must be different?*

2. *How many distinct ways are there to arrange the 5 letters of the word ROYAL?*

3. *Determine the number of ways to place 4 couples in a row if each couple seats together.*

4. *How many distinct ways can 8 persons, including Ram and Shyam, sit in a row, with Ram and Shyam sitting next to each other?*

Proposition 4.1.9. **[principle of disjoint pre-images of equal size]** *Let A, B be finite sets and $f : A \to B$ be a function such that for each pair $b_1, b_2 \in B$ we have $|f^{-1}(b_1)| = k = |f^{-1}(b_2)|$ (recall that $f^{-1}(b_1) \cap f^{-1}(b_2) = \emptyset$). Then, $|A| = k|B|$.*

Discussion 4.1.10. Consider the word $AABAB$. Give subscripts to the three As and the two Bs and complete the following list. Notice that each of them will give us $AABAB$ if we erase the subscripts.

$A_1A_2B_1A_3B_2$	$A_1A_2B_1B_2A_3$	$A_1A_2A_3B_1B_2$	$A_1A_2A_3B_2B_1$	$A_1A_2B_2B_1A_3$
$A_1A_2B_2A_3B_1$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$B_2A_3B_1A_1A_2$	$B_2A_3B_1A_2A_1$

Example 4.1.11. How many words of size 5 are there which use three A's and two B's?

Ans: Put $A = \{$arrangements of $A_1, A_2, A_3, B_1, B_2\}$ and $B = \{$words of size 5 which use three A's and two B's$\}$. For each arrangement $a \in A$, define $f(a)$ to be the word in B obtained by erasing the subscripts. Then, the function $f : A \to B$ satisfies:

'for each $b, c \in B, b \neq c$, we have $|f^{-1}(b)| = |f^{-1}(c)| = 3!2!$ and $f^{-1}(b) \cap f^{-1}(c) = \emptyset$'.

Thus, by Proposition 4.1.9, $|B| = \frac{|A|}{3!2!} = \frac{5!}{3!2!}$.

Remark 4.1.12. *Let us fix $n, k \in \mathbb{N}$ with $0 \leq k \leq n$ and ask the question 'how many words of size n are there which uses k many A's and $(n - k)$ many B's'?*
Ans: *Put $A = \{$arrangements of $A_1A_2 \ldots A_kB_1B_2 \ldots B_{n-k}\}$ and $B = \{$words of size n which uses k many A's and $(n - k)$ many B's$\}$ and proceed as above to get*

$$|B| = \frac{|A|}{k!(n-k)!} = \frac{n!}{k!(n-k)!}$$

as the required answer. Observe that the above argument implies $\frac{n!}{k!(n-k)!} \in \mathbb{Z}$. We denote this number by $P(n; k)$. Note that $P(n; k) = P(n; n - k)$, Also, as per convention, $P(n; k) = 0$, whenever $k < 0$ or $n < k$.

The above idea is further generalized below.

Definition 4.1.13. A **multiset** is a collection of objects where an object can appear more than once. So, a set is a multiset. Note that $\{a, a, b, c, d\}$ and $\{a, b, a, c, d\}$ are the same 5-multisets.

Theorem 4.1.14. **[Arrangements]** *Let us fix $n, k \in \mathbb{N}$ with $1 \leq k \leq n$ and let S be a multiset containing $n_i \in \mathbb{N}$ objects of i-th type, for $i = 1, \ldots, k$ with $n = \sum\limits_{i=1}^{k} n_i$. Then, there are $\dfrac{(n_1 + \cdots + n_k)!}{n_1!n_2! \cdots n_k!} = \dfrac{n!}{n_1!n_2! \cdots n_k!}$ arrangements of the objects in S.*

Proof. Assume that S consists of n_i copies of A_i, $i = 1, \ldots, k$. Put
$A = \{A_{11}, \ldots, A_{1n_1}, A_{21}, \ldots, A_{2n_2}$ ________________$\}$ and
$B = \{$words of size ____________ made using elements of ____$\}$. For each arrangement $a \in A$, define $f(a)$ to be the word in B obtained by erasing the right subscripts of the objects of a. Then, the function $f : A \to B$ satisfies:

'for each $b, c \in B$, $b \neq c$, we have $|f^{-1}(b)| = |f^{-1}(c)| =$ ________ and $f^{-1}(b) \cap f^{-1}(c) = \emptyset$'.

Thus, by Proposition 4.1.9, $|B| = \frac{|A|}{n_1! \cdots n_k!} = \frac{(n_1 + \cdots + n_k)!}{n_1! \cdots n_k!} = \frac{n!}{n_1! n_2! \cdots n_k!}$. ■

Theorem 4.1.15. [**Allocation I: distinct locations; identical objects (n_i of type i); at most one per place**] *Fix a positive integer k and for $1 \leq i \leq k$, let G_i's be boxes containing $n_i \in \mathbb{N}$ identical objects. If the objects in distinct boxes are non-identical and $n \geq \sum\limits_{i=1}^{k} n_i$ then, the number of allocations of the objects in n distinct locations $l_1, \ldots, l_n$, each location receiving at most one object, is $\frac{n!}{n_1! \cdots n_k! (n - \sum n_i)!}$.*

Proof. Consider a new group G_{k+1} with $n_{k+1} = n - \sum\limits_{1}^{k} n_i$ objects of a new type. Notice that an allocation of objects from $G_1, \ldots, G_k$ to n distinct places, where each location receives at most one object, gives a unique arrangement of elements of $G_1, \ldots, G_{k+1}$.[1] Thus, the number of allocations of objects from $G_1, \ldots, G_k$ to n distinct places, where each location receives at most one object, is the same as the number of arrangements of elements of $G_1, \ldots, G_{k+1}$. By Theorem 4.1.14, this number is $\frac{n!}{n_1! \cdots n_k! (n - \sum n_i)!}$. ■

Definition 4.1.16. Let $n, n_1, n_2, \ldots, n_k \in \mathbb{N}$. Then, by $P(n; n_1, \ldots, n_k)$, we denote the number

$$\frac{n!}{n_1! \cdots n_k! (n - \sum n_i)!}.$$

Thus, $P(6; 1, 1, 1) = P(6, 3)$. As a convention, $P(n; n_1, \ldots, n_k) = 0$ whenever either $n_i < 0$; for some $i, 1 \leq i \leq k$, or $\sum\limits_{i=1}^{k} n_i > n$. Many texts use $C(n; n_1, \cdots, n_k)$ to mean $P(n; n_1, \cdots, n_k)$. We shall interchangeably use them.

Definition 4.1.17. [*r*-**combination**] An r-**combination** of an n-set S is an r-subset of S. The number of r-subsets of an n-set is denoted by $C(n, r)$. Thus, for any natural number n, $C(n, 0) = C(n, n) = 1$.

Theorem 4.1.18. [**Combination**] $C(n, r) = P(n; r) = \frac{n!}{r!(n-r)!}$.

Proof. By Theorem 4.1.15, the number of allocations of r identical objects in n distinct places $(p_1, \ldots, p_n)$ with each place receiving at most 1 is $P(n; r)$. Note that each such allocation A uniquely corresponds to a r-subset of $\{1, 2, \ldots, n\}$, namely to $\{i \mid p_i \text{ receives an object by } A\}$. Thus, $C(n, r) = P(n; r) = \frac{n!}{r!(n-r)!}$. ■

Example 4.1.19. In how many ways can you allocate 3 identical passes to 10 students so that each student receives at most one? **Ans:** $C(10, 3)$

Theorem 4.1.20. [**Pascal**] $C(n, r) + C(n, r + 1) = C(n + 1, r + 1)$.

[1] Take an allocation of objects from $G_1, \ldots, G_k$ to n distinct places, where each location receives at most one object. There are n_{k+1} locations which are empty. Supply an object from G_{k+1} to each of these locations. We have created an arrangement of elements of $G_1, \ldots, G_{k+1}$. Conversely, take an arrangement of elements of $G_1, \ldots, G_{k+1}$. View this as an allocation of elements of $G_1, \ldots, G_{k+1}$ to n distinct places. Empty the places which have received elements from G_{k+1}. We have created an allocation of elements of $G_1, \ldots, G_k$ to n distinct places, where each location receives at most one object.

Proof. By Theorem 4.1.18, $C(n,r) = \frac{n!}{r!(n-r)!}$. Now verify the above identity to get the result. ■

Experiment

Complete the following list by filling the left list with all 3-subsets of $\{1,2,3,4,5\}$ and the right list with 3-subsets of $\{1,2,3,4\}$ as well as with 2-subsets of $\{1,2,3,4\}$ as shown below.

$$C(5,3)\left\{\begin{array}{l}\{1,2,3\}\\ \\ \\ \{2,3,4\}\\ \{1,2,5\}\\ \\ \\ \\ \{3,4,5\}\end{array}\right. \quad \Bigg\| \quad \begin{array}{l}\left.\begin{array}{l}\{1,2,3\}\\ \\ \\ \{2,3,4\}\end{array}\right\} C(4,3)\\ \left.\begin{array}{l}\{1,2\}\\ \\ \\ \\ \{3,4\}\end{array}\right\} C(4,2)\end{array}$$

Theorem 4.1.21. **[Alternate proof of Pascal's Theorem 4.1.20]** *Here we supply a* **combinatorial proof***, i.e., 'by associating the numbers with objects'. Let $S = \{1,2,\ldots,n,n+1\}$ and A be an $(r+1)$-subset of S. Then, there are $C(n+1,r+1)$ such sets with either $n+1 \in A$ or $n+1 \notin A$.*

Note that $n+1 \in A$ if and only if $A \setminus \{n+1\}$ is an r-subset of $\{1,2,\ldots,n\}$. So, the number of $(r+1)$-subsets of $\{1,2,\ldots,n,n+1\}$ which contain the element $n+1$ is, by definition, $C(n,r)$.

Also, $n+1 \notin A$ if and only if A is an $(r+1)$-subset of $\{1,2,\ldots,n\}$. So, a set A which does not contain $n+1$ can be formed in $C(n,r+1)$ ways. Hence, an $(r+1)$-subset of S can be formed, by definition, in $C(n,r)+C(n,r+1)$ ways. Thus, the required result follows. ■

Experiment

Here we consider subsets of $\{1,2,3,4\}$. Complete the following list by using 0's, 1's, x's and y's, where x and y are commuting ($xy = yx$) symbols.

$\emptyset$	0000	$yyyy = y^4$
$\{1\}$	1000	$xyyy = xy^3$
$\{2\}$	0100	$yxyy = xy^3$
$\{3\}$	0010	$yyxy = xy^3$
$\{4\}$	0001	$yyyx = xy^3$
$\{1,2\}$	1100	$xxyy = x^2y^2$
$\{1,2,3,4\}$	1111	$xxxx = x^4$

Practice **4.1.22.** *Give a combinatorial proof of $C(n,r) = C(n,n-r)$, whenever $n,r \in \mathbb{N}$ with $0 \le r \le n$.*

Theorem 4.1.23. **[Allocation II: distinct locations; distinct objects; n_i at place i]** *The number of ways of allocating objects $o_1,\ldots,o_n$ into pockets $p_1,\ldots,p_k$ so that pocket p_i contains n_i objects, is $P(n;n_1,\ldots,n_k)$.*

Proof. Task has k compulsory parts: select n_1 for pocket p_1 and so on. So, the answer is $C(n,n_1)C(n-n_1,n_2)\cdots C(n-n_1-\cdots-n_{k-1},n_k) = P(n;n_1,\ldots,n_k)$.

Alternate. Take an allocation of $o_1,\ldots,o_n$ into pockets $p_1,\ldots,p_k$ so that the pocket p_i gets n_i objects. This is an allocation of n_1 copies of p_1, $\cdots$, n_k copies of p_k into locations $o_1,\ldots,o_n$ where each location gets exactly one. Hence, the answer is $P(n;n_1,\ldots,n_k)$. ■

Exercise **4.1.24.** *1. In a class there are 17 girls and 20 boys. A committee of 5 students is to be formed to represent the class.*

(a) Determine the number of ways of forming the committee consisting of 5 students.

(b) Suppose the committee also needs to choose two different people from among themselves, who will act as "spokesperson" and "treasurer". In this case, determine the number of ways of forming a committee consisting of 5 students. Note that two committees are different if

i. either the members are different, or

ii. even if the members are the same, they have different students as spokesperson and/or treasurer.

(c) Due to certain restrictions, it was felt that the committee should have at least 3 girls. In this case, determine the number of ways of forming the committee consisting of 5 students (no one is to be designated as spokesperson and/or treasurer).

2. Combinatorially prove the following identities:

(a) $kC(n,k) = nC(n-1,k-1)$.

(b) [**Newton's Identity**] *:* $C(n,r)C(r,k) = C(n,k)C(n-k,r-k)$.

(c) $C(n,r) = C(r,r)C(n-r,0) + C(r,r-1)C(n-r,1) + \cdots + C(r,0)C(n-r,r)$.

(d) $C(n,0)^2 + C(n,1)^2 + \cdots + C(n,n)^2 = C(2n,n)$.

3. Determine the number of ways of selecting a committee of m *people from a group consisting of* n_1 *women and* n_2 *men, with* $n_1 + n_2 \geq m$.

4. Determine the number of ways of arranging the letters of the word

(a) $ABRACADABARAARCADA$.

(b) $KAGARTHALAMNAGARTHALAM$.

5. How many anagrams of $MISSISSIPPI$ *are there so that no two* S *are adjacent?*

6. How many rectangles are there in an $n \times n$ *square? How many squares are there?*

7. Show that a product of n *consecutive natural numbers is always divisible by* $n!$.

8. Show that $(m!)^n$ *divides* $(mn)!$.

9. If n *points are placed on the circumference of a circle and all the lines connecting them are joined, what is the largest number of points of intersection of these lines inside the circle that can be obtained?*

10. Prove that $C(pn, pn-n)$ *is a multiple of* p *in two ways. Hint: Newton's identity.*

11. How many ways are there to form the word MATHEMATICIAN starting from any side and moving only in horizontal or vertical directions?

```
                        M
                      M A M
                    M A T A M
                  M A T H T A M
                M A T H E H T A M
              M A T H E M E H T A M
            M A T H E M A M E H T A M
          M A T H E M A T A M E H T A M
        M A T H E M A T I T A M E H T A M
      M A T H E M A T I C I T A M E H T A M
    M A T H E M A T I C I C I T A M E H T A M
  M A T H E M A T I C I A I C I T A M E H T A M
M A T H E M A T I C I A N A I C I T A M E H T A M
```

12. (a) In how many ways can one arrange n *different books in* m *different boxes kept in a row, if books inside the boxes are also kept in a row?*

(b) What if no box can be empty?

13. Prove by induction that $2^n | (n+1) \cdots (2n)$.

4.1.1 Multinomial theorem

Definition 4.1.25. Let x, y and z be commuting symbols. Then, by an **algebraic expansion**[1] of $(x+y+z)^n$ we mean an expansion where each term is of the form $\alpha x^i y^j z^k$ so that two terms differ in the degree of at least one of x, y, or z. By a **word expansion**[2] of $(x+y+z)^n$ we mean an expansion where each term is a word of length n using symbols x, y, z. Expansions for $(x_1+\cdots+x_r)^n$, whenever x_i's are commuting symbols, may be defined in a similar way.

Example 4.1.26.

1. $x^3+3xy^2+y^3+3yx^2$ is an algebraic expansion of $(x+y)^3$, where as $xxx+xxy+xyx+xyy+yxx+yxy+yyx+yyy$ is a word expansion of $(x+y)^3$.
2. Take the word expansion of $(X+Y+Z)^9$. A term with exactly two X's and exactly three Y's is nothing but an arrangement of two X's, three Y's and four Z's. So, the coefficient of $X^2Y^3Z^4$ in the algebraic expansion of $(X+Y+Z)^9$ is $P(9;2,3,4)$.
3. Consider $(x+y+z)^n = \underbrace{(x+y+z)\cdot(x+y+z)\cdot\cdots\cdot(x+y+z)}_{n \text{ times}}$. Then, in this expression, we need to choose, say

   (a) i places from the n possible places for x $(i \geq 0)$,

   (b) j places from the remaining $n-i$ places for y $(j \geq 0)$, and

   (c) the $n-i-j$ left out places for z (with $n-i-j \geq 0$).

   Thus, we get

$$(x+y+z)^n = \sum_{i,j\geq 0, i+j\leq n} C(n,i)C(n-i,j)x^i y^j z^{n-i-j} = \sum_{i,j\geq 0, i+j\leq n} P(n;i,j)x^i y^j z^{n-i-j}.$$

Theorem 4.1.27. [**Multinomial Theorem**] *Fix a positive integer n and let $x_1, x_2, \ldots, x_n$ be a collection of commuting symbols. Then, for $n = n_1+\cdots+n_k$, the coefficient of $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$ in the algebraic expansion of $(x_1+\cdots+x_k)^n$ is $P(n;n_1,\cdots,n_k)$. So*

$$(x_1+\cdots+x_k)^n = \sum_{\substack{n_1,\ldots,n_k\geq 0\\ n_1+\cdots+n_k=n}} P(n;n_1,\cdots,n_k)\, x_1^{n_1}\cdots x_k^{n_k}.$$

Proof. The proof is left as an exercise for the reader. ■

As a special case, we have the famous binomial theorem.

Corollary 4.1.28. [**Binomial Theorem**] $(x+y)^n = \sum\limits_{k=0}^{n} C(n,k)x^{n-k}y^k$. ‼

Example 4.1.29. Form words of size 5 using letters from 'MATHEMATICIAN' (including multiplicity, that is, you may use M at most twice). How many are there?

Ans: $\displaystyle\sum_{\substack{k_1+\cdots+k_8=5\\ k_1\leq 2,k_2\leq 3,k_3\leq 2,k_4\leq 1,k_5\leq 1,k_6\leq 2,k_7\leq 1,k_8\leq 1}} C(5;k_1,\cdots,k_8).$

EXERCISE **4.1.30.** *1. Show that $|\mathcal{P}(\{1,2,\ldots,n\})| = 2^n$ in the following ways.*

(a) By using Binomial Theorem.

(b) By using 'select a subset is a task with n compulsory parts'.

(c) By associating a subset with a 0-1 string of length n and evaluating their values in base-2.

(d) Arguing in the line of 'a subset of $\{1,2,\ldots,n,n+1\}$ either contains $n+1$ or not' and using induction.

[1] Nonstandard notion

[2] Nonstandard notion

2. *Let S be a set of size n. Then, prove in two different ways that the number of subsets of S of odd size is the same as the number of subsets of S of even size, or equivalently* $\sum\limits_{k\geq 0} C(n,2k) = \sum\limits_{k\geq 0} C(n,2k+1) = 2^{n-1}$.

3. *Prove the following identities on Binomial coefficients.*

   (a) $\sum\limits_{k=\ell}^{n} C(k,\ell)C(n,k) = C(n,\ell)2^{n-\ell}$.

   (b) $C(m+n,\ell) = \sum\limits_{k=0}^{\ell} C(m,k)\ C(n,\ell-k)$.

   (c) $C(n,\ell) = \sum\limits_{k=0}^{t} C(t,k)\ C(n-t,\ell-k) = \sum\limits_{k=0}^{n} C(t,k)\ C(n-t,\ell-k)$, *for any* $t, 0\leq t\leq n$.

   (d) $C(n+r+1,r) = \sum\limits_{\ell=0}^{r} C(n+\ell,\ell)$.

   (e) $C(n+1,r+1) = \sum\limits_{\ell=r}^{n} C(\ell,r)$.

4. *Evaluate* $\sum\limits_{k=0}^{n}(2k+1)\ C(n,2k+1)$ *and* $\sum\limits_{k=0}^{n}(5k+3)\ C(n,2k+1)$, *whenever* $n\geq 3$.

5. **[Generalized Pascal]** *Assume that* $k_1+\cdots+k_m = n$. *Show that*

$$C(n;k_1,\ldots,k_m) = C(n-1;k_1-1,\ldots,k_m)+\cdots+C(n-1;k_1,\ldots,k_m-1).$$

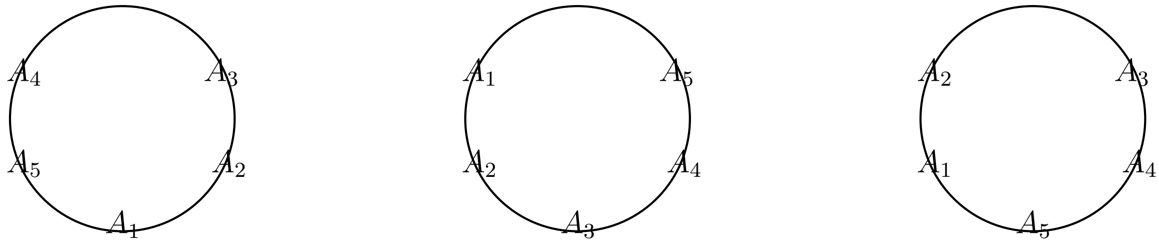
6. *What is* $\sum\limits_{k_1+\ldots+k_m=n} C(n;k_1,\ldots,k_m)$*?*

7. *Put* $l = \lfloor \frac{m}{2} \rfloor$. *What is* $\sum\limits_{k_1+\ldots+k_m=n} (-1)^{k_2+k_4+\cdots+k_{2l}} C(n;k_1,\ldots,k_m)$*?*

4.2 Circular Permutations

Definition 4.2.1. [Circular permutation/arrangement] A **circular permutation** is an arrangement of n distinct objects on a circle. Two circular arrangements are the same if each element has the same 'clockwise adjacent' element. When $|S| = n$, we write 'a circular arrangement of S' to mean 'a circular arrangement of elements of S'. By $[x_1,x_2,\ldots,x_n,x_1]$ we shall denote a circular arrangement keeping the anticlockwise direction in picture.

Example 4.2.2. Exactly two pictures in Figure 4.1 represent the same circular permutation.



$[A_1,A_2,A_3,A_4,A_5,A_1]$ $[A_1,A_5,A_4,A_3,A_2,A_1]$

Figure 4.1: Circular permutations

Example 4.2.3. Determine the number of circular permutations of $X = \{A_1,A_2,A_3,A_4,A_5\}$?

Ans: 4!. *Proof.* Let $B = \{\text{circular permutations of } X\}$ and $A = \{\text{permutations of } X\}$. Now, define $f: A\to B$ as $f(a) = b$ if a is obtained by breaking the cycle b at some gap and then following in the anticlockwise direction. For example, if we break the leftmost circular permutation in Figure 4.1 at the gap between A and B, we get $[A_2, A_3, A_4, A_5, A_1]$. Notice that $|f^{-1}(b)| = 5$, for each $b \in B$. Further if $b, c \in B$, then $f^{-1}(b) \cap f^{-1}(c) = \emptyset$ (why?[1]). Thus, by the principle of disjoint pre-images of equal size, the number of circular permutations is $5!/5$. ■

Theorem 4.2.4. [Circular permutations] *The number of circular permutations of* $\{1, 2, \ldots, n\}$ *is* $(n-1)!$.

Proof. A proof may be obtained on the line of the previous example. Here we give an alternate proof. Put $A = \{$circular permutations of $\{1, 2, 3, 4, 5\}\}$. Put $B = \{$permutations of $\{1, 2, 3, 4\}\}$. Define $f : A \to B$ as $f([5, x_1, x_2, x_3, x_4, 5]) = [x_1, x_2, x_3, x_4]$. Define $g : B \to A$ as $g([x_1, x_2, x_3, x_4]) = [5, x_1, x_2, x_3, x_4, 5]$. Then, $g \circ f(a) = a$, for each $a \in A$ and $f \circ g(b) = b$, for each $b \in B$. Hence, by the bijection principle (see Theorem 1.2.30) f is a bijection. ■

Example 4.2.5. Find the number of circular arrangements of $\{A, B, B, C, C, D, D, E, E\}$.

Ans: There is only one A. Cutting A out from a circular arrangement we get a unique arrangement of $\{B, B, C, C, D, D, E, E\}$. So, the required answer is $\frac{8!}{2!^4}$.

Definition 4.2.6. [Rotation, Orbit size]

1. Given an arrangement $[X_1, \ldots, X_n]$, by a **rotation** $R_1([X_1, \ldots, X_n])$, in short $R_1(X_1, \ldots, X_n)$, we mean $[X_2, \ldots, X_n, X_1]$ and by $R_2(X_1, \ldots, X_n)$ we mean $[X_3, \ldots, X_n, X_1, X_2]$. On similar lines, we define R_i, $i \in \mathbb{N}$ and put $R_0(X_1, \ldots, X_n) = [X_1, \ldots, X_n]$. Thus, for each $k \in \mathbb{N}$,
$$R_0(X_1, \ldots, X_n) = R_{kn}(X_1, \ldots, X_n) = [X_1, \ldots, X_n].$$

2. The **orbit size** of an arrangement $[X_1, \ldots, X_n]$ is the smallest positive integer i which satisfies $R_i(X_1, \ldots, X_n) = [X_1, \ldots, X_n]$. In that case, we call
$$\Big\{R_0(X_1, \ldots, X_n), R_1(X_1, \ldots, X_n), \ldots, R_{i-1}(X_1, \ldots, X_n)\Big\}$$
the **orbit** of $[X_1, \ldots, X_n]$.

Example 4.2.7.

1. We have $R_1(ABCABCABC) = [BCABCABCA]$, $R_2(ABCABCABC) = [CABCABCAB]$ and $R_3(ABCABCABC) = [ABCABCABC]$. Thus, orbit size of $ABCABCABC$ is 3.

2. An arrangement of $S = \{A, A, B, B, C, C\}$ with orbit size 6 is $[AABCBC]$. An arrangement of S with orbit size 3 is $[ACBACB]$.

3. There is no arrangement of $\{A, A, B, B, C, C\}$ with orbit size 2. In fact, if $[X_1X_2 \cdots X_6]$ is an arrangement with orbit size 2 then, $[X_1X_2X_3X_4X_5X_6] = [X_3X_4X_5X_6X_1X_2]$. Thus, $X_1 = X_3 = X_5$ which is not possible.

4. There is no arrangement of $\{A, A, B, B, C, C\}$ with orbit size 1 or 2 or 4 or 5.

5. There are 3! arrangements of $\{A, A, B, B, C, C\}$ with orbit size 3.

6. Take an arrangement of $\{A, A, B, B, C, C\}$ with orbit size 3. Make a circular arrangement by joining the ends. How many distinct arrangements can we generate by breaking the circular arrangement at gaps?

   Ans: 3. They are the elements of the same orbit.

[1] Think of creating the circular permutation from a given permutation.

7. Take an arrangement of $\{A, A, B, B, C, C\}$ with orbit size 6. Make a circular arrangement by joining the ends. How many distinct arrangements can we generate by breaking the circular arrangement at gaps?

   Ans: 6. They are the elements of the same orbit.

8. Take an arrangement of n elements with orbit size k. Make a circular arrangement by joining the ends. How many distinct arrangements can we generate by breaking the circular arrangement at gaps?

   Ans: k. They are the elements of the same orbit.

9. If we take the set of all arrangements of a finite multiset and group them into orbits (notice that each orbit gives us exactly one circular arrangement), then the number of orbits is the number of circular arrangements.

Example 4.2.8. Find the number of circular arrangements of $S = \{A, A, B, B, C, C, D, D, E, E\}$.

Ans: There are two types of arrangements of S: one of orbit size 10 and the other of orbit size 5. The number of arrangements of S with orbit size 5 is 5!. So, they can generate 4! distinct circular arrangements. The number of arrangements of S with orbit size 10 is $\frac{10!}{2!2!2!2!2!} - 5!$. Hence, they can generate $\frac{10!}{2!2!2!2!2!10} - \frac{5!}{10}$ distinct circular arrangements. Thus, the total number of circular arrangements is $4! + \frac{10!}{2!2!2!2!2!10} - \frac{5!}{10}$.

Example 4.2.9. Suppose, we are given an arrangement $[X_1, \dots, X_{10}]$ of five A's and five B's. Can it have an orbit size 3?

Ans: No. To see this assume that it's orbit size is 3. Then,

$$[X_1, \dots, X_{10}] = R_3(X_1, \dots, X_{10}) = R_6(X_1, \dots, X_{10}) = R_9(X_1, \dots, X_{10}) = R_2(X_1, \dots, X_{10}).$$

Since 3 was the least positive integer with $R_3(X_1, \dots, X_{10}) = [X_1, \dots, X_{10}]$, we arrive at a contradiction. Hence, the orbit size cannot be 3.

Proposition 4.2.10. *The orbit size of an arrangement of an n-multiset is a divisor of n.*

Proof. Suppose, the orbit size of $[X_1, \dots, X_n]$ is k and $n = kp + r$, for some $r, 0 < r < k$. Then,

$$R_k(X_1, \dots, X_n) = R_{2k}(X_1, \dots, X_n) = \cdots = R_{kp}(X_1, \dots, X_n) = R_{k-r}(X_1, \dots, X_n).$$

Thus, $R_{k-r}(X_1, \dots, X_n) = [X_1, \dots, X_n]$, contradicting the minimality of k. Hence, a contradiction and therefore $r = 0$. Or equivalently, k divides n. ■

Proposition 4.2.11. *Let $S_1 = \{P_{i_1}, P_{i_2}, \dots, P_{i_k}\}$ and $S_2 = \{P_{j_1}, P_{j_2}, \dots, P_{j_l}\}$ be any two orbits of certain arrangements of an n-multiset. Then, either $S_1 \cap S_2 = \emptyset$ or $S_1 = S_2$.*

Proof. If $S_1 \cap S_2 = \emptyset$, then there is nothing to prove. So, let there exists an arrangement $P_t \in S_1 \cap S_2$. Then, by definition, there exist rotations R_1 and R_2 such that $R_1(P_{i_1}) = P_t$ and $R_2(P_{j_1}) = P_t$. Thus, $R_2^{-1}(P_t) = P_{j_1}$ and hence $R_2^{-1}(R_1(P_{i_1})) = R_2^{-1}(P_t) = P_{j_1}$. Therefore, we see that the arrangement $P_{j_1} \in S_1$ and hence $S_2 \subseteq S_1$. A similar argument implies that $S_1 \subseteq S_2$ and hence $S_1 = S_2$. ■

Definition 4.2.12. **[Binary operation]** Let $[X_1, \dots, X_n]$ and $[Y_1, \dots, Y_n]$ be two arrangements of an n-multiset. Then, in the remainder of this section,

1. we shall consider expressions like $[X_1, \dots, X_n] + [Y_1, \dots, Y_n]$.

2. by $[R_i + R_j](X_1, \dots, X_n)$, we mean the expression $R_i(X_1, \dots, X_n) + R_j(X_1, \dots, X_n)$.

3. by $R_i([X_1, \dots, X_n] + [Y_1, \dots, Y_n])$ we denote the expression $R_i(X_1, \dots, X_n) + R_i(Y_1, \dots, Y_n)$.

Example 4.2.13. Think of all arrangements $P_1, \ldots, P_n$, $n = \frac{6!}{3!3!}$, of three A's and three B's. How many copies of $[ABCABC]$ are there in $[R_0 + \cdots + R_5](P_1 + \cdots + P_n)$?

Ans: Of course 6. To see this, note that R_0 takes $[ABCABC]$ to itself; R_1 will take $[CABCAB]$ to $[ABCABC]$; R_2 will take $[BCABCA]$ to $[ABCABC]$; and so on.

Example 4.2.14. Let $P = [X_1, \ldots, X_{12}]$ be an arrangement of a 12-multiset with orbit size 3. Since, the orbit size of P is 3, the set $S = \{P, R_1(P), R_2(P)\}$ forms the orbit of P. Thus, the rotations R_0, R_3, R_6 and R_9 fix each element of S, *i.e.*, $R_i(R_j(P)) = R_j(P)$ for all $i \in \{0, 3, 6, 9\}$ and $j \in \{0, 1, 2\}$. In other words, $[R_0 + \cdots + R_{11}](P)$ accounts for $\underline{4}$ counts of the same circular arrangement, where 4 is nothing but the number of rotations fixing P. Thus, we see that

$$\begin{aligned}
[R_0 + R_1 + \quad \cdots \quad & + R_{11}](P + R_1(P) + R_2(P)) \\
&= [R_0 + R_1 + \cdots R_{11}](P) + [R_0 + R_1 + \cdots R_{11}](R_1(P)) \\
&\qquad\qquad + [R_0 + R_1 + \cdots R_{11}](R_2(P)) \\
&= 4(P + R_1(P) + R_2(P)) + 4(P + R_1(P) + R_2(P)) + 4(P + R_1(P) + R_2(P)) \\
&= 12(P + R_1(P) + R_2(P))
\end{aligned}$$

The proof of the next result is similar to the idea in the above example and hence is omitted.

Proposition 4.2.15. *Let $P_1, \ldots, P_n$ be all the arrangements of an m-multiset. Then,*

$$[R_0 + \cdots + R_{m-1}](P_1 + \cdots + P_n) = m(P_1 + \cdots + P_n).$$

Let P be an arrangement of an m-multiset with orbit size k. Then, by Proposition 4.2.10 k divides m. Now, from the understanding obtained from the above example, we note that $[R_0 + \cdots + R_{m-1}](P)$ accounts for $\dfrac{m}{k}$ counts of the same circular arrangement, where $\dfrac{m}{k}$ is nothing but 'the number of rotations fixing P'. Also, by Proposition 4.2.11, we know that two orbits are either disjoint or the same and hence the next two results are immediate. Therefore, the readers are supposed to provide a proof of the following results.

Discussion 4.2.16. Let $P_1, \ldots, P_n$ be all the arrangements of an m-multiset. Then,

$$\begin{aligned}
\sum_{P_i} \text{the number of rotations fixing } P_i &= \sum_{P_i} [R_0 + \cdots + R_{m-1}](P_i) \\
&= m(P_1 + \cdots + P_n) \\
&= m(\text{the number of circular arrangements}).
\end{aligned}$$

Discussion 4.2.17. Let $P_1, \ldots, P_n$ be all the arrangements of an m-multiset and $\{R_0, R_1, \ldots, R_{m-1}\}$ the set of all rotations. Then,

$$\begin{aligned}
\sum_{P_i} \text{the number of rotations fixing } P_i &= \sum_{P_i} |\{R_j \mid R_j(P_i) = P_i\}| = |\{(P_i, R_j) \mid R_j(P_i) = P_i\}| \\
&= \sum_{R_j} |\{P_i \mid R_j(P_i) = P_i\}| \\
&= \sum_{R_j} \text{the number of } P_i\text{'s fixed by } R_j.
\end{aligned}$$

Hence, using Discussion 4.2.16, the number of circular arrangements is

$$\frac{1}{m} \sum_{R_j \text{ a rotation}} \text{the number of } P_i\text{'s fixed by } R_j.$$

Example 4.2.18.

1. How many circular arrangements of $\{A, A, A, B, B, B, C, C, C\}$ are there?

   Ans: R_0 fixes $\frac{9!}{3!3!3!}$ arrangements, None of R_1, R_2, R_4, R_5, R_7 andR_8 fixes any arrangement, R_3 and R_6 fixes $3!$ arrangements, namely the $3!$ arrangements of X, Y, Z, where $X = AAA, Y = BBB$ and $Z = CCC$.

   Thus, the number of circular arrangements is $\frac{1}{9}\left[\frac{9!}{3!3!3!} + 3! + 3!\right] = \frac{5\cdot6\cdot7\cdot8+12}{9} = \frac{564}{3} = 188.$

2. Determine the number of circular arrangements of size 5 using the alphabets A, B and C.

   Ans: In this case, R_0 fixes all the 3^5 arrangements. The rotations R_1, R_2, R_3 and R_4 fixes the arrangements $AAAAA, BBBBB$ and $CCCCC$. Hence, the required number is $\frac{1}{5}\left(3^5 + 4 \cdot 3\right) = 51$.

   Verify that the answer will be 8 if we have just two alphabets A and B.

EXERCISE **4.2.19.**

1. *If there are n girls and n boys then what is the number of ways of making them sit around a circular table in such a way that no two girls are adjacent and no two boys are adjacent?*

2. *Persons $P_1, \ldots, P_{100}$ are seating on a circle facing the center and talking. If P_i talks lie, then the*

   (a) *person to his right talks truth. So, the minimum number of persons talking truth is ______.*

   (b) *second person to his right talks truth'? So, the minimum number of persons talking truth is ______.*

   (c) *next two persons to his right talk truth'? So, the minimum number of persons talking truth is ______.*

3. *Let us assume that any two garlands are same if one can be obtained from the other by rotation. Then, determine the number of distinct garlands that can be formed using 6 flowers, if the flowers*

   (a) *are of 2 colors, say 'red' and 'blue'.*

   (b) *are of 3 different colors.*

   (c) *are of k different colors, for some $k \in \mathbb{N}$.*

   (d) *of 'red' color are 2 and that of 'blue' color is 4.*

4. *Find the number of circular permutations of $\{A, A, B, B, C, C, C, C\}$.*

4.3 Solutions in Non-negative Integers

Definition 4.3.1. [Solution in non-negative integers] Recall that $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. A point $\mathbf{p} = (p_1, \ldots, p_k) \in \mathbb{N}_0^k$ with $p_1 + \cdots + p_k = n$ is called a solution of the equation $x_1 + \cdots + x_k = n$ in non-negative integers or a solution of $x_1 + \cdots + x_k = n$ in $\mathbb{N}_0$. Two solutions $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_k)$ are said to be the same if $p_i = q_i$, for each $i = 1, \ldots, k$. Thus, $(5, 0, 0, 5)$ and $(0, 0, 5, 5)$ are two different solutions of $x + y + z + t = 10$ in $\mathbb{N}_0$.

Example 4.3.2. Determine the number of

1. words which uses 3 A's and 6 B's.

2. arrangements of 3 A's and 6 B's.

3. distinct strings that can be formed using 3 A's and 6 B's.

4. solutions of the equation $x_1 + x_2 + x_3 + x_4 = 6$, where each $x_i \in \mathbb{N}_0$ and $0 \le x_i \le 6$.

5. ways of placing 6 indistinguishable balls into 4 distinguishable boxes.

6. 3 subsets of an 9-set.

   Ans: Observe that all the problems correspond to forming strings using +'s (or |'s or bars) and 1's (or balls or dots) in place of A'a and B's, respectively?

$BBABBBABA$	$11 + 111 + 1 + = 2 + 3 + 1 + 0$	• • | • • • | • |
$ABBBBBAAB$	$+11111 + +1 = 0 + 5 + 0 + 1$	| • • • • • | | •
$ABBBABABB$	$+111 + 1 + 11 = 0 + 3 + 1 + 2$	| • • • | • | • •

Figure 4.2: Understanding the three problems

   Note that the A's are indistinguishable among themselves and the same holds for B's. Thus, we need to find 3 places, from the $9 = 3 + 6$ places, for the A's. Hence, the answer is $C(9, 3)$. The answer will remain the same as we just need to replace A's with +'s (or |'s) and B's with 1's (or balls) in any string of 3 A's and 6 B's. See Figure 4.2 or note that four numbers can be added using 3 +'s or four adjacent boxes can be created by putting 3 vertical lines or |'s.

In general, we have the following result.

Theorem 4.3.3. [**solutions in** $\mathbb{N}_0$] *The number of solutions of* $x_1 + \cdots + x_r = n$ *in* $\mathbb{N}_0$ *is* $C(n+r-1, n)$.

Proof. Each solution $(x_1, \ldots, x_r)$ may be viewed as an arrangement of n dots and $r - 1$ bars.

'Put x_1 many dots; put a bar; put x_2 many dots; put another bar; continue; and end by putting x_r many dots.'

For example, $(0, 2, 1, 0, 0)$ is associated to $|{\bullet}{\bullet}|{\bullet}||$ and vice-versa. Thus, there are $C(n+r-1, r-1)$ arrangements of n dots and $r - 1$ bars. ■

Theorem 4.3.4. *(a) The number of solutions of* $x_1 + \cdots + x_r \le n$ *in non-negative integers is* $C(n + r, n)$.

(b) The number of terms in the algebraic expansion of $(x_1 + \cdots + x_r)^n$ *is* $C(n + r - 1, n)$.

Proof. (a) Any solution of $x_1 + \cdots + x_r \le n$ uniquely corresponds to a solution of $x_1 + \cdots + x_r + y = n$ in non-negative integers..

(b) Note that each term in the algebraic expansion of $(x_1 + \cdots + x_r)^n$ has the form $x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}$, with $i_1 + i_2 + \cdots + i_r = n$. Thus, each term uniquely corresponds to a solution of $i_1 + i_2 + \cdots + i_r = n$ in non-negative integers. ■

Theorem 4.3.5. [r**-multiset**] *The number of* r*-multisets of elements of* $\{1, 2, \ldots, n\}$ *is* $C(n + r - 1, n - 1)$.

Proof. Let A be an r-multiset. Let d_i be the number of copies of i in A. Then, any solution of $d_1 + \cdots + d_n = r$ in non-negative integers gives A uniquely. Hence, the conclusion.

Alternate. Put $A = \{$arrangements of $n-1$ dots and r bars$\}$. Put $B = \{r$-multisets of $\{1, 2, \ldots, n\}\}$. For $a \in A$, define $f(a)$ to be the multiset

$$f(a) = \{d(i) + 1 \mid \text{ where } d(i) \text{ is the number of dots to the left of the } i\text{-th bar}\}.$$

For example, $|| \bullet \bullet | \bullet ||$ gives us $\{1, 1, 3, 4, 4\}$. It is easy to define $g : B \to A$ so that $f(g(b)) = b$, for each $b \in B$ and $g(f(a)) = a$, for each $a \in A$. Thus, by the bijection principle (see Theorem 1.2.30), $|A| = |B|$. Also, we know that $|A| = C(n + r - 1, n - 1)$ and hence the required result follows. ■

Example 4.3.6. 1. There are 5 kinds of ice-creams available in our market complex. In how many ways can you buy 15 of them for a party?

Ans: Suppose you buy x_i ice-creams of the i-th type. Then, the problem is the same as finding the number of solutions of $x_1 + \cdots + x_5 = 15$ in non-negative integers.

2. How many solutions in $\mathbb{N}_0$ are there to $x + y + z = 60$ such that $x \geq 3, y \geq 4, z \geq 5$?

Ans: (x, y, z) is such a solution if and only if $(x - 3, y - 4, z - 5)$ is a solution to $x + y + z = 48$ in $\mathbb{N}_0$. So, answer is $C(50, 2)$.

3. How many solutions in $\mathbb{N}_0$ are there to $x + y + z = 60$ such that $20 \geq x \geq 3, 30 \geq y \geq 4, 40 \geq z \geq 5$?

Ans: We are looking for solution in $\mathbb{N}_0$ of $x + y + z = 48$ such that $x \leq 17, y \leq 26$ and $z \leq 35$. Let $A = \{(x, y, z) \in \mathbb{N}_0^3 \mid x + y + z = 48\}$, $A_x = \{(x, y, z) \in \mathbb{N}_0^3 \mid x + y + z = 48, x \geq 18\}$, $A_y = \{(x, y, z) \in \mathbb{N}_0^3 \mid x + y + z = 48, y \geq 27\}$ and $A_z = \{(x, y, z) \in \mathbb{N}_0^3 \mid x + y + z = 48, z \geq 36\}$. We know that $|A| = C(50, 2)$. Our answer is then $C(50, 2) - |A_x \cup A_y \cup A_z|$. Very soon we will learn to find the value of $|A_x \cup A_y \cup A_z|$.

EXERCISE **4.3.7.** *1. Determine the number of solutions of $x + y + z = 7$ with $x, y, z \in \mathbb{N}$?*

2. Find the number of allocations of n identical objects to r distinct locations so that location i gets at least $p_i \geq 0$ elements, $i = 1, 2, \cdots, r$.

3. In how many ways can we pick integers $x_1 < x_2 < x_3 < x_4 < x_5$, from $\{1, 2, \ldots, 20\}$ so that $x_i - x_{i-1} \geq 3$, $i = 2, 3, 4, 5$? Solve in three different ways.

4. Find the number of solutions in non-negative integers of $a + b + c + d + e < 11$.

5. In a room, there are 2 distinct book racks with 5 shelves each. Each shelf is capable of holding up to 10 books. In how many ways can we place 10 distinct books in two racks?

6. How many 4-letter words (with repetition) are there with the letters in alphabetical order?

7. Determine the number of non-decreasing sequences of length r using the numbers $1, 2, \ldots, n$.

8. In how many ways can m indistinguishable balls be put into n distinguishable boxes with the restriction that no box is empty.

9. How many 26-letter permutations of the ENGLISH alphabets have no 2 vowels together?

10. How many 26-letter permutations of the ENGLISH alphabets have at least two consonants between any two vowels?

11. How many ways are there to select 10 integers from the set $\{1, 2, \ldots, 100\}$ such that the positive difference between any two of the 10 integers is at least 3.

12. How many 10-element subsets of the ENGLISH alphabets do not have a pair of consecutive letters?

13. How many 10-element subsets of the ENGLISH alphabets have a pair of consecutive letters?

14. How many ways are there to distribute 50 balls to 5 persons if Ram and Shyam together get no more than 30 and Mohawk gets at least 10?

15. How many arrangements of the letters of KAGARTHALAMNAGARTHALAM have no 2 vowels adjacent?

16. How many arrangements of the letters of RECURRENCERELATION have no 2 vowels adjacent?

17. *How many ways are there to arrange the letters in $ABRACADABARAARCADA$ such that the first*

    (a) *A precedes the first B?*

    (b) *B precedes the first A and the first D precedes the first C?*

    (c) *B precedes the first A and the first A precedes the first C?*

18. *How many ways are there to arrange the letters in $KAGARTHALAMNAGARTHATAM$ such that the first*

    (a) *A precedes the first T?*

    (b) *M precedes the first G and the first H precedes the first A?*

    (c) *M precedes the first G and the first T precedes the first G?*

19. *In how many ways can we pick* 20 *letters from* 10 *A's,* 15 *B's and* 15 *C's?*

20. *Determine the number of ways to sit* 10 *men and* 7 *women so that no* 2 *women sit next to each other?*

21. *How many ways can* 8 *persons, including Ram and Shyam, sit in a row with Ram and Shyam not sitting next to each other?*

22. *Evaluate* $\sum\limits_{i_1=1}^{n}\sum\limits_{i_2=1}^{i_1}\sum\limits_{i_3=1}^{i_2}\cdots\sum\limits_{i_k=1}^{i_{k-1}} 1.$

23. *Evaluate* $\sum\limits_{i_1=1}^{9}\sum\limits_{i_2=1}^{i_1}\sum\limits_{i_3=1}^{i_2}\cdots\sum\limits_{i_9=1}^{i_8} i_9^2.$

4.4 Set Partitions

Recall that a partition of a set S is a collection of pairwise disjoint nonempty subsets whose union is S. For clarity, let us look at a few examples once again.

Example 4.4.1. (a) $\big\{\{1,2\},\{3\},\{4,5,6\}\big\}$, $\big\{\{1,3\},\{2\},\{4,5,6\}\big\}$ and $\big\{\{1,2,3,4\},\{5\},\{6\}\big\}$ are both partitions of $\{1,2,3,4,5,6\}$ into 3 subsets.

(b) There are $2^{n-1}-1$ partitions of $\{1,2,\ldots,n\}$, $n \geq 2$ into two subsets. To see this, observe that for each nontrivial subset $A \in \mathcal{P}(\{1,2,\ldots,n\})$, the set $\{A, A^c\}$ is a partition of $\{1,2,\ldots,n\}$ into two subsets. Since, the total number of nontrivial subsets of $\mathcal{P}(\{1,2,\ldots,n\})$ equals 2^n-2, the required result follows.

(c) Number of allocations of 7 students into 7 different project groups so that each group has one student, is $7! = C(7;1,1,1,1,1,1,1)$ but the number of partitions of a set of 7 students into 7 subsets is 1.

(d) In how many ways can I write $\Big\{\{1,2\},\{3,4\},\{5,6\},\{7,8,9\},\{10,11,12\}\Big\}$ on a piece of paper, with the condition that sets have to be written in a row in increasing size?

Ans: Let us write a few first.

$\Big\{\{1,2\},\{3,4\},\{5,6\},\{7,8,9\},\{10,11,12\}\Big\}$	correct
$\Big\{\{2,1\},\{3,4\},\{5,6\},\{7,8,9\},\{10,11,12\}\Big\}$	correct
$\Big\{\{5,6\},\{3,4\},\{1,2\},\{10,11,12\},\{9,7,8\}\Big\}$	correct
$\Big\{\{2,3\},\{1,4\},\{5,6\},\{7,8,9\},\{10,11,12\}\Big\}$	incorrect, not the same partition
$\Big\{\{2,1\},\{3,4\},\{7,8,9\},\{5,6\},\{10,11,12\}\Big\}$	incorrect, not satisfying the condition

There are $3!(2!)^3 \times 2!(3!)^2$ ways. Notice that from each written partition, if I remove the brackets I get an arrangement of elements of $\{1,2,\ldots,12\}$.

(e) How many arrangements do I generate from a partition with p_i subsets of size n_i, $n_1 < \cdots < n_k$?

Ans: $p_1!(n_1!)^{p_1}\cdots p_k!(n_k!)^{p_k} = \displaystyle\prod_{i=1}^{k}[p_i!(n_i!)^{p_i}]$.

Theorem 4.4.2. [**Set partition**] *The number of partitions of* $\{1,2,\ldots,n\}$ *with* p_i *subsets of size* n_i, $n_1 < \cdots < n_k$ *is*

$$\frac{n!}{(n_1!)^{p_1}p_1!\cdots(n_k!)^{p_k}p_k!}.$$

Proof. Note that each such partition generates $\prod\limits_{i=1}^{k}[p_i!(n_i!)^{p_i}]$ arrangement of elements of $\{1,2,\ldots,n\}$. Conversely, for each arrangement of elements of $\{1,2,\ldots,n\}$ we can easily construct a partition of the above type which can generate this arrangement. Thus, the proof is complete. ■

Definition 4.4.3. Stirling numbers of the second kind, denoted $S(n,r)$, is the number of partitions of $\{1,2,\ldots,n\}$ into r-subsets (r-parts). By convention, $S(n,r)=1$, if $n=r$ and 0, whenever either '$n>0$ and $r=0$' or '$n<r$'.

Theorem 4.4.4. [**recurrence for** $S(n,r)$] $S(n+1,r) = S(n,r-1) + rS(n,r)$.

Proof. Write an r-partition of $\{1,2,\ldots,n,n+1\}$ and erase $n+1$ from it. That is, if $\{n+1\}$ is an element of an r-partition, then the number of such partitions become $S(n,r-1)$; else $n+1$ appears in one of the element of an r-partition of $\{1,2,\ldots,n\}$, which gives the number $rS(n,r)$. ■

Example 4.4.5. Determine the number of ways of putting n distinguishable/distinct balls into r indistinguishable boxes with the restriction that no box is empty.

Ans: Let A be the set of n distinct balls and let the balls in i-th box be B_i, $1 \le i \le r$.

1. Since each box is non-empty, each B_i is non-empty.

2. Also, each ball is in some box and hence $\bigcup\limits_{i=1}^{r} B_i = A$.

3. As the boxes are indistinguishable, we arrange the boxes in non-increasing order, *i.e.*, $|B_1| \ge \cdots \ge |B_r|$.

Thus, $B_1, B_2, \ldots, B_r$ is a partition of A into r-parts. Hence, the required number of ways is given by $S(n,r)$, the Stirling number of the second kind.

To proceed further, consider the following example.

Example 4.4.6. Let $A = \{a, b, c, d, e\}$ and $S = \{1, 2, 3\}$. Define an onto function $f : A \to S$ by $f(a) = f(b) = f(c) = 1, f(d) = 2$ and $f(e) = 3$. Then, f gives a partition $B_1 = \{a, b, c\}, B_2 = \{d\}$ and $B_3 = \{e\}$ of A into 3-parts. Also, let $A_1 = \{a, d\}, A_2 = \{b, e\}$ and $A_3 = \{c\}$ be a partition of A into 3-parts. Then, this partition gives 3! onto functions from A into S, each of them being a one-to-one function from $\{A_1, A_2, A_3\}$ to S, namely,

$$\begin{array}{lcl}
f_1(a) = f_1(d) = 1,\ f_1(b) = f_1(e) = 2, f_1(c) = 3, & \Leftrightarrow & f_1(A_1) = 1, f_1(A_2) = 2, f_1(A_3) = 3 \\
f_2(a) = f_2(d) = 1,\ f_2(b) = f_2(e) = 3, f_2(c) = 2, & \Leftrightarrow & f_2(A_1) = 1, f_2(A_2) = 3, f_2(A_3) = 2 \\
f_3(a) = f_3(d) = 2,\ f_3(b) = f_3(e) = 1, f_3(c) = 3, & \Leftrightarrow & f_3(A_1) = 2, f_3(A_2) = 1, f_3(A_3) = 3 \\
f_4(a) = f_4(d) = 2,\ f_4(b) = f_4(e) = 3, f_4(c) = 1, & \Leftrightarrow & f_4(A_1) = 2, f_4(A_2) = 3, f_4(A_3) = 1 \\
f_5(a) = f_5(d) = 3,\ f_5(b) = f_5(e) = 1, f_5(c) = 2, & \Leftrightarrow & f_5(A_1) = 3, f_5(A_2) = 1, f_5(A_3) = 2 \\
f_6(a) = f_6(d) = 3,\ f_6(b) = f_6(e) = 2, f_6(c) = 1, & \Leftrightarrow & f_6(A_1) = 3, f_6(A_2) = 2, f_6(A_3) = 1.
\end{array}$$

Lemma 4.4.7. *The total number of onto functions $f : \{1, 2, \ldots, r\} \to \{1, 2, \ldots, n\}$ is $n!S(r, n)$.*

Proof. 'f is onto' means 'for all $y \in \{1, 2, \ldots, n\}$ there exists $x \in \{1, 2, \ldots, r\}$, such that $f(x) = y$'. Therefore, the number of onto functions is 0, whenever $r < n$. So, we assume that $r \geq n$. Then,

1. for each $i \in \{1, 2, \ldots, n\}$, $f^{-1}(i) = \{x \in \{1, 2, \ldots, r\} \mid f(x) = i\}$ is a non-empty set (f is onto).
2. $f^{-1}(i) \cap f^{-1}(j) = \emptyset$, whenever $1 \leq i \neq j \leq n$ (f is a function).
3. $\bigcup\limits_{i=1}^{n} f^{-1}(i) = \{1, 2, \ldots, r\}$ (domain of f is $\{1, 2, \ldots, r\}$).

Therefore, $f^{-1}(i)$'s give a partition of $\{1, 2, \ldots, r\}$ into n-parts. Also, note that each such function f, gives a one-to-one function from $\{f^{-1}(1), \ldots, f^{-1}(r)\}$ to $\{1, 2, \ldots, n\}$.

Conversely, for each partition $A_1, A_2, \ldots, A_n$ of $\{1, 2, \ldots, r\}$ into n-parts, we get $n!$ one-to-one function from $\{A_1, A_2, \ldots, A_n\}$ to $\{1, 2, \ldots, n\}$. Hence,

$$\begin{aligned}
&\big|\{f : \{1, 2, \ldots, r\} \to \{1, 2, \ldots, n\} \mid f \text{ is onto}\}\big| = \\
&\qquad \big|\{g : \{A_1, A_2, \ldots, A_n\} \to \{1, 2, \ldots, n\} \mid g \text{ is one-to-one}\}\big| \times \\
&\qquad\qquad \big|\text{Partition of } \{1, 2, \ldots, r\} \text{ into } n\text{-parts}\big| = n!\ S(r, n).
\end{aligned}$$

Thus, the required result follows. ■

Lemma 4.4.8. *Let $r, n \in \mathbb{N}$ and $\ell = \min\{r, n\}$. Then,*

$$n^r = \sum_{k=1}^{\ell} C(n, k)k!S(r, k). \tag{4.1}$$

Proof. Let $A = \{f \mid f : \{1, 2, \ldots, r\} \to \{1, 2, \ldots, n\}\}$. We compute $|A|$ by two different methods.
Method 1: By Theorem 4.1.2, $|A| = n^r$.
Method 2: Let $f_0 : \{1, 2, \ldots, r\} \to \{1, 2, \ldots, n\}$ be any function. Then, f_0 is an onto function from $\{1, 2, \ldots, r\}$ to Im $(f_0) = f_0(\{1, 2, \ldots, r\})$. Moreover, , for some $k, 1 \leq k \leq \ell = \min\{r, n\}$. Thus, $A = \bigcup\limits_{k=1}^{\ell} A_k$, where $A_k = \{f : \{1, 2, \ldots, r\} \to \{1, 2, \ldots, n\} \mid |f(\{1, 2, \ldots, r\})| = k\}$ and $A_k \cap A_j = \emptyset$, whenever $1 \leq j \neq k \leq \ell$. Now, using Theorem 4.1.18, a subset of $\{1, 2, \ldots, n\}$ of size k can be selected in $C(n, k)$ ways. Thus, for $1 \leq k \leq \ell$,

$$|A_k| = \big|\{K : K \subseteq \{1, 2, \ldots, n\}, |K| = k\}\big| \times \big|\{f : \{1, 2, \ldots, r\} \to K \mid f \text{ is onto}\}\big| = C(n, k)k!S(r, k).$$

Therefore,

$$|A| = \left|\bigcup_{k=1}^{\ell} A_i\right| = \sum_{k=1}^{\ell} |A_k| = \sum_{k=1}^{\ell} C(n,k)k!S(r,k).$$

Hence, using the two counting methods, the required result follows. ■

Remark 4.4.9. 1. *The following two problems are equivalent.*

(a) *Count the number of onto functions $f : \{1,2,\ldots,r\} \to \{1,2,\ldots,n\}$.*

(b) *Count the number ways to put r distinguishable/distinct balls into n distinguishable/distinct boxes so that no box is empty.*

2. *The numbers $S(r,k)$ can be recursively calculated using Equation (4.1). For example, we show that $S(m,1) = 1$, for all $m \geq 1$.*

Ans: *Take $n \geq 1$ and $r = 1$ in Equation (4.1) to get*

$$n = n^1 = \sum_{k=1}^{1} C(n,k)k!S(1,k) = C(n,1)1!S(1,1) = nS(1,1).$$

Thus, $S(1,1) = 1$. Take $n = 1$ and $r \geq 2$ in Equation (4.1) to get

$$1 = 1^r = \sum_{k=1}^{1} C(1,k)k!S(r,k) = S(r,1).$$

3. *As exercise, verify that $S(5,2) = 15,\ S(5,3) = 25, ; S(5,4) = 10,\ S(5,5) = 1$.*

Exercise **4.4.10.** 1. *Determine the number of ways of*

(a) *selecting r distinguishable objects from n distinguishable objects, when $n \geq r$.*

(b) *distributing 20 distinct toys among 4 children if each children gets 5 toys?*

(c) *placing r distinguishable balls into n indistinguishable boxes if no box is empty?*

(d) *placing r distinguishable balls into n indistinguishable boxes?*

2. *For $n \in \mathbb{N}$, let $b(n)$ denote the number of partitions of the set $\{1,2,\ldots,n\}$. Then, $b(n) = \sum\limits_{r=0}^{n} S(n,r)$ is called the n^{th} Bell number. By definition, $b(0) = 1 = b(1)$. Determine $b(n)$, for $2 \leq n \leq 5$.*

3. *Fix $n \in \mathbb{N}$. Then, a* composition *of n is an expression of n as a sum of positive integers. For example, if $n = 4$, then the distinct compositions are*

$$4,\ 3+1,\ 1+3,\ 2+2,\ 2+1+1,\ 1+1+2,\ 1+2+1,\ 1+1+1+1.$$

Let $S_k(n)$ denote the number of compositions of n into k parts. Then, $S_1(4) = 1,\ S_2(4) = 3,\ S_3(4) = 3$ and $S_4(4) = 1$. Determine $S_k(n)$, for $1 \leq k \leq n$ and $\sum\limits_{k \geq 1} S_k(n)$.

4. *Let $S = \{f \mid f : \{1,2,\ldots,r\} \to \{1,2,\ldots,n\}\}$. Compute $|S|$ in two ways to prove $(n+1)^r = \sum\limits_{k=0}^{r} C(r,k)n^k$.*

5. *Suppose 13 people get on the lift at level $\circ$. If all the people get down at some level, say 1, 2, 3, 4 and 5 then, calculate the number of ways of getting down if at least one person gets down at each level.*

Definition 4.4.11. **[Partition of a number]** Let $n, k \in \mathbb{N}$. A **partition of** n **into** k **parts** is a tuple $(x_1, \cdots, x_k) \in \mathbb{N}^k$ written in non-increasing order such that $x_1 + \cdots + x_k = n$. It may be viewed as a k-multiset $S \subseteq \mathbb{N}$ with sum n. By $\pi_n(k)$, we denote the number of partitions of n into exactly k parts and by π_n, the number of partitions of n. Conventionally $\pi_0 = 1$ and $\pi_n(k) = 0$, whenever $k > n$.

Remark 4.4.12. *$\pi_7(4) = 3$ as the partitions of 7 into 4-parts are $4+1+1+1$, $3+2+1+1$ and $2+2+2+1$. Verify that $\pi_7(2) = 3$ and $\pi_7(3) = 4$.*

Example 4.4.13. Determine the number of ways of placing r indistinguishable balls into n indistinguishable boxes

1. with the restriction that no box is empty.

   Ans: As the balls are indistinguishable, we need to count the number of balls in each box. As the boxes are indistinguishable, arrange them so that the number of balls inside boxes are in non-increasing order. Also, each box is non-empty and hence the answer is $\pi_r(n)$.

2. with no restriction.

   Ans: Let us place one ball in each box. Now 'placing r indistinguishable ball into n indistinguishable boxes with no restriction' is same as 'placing $r+n$ indistinguishable balls into n indistinguishable boxes so that no box is empty.' Therefore, the required answer is $\pi_{m+n}(n)$.

Exercise **4.4.14.**

1. *Calculate $\pi(n)$, for $n = 1, 2, 3, \ldots, 8$.*
2. *Prove that $\pi_{2r}(r) = \pi(r)$, for any $r \in \mathbb{N}$.*
3. *For a fixed $n \in \mathbb{N}$ determine a recurrence relation for the numbers $\pi_n(r)$'s for $1 \leq r \leq n$.*

Definition 4.4.15. The **Stirling number of the first kind**, denoted $s(n,k)$, is the coefficient of x^k in $x^{\underline{n}}$, where $x^{\underline{n}}$ is called the **falling factorial** and equals $x(x-1)(x-2)\cdots(x-n+1)$. The **rising factorial** $x^{\overline{n}}$ is defined as $x(x+1)(x+2)\cdots(x+n-1)$.

Exercise **4.4.16.** *Prove by induction that*

1. *$s(n,m)(-1)^{n-m}$ is the coefficient of x^m in $x^{\overline{n}}$ and $|s(n,m)| = s(n,m)(-1)^{n-m}$.*
2. *Let $a(n,k)$ denote the number of permutations of $\{1, 2, \ldots, n\}$ which have k disjoint cycles. For example, $a(4,2) = 11$ as it corresponds to the permutations $(12)(34)$, $(13)(24)$, $(14)(23)$, $(1)(234)$, $(1)(243)$, $(134)(2)$, $(143)(2)$, $(124)(3)$, $(142)(3)$, $(123)(4)$ and $(132)(4)$. By convention, $a(0,0) = 1$ and $a(n,0) = 0 = a(0,n)$, whenever $n \geq 1$. Determine prove that the numbers $a(n,k)$'s satisfy*
   $$a(n,k) = (n-1)a(n-1,k) + a(n-1,k-1).$$
3. *Prove that $a(n,m) = |s(n,m)|$ for all $n, m \in \mathbb{N}_0$.*

4.5 Lattice Paths and Catalan Numbers

Consider a lattice of integer lines in $\mathbb{R}^2$ and let $S = \{(m,n) \mid m, n = 0, 1, \ldots\}$ be the said of points on the lattice. For a pair of points, say $A = (m_1, n_1)$ and $B = (m_2, n_2)$ with $m_1 \leq m_2$ and $n_1 \leq n_2$, we define a **lattice path** from A to B to be a subset $\{e_1, \ldots, e_k\}$ of S such that if $e_i = (x,y)$ then e_{i+1} is either $(x+1, y)$ or $(x, y+1)$, for $1 \leq i \leq k-1$. That is, at each step we move either one unit right, denoted R, or one unit up, denoted U (see Figure 4.3).

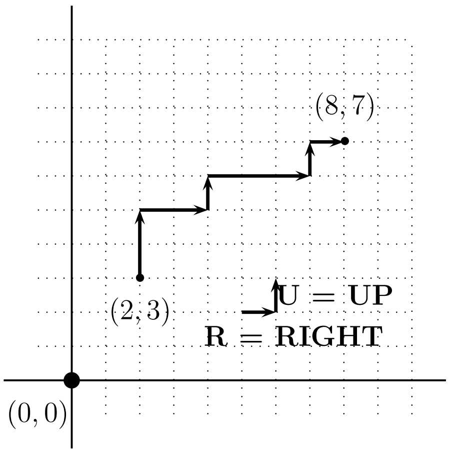


Figure 4.3: A lattice with a lattice path from $(2, 3)$ to $(8, 7)$

Example 4.5.1. 1. Determine the number of lattice paths from $(0, 0)$ to (m, n).

Ans: As at each step, the unit increase is either R or U, we need to take n many R steps and m many U steps to reach (m, n) from $(0, 0)$. So, any arrangement of n many R's and m many U's will give such a path uniquely. Hence, the answer is $C(m + n, m)$.

2. Use the method of lattice paths to prove $\sum\limits_{\ell=0}^{m} C(n + \ell, \ell) = C(n + m + 1, m)$.

Ans: Observe that $C(n + m + 1, m)$ is the number of lattice paths from $(0, 0)$ to $(m, n + 1)$ and the left hand side is the number of lattice paths from $(0, 0)$ to (ℓ, n), where $0 \le \ell \le m$. Fix $\ell, 0 \le \ell \le m$ and let P be a lattice path from $(0, 0)$ to (ℓ, n). Then, the path $P \cup Q$, where $Q = URR \cdots R$ with R appearing $m - \ell$ times, gives a lattice path from $(0, 0)$ to $(m, n + 1)$, namely

$$(0, 0) \xrightarrow{P} (\ell, n) \xrightarrow{U} (\ell, n + 1) \xrightarrow{Q} (m, n + 1).$$

These lattice paths for $0 \le \ell \le m$ are all distinct and hence the result follows.

Exercise **4.5.2.** *1. Give a bijection between 'the solution set of $x_0 + x_1 + x_2 + \cdots + x_k = n$ in non-negative integers' and 'the number of lattice paths from $(0, 0)$ to (n, k)'.*

2. Use lattice paths to construct a proof of $\sum\limits_{k=0}^{n} C(n, k) = 2^n$.

3. Use lattice paths to construct a proof of $\sum\limits_{k=0}^{n} C(n, k)^2 = C(2n, n)$. [Hint: $C(n, k)$ is the number of lattice paths from $(0, 0)$ to $(n - k, k)$ as well as from $(n - k, k)$ to (n, n).]

Discussion 4.5.3. As observed earlier, the number of lattice paths from $(0, 0$ to (n, n) is $C(2n, n)$. Suppose, we wish to take paths so that at no step the number of U's exceeds the number of R's. Then, what is the number of such paths?

Ans: Call an arrangement of n many U's and n many R's a 'bad path' if the number of U's exceeds the number of R's at least once. For example, the path *RRUUURRU* is a 'bad path'. To each such arrangement, we correspond another arrangement of $n+1$ many U's and $n-1$ many R's in the following way: spot the first place where the number of U's exceeds that of R's in the 'bad path'. Then, from the next letter onwards change R to U and U to R. For example, the bad path *RRUUURRU* corresponds to the path *RRUUUUUR*. Notice that this is a one-one correspondence. Thus, the number of bad paths is $C(2n, n - 1)$. So, the answer to the question is $C(2n, n) - C(2n, n - 1) = \dfrac{C(2n, n)}{n + 1}$.

Definition 4.5.4. **[Catalan number]** The nth **Catalan number**, denoted C_n, is the number of different representations of the product $A_1 \cdots A_{n+1}$ of $n+1$ square matrices of the same size using n pairs of brackets. By convention $C_0 = 1$.

Theorem 4.5.5. **[Catalan number]** *Prove that $C_n = \frac{C(2n,n)}{n+1}$ for all $n \in \mathbb{N}$.*

Proof. Claim: After the $(n-k)$-th '(', there are at least $k+2$ many A's. To see this pick the substring starting right from the $(n-k)$-th '(' till we face $(k+1)$ many ')'s. This substring represents a product of matrices. So, it must contain $(k+2)$ many A_i's.

Given one representation of the product, replace each A_i by A. Drop the right brackets to have a sequence of n many '('s and $n+1$ many A's. Thus, the number of A's used till the $n-k$th '(' is at most $n+1-(k+2) = n-k-1$. So, the number of A's never exceeds the number of '('.

Conversely, given such an arrangement, we can put back the ')'s: find two consecutive letters from the last '('; put a right bracket after them; treat (AA) as a letter; repeat the process. For example,

$$((A((AAAA \to ((A((AA)AA \to ((A((AA)A)A \to ((A((AA)A))A = ((A((AA)A))A)$$

By previous example the number of such arrangements is $\frac{C(2n,n)}{n+1}$. ■

The readers who are interested in knowing more about Catalan numbers should look at the book "enumerative combinatorics" by Stanley [12].

EXERCISE **4.5.6.**

1. *Give a recurrence relation for C_n's (i.e., a formula for C_n involving $C_0, \ldots, C_{n-1}$). Hence, show that $C_n = C(2n,n)/(n+1)$.*

2. *Give an arithmetic proof of the fact that $(n+1)$ divides $C(2n,n)$.*

3. *A man is standing on the edge of a swimming pool (facing it) holding a bag containing n blue and n red balls. He randomly picks up one ball at a time and discards it. If the ball is blue he takes a step back and if the ball is red, he takes a step forward. What is the probability of his falling into the swimming pool?*

4. *Consider a regular polygon with vertices $1, 2, \cdots, n$. In how many ways can we divide the polygon into triangles using $(n-3)$ non-crossing diagonals?*

5. *How many arrangements of n blue and n red balls are there such that at any position in the arrangement the number of blue balls (till that position) is at most one more than the number of red balls (till that position)?*

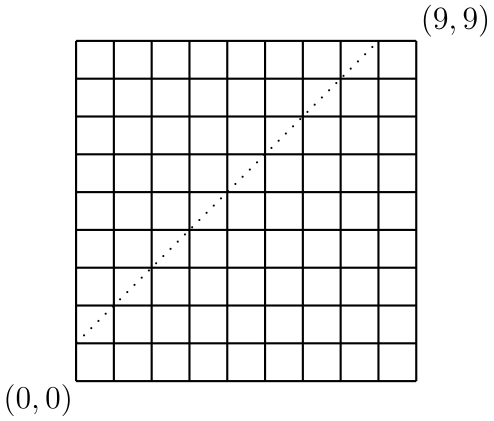
6. *We want to write a matrix of size 10×2 using numbers $1, \ldots, 20$ with each number appearing exactly once. Then, determine the number of such matrices in which the numbers*

   (a) *increase from left to right?*

   (b) *increase from up to down?*

   (c) *increase from left to right and up to down?*

7. *How many lattice paths are there from $(0,0)$ to $(9,9)$ which does not cross the dotted line?*



4.6 Some Generalizations

1. Let $n, k \in \mathbb{N}$ with $0 \leq k \leq n$. Then, in Theorem 4.1.18, we saw that $C(n,k) = \dfrac{n!}{k!(n-k)!}$. Hence, we can think of $C(n,k) = \dfrac{n \cdot (n-1) \cdots (n-k+1)}{k!}$. With this understanding, we generalize $C(n,k)$ for any $n \in \mathbb{R}$ and $k \in \mathbb{N}_0$ as follows:

$$C(n,k) = \begin{cases} 0, & \text{if } \ k < 0 \\ 0, & \text{if } \ n = 0, n \neq k \\ 1, & \text{if } \ n = k \\ \dfrac{n \cdot (n-1) \cdots (n-k+1)}{k!}, & \text{otherwise.} \end{cases} \tag{4.2}$$

With the notations as above, we give the generalized binomial theorem without proof.

Theorem 4.6.1. **[Generalized binomial theorem]** *Let n be any real number. Then,*

$$(1+x)^n = 1 + C(n,1)x + C(n,2)x^2 + \cdots + C(n,r)x^r + \cdots .$$

In particular, $(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots$ *and if* $a, b \in \mathbb{R}$ *with* $|a| < |b|$, *then*

$$(a+b)^n = b^n \left(1 + \frac{a}{b}\right)^n = b^n \sum_{r \geq 0} C(n,r) \left(\frac{a}{b}\right)^r = \sum_{r \geq 0} C(n,r) a^r b^{n-r}.$$

Let us now understand Theorem 4.6.1 through the following examples.

(a) Let $n = \dfrac{1}{2}$. In this case, for $k \geq 1$, Equation (4.2) gives

$$C\left(\frac{1}{2}, k\right) = \frac{\frac{1}{2} \cdot (\frac{1}{2} - 1) \cdots (\frac{1}{2} - k + 1)}{k!} = \frac{1 \cdot (-1) \cdots (3 - 2k)}{2^k k!} = \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}(k-1)!k!}.$$

Thus,

$$(1+x)^{1/2} = \sum_{k \geq 0} C(\frac{1}{2}, k) x^k = 1 + \frac{1}{2}x + \frac{-1}{2^3}x^2 + \frac{1}{2^4}x^3 + \sum_{k \geq 4} \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}(k-1)!k!} x^k.$$

The above expression can also be obtained by using the Taylor series expansion of $f(x) = (1+x)^{1/2}$ around $x = 0$. Recall that the Taylor series expansion of $f(x)$ around $x = 0$ equals $f(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \sum\limits_{k \geq 3} \frac{f^{(k)}(0)}{k!} x^k$, where $f(0) = 1$, $f'(0) = \frac{1}{2}$, $f''(0) = \frac{-1}{2^2}$ and in general $f^{(k)}(0) = \frac{1}{2} \cdot (\frac{1}{2} - 1) \cdots (\frac{1}{2} - k + 1)$, for $k \geq 3$.

(b) Let $n = -r$, where $r \in \mathbb{N}$. Then, for $k \geq 1$, Equation (4.2) gives $C(-r,k) = \dfrac{-r\cdot(-r-1)\cdots(-r-k+1)}{k!} =$ $(-1)^k C(r+k-1,k)$. Thus,

$$(1+x)^n = \frac{1}{(1+x)^r} = 1 - rx + C(r+1,2)x^2 + \sum_{k\geq 3} C(r+k-1,k)(-x)^k.$$

2. Let $n, m \in \mathbb{N}$. Recall the identity $n^m = \sum\limits_{k=0}^{m} C(n,k)k!S(m,k) = \sum\limits_{k=0}^{n} C(n,k)k!S(m,k)$ in Equation (4.1). Note that for each $m \in \mathbb{N}$, the above identity equals $X = AY$, where

$$X = \begin{bmatrix} 0^m \\ 1^m \\ 2^m \\ 3^m \\ \vdots \\ n^m \end{bmatrix}, \quad A = \begin{bmatrix} C(0,0) & 0 & 0 & \cdots & 0 \\ C(1,0) & C(1,1) & 0 & \cdots & 0 \\ C(2,0) & C(2,1) & C(2,2) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C(n,0) & C(n,1) & C(n,2) & \cdots & C(n,n) \end{bmatrix} \text{ and } Y = \begin{bmatrix} 0!S(m,0) \\ 1!S(m,1) \\ 2!S(m,2) \\ \vdots \\ n!S(m,n) \end{bmatrix}.$$

As A is lower triangular with $\det(A) = 1$, it has an inverse and each entry of A^{-1} has a similar form. So, $Y = A^{-1}X$, where

$$A^{-1} = \begin{bmatrix} C(0,0) & 0 & 0 & 0 & \cdots & 0 \\ -C(1,0) & C(1,1) & 0 & 0 & \cdots & 0 \\ C(2,0) & -C(2,1) & C(2,2) & 0 & \cdots & 0 \\ -C(3,0) & C(3,1) & -C(3,2) & C(3,3) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^n C(n,0) & (-1)^{n-1}C(n,1) & (-1)^{n-2}C(n,2) & (-1)^{n-3}C(n,3) & \cdots & C(n,n) \end{bmatrix}.$$

Hence, for $n, m \in \mathbb{N}$, we have

$$S(m,n) = \frac{1}{n!}\sum_{k\geq 0}(-1)^k C(n,k)(n-k)^m. \tag{4.3}$$

3. The above matrix inversion implies that for $n \in \mathbb{N}_0$, the identity

$$a(n) = \sum_{k\geq 0} C(n,k)b(k) \text{ holds if and only if } b(n) = \sum_{k\geq 0}(-1)^k C(n,k)a(k) \text{ holds.}$$

We end this chapter with another set of exercises.

Exercise **4.6.2.** *1. Prove that there exists a bijection between any two of the following sets.*

(a) The set of words of length n on an alphabet consisting of m letters.

(b) The set of maps of an n-set into an m-set.

(c) The set of distributions of n distinct objects into m distinct boxes.

(d) The set of n-tuples on m letters.

2. Prove that there exists a bijection between any two of the following sets.

(a) The set of n letter words with distinct letters out of an alphabet consisting of m letters.

(b) The set of one-one functions from an n-set into an m-set.

(c) The set of distributions of n distinct objects into m distinct boxes, subject to 'if an object is put in a box, no other object can be put in the same box'.

(d) *The set of n-tuples on m letters, without repetition.*

(e) *The set of permutations of m symbols taken n at a time.*

3. *Prove that there exists a bijection between any two of the following sets.*

   (a) *The set of increasing words of length n on m ordered letters.*

   (b) *The set of distributions on n non-distinct objects into m distinct boxes.*

   (c) *The set of combinations of m symbols taken n at a time with repetitions permitted.*

Chapter 5

Advanced Counting Principles

5.1 Pigeonhole Principle

Discussion 5.1.1. **[Pigeonhole principle (PHP)]**

PHP1. If $n+1$ pigeons stay in n holes then there is a hole with at least two pigeons.

PHP2. If $kn+1$ pigeons stay in n holes then there is a hole with at least $k+1$ pigeons.

PHP3. If $p_1 + \cdots + p_n + 1$ pigeons stay in n holes then there is a hole i with at least $p_i + 1$ pigeons.

Example 5.1.2. 1. Consider a tournament of $n > 1$ players, where each pair plays exactly once and each player wins at least once. Then, there are two players with the same number of wins.

Ans: Number of wins vary from 1 to $n-1$ and there are n players.

2. A bag contains 5 red, 8 blue, 12 green and 7 yellow marbles. The least number of marbles to be chosen to ensure that there are

   (a) at least 4 marbles of the same color is 13,

   (b) at least 7 marbles of the same color is 24,

   (c) at least 4 red or at least 7 of any other color is 22.

3. In a group of 6 people, prove that there are three mutual friends or three mutual strangers.

   Ans: Let a be a person in the group. Let F be the set of friends of a and S the set of strangers to a. Clearly $|S| + |F| = 5$. By PHP either $|F| \geq 3$ or $|S| \geq 3$.

   Case 1: $|F| \geq 3$. If any two in F are friends then those two along with a are three mutual friends. Else F is a set of mutual strangers of size at least 3.

   Case 2: $|S| \geq 3$. If any pair in S are strangers then those two along with a are three mutual strangers. Else S becomes a set of mutual friends of size at least 3.

4. If 7 points are chosen inside or on the unit circle, then there is a pair of points which are at a distance at most 1.

   Ans: To see this divide the circle into 6 equal cone type parts creating an angle of 60^o with the center. By PHP there is a part containing at least two points. The distance between these two is at most 1.

5. If $n+1$ integers are selected from $\{1, 2, \ldots, 2n\}$, then there is a pair which has the property that one of them divides the other.

   Ans: Each number has the form $2^k s$, where $s = 2m+1$ is an odd number. There are n odd numbers. If we select $n+1$ numbers from S, by PHP some two of them (say, x, y) have the same odd part, that is, $x = 2^i s$ and $y = 2^j s$. If $i \leq j$, then $x|y$, otherwise $y|x$. ■

6. (a) Let $r_1, r_2, \cdots, r_{mn+1}$ be a sequence of $mn+1$ distinct real numbers. Then, prove that there is a subsequence of $m+1$ numbers which is increasing or there is a subsequence of $n+1$ numbers which is decreasing.

   Ans: Define l_i to be the maximum length of an increasing subsequence starting at r_i. If some $l_i \geq m+1$ then we have nothing to prove. So, let $1 \leq l_i \leq m$. Since (l_i) is a sequence of $mn+1$ integers, by PHP, there is one number which repeats at least $n+1$ times. Let $l_{i_1} = l_{i_2} = \cdots = l_{i_{n+1}} = s$, where $i_1 < i_2 < \cdots < i_{n+1}$. Notice that $r_{i_1} > r_{i_2}$, because if $r_{i_1} < r_{i_2}$, then 'r_{i_1} together with the increasing sequence of length s starting with r_{i_2}' gives an increasing sequence of length $s+1$. Similarly, $r_{i_2} > r_{i_3} > \cdots > r_{i_{n+1}}$ and hence the required result holds.

   Alternate. Let $S = \{r_1, r_2, \cdots, r_{mn+1}\}$ and define a map $f : S \to \mathbb{Z} \times \mathbb{Z}$ by $f(r_i) = (s, t)$, for $1 \leq i \leq mn+1$, where s equals the length of the largest increasing subsequence starting with r_i and t equals the length of the largest decreasing subsequence ending at r_i. Now, if either $s \geq m+1$ or $t \geq n+1$, we are done. If not, then note that $1 \leq s \leq m$ and $1 \leq t \leq n$. So, the number of tuples (s, t) is at most mn. Thus, the $mn+1$ distinct numbers are being mapped to mn tuples and hence by PHP there are two numbers $r_i \neq r_j$ such that $f(r_i) = f(r_j)$. Now, proceed as in the previous case to get the required result.

   (b) Does the above statement hold for every collection of mn distinct numbers? No. Consider the sequence:

$$n, n-1, \cdots, 1, 2n, 2n-1, \ldots, n+1, 3n, 3n-1, \cdots, 2n+1, \cdots, mn, mn-1, \cdots, mn-n+1.$$

7. Given any 1010 integers, prove that there is a pair that either differ by, or sum to, a multiple of 2017. Is this true if we replace 1010 by 1009?

   Ans: Let the numbers be $n_1, n_2, \ldots, n_{1010}$ and $S = \{n_1 - n_k, n_1 + n_k : k = 2, \ldots, 1010\}$. Then, $|S| = 2018$ and hence, at least two of them will have the same remainder when divided by 2017. Then, consider their difference. For the later part, consider $\{0, 1, 2, \ldots, 1008\}$.

8. Let $a \in \mathbb{R} \setminus \mathbb{Q}$. Then, there are infinitely many rational numbers $\frac{p}{q}$ such that $|a - \frac{p}{q}| < \frac{1}{q^2}$.

   Ans: Enough to show that there are infinitely many $(p, q) \in \mathbb{Z}^2$ with $|qa - p| < \frac{1}{q}$. As a is irrational, note that for every $m \in \mathbb{N}$, $0 < ia - \lfloor ia \rfloor < 1$, for $i = 1, \ldots, m+1$. Hence, by PHP there exist i, j with $i < j$ such that

$$|(j-i)a - (\lfloor ja \rfloor - \lfloor ia \rfloor)| < \frac{1}{m} \leq \frac{1}{j-i}.$$

   Then, the tuple $(p_1, q_1) = (\lfloor ja \rfloor - \lfloor ia \rfloor, j - i)$ satisfies the required property. To generate another tuple, find m_2 such that

$$\frac{1}{m_2} < |a - \frac{p_1}{q_1}|$$

   and proceed as before to get (p_2, q_2) such that $|q_2 a - p_2| < \frac{1}{m_2} \leq \frac{1}{q_2}$. Since $|a - \frac{p_2}{q_2}| < \frac{1}{m_2} < |a - \frac{p_1}{q_1}|$, we have $\frac{p_1}{q_1} \neq \frac{p_2}{q_2}$. Now use induction to get the required result.

9. Prove that there exist two powers of 3 whose difference is divisible by 2017.

   Ans: Let $S = \{1 = 3^0, 3, 3^2, 3^3, \ldots, 3^{2017}\}$. Then, $|S| = 2018$. As the remainders of any integer when divided by 2017 is $0, 1, 2, \ldots, 2016$, by PHP, there is a pair which has the same remainder. Hence, 2017 divides $3^j - 3^i$ for some i, j.

10. Prove that there exists a power of three that ends with 0001.

    Ans: Let $S = \{1 = 3^0, 3, 3^2, 3^3, \ldots\}$. Now, divide each element of S by 10^4. As $|S| > 10^4$, by PHP, there exist $i > j$ such that the remainders of 3^i and 3^j, when divided by 10^4, are equal. But $\gcd(10^4, 3) = 1$ and thus, 10^4 divides $3^\ell - 1$. That is, $3^\ell - 1 = s \cdot 10^4$ for some positive integer s. That is, $3^\ell = s \cdot 10^4 + 1$ and hence the result follows.

EXERCISE **5.1.3.** *1. Consider the poset $(X = \mathcal{P}(\{1,2,3,4\}), \subseteq)$. Write 6 maximal chains $P_1, \ldots P_6$ (need not be disjoint) such that $\underset{i}{\cup} P_i = X$. Let $A_1, \ldots, A_7$ be 7 distinct subsets of $\{1,2,3,4\}$. Use PHP, to prove that there exist i, j such that $A_i, A_j \in P_k$, for some k. That is, $\{A_1, \ldots, A_7\}$ cannot be an anti-chain. Conclude that this holds as the width of the poset is 6.*

2. Let $\{x_1, \ldots, x_9\} \subseteq \mathbb{N}$ with $\sum\limits_{i=1}^{9} x_i = 30$. Then, prove that there exist $i, j, k \in \{1, 2, \ldots, 9\}$ with $x_i + x_j + x_k \geq 12$.

3. Pick any 6 integers from $\{1, 2, \ldots, 10\}$, then there exists a pair with odd sum.

4. Any 14-subset of $\{1, 2, \ldots, 46\}$ has four elements a, b, c, d such that $a + b = c + d$.

5. In a row of 12 chairs 9 are filled. Then, some 3 consecutive chairs are filled. Will 8 work?

6. Every n-sequence of integers has a consecutive subsequence with sum divisible by n.

7. Let $n > 3$ and $S \subseteq \{1, 2, \ldots, n\}$ of size $m = \lfloor \frac{n+2}{2} \rfloor + 1$. Then, there exist $a, b, c \in S$ such that $a + b = c$.

8. Let $a, b \in \mathbb{N}$, $a < b$. Given more than half of the integers in the set $\{1, 2, \ldots, a + b\}$, there is a pair which differ by either a or b.

9. Consider a chess board with two of the diagonally opposite corners removed. Is it possible to cover the board with pieces of rectangular dominos whose size is exactly two board squares?

10. Mark the centers of all squares of an 8×8 chess board. Is it possible to cut the board with 13 straight lines not passing through any center, so that every piece had at most 1 center?

11. Fifteen squirrels have 100 nuts. Then, some two squirrels have equal number of nuts.

12. Suppose that $f(x)$ is a polynomial with integer coefficients. If

(a) $f(x) = 2$ for three distinct integers, then for no integer x, $f(x)$ can be equal to 3.

(b) $f(x) = 14$ for three distinct integers, then for no integer x, $f(x)$ can be equal to 15.

(c) $f(x) = 11$ for five distinct integers, then for no integer x, $f(x)$ can be equal to 9.

13. Choose 5 points at random inside an equilateral triangle of side 1 unit, then there exists a pair which have distance at most 0.5 units.

14. Prove that among any 55 integers $1 \leq x_1 < x_2 < x_3 < \cdots < x_{55} \leq 100$, there is a pair with difference 9, a pair with difference 10, a pair with difference 12 and a pair with difference 13. Surprisingly, there need not be a pair with difference 11.

15. Let $\{x_1, x_2, \ldots, x_n\} \subseteq \mathbb{Z}$. Prove that there exist $1 \leq i \leq j \leq n$ such that

(a) $x_i + x_{i+1} + \cdots + x_{j-1} + x_j$ is a multiple of 2017, whenever $n \geq 2017$.

(b) $x_j + x_i$ or $x_j - x_i$ is a multiple of 2017, whenever $n \geq 1010$.

16. Let A and B be two discs, each having $2n$ equal sectors. On disc A, n sectors are colored red and n are colored blue. The sectors of disc B are colored arbitrarily with red and blue colors. Show that there is a way of putting the two discs, one above the other, so that at least n corresponding sectors have the same colors.

17. *There are 7 distinct real numbers. Is it possible to select two of them, say x and y such that $0 < \frac{x-y}{1+xy} < \frac{1}{\sqrt{3}}$?*

18. *If n is odd then for any permutation p of $\{1, 2, \ldots, n\}$ the product $\prod\limits_{i=1}^{n} \big(i - p(i)\big)$ is even.*

19. *Fix a positive $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then, $S = \{m + n\alpha : m, n \in \mathbb{Z}\}$ is dense in $\mathbb{R}$.*

20. *If more than half of the subsets of $\{1, 2, \ldots, n\}$ are selected, then some two of the selected subsets have the property that one is a subset of the other.*

21. *Given any ten 4-subsets of $\{1, 2, \ldots, 11\}$,, some two of them have at least 2 elements in common.*

22. *A person takes at least one aspirin a day for 30 days. If he takes 45 aspirin altogether then prove that in some sequence of consecutive days he takes exactly 14 aspirins.*

23. *If 58 entries of a 14×14 matrix are 1, then there is a 2×2 submatrix with all entries 1.*

24. *Let A and B be two finite non-empty sets with $B = \{b_1, b_2, \ldots, b_m\}$. Let $f : A \to B$ be any function. Then, for any non-negative integers $a_1, a_2, \ldots, a_m$ if $|A| = a_1 + a_2 + \cdots + a_m - m + 1$ then prove that there exists an $i, 1 \le i \le m$ such that $|f^{-1}(b_i)| \ge a_i$.*

25. *Each of the given 9 lines cuts a given square into two quadrilaterals whose areas are in the ratio $2 : 3$. Prove that at least three of these lines pass through the same point.*

26. *Five points are chosen at the nodes of a square lattice (view $\mathbb{Z} \times \mathbb{Z}$). Why is it certain that a mid-point of some two of them is a lattice point?*

27. *Take 25 points on a plane satisfying 'among any three of them there is a pair at a distance less than 1'. Then, some circle of unit radius contains at least 13 of the given points.*

28. *If each point of a circle is colored either red or blue, then show that there exists an isosceles triangle with vertices of the same color.*

29. *Each point of the plane is colored red or blue, then prove the following.*
    (a) *There exist two points of the same color which are at a distance of 1 unit.*
    (b) *There is an equilateral triangle all of whose vertices have the same color.*
    (c) *There is a rectangle all of whose vertices have the same color.*

30. *Let $S \subseteq \{1, 2, \ldots, 100\}$ be a 10-set. Then, some two disjoint subsets of S have equal sum.*

31. *Fix a positive integer n. Prove that there exists an $\ell \in \mathbb{N}$ such that n divides $2^\ell - 1$.*

32. *Does there exist a multiple of 2017 that is formed using only the digits*
    (a) *2? Justify your answer.*
    (b) *2 and 3 and the number of 2's and 3's are equal? Justify your answer.*

33. *Each natural number has a multiple of the form $9 \cdots 90 \cdots 0$, with at least one 9.*

5.2 Principle of Inclusion and Exclusion

We start this section with the following example.

Example 5.2.1. How many natural numbers $n \le 1000$ are not divisible by any of $2, 3$?

Ans: Let $A_2 = \{n \in \mathbb{N} \mid n \le 1000,\ 2|n\}$ and $A_3 = \{n \in \mathbb{N} \mid n \le 1000,\ 3|n\}$. Then, $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 500 + 333 - 166 = 667$. So, the required answer is $1000 - 667 = 333$.

We now generalize the above idea whenever we have 3 or more sets.

Theorem 5.2.2. **[Principle of inclusion and exclusion]** *Let $A_1, \cdots, A_n$ be finite subsets of a set U. Then,*

$$\Big|\overset{n}{\underset{i=1}{\cup}} A_i\Big| = \sum_{k=1}^{n}(-1)^{k+1}\Bigg[\sum_{1\le i_1<\cdots<i_k\le n} \big|A_{i_1}\cap\cdots\cap A_{i_k}\big|\Bigg]. \tag{5.1}$$

Or equivalently, the number of elements of U which are in none of $A_1, A_2, \ldots, A_n$ equals

$$|U| - \Big|\overset{n}{\underset{i=1}{\cup}} A_i\Big| = |U| - \sum_{k=1}^{n}(-1)^{k}\Bigg[\sum_{1\le i_1<\cdots<i_k\le n} \big|A_{i_1}\cap\cdots\cap A_{i_k}\big|\Bigg].$$

Proof. Let $x \notin \overset{n}{\underset{i=1}{\cup}} A_i$. Then, we show that inclusion of x in some A_i contributes (increases the value) 1 to both sides of Equation (5.1). So, assume that x is included only in the sets $A_1, \cdots, A_r$. Then, the contribution of x to $|A_{i_1}\cap\cdots\cap A_{i_k}|$ is 1 if and only if $\{i_1,\ldots,i_k\}\subseteq\{1,2,\ldots,r\}$. Hence, the contribution of x to $\sum\limits_{1\le i_1<\cdots<i_k\le n} |A_{i_1}\cap\cdots\cap A_{i_k}|$ is $C(r,k)$. Thus, the contribution of x to the right hand side of Equation (5.1) is

$$C(r,1) - C(r,2) + C(r,3) - \cdots + (-1)^{r+1}C(r,r) = 1.$$

The element x clearly contributes 1 to the left hand side of Equation (5.1) and hence the required result follows. The proof of the equivalent condition is left for the readers. ■

Example 5.2.3. How many integers between 1 and 10000 are divisible by none of $2, 3, 5, 7$?

Ans: For $i \in \{2,3,5,7\}$, let $A_i = \{n \in \mathbb{N} \mid n \le 10000,\ i|n\}$. Therefore, the required answer is $10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$.

Definition 5.2.4. **[Euler totient function]** For a fixed $n \in \mathbb{N}$, the **Euler's totient function** is defined as $\varphi(n) = |\{k \in \mathbb{N} : k \le n, \gcd(k,n) = 1\}|$.

Theorem 5.2.5. *Let $n = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$, be a factorization of n into distinct primes $p_1, \ldots, p_k$. Then, $\varphi(n) = n\big(1-\frac{1}{p_1}\big)\big(1-\frac{1}{p_2}\big)\cdots\big(1-\frac{1}{p_k}\big)$.*

Proof. For $1 \le i \le k$, let $A_i = \{m \in \mathbb{N} : m \le n, p_i|m\}$. Then,

$$\begin{aligned} \varphi(n) &= n - |\underset{i}{\cup} A_i| = n\Big[1 - \sum_{i=1}^{k}\frac{1}{p_i} + \sum_{1\le i<j\le k}\frac{1}{p_ip_j} - \cdots + (-1)^k\frac{1}{p_1p_2\cdots p_k}\Big] \\ &= n\big(1-\frac{1}{p_1}\big)\big(1-\frac{1}{p_2}\big)\cdots\big(1-\frac{1}{p_k}\big) \end{aligned}$$

as $|A_i| = \frac{n}{p_i}$, $|A_i \cap A_j| = \frac{n}{p_ip_j}$ and so on. Thus, the required result follows. ■

Definition 5.2.6. A **derangement** of objects in a finite set S is a permutation/arrangement σ on S such that for all $x, \sigma(x) \ne x$.

For example, $2,1,4,3$ is a derangement of $1,2,3,4$. The number of derangements of $1,2,\ldots,n$ is denoted by D_n. By convention, $D_0 = 1$. Also, we use $a \approx b$ to mean that b is an approximate value of a.

Theorem 5.2.7. *For $n \in \mathbb{N}$, $D_n = n!\sum\limits_{k=0}^{n}\frac{(-1)^k}{k!}$. Thus, $\frac{D_n}{n!} \approx \frac{1}{e}$.*

Proof. For each $i, 1 \leq i \leq n$, let A_i be the set of arrangements σ such that $\sigma(i) = i$. Then, verify that $|A_i| = (n-1)!$, $|A_i \cap A_j| = (n-2)!$ and so on. Thus,

$$|\underset{i}{\cup} A_i| = n.(n-1)! - C(n,2)(n-2)! + \cdots + (-1)^{n-1}C(n,n)0! = n!\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k!}.$$

So, $D_n = n! - |\underset{i}{\cup} A_i| = n! \sum\limits_{k=0}^{n} \frac{(-1)^k}{k!}$. Furthermore, $\lim\limits_{n\to\infty} \dfrac{D_n}{n!} = \dfrac{1}{e}$. ■

Example 5.2.8. For $n \in \mathbb{N}$, how many square-free integers do not exceed n?

Ans: Let $P = \{p_1, \cdots, p_s\}$ be the set of primes not exceeding $\sqrt{n}$ and for $1 \leq i \leq s$, let A_i be the set of integers between 1 and n that are multiples of p_i^2. It is easy to see that

$$|A_i| = \lfloor \frac{n}{p_i^2} \rfloor, \quad |A_i \cap A_j| = \lfloor \frac{n}{p_i^2 p_j^2} \rfloor,$$

and so on. So, the number of square-free integers not greater than n is

$$n - |\bigcup_{i=1}^{s} A_i| = n - \sum_{i=1}^{s} \lfloor \frac{n}{p_i^2} \rfloor + \sum_{1\leq i<j\leq s} \lfloor \frac{n}{p_i^2p_j^2} \rfloor - \sum_{1\leq i<j<k\leq s} \lfloor \frac{n}{p_i^2p_j^2p_k^2} \rfloor + \cdots$$

For $n = 100$, we have $P = \{2, 3, 5, 7\}$. So, the number of square-free integers not exceeding 100 is

$$100 - \lfloor \frac{100}{4} \rfloor - \lfloor \frac{100}{9} \rfloor - \lfloor \frac{100}{25} \rfloor - \lfloor \frac{100}{49} \rfloor + \lfloor \frac{100}{36} \rfloor + \lfloor \frac{100}{100} \rfloor = 61.$$

EXERCISE **5.2.9.**

1. *Let $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$. Then, $\varphi(mn) = \varphi(m)\varphi(n)$.*
2. *Let $n \in \mathbb{N}$. Then, use inclusion-exclusion to prove $S(n,r) = \frac{1}{r!}\sum\limits_{i=0}^{r-1}(-1)^i C(r,i)(r-i)^n$.*
3. *Show that $\sum\limits_{k=0}^{m}(-1)^k C(m,k)(m-k)^n = \begin{cases} n! & \text{if } m = n \\ 0 & \text{if } m > n. \end{cases}$*
4. *Determine the number of 10-letter words using ENGLISH alphabets that does not contain all the vowels.*
5. *In a school there are 12 students who take an art course A, 20 who take a biology course B, 20 who take a chemistry course C and 8 who take a dance course D. There are 5 students who take both A and B, 7 students who take both A and C, 4 students who take both A and D, 16 students who take both B and C, 4 students who take both B and D and 3 students who take who take both C and D. There are 3 who take A, B and C; 2 who take A, B and D; 3 who take A, C and D; and 2 who take B, C and D. Finally there are 2 in all four courses and further 71 students who have not taken any of these courses. Find the total number of students.*
6. *Determine all integers n satisfying $\varphi(n) = 13$.*
7. *Determine all integers n satisfying $\varphi(n) = 12$.*
8. *For each fixed $n \in \mathbb{N}$, use mathematical induction to prove that $\sum\limits_{d|n}\varphi(d) = n$.*
9. *A function $f : \mathbb{N} \to \mathbb{N}$ is said to be* **multiplicative** *if $f(nm) = f(n)f(m)$, whenever $\gcd(n,m) = 1$.*
   (a) *Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions satisfying $f(n) = \sum\limits_{d|n} g(d)$ and $f(1) = g(1) = 1$. If f is multiplicative then use induction to show that g is also multiplicative.*
   (b) *Imagine the fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. Reduce the fractions to standard form by canceling the common factors and regroup to show that $n = \sum\limits_{d|n}\varphi(d)$. For example,*

$$\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6} \to \frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, 1 \to 1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{6}, \frac{5}{6}.$$

(c) *Use the first part to conclude that φ is multiplicative.*

10. *Show that for $n \geq 2$, $D_n = \lfloor \frac{n!}{e} + \frac{1}{2} \rfloor$.*

11. *Prove combinatorially: $\sum\limits_{i=0}^{n} C(n,i) D_{n-i} = n!$.*

12. *Find the number of non-negative integer solutions of $a+b+c+d = 27$, where $1 \leq a \leq 5$, $2 \leq b \leq 7$, $3 \leq c \leq 9$, $4 \leq d \leq 11$.*

13. *Let x be a positive integer less than or equal to 9999999.*

    (a) *Find the number of x's for which the sum of the digits in x equals 30.*

    (b) *How many of the solutions obtained in the first part consist of 7 digits?*

14. *Determine the number of ways to arrange 10 digits $0, 1, \ldots, 9$, so that the digit i is never followed immediately by $i+1$.*

15. *Determine the number of strings of length 15 consisting of the 10 digits, $0, 1, \ldots, 9$, so that no string contains all the 10 digits.*

16. *Determine the number of ways of permuting the 26 letters of the ENGLISH alphabets so that none of the patterns lazy, run, show and pet occurs.*

17. *Let $S = \{(n_1, n_2, n_3) \mid n_i \in \mathbb{N}, \sum n_i = 15\}$. Evaluate $\sum\limits_{(n_1,n_2,n_3) \in S} \dfrac{15!}{n_1! n_2! n_3!}$.*

18. *Each of the 9 senior students said: 'the number of junior students I want to help is exactly one'. There were 4 junior students a, b, c, d, who wanted their help. The allocation was done randomly. What is the probability that either a has exactly two seniors to help him or b has exactly 3 seniors to help him or c has no seniors to help him?*

5.3 Generating Functions

This is one of the strongest tools in combinatorics. We start with the definition of formal power series over $\mathbb{Q}$ and develop the theory of generating functions. This is then used to get closed form expressions for some known recurrence relations and are then further used to get some binomial identities.

Definition 5.3.1. 1. An algebraic expression of the form $f(x) = \sum\limits_{n \geq 0} a_n x^n$, where $a_n \in \mathbb{Q}$ for all $n \geq 0$, is called a **formal power series** in the indeterminate x over $\mathbb{Q}$. By $\mathfrak{P}(x)$, we denote the set of all formal power series in x and by $\text{CF}[x^n, f]$, the coefficient of x^n in f, *e.g.*, $\text{CF}\left[x^n, \sum\limits_{n \geq 0} a_n x^n\right] = a_n$.

2. Two elements $f, g \in \mathfrak{P}(x)$ are said to be equal if $\text{CF}[x^n, f] = \text{CF}[x^n, g]$ for all $n \geq 0$.

3. Let $f(x) = \sum\limits_{n \geq 0} a_n x^n$, $g(x) = \sum\limits_{n \geq 0} b_n x^n \in \mathfrak{P}(x)$. Then, their

    (a) sum/addition is defined by $\text{CF}[x^n, f+g] = \text{CF}[x^n, f] + \text{CF}[x^n, g]$.

    (b) product (called the **Cauchy product**) is defined by $\text{CF}[x^n, f \cdot g] = c_n = \sum\limits_{k=0}^{n} a_k b_{n-k}$.

Before proceeding further, we consider the following examples.

Example 5.3.2. 1. How many words of size 8 can be formed with 6 copies of A and 6 copies of B?

Ans: $\sum\limits_{k=2}^{6} C(8,k)$, as we just need to choose k places for A, where $2 \leq k \leq 6$.

Alternate. In any such word, we need m many A's and n many B's with $m+n=8$, $m \leq 6$ and $n \leq 6$. Also, the number of words with m many A's and n many B's is $\dfrac{8!}{m!n!}$. We identify this number with $\dfrac{8!x^m y^n}{m!n!}$ and note that this is a term of degree 8 in

$$8!\Big[1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\frac{x^5}{5!}+\frac{x^6}{6!}\Big]\Big[1+y+\frac{y^2}{2!}+\frac{y^3}{3!}+\frac{y^4}{4!}+\frac{y^5}{5!}+\frac{y^6}{6!}\Big].$$

If we replace y by x, then our answer is

$$\begin{aligned} & 8!\text{CF}\Big[x^8, (1+x+\tfrac{x^2}{2!}+\tfrac{x^3}{3!}+\tfrac{x^4}{4!}+\tfrac{x^5}{5!}+\tfrac{x^6}{6!})(1+x+\tfrac{x^2}{2!}+\tfrac{x^3}{3!}+\tfrac{x^4}{4!}+\tfrac{x^5}{5!}+\tfrac{x^6}{6!})\Big] \\ = {} & 8!\text{CF}\Big[x^8, (\tfrac{x^2}{2!}+\tfrac{x^3}{3!}+\tfrac{x^4}{4!}+\tfrac{x^5}{5!}+\tfrac{x^6}{6!})(\tfrac{x^2}{2!}+\tfrac{x^3}{3!}+\tfrac{x^4}{4!}+\tfrac{x^5}{5!}+\tfrac{x^6}{6!})\Big] \\ = {} & 8!\text{CF}\Big[x^8, (\tfrac{x^2}{2!}+\tfrac{x^3}{3!}+\cdots)(\tfrac{x^2}{2!}+\tfrac{x^3}{3!}+\cdots)\Big] \\ = {} & 8!\text{CF}\big[x^8, (e^x-1-x)^2 = e^{2x}+1+x^2-2xe^x-2e^x+2x\big] = 8!\big(\tfrac{2^8}{8!}-\tfrac{2}{7!}-\tfrac{2}{8!}\big) = 238. \end{aligned}$$

2. How many anagrams are there of the word $MISSISSIPPI$?

   Ans: Using basic counting, the answer is $\dfrac{11!}{4!4!2!}$. For another understanding, the readers should note that

$$\begin{aligned} \frac{11!}{4!4!2!} &= 11!\,\text{CF}\Big[x^{11}, (1+x)\big(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}\big)^2\big(1+x+\frac{x^2}{2!}\big)\Big] \\ &= 11!\,\text{CF}\Big[x^{11}, \big(x+\frac{x^2}{2!}+\cdots\big)\big(\frac{x^4}{4!}+\frac{x^5}{5!}+\cdots\big)^2\big(\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\big)\Big] \end{aligned}$$

   as we need to have x, $\dfrac{x^4}{4!}$, $\dfrac{x^4}{4!}$ and $\dfrac{x^2}{2!}$ for the alphabets M, I, S and P, respectively.

3. Prove that the number of non-negative integer solutions of $u+v+w+t=10$ equals $\text{CF}\big[x^{10}, (1+x+x^2+\cdots$

   Ans: Note that u can take any value from 0 to 10 which corresponds to $1+x+\cdots+x^{10}$. Hence, using Theorem 4.6.1, the required answer is

$$\text{CF}\big[x^{10}, (1+x+x^2+\cdots)^4 = (1-x)^{-4}\big] = C(13,10) = \frac{4\cdot 5\cdots\cdot 13}{10!}.$$

Definition 5.3.3. Let $(b_r)_0^\infty$ be a sequence of integers. Then,

1. the **ordinary generating function** (**ogf**) is the formal power series

$$b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots, \text{ and}$$

2. the **exponential generating function** (**egf**) is the formal power series

$$b_0 + b_1x + b_2\frac{x^2}{2!} + b_3\frac{x^3}{3!} + \cdots.$$

If there exists an $M \in \mathbb{N}$ such that $b_r = 0$ for all $r \geq M$, then the generating functions have finitely many terms.

Example 5.3.4. What is the number of non-negative integer solutions of $2a+3b+5c=r$, $r \in \mathbb{N}_0$?

Ans: Note that $a \in \mathbb{N}_0$ and hence $2a$ corresponds to the formal power series $1+x^2+x^4+\cdots$. Thus, we need to consider the ogf

$$(1+x^2+x^4+\cdots)(1+x^3+x^6+\cdots)(1+x^5+x^{10}+\cdots) = \frac{1}{(1-x^2)(1-x^3)(1-x^5)}.$$

Hence, the required answer is $\text{CF}\Big[x^r, \dfrac{1}{(1-x^2)(1-x^3)(1-x^5)}\Big]$.

Remark 5.3.5. *1. Let* $f(x) = \sum\limits_{n\ge 0} a_n \frac{x^n}{n!}, g(x) = \sum\limits_{n\ge 0} b_n \frac{x^n}{n!} \in \mathfrak{P}(x)$. *Then, in case of egf, their product equals* $\sum\limits_{n\ge 0} d_n \frac{x^n}{n!}$*, where* $d_n = \sum\limits_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$*, for* $n \ge 0$.

2. Note that $e^{e^x-1} \in \mathfrak{P}(x)$ *as* $e^y = \sum\limits_{n\ge 0} \frac{y^n}{n!}$ *implies that* $e^{e^x-1} = \sum\limits_{n\ge 0} \frac{(e^x-1)^n}{n!}$ *and*

$$\text{CF}\big[x^m, e^{e^x-1}\big] = \text{CF}\left[x^m, \sum_{n\ge 0} \frac{(e^x-1)^n}{n!}\right] = \sum_{n=0}^{m} \text{CF}\left[x^m, \frac{(e^x-1)^n}{n!}\right]. \tag{5.2}$$

That is, for each $m \ge 0$, $\text{CF}\big[x^m, e^{e^x-1}\big]$ *is a sum of a finite number of rational numbers. Whereas, the expression* $e^{e^x} \notin \mathfrak{P}(x)$ *requires infinitely many computation for* $\text{CF}\big[x^m, e^{e^x}\big]$*, for all* $m \ge 0$.

With the algebraic operations as defined in Definition 5.3.1.3, it can be checked that $\mathfrak{P}(x)$ forms a Commutative Ring with identity, where the identity element is given by the formal power series $f(x) = 1$. In this ring, the element $f(x) = \sum\limits_{n\ge 0} a_n x^n$ is said to have a **reciprocal** if there exists another element $g(x) = \sum\limits_{n\ge 0} b_n x^n \in \mathfrak{P}(x)$ such that $f(x)\cdot g(x) = 1$. So, the question arises, under what conditions on $\text{CF}[x^n, f]$, can we find $g(x) \in \mathfrak{P}(x)$ such that $f(x)g(x) = 1$. The answer to this question is given in the following proposition.

Proposition 5.3.6. *The reciprocal of* $f \in \mathfrak{P}(x)$ *exists if and only if* $\text{CF}\big[x^0, f\big] \neq 0$.

Proof. Let $g(x) = \sum\limits_{n\ge 0} b_n x^n \in \mathfrak{P}(x)$ be the reciprocal of $f(x) = \sum\limits_{n\ge 0} a_n x^n$. Then, $f(x)g(x) = 1$ if and only if $\text{CF}\big[x^0, f\cdot g\big] = 1$ and $\text{CF}[x^n, f\cdot g] = 0$, for all $n \ge 1$.

But, by definition of the Cauchy product, $\text{CF}\big[x^0, f\cdot g\big] = a_0 b_0$. Hence, if $a_0 = \text{CF}\big[x^0, f\big] = 0$ then $\text{CF}\big[x^0, f\cdot g\big] = 0$ and thus, f cannot have a reciprocal. However, if $a_0 \neq 0$, then the coefficients $\text{CF}[x^n, g] = b_n$'s can be recursively obtained as follows:
$b_0 = 1/a_0$ as $1 = c_0 = a_0 b_0$;
$b_1 = -(a_1 b_0)/a_0$ as $0 = c_1 = a_0 b_1 + a_1 b_0$;
$b_2 = -(a_2 b_0 + a_1 b_1)/a_0$ as $0 = c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$; and in general, if we have computed b_k, for $k \le r$, then using $0 = c_{r+1} = a_{r+1} b_0 + a_r b_1 + \cdots + a_1 b_r + a_0 b_{r+1}$,
$b_{r+1} = -(a_{r+1} b_0 + a_r b_1 + \cdots + a_1 b_r)/a_0$. Hence, the required result follows. ■

Note that, in Proposition 5.3.6, $b_n \in \mathbb{Q}$ as $a_0 \in \mathbb{Q}$. We now look at the composition of formal power series. Recall that, if $f(x) = \sum\limits_{n\ge 0} a_n x^n, g(x) = \sum\limits_{n\ge 0} b_n x^n \in \mathfrak{P}(x)$ then the composition

$$(f \circ g)(x) = f(g(x)) = \sum_{n\ge 0} a_n (g(x))^n = \sum_{n\ge 0} a_n (\sum_{m\ge 0} b_m x^m)^n$$

may not be defined (just to compute the constant term of the composition, one may have to look at an infinite sum of rational numbers). For example, let $f(x) = e^x$ and $g(x) = x + 1$. Note that $g(0) = 1 \neq 0$. Here, $(f \circ g)(x) = f(g(x)) = f(x+1) = e^{x+1}$. So, as function $f \circ g$ is well defined, but there is no formal procedure to write e^{x+1} as $\sum\limits_{k\ge 0} a_k x^k \in \mathfrak{P}(x)$ (*i.e.*, with $a_k \in \mathbb{Q}$) and hence e^{x+1} is not a formal power series over $\mathbb{Q}$. The next result gives the condition under which the composition $(f \circ g)(x)$ is well defined.

Proposition 5.3.7. *Let* $f, g \in \mathfrak{P}(x)$. *Then, the composition* $(f \circ g)(x) \in \mathfrak{P}(x)$ *if either* f *is a polynomial or* $\text{CF}\big[x^0, g(x)\big] = 0$. *Moreover, if* $\text{CF}\big[x^0, f(x)\big] = 0$*, then there exists* $g \in \mathfrak{P}(x)$*, with* $\text{CF}\big[x^0, g(x)\big] = 0$*, such that* $(f \circ g)(x) = x$. *Furthermore,* $(g \circ f)(x) \in \mathfrak{P}(x)$ *and* $(g \circ f)(x) = x$.

Proof. As $(f \circ g)(x) \in \mathfrak{P}(x)$, let $(f \circ g)(x) = \sum\limits_{n \geq 0} c_n x^n$ and suppose that either f is a polynomial or $\text{CF}\big[x^0, g(x)\big] = 0$. Then, to compute $c_k = \text{CF}\big[x^k, (f \circ g)(x)\big]$, for $k \geq 0$, one just needs to consider the terms $\sum\limits_{n=0}^{k} a_n (g(x))^n$, whenever $f(x) = \sum\limits_{n \geq 0} a_n x^n$. Hence, each $c_k \in \mathbb{Q}$ and thus, $(f \circ g)(x) \in \mathfrak{P}(x)$. This completes the proof of the first part. We leave the proof of the other part for the reader. ∎

The proof of the next result is left for the reader.

Proposition 5.3.8. **[Basic tricks]** *Recall the following statements from Binomial theorem and Theorem 4.6.1.*

1. $\text{CF}\big[x^n, (1-x)^{-r} = (1 + x + x^2 + \cdots)^r\big] = C(n+r-1, n)$.
2. $(1 - x^m)^n = 1 - C(n,1)x^m + C(n,2)x^{2m} - \cdots + (-1)^n x^{nm}$.
3. $(1 + x + x^2 + \cdots + x^{m-1})^n = \left(\dfrac{1 - x^m}{1 - x}\right)^n = (1 - x^m)^n (1 + x + x^2 + \cdots)^n$.

We now define the formal differentiation in $\mathfrak{P}(x)$ and give some important results. The proof is left for the reader.

Definition 5.3.9. Let $f(x) = \sum\limits_{n \geq 0} a_n x^n \in \mathfrak{P}(x)$. Then, the formal differentiation of $f(x)$, denoted $f'(x)$, is defined by

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} + \cdots = \sum_{n \geq 1} n a_n x^{n-1}.$$

Proposition 5.3.10. **[ogf: tricks]** *Let $g(x), h(x)$ be the ogf's for the sequences $(a_r)_0^\infty$, $(b_r)_0^\infty$, respectively. Then, the following are true.*

1. *$Ag(x) + Bh(x)$ is the ogf for $(Aa_r + Bb_r)_0^\infty$.*
2. *$(1-x)g(x)$ is the ogf for the sequence $a_0, a_1 - a_0, a_2 - a_1, \cdots$.*
3. *$(1 + x + x^2 + \cdots)g(x) = (1-x)^{-1}g(x)$ is the ogf for $(M_r)_0^\infty$, where $M_r = a_r + a_{r-1} + \cdots + a_0$.*
4. *$g(x)h(x)$ is the ogf for $(c_r)_0^\infty$, where $c_r = a_0 b_r + a_1 b_{r-1} + a_2 b_{r-2} + \cdots + a_r b_0$.*
5. *$xf'(x)$ is the ogf for $(ra_r)_1^\infty$.*

Proof. For example, to prove (3), note that if $g(x) = a_0 + a_1 x + a_2 x^2 + \cdots$, then the coefficient of x^2 in $(1 + x + x^2 + \cdots)(a_0 + a_1 x + a_2 x^2 + \cdots)$ is $a_2 + a_1 + a_0$. ∎

Example 5.3.11. 1. Let $a_r = 1$ for all $r \geq 0$. Then, the ogf of the sequence $(a_r)_0^\infty$ equals $1 + x + x^2 + \cdots = (1-x)^{-1} = f(x)$. So, for $r \geq 0$, the ogf for

   (a) $a_r = r$ is $xf'(x)$ and

   (b) $a_r = r^2$ is $x\big(f'(x) + xf''(x)\big)$.

   (c) $a_r = 3r + 5r^2$ is $3xf'(x) + 5\big(xf'(x) + x^2 f''(x)\big) = 8x(1-x)^{-2} + 10x^2(1-x)^{-3}$.

2. Determine the number of ways to distribute 50 coins among 30 students so that no student gets more than 4 coins equals

$$\begin{aligned} \text{CF}\big[x^{50}, (1 + x + x^2 + x^3 + x^4)^{30}\big] &= \text{CF}\big[x^{50}, (1 - x^5)^{30}(1-x)^{-30}\big] \\ &= C(79, 50) - 30C(74, 45) + C(30, 2)C(69, 40) + \cdots \\ &= \sum_{i=0}^{10} (-1)^i C(30, i) C(79 - 5i, 50 - 5i). \end{aligned}$$

3. For $n, r \in \mathbb{N}$, determine the number of solutions to $y_1 + \cdots + y_n = r$ with $y_i \in \mathbb{N}_0, 1 \leq i \leq n$.

   Ans: Recall that this number equals $C(r+n-1, r)$ (see Theorem 4.3.3).

   Alternate. We can think of the problem as follows: the above system can be interpreted as coming from the monomial x^r, where $r = y_1 + \cdots + y_n$. Thus, the problem reduces to finding the coefficients of x^{y_k} of a formal power series, for $y_k \geq 0$. Now, recall that $\text{CF}\big[x^{y_k}, (1-x)^{-1}\big] = 1$. Hence, the question reduces to computing

$$\text{CF}\left[x^r, \frac{1}{(1-x)(1-x)\cdots(1-x)}\right] = \text{CF}\left[x^r, \frac{1}{(1-x)^n}\right] = C(r+n-1, r).$$

4. Evaluate $\sum\limits_{k=0}^{\infty} \frac{1}{2^k} k$. Put $f(x) = (1-x)^{-1}$. Then, using Proposition 5.3.10, the required sum is $\frac{1}{2} f'(1/2) = 2$. Alternately (rearranging terms of an absolutely convergent series) it is

$$\begin{array}{ll}
\frac{1}{2} & + \\
\frac{1}{4} + \frac{1}{4} & + \\
\frac{1}{8} + \frac{1}{8} + \frac{1}{8} & + \\
\vdots & \\
\hline
1 + \frac{1}{2} + \cdots & = 2.
\end{array}$$

5. Determine a closed form expression for $\sum\limits_{n \geq 0} n x^n \in \mathfrak{P}(x)$.

   Ans: As $(1-x)^{-1} = \sum\limits_{n\geq 0} x^n$, one has $(1-x)^{-2} = \big((1-x)^{-1}\big)' = \left(\sum\limits_{n\geq 0} x^n\right)' = \sum\limits_{n\geq 0} n x^{n-1}$. Thus, the closed form expression is $\dfrac{x}{(1-x)^2}$.

   Alternate. Let $S = \sum\limits_{n\geq 0} n x^n = x + 2x^2 + 3x^3 + \cdots$. Then, $xS = x^2 + 2x^3 + 3x^4 + \cdots$. Hence, $(1-x)S = \sum\limits_{k\geq 1} x^k = x \sum\limits_{k \geq 0} x^k = \dfrac{x}{1-x}$. Thus, $S = \dfrac{x}{(1-x)^2}$.

6. Determine the sum of the first N positive integers.

   Ans: Using previous example, note that $k = \text{CF}\big[x^{k-1}, (1-x)^{-2}\big]$. Therefore, by Proposition 5.3.10, one has $\sum\limits_{k=1}^{N} k = \text{CF}\big[x^{N-1}, \big((1-x)^{-1} \cdot (1-x)^{-2}\big]\big)$ and hence

$$\sum_{k=1}^{N} k = \text{CF}\big[x^{N-1}, (1-x)^{-3}\big] = C(N+1, N-1) = \frac{N(N+1)}{2}.$$

7. Determine the sum of the squares of the first N positive integers.

   Ans: Recall $\sum\limits_{n\geq 0} n x^n = \frac{x}{(1-x)^2}$. Thus, $\sum\limits_{n\geq 0} n^2 x^n = x\left(\sum\limits_{n\geq 0} n x^n\right)' = x\left(\frac{x}{(1-x)^2}\right)' = \dfrac{x(1+x)}{(1-x)^3}$. Hence,

$$\begin{aligned}
\sum_{k=1}^{N} k^2 &= \text{CF}\left[x^N, \frac{1}{1-x} \cdot \frac{x(1+x)}{(1-x)^3}\right] = \text{CF}\left[x^{N-1}, \frac{1}{(1-x)^4}\right] + \text{CF}\left[x^{N-2}, \frac{1}{(1-x)^4}\right] \\
&= C(N+2, N-1) + C(N+1, N-2) = \frac{N(N+1)(2N+1)}{6}.
\end{aligned}$$

Exercise **5.3.12.** *1. For $n, r \in \mathbb{N}$ and $x_i \in \mathbb{N}_0$ for $1 \leq i \leq n$, determine the number of solutions to $x_1 + 2x_2 + \cdots + n x_n = r$.*

2. Determine $\sum\limits_{k=0}^{\infty} \frac{1}{2^k} C(n+k-1, k)$.

3. *Find the number of non-negative integer solutions of* $a+b+c+d+e=27$, *satisfying*
   (a) $3 \le a \le 8$,
   (b) $3 \le a, b, c, d \le 8$
   (c) c *is a multiple of* 3 *and* e *is a multiple of* 4.

4. *Determine the number of ways in which* 100 *voters can cast their* 100 *votes for* 10 *candidates such that no candidate gets more than* 20 *votes.*

5. *Determine a closed form expression for* $\sum\limits_{k=1}^{N} k^3$.

6. *Determine a closed form expression for* $\sum\limits_{n\ge0} \dfrac{n^2+n+6}{n!}$.

7. *Verify the following table of formal power series.*

Table of Formal Power Series

$e^x = \sum\limits_{k\ge0} \frac{x^k}{k!}$	$(1+x)^n = \sum\limits_{r\ge0} C(n,k)x^k, n \in \mathbb{N}_0$
$\cos(x) = \sum\limits_{r\ge0} \frac{(-1)^r x^{2r}}{(2r)!}$	$\sin(x) = \sum\limits_{r\ge0} \frac{(-1)^r x^{2r+1}}{(2r+1)!}$
$\cosh(x) = \sum\limits_{r\ge0} \frac{x^{2r}}{(2r)!}$	$\sinh(x) = \sum\limits_{r\ge0} \frac{x^{2r+1}}{(2r+1)!}$
Radius of convergence: $\lvert x\rvert < 1$	
$\log(1-x) = -\sum\limits_{k\ge1} \frac{x^k}{k}$	
$\frac{1}{1-x} = \sum\limits_{k\ge0} x^k$	$\frac{1}{(1-x)^n} = \sum\limits_{k\ge0} C(n+k-1,k)x^k, n \in \mathbb{N}$
$\frac{(1+x)^n}{x^r} = \sum\limits_{k\ge-r} C(n,r+k)x^k$	$\frac{x^n}{(1-x)^{n+1}} = \sum\limits_{k\ge0} C(k,n)x^k, n \in \mathbb{N}_0$
Radius of convergence: $\lvert x\rvert < \frac{1}{4}$	
$\frac{1}{\sqrt{1-4x}} = \sum\limits_{k\ge0} C(2k,k)x^k$	$\frac{1-\sqrt{1-4x}}{2x} = \sum\limits_{k\ge0} \frac{1}{k+1} C(2k,k)x^k$

Definition 5.3.13. For $n, k \in \mathbb{N}$, let $(n_1, n_2, \cdots, n_k)$ be a partition of $n \in \mathbb{N}$ into k parts. So, $n_i \ge n_{i+1}$, for $1 \le i \le k-1$. Then, the **Ferrer's Diagram** of $(n_1, n_2, \cdots, n_k)$ is a pictorial representation (pattern) using dots in the following way: place n_1 dots in the first row. The n_2 dots in the second row are placed in such a way to cover the first n_2 dots of the first row and so on (see Figure 5.1).

Example 5.3.14. 1. $(1,1,1,1)$, $(2,2)$, $(2,1,1)$ are a few partitions of 4.

2. Ferrer's diagram for $\lambda = (5,3,3,2,1,1)$ and λ' are given below.

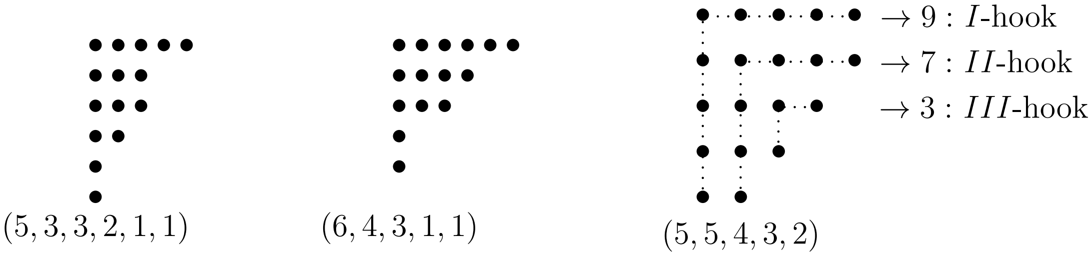


Figure 5.1: Ferrer's diagram of $\lambda = (5,3,3,2,1,1)$, λ' and hook length of $(5,5,4,3,2)$

3. Let λ be a partition and μ it's Ferrer's diagram. Then, the diagram μ' obtained by interchanging the rows and columns of μ is called the **conjugate** of λ, denoted λ'. Thus, the conjugate of the partition $(5,3,3,2,1,1)$ is $(6,4,3,1,1)$, another partition of 15.

Definition 5.3.15. A partition λ is said to be **self conjugate** if the Ferrer's diagram of λ and λ' is the same.

Example 5.3.16. Find a one-one correspondence between self conjugate partitions and partitions of n into distinct odd terms.

Ans: Let λ be a self conjugate partition with k diagonal dots. For $1 \le i \le k$, define $n_i =$ number of dots in the i-th 'hook' (dotted lines in Figure 5.1). Since λ is self-conjugate, each of n_i's are odd.

Conversely, given any partition, say $(x_1, \ldots, x_k)$ with odd terms, we can get a self conjugate partition by putting x_1 dots in the first 'hook', x_2 dots in the second 'hook' and so on. Since each x_i is odd, the hook is symmetric and $x_i \le x_{i-1} + 2$, for $2 \le i \le k$, implies that the corresponding diagram of dots is indeed a Ferrer's diagram and hence the result follows.

Theorem 5.3.17. **[Euler: partition of** n**]** *The generating function for* π_n *is*

$$\varepsilon(x) = (1+x+x^2+\cdots)(1+x^2+x^4+\cdots)\cdots(1+x^n+x^{2n}+\cdots) = \frac{1}{(1-x)(1-x^2)\cdots(1-x^n)}.$$

Proof. Note that any partition λ of n has m_1 copies of 1, m_2 copies of 2 and so on till m_n copies of n, where $m_i \in \mathbb{N}_0$ for $1 \le i \le n$ and $\sum\limits_{i=1}^{n} m_i = n$. Hence, λ uniquely corresponds to $(x^1)^{m_1}(x^2)^{m_2}\cdots(x^n)^{m_n}$ in the word-expansion of

$$(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)\cdots(1+x^n+x^{2n}+\cdots).$$

Thus, $\pi_n = \text{CF}[x^n, \varepsilon(x)]$. ■

Example 5.3.18. Let $f(n)$ be the number of partitions of n in which no part is 1. Then, note that the ogf for $f(n)$ is $(1-x)\varepsilon(x)$. Hence, using Proposition 5.3.10, $f(n) = \pi_n - \pi_{n-1}$.

Alternate. Let $\lambda = (n_1, \ldots, n_k)$ be a partition of n with $n_k = 1$. Then, λ gives a partition of $n-1$, namely $(n_1, \ldots, n_{k-1})$. Conversely, if $\mu = (t_1, \ldots, t_k)$ is a partition of $n-1$, then $(t_1, \ldots, t_k, 1)$ is a partition of n with last part 1, Hence, the required result follows.

The next result is the same idea as Theorem 5.3.17 and hence the proof is omitted.

Theorem 5.3.19. *The number of partitions of n with entries at most r is* $\text{CF}\left[x^n, \prod\limits_{i=1}^{r} \frac{1}{1-x^i}\right]$.

Corollary 5.3.20. *Fix $n, r \in \mathbb{N}$. Then, the ogf for the number of partitions of n into at most r parts, is* $\frac{1}{(1-x)(1-x^2)\cdots(1-x^r)}$.

Proof. Note that by using Ferrer's diagram (taking conjugate) we see that the number of partitions of n into at most r parts is same as the number of partitions of n with entries at most r. So, by Theorem 5.3.19, this number is $\text{CF}\left[x^n, \prod\limits_{i=1}^{r} \frac{1}{1-x^i}\right]$. ■

Theorem 5.3.21. **[ogf of** $\pi_n(r)$**]** *Fix $n, r \in \mathbb{N}$. Then, the ogf for $\pi_n(r)$, the number of partitions of n into r parts, is* $\frac{x^r}{(1-x)(1-x^2)\cdots(1-x^r)}$.

Proof. Consider a partition $(\lambda_1, \ldots, \lambda_r)$ of n. So, $n \ge r$. Assume that $\lambda_1, \ldots, \lambda_k > 1$ and $\lambda_{k+1}, \ldots, \lambda_r = 1$. Then $(\lambda_1 - 1, \ldots, \lambda_k - 1)$ is a partition of $n-r$ into at most r parts.

Conversely, if $(\mu_1, \ldots, \mu_k), k \le r$, is a partition of $n-r$ into at most r parts, then $(\mu_1 + 1, \ldots, \mu_k + 1, 1, \ldots, 1)$, where the number of 1's is $r-k$ times, is an r partition of n.

Thus, the number of r partitions of n is the same as the number of partitions of $n-r$ with at most r parts. Thus, by Corollary 5.3.20 the required number is $\text{CF}\left[x^{n-r}, \frac{1}{(1-x)(1-x^2)\cdots(1-x^r)}\right]$. Hence, the ogf for $\pi_n(r)$ is

$$\frac{x^r}{(1-x)(1-x^2)\cdots(1-x^r)}.$$

■

Exercise **5.3.22.** 1. *For $n, r \in \mathbb{N}$, prove that $\pi_n(r)$ is the number of partitions of $n + C(r,2)$ into r unequal parts.*

2. *Let $P, M \subseteq \mathbb{N}$ and $f(n)$ be the number of partitions of n where parts are from P and multiplicities are from M. Find the generating function for the numbers $f(n)$.*

Theorem 5.3.23. *Suppose there are k types of objects.*

1. *If there is an unlimited supply of each object, then the egf of the number of r-permutations is e^{kx}.*

2. *If there are m_i copies of i-th object, then the egf of the number of r-permutations is*

$$\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{m_1}}{m_1!}\right)\cdots\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{m_k}}{m_k!}\right).$$

3. *Moreover, $n!S(r,n)$ is the coefficient of $\frac{x^r}{r!}$ in $(e^x-1)^n$.*

Proof. Part 1: Since there are unlimited supply of each object, the egf for each object corresponds to $e^x = 1 + x + \cdots + \dfrac{x^n}{n!} + \cdots$. Hence, the required result follows.

Part 2: Argument is similar to that of Part 1 and is omitted.

Part 3: Recall that $n!S(r,n)$ is the number of surjections from $\{1, 2, \ldots, r\}$ to $X = \{s_1, \cdots, s_n\}$. Each surjection can be viewed as word of length r of elements of X, with each s_i appearing at least once. Thus, we need a selection of $k_i \in \mathbb{N}$ copies of s_i, with $\sum\limits_{i=1}^{n} k_i = r$. Also, by Theorem 4.1.23, this number equals $C(r; k_1, \cdots, k_n)$. Hence,

$$n!S(r,n) = r!\text{CF}\left[x^r, \left(x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)^n\right] = \text{CF}\left[\frac{x^r}{r!}, (e^x-1)^n\right].$$

■

Example 5.3.24. 1. In how many ways can you get Rs 2007 using denominations $1, 10, 100, 1000$ only?

Ans: $\text{CF}\left[x^{2007}, \dfrac{1}{(1-x)(1-x^{10})(1-x^{100})(1-x^{1000})}\right]$.

2. If we use at most 9 of each denomination in Part 1, then this number is

$$\text{CF}\left[x^{2007}, \left(\sum_{i=1}^{9} x^i\right)\left(\sum_{i=1}^{9} x^{10i}\right)\left(\sum_{i=1}^{9} x^{100i}\right)\left(\sum_{i=1}^{9} x^{1000i}\right)\right] = \text{CF}\left[x^{2007}, \frac{1-x^{10000}}{1-x}\right] = 1.$$

3. Every natural number has a unique base-r representation ($r \geq 2$). Note that Part 2 corresponds to the case $r = 10$.

4. Consider n integers $k_1 < k_2 < \cdots < k_n$ with $\gcd(k_1, \ldots, k_n) = 1$. Then, the number of natural numbers not having a partition using $\{k_1, \ldots, k_n\}$ is finite. Determining the largest such integer (**Frobenius number**) is the coin problem/ money changing problem. The general problem is NP-hard. No closed form formula is known for $n > 3$.

Notice!

Some times we have a way to obtain a recurrence relation from the generating function. This is important and hence study the next example carefully.

Example 5.3.25. 1. Suppose $F = \dfrac{1}{(1-x)(1-x^{10})(1-x^{100})(1-x^{1000})} = \sum\limits_{n\geq 0} a_n x^n$. Then, taking log and differentiating, we get

$$F' = F\left[\frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}}\right].$$

So,

$$na_n = \text{CF}\big[x^{n-1}, F'\big] = \text{CF}\left[x^{n-1}, F\left[\frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}}\right]\right] = \sum_{k=1}^{n} a_{n-k} b_k,$$

where

$$b_k = \text{CF}\left[x^{k-1}, \left[\frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}}\right]\right] = \begin{cases} 1 & \text{if } 10 \nmid k \\ 11 & \text{if } 10|k, 100 \nmid k \\ 111 & \text{if } 100|k, 1000 \nmid k \\ 1111 & \text{else.} \end{cases}$$

2. We know that $\lim\limits_{n\to\infty} \sum\limits_{k=1}^{n} \frac{1}{k} = \infty$. What about $\lim\limits_{n\to\infty} \sum\limits_{k=1}^{n} \frac{1}{p_k}$, where p_k is the k-th prime?

Ans: For $n > 1$, let $s_n = \sum\limits_{k=1}^{n} \frac{1}{k}$. Then, note that

$$s_n \leq \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{9} + \cdots\right)\cdots\left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots\right) = \prod_{k=1}^{n}(1 + \frac{1}{p_k - 1}).$$

Thus,

$$\log s_n \leq \log\left(\prod_{k=1}^{n}(1 + \frac{1}{p_k - 1})\right) \leq \sum_{k=1}^{n}\log(1 + \frac{1}{p_k - 1}) \leq \sum_{k=1}^{n}\frac{1}{p_k - 1} \leq 1 + \sum_{k=1}^{n-1}\frac{1}{p_k}.$$

As $n \to \infty$, we see that $\lim\limits_{n\to\infty} \sum\limits_{i=1}^{n} \frac{1}{p_i} = \infty$ as $\lim\limits_{n\to\infty} \log s_n = \infty$.

3. Let X be the set of natural numbers with only prime divisors $2, 3, 5, 7$. Then,

$$1 + \sum_{n\in X}\frac{1}{n} = (1 + \frac{1}{2} + \frac{1}{4} + \cdots)(1 + \frac{1}{3} + \frac{1}{9} + \cdots)\cdots(1 + \frac{1}{7} + \frac{1}{49} + \cdots) = \frac{2}{1}\frac{3}{2}\frac{5}{4}\frac{7}{6} = \frac{35}{8}.$$

EXERCISE **5.3.26.** *1. Let $\sigma(n) = \sum\limits_{d|n} d$, for $n \in \mathbb{N}$. Then, prove that $n\pi_n = \sum\limits_{k=1}^{n} \pi_{n-k}\sigma(k)$.*

2. A Durfee square is the largest square in a Ferrer's diagram. Find the generating function for the number of self conjugate partitions of n with a fixed size k of Durfee square. Hence, show that $(1+x)(1+x^3)\cdots = 1 + \sum\limits_{k=1}^{\infty} \dfrac{x^{k^2}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}$.

3. Show that the number of partitions of n into distinct terms (each term is distinct) is the same as the number of partitions of n into odd terms (each term is odd).

4. Find the number of r-digit binary numbers that can be formed using an even number of 0's and an even number of 1's.

5. Find the egf of the number of words of size r using A, B, C, D, E,

(a) if the word has all the letters and the letter A appears an even many times.

(b) if the word has all the letters and the first letter of the word appears an even number of times.

6. *A permutation σ of $\{1, 2, \ldots, n\}$ is said to be* **connected** *if there does not exist k, $1 \le k < n$ such that σ takes $\{1, 2, \ldots, k\}$ to itself. Let c_n denote the number of connected permutations of $\{1, 2, \ldots, n\}$ (put $c_0 = 0$), then show that*

$$\sum_{k=1}^{n} c_k (n-k)! = n!.$$

Hence, derive the relationship between the generating functions of $(n!)$ and (c_n).

7. *Let $f(n, r)$ be the number of partitions of n where each part repeats less than r times. Let $g(n, r)$ be the number of partition of n where no part is divisible by r. Show that $f(n, r) = g(n, r)$.*

8. *Find the number of 9-sequences that can be formed using $0, 1, 2, 3$ in each case.*

   (a) The sequence has an even number of 0's.

   (b) The sequence has an odd number of 1's and an even number of 0's.

   (c) No digit appears exactly twice.

5.4 Recurrence Relation

Definition 5.4.1. A **recurrence relation** is a way of recursively defining the terms of a sequence as a function of preceding terms together with certain initial conditions.

Example 5.4.2. $a_n = 3 + 2a_{n-1}$ for $n \ge 1$ with the **initial condition** $a_0 = 1$ is a recurrence relation. Note that it completely determines the sequence $(a_n) = \{1, 5, 13, 29, 61, \ldots\}$.

Definition 5.4.3. For a sequence (a_n), the **first difference** $d(a_n)$ is $a_n - a_{n-1}$. The **k-th difference** $d^k(a_n) = d^{k-1}(a_n) - d^{k-1}(a_{n-1})$. A **difference equation** is an equation involving a_n and its differences.

Example 5.4.4. 1. $a_n - d^2(a_n) = 5$ is a difference equation. But, note that it doesn't give a recurrence relation as we don't have any initial condition(s).

2. Every recurrence relation can be expressed as a difference equation. The difference equation corresponding to the recurrence relation $a_n = 3 + 2a_{n-1}$ is $a_n = 3 + 2(a_n - d(a_n))$.

Definition 5.4.5. A **solution** of a recurrence relation is a function $u(n)$, generally denoted by u_n, satisfying the recurrence relation.

Example 5.4.6. 1. $u_n = 2^{n+2} - 3$ is a solution of $a_n = 3 + 2a_{n-1}$ with $a_0 = 1$.

2. The **Fibonacci sequence** is given by $a_n = a_{n-1} + a_{n-2}$ for $n \ge 2$ with $a_0 = 0$, $a_1 = 1$. Use $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$ and $\left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{3-\sqrt{5}}{2}$ to verify that $a_n = \dfrac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ is a solution of the recurrence relation that defines the Fibonacci sequence.

Definition 5.4.7. A recurrence relation is a **linear nonhomogeneous recurrence relation** with constant coefficients (**LNHRRCC**) of order r if, for a known function f

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + f(n), \text{ where } c_i \in \mathbb{R} \text{ for } 1 \le i \le r, c_r \ne 0. \tag{5.3}$$

If $f = 0$, then Equation (5.3) is homogeneous and is called the associated **linear homogeneous recurrence relation** with constant coefficients (**LHRRCC**).

Theorem 5.4.8. *For $k \in \mathbb{N}$, let $f_i, 1 \le i \le k$ be known functions. Consider the k LNHRRCC*

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + f_i(n) \text{ for } i = 1, \ldots, k, \tag{5.4}$$

with the same set of initial conditions. If $u_i(n)$, for $1 \leq i \leq k$, is a solution of the i-th recurrence then,

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + \sum_{i=1}^{k} \alpha_i f_i(n) \tag{5.5}$$

under the same set of initial conditions has $\sum\limits_{i=1}^{k} \alpha_i u_i(n)$ as it's solution.

Proof. The proof is left as an exercise for the reader.

Definition 5.4.9. Consider a LHRRCC $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$ with $c_r \neq 0$. If $a_n = x^n$ is a solution, then either $x = 0$ or x is a root of

$$x^r - c_1 x^{r-1} - \cdots - c_r = 0. \tag{5.6}$$

Equation (5.6) is called the characteristic equation of the given LHRRCC. If $x_1, \ldots, x_r$ are the roots of Equation (5.6), then $a_n = x_i^n$ (and hence $a_n = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for $\alpha_i \in \mathbb{R}$) is a solution of the given LHRRCC.

Theorem 5.4.10. [**General solution: distinct roots**] *If the roots x_i, $i = 0, \ldots, r-1$ of Equation (5.6) are distinct, then every solution $u(n)$ is a linear combination of x_i^n. Moreover, the solution is unique if we are given r consecutive initial conditions.*

Proof. Let $u(n)$ be any solution. Then, we need to show that there exist $\alpha_i \in \mathbb{R}, 0 \leq i \leq r-1$, such that $u(n) = \sum\limits_{i=0}^{r-1} \alpha_i x_i^n$. Substituting $n = 0, 1, \ldots, r-1$, one obtains the linear system

$$\begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(r-1) \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ x_0 & \cdots & x_{r-1} \\ & \ddots & \\ x_0^{r-1} & \cdots & x_{r-1}^{r-1} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{r-1} \end{bmatrix}$$

in the unknowns α_i's $0 \leq i \leq r-1$. Since the above $r \times r$ matrix (commonly known as the Vandermonde matrix) is invertible, there exist $\alpha_0, \ldots, \alpha_{r-1}$, such that $u(m) = \sum\limits_{i=0}^{r-1} \alpha_i x_i^m$ for $0 \leq m \leq r-1$. Hence, we have proved the result for the first r values of $u(n)$. So, let us assume that the result is true for $n < k$. Then, by definition

$$u(k) = \sum_{j=1}^{r} c_j h(k-j) = \sum_{j=1}^{r} c_j \sum_{i=0}^{r-1} \alpha_i x_i^{k-j} = \sum_{i=0}^{r-1} \alpha_i \sum_{j=1}^{r} c_j x_i^{k-j} = \sum_{i=0}^{r-1} \alpha_i x_i^k,$$

as for $n = k$, x_i^k is a solution of Equation (5.6). Thus, by PMI, $u(n) = \sum\limits_{i=0}^{r-1} \alpha_i x_i^n$ for all n. The uniqueness is left as an exercise for the reader. ■

Example 5.4.11.

1. Solve $a_n - 4a_{n-2} = 0$ for $n \geq 2$ with $a_0 = 1$ and $a_1 = 1$.

   Ans: Note that ± 2 are the roots of the characteristic equation, $x^2 - 4 = 0$. As the roots are distinct, the general solution is $a_n = \alpha(-2)^n + \beta 2^n$ for $\alpha, \beta \in \mathbb{R}$. The initial conditions give $\alpha + \beta = 1$ and $2\beta - 2\alpha = 1$. Hence, $\alpha = \frac{1}{4}, \beta = \frac{3}{4}$. Thus, the unique solutions is $a_n = 2^{n-2}\big(3 + (-1)^n\big)$.

2. Solve $a_n = 3a_{n-1} + 4a_{n-2}$ for $n \geq 2$ with $a_0 = 1$ and $a_1 = c$, a constant.

   Ans: Note that -1 and 4 are the roots of the characteristic equation, $x^2 - 3x - 4 = 0$. As the roots are distinct, the general solution is $a_n = \alpha(-1)^n + \beta 4^n$ for $\alpha, \beta \in \mathbb{R}$. Now, the initial conditions imply $\alpha = \frac{4-c}{5}$ and$\beta = \frac{1+c}{5}$. Thus, the unique general solution is

(a) $a_n = \dfrac{(4-c)(-1)^n}{5} + \dfrac{(1+c)4^n}{5}$, if $c \neq 4$.
(b) $a_n = 4^n$, if $c = 4$.

3. Solve the Fibonacci recurrence $a_n = a_{n-1} + a_{n-2}$ with initial conditions $a_0 = 0, a_1 = 1$.

   Ans: In this case, note that the roots of the characteristic equation, $x^2 - x - 1 = 0$, are $\frac{1\pm\sqrt{5}}{2}$. As the roots are distinct, the general solution is $a_n = \alpha\big(\frac{1+\sqrt{5}}{2}\big)^n + \beta\big(\frac{1-\sqrt{5}}{2}\big)^n$ for $\alpha, \beta \in \mathbb{R}$. Now, using the initial conditions, we get $\alpha = \frac{1}{\sqrt{5}}, \beta = -\alpha$. Hence, the required solution is

$$a_n = \alpha\Big(\frac{1+\sqrt{5}}{2}\Big)^n + \beta\Big(\frac{1-\sqrt{5}}{2}\Big)^n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \tag{5.7}$$

Theorem 5.4.12. **[General solution: multiple roots]** *Let t is a root of Equation (5.6) of multiplicity s. Then, $u(n) = t^n \left(\sum\limits_{i=0}^{s-1} \alpha_i n^i\right)$, for $\alpha_i \in \mathbb{R}, 0 \le i \le s-1$, is a solution (**basic solution**). In general, if t_i is a root of Equation (5.6) with multiplicity s_i), for $i = 1, \ldots, k$, then every solution is a sum of the k basic solutions.*

Proof. It is given that t is a zero of the polynomial $F = x^r - c_1x^{r-1} - \cdots - c_r$ of multiplicity s. Put $G_0 = x^{n-r}F = x^n - c_1x^{n-1} - \cdots - c_rx^{n-r}$ and $G_1 = xG_0'$, $G_2 = xG_1'$, …, $G_{s-1} = xG_{s-2}'$. Then, each of $G_0, G_1, \ldots, G_{s-1}$ has a zero at t. That is, for $i = 0, 1, \ldots, s-1$, we have

$$G_i(t) = t^n n^i - c_1 t^{n-1}(n-1)^i - \ldots - c_r t^{n-r}(n-r)^i = 0.$$

Thus, for any choice of $\alpha_i \in \mathbb{R}, 0 \le i \le s-1$, if one defines $P(k) = \sum\limits_{i=1}^{s-1} k^i \alpha_i$, for $k \ge 0$ then

$$\sum_{i=0}^{s-1} \alpha_i G_i(t) = t^n P(n) - c_1 t^{n-1} P(n-1) - \cdots - c_r t^{n-r} P(n-r) = 0.$$

Thus, by definition $u(n) - c_1u(n-1) - \cdots - c_ru(n-r) = 0$. Hence, $u(n)$ is a solution of the LHRRCC. The other part of the proof is left for the reader. ■

Example 5.4.13. Suppose that an LHRRCC has roots $2, 2, 3, 3, 3$. Then, the general solution is given by $2^n(\alpha_1 + n\alpha_2) + 3^n(\beta_1 + n\beta_2 + n^2\beta_3)$.

Theorem 5.4.14. **[LNHRRCC]** *Consider the LNHRRCC in Equation (5.3) and let u_n be a general solution to the associated LHRRCC. If v_n is a particular solution of the LNHRRCC, then $a_n = u_n + v_n$ is a general solution of the LNHRRCC.*

Proof. The proof is left for the reader. ■

Notice!

No general algorithm are there to solve an LNHRRCC. If $f(n) = a^n$ or n^k or a linear combination of these, then a particular solution can be easily obtained.

Obtaining particular solution after knowledge of the characteristic roots.

1. If $f(n) = a^n$ and a is not a root of Equation (5.3), then $v_n = ca^n$.
2. If $f(n) = a^n$ and a is a root of Equation (5.3) of multiplicity t, then $v_n = cn^ta^n$.
3. If $f(n) = n^k$ and 1 is not a root of Equation (5.3), then use $v_n = c_0 + c_1n + \cdots + c_kn^k$.
4. If $f(n) = n^k$ and 1 is a root of Equation (5.3) of multiplicity t, then $v_n = n^t(c_0 + c_1n + \cdots + c_kn^k)$.

Example 5.4.15. 1. Let $a_n = 3a_{n-1} + 2n$ for $n \geq 1$ with $a_0 = 1$.

Ans: Observe that 3 is the characteristic root of the associated LHRRCC ($a_n = 3a_{n-1}$). Thus, the general solution of LHRRCC is $u_n = 3^n\alpha$. Note that 1 is not a characteristic root and hence a particular solution is $a+nb$, where a and b are to be computed using $a+nb = 3(a+(n-1)b)+2n$. This gives $a = \frac{-3}{2}$ and $b = -1$. Hence, $a_n = 3^n\alpha - n - \dfrac{3}{2}$. Using $a_0 = 1$, check that $\alpha = \dfrac{5}{2}$.

2. Let $a_n = 3a_{n-1} - 2a_{n-2} + 3(5)^n$ for $n \geq 3$ with $a_1 = 1, a_2 = 2$.

Ans: Observe that 1 and 2 are the characteristic roots of the associated LHRRCC ($a_n = 3a_{n-1} - 2a_{n-2}$). Thus, the general solution of the LHRRCC is $u_n = \alpha 1^n + \beta 2^n$. Note that 5 is not a characteristic root and thus, $v_n = c5^n$ is a particular solution of LNHRRCC if and only if $c5^n = 3c5^{n-1} - 2c5^{n-2} + 3(5)^n$. That is, if and only if $c = 25/4$. Hence, the general solution of LNHRRCC equals $a_n = \alpha + \beta 2^n + (25/4)5^n$, where compute α and β using the initial conditions.

3. In the above take $f(n) = 3(2^n)$. Then, we see that with $c(2)^n$ as a choice for a particular solution, we will have $4c = 6c - 2c + 12$, an absurd statement. But, with the choice $cn(2)^n$, we have $4nc = 6(n-1)c - 2(n-2)c + 12$, implying $c = 6$. Hence, the general solution of LNHRRCC is $a_n = \alpha + \beta 2^n + 6n2^n$, where compute α and β using the initial conditions.

5.5 Generating Function from Recurrence Relation

Sometimes we can find a solution to the recurrence relation using the generating function of a_n.

Example 5.5.1. 1. Consider $a_n = 2a_{n-1} + 1$, $a_0 = 1$.

Ans: Let $F(x) = a_0 + a_1x + \cdots$ be the generating function for $\{a_i\}$. Then,

$$F = 1 + \sum_{i=1}^{\infty} a_i x^i = 1 + \sum_{i=1}^{\infty}(2a_{i-1} + 1)x^i = \sum_{i=0}^{\infty} x^i + 2x\sum_{i=0}^{\infty} a_i x^i = \frac{1}{1-x} + 2xF.$$

Hence, $F = \frac{1}{(1-x)(1-2x)} = \frac{2}{1-2x} - \frac{1}{1-x}$. Thus, $a_n = \text{CF}[x^n, F] = 2^{n+1} - 1$.

2. Find the ogf F for the Fibonacci recurrence relation $a_n = a_{n-1} + a_{n-2}$, $a_0 = 0, a_1 = 1$.

Ans: Define $F(x) = \sum\limits_{n\geq 0} a_n x^n = \sum\limits_{n\geq 1} a_n x^n$. Then using the recurrence relation, we have

$$F(x) = \sum_{n\geq 0} a_n x^n = x + \sum_{n\geq 2}(a_{n-1} + a_{n-2})\, x^n = x + (x + x^2)F(x).$$

So, $F(x) = \frac{x}{1-x-x^2}$. Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Then it can be checked that $(1-\alpha x)(1-\beta x) = 1 - x - x^2$ and

$$F(x) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right) = \frac{1}{\sqrt{5}}\left(\sum_{n\geq 0}\alpha^n x^n - \sum_{n\geq 0}\beta^n x^n\right).$$

Therefore, $a_n = \text{CF}[x^n, F(x)] = \dfrac{1}{\sqrt{5}} \sum\limits_{n\geq 0} (\alpha^n - \beta^n)$, which equals Equation (5.7).

The next result follows using a small calculation and hence the proof is left for the reader.

Theorem 5.5.2. [Obtaining generating function from recurrence relation] *Consider the r-th order LHRRCC given by*

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} \text{ with initial conditions } a_i = A_i \text{ for } i = 0, 1, \ldots, r-1. \tag{5.8}$$

Then, the generating function of Equation (5.8) *equals*

$$\frac{\sum\limits_{i=0}^{r-1} A_i x^i \;-\; c_1 x \sum\limits_{i=0}^{r-2} A_i x^i \;-\; c_2 x^2 \sum\limits_{i=0}^{r-3} A_i x^i \;-\; \cdots \;-\; c_{r-1} x^{r-1} A_0}{1 \;-\; c_1 x \;-\; \cdots \;-\; c_r x^r}.$$

Example 5.5.3. 1. Find the ogf for the Catalan numbers C_n's.

Ans: Let $g(x) = 1 + \sum\limits_{n\geq 1} C_n x^n$, where $C_n = \frac{C(2n,n)}{n+1} = \frac{2(2n-1)}{n+1} C_{n-1}$ with $C_0 = 1$. Then,

$$\begin{aligned} g(x) - 1 &= \sum_{n\geq 1} C_n x^n = \sum_{n\geq 1} \frac{2(2n-1)}{n+1} C_{n-1} x^n \\ &= \sum_{n=1}^{\infty} \frac{4n+4}{n+1} C_{n-1} x^n + \sum_{n=1}^{\infty} \frac{-6}{n+1} C_{n-1} x^n = 4xg(x) + \frac{-6}{x} \int_0^x tg(t)dt. \end{aligned}$$

So, $[g(x) - 1 - 4xg(x)]x = -6 \int\limits_0^x tg(t)dt$. Now, we differentiate with respect to x to get $x(1-4x)g' + (1-2x)g = 1$. To solve the ode, we first observe that

$$\int \frac{1-2x}{x(1-4x)} = \int \left[\frac{1}{x} + \frac{2}{1-4x}\right] = \ln\left(\frac{x}{\sqrt{1-4x}}\right).$$

Thus, the integrating factor of the given ode is $\frac{x}{\sqrt{1-4x}}$. Hence, the ode can be re-written as

$$g(x)' \frac{x}{\sqrt{1-4x}} + g(x) \frac{1-2x}{(1-4x)^{3/2}} = \frac{1}{(1-4x)^{3/2}} \Leftrightarrow \frac{d}{dx}\left[g(x) \frac{x}{\sqrt{1-4x}}\right] = \frac{1}{(1-4x)^{3/2}}.$$

Hence, $g(x) \frac{x}{\sqrt{1-4x}} = \frac{1}{2\sqrt{1-4x}} + C$, where $C \in \mathbb{R}$. Or, equivalently $2xg(x) = 1 + 2C\sqrt{1-4x}$. Note that $C = -\frac{1}{2}$ as $C_0 = \lim\limits_{x\to 0} g(x) = 1$. Thus, the ogf of the Catalan numbers is

$$g(x) = \frac{1 - \sqrt{1-4x}}{2x}.$$

Alternate. Recall that C_n is the number of representations of the product of $n+1$ square matrices of the same size, using n pairs of brackets. From such a representation, remove the leftmost and the rightmost brackets to obtain the product of two representations of the form:

$$A_1(A_2 \cdots A_{n+1}),\ (A_1A_2)(A_3 \cdots A_{n+1}),\ \cdots,\ (A_1 \cdots A_k)(A_{k+1} \cdots A_{n+1}),\ \cdots,\ (A_1 \cdots A_n)A_{n+1}.$$

Hence, we see that

$$C_n = C_0 C_{n-1} + C_1 C_{n-2} + \cdots + C_{n-1} C_0. \tag{5.9}$$

Thus, if we define $g(x) = \sum\limits_{n=0}^{\infty} C_n x^n$, then for $n \geq 1$,

$$\text{CF}\big[x^{n-1}, g(x)^2\big] = \text{CF}\left[x^{n-1}, \left(\sum_{n=0}^{\infty} C_n x^n\right)^2\right] = \sum_{i=0}^{n-1} C_i C_{n-1-i} = C_n \text{ using Equation (5.9).}$$

That is, $\text{CF}\big[x^n, xg(x)^2\big] = C_n$. Hence, $g(x) = 1 + xg(x)^2$. Solving for $g(x)$, we get

$$g(x) = \frac{1}{2}\left(\frac{1}{x} \pm \sqrt{\frac{1}{x^2} - \frac{4}{x}}\right) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

As the function g is continuous (being a power series in the domain of convergence) and $\lim\limits_{x\to 0} g(x) = C_0 = 1$, it follows that

$$g(x) = \frac{1 - \sqrt{1-4x}}{2x}.$$

2. Fix $r \in \mathbb{N}$ and let (a_n) be a sequence with $a_0 = 1$ and $\sum\limits_{k=0}^{n} a_k a_{n-k} = C(n+r, r)$, for all $n \geq 1$. Determine a_n.

   Ans: Let $g(x) = \sum\limits_{n \geq 0} a_n x^n$. Then, note that $C(n+r, r) = c(n+(r+1)-1, n)$. Hence,

$$g(x)^2 = \sum_{n\geq 0}\left(\sum_{k=0}^{n} a_k a_{n-k}\right) x^n = \sum_{n\geq 0} C(n+r, r)x^n = \sum_{n\geq 0} C(n+r, n)x^n = \frac{1}{(1-x)^{r+1}}.$$

   Hence, $a_n = \text{CF}\Big[x^n, \frac{1}{(1-x)^{(r+1)/2}}\Big]$. For example, for $r = 2$ (see Equation (4.2)),

$$a_n = (-1)^n C(-3/2, n) = \frac{3 \cdot 5 \cdot 7 \cdots (2n+1)}{2^n \; n!} = \frac{(2n+1)!}{2^{2n} n! n!}.$$

3. Determine the sequence $\{f(n,m) \mid n, m \in \mathbb{N}_0\}$ which satisfies $f(n,0) = 1$ for all $n \geq 0$, $f(0,m) = 0$ for all $m > 0$ and

$$f(n,m) = f(n-1,m) + f(n-1,m-1) \text{ for } (n,m) \neq (0,0). \tag{5.10}$$

   Ans: For $n \geq 1$, define $F_n(x) = \sum\limits_{m\geq 0} f(n,m)x^m = 1 + \sum\limits_{m \geq 1} f(n,m)x^m$. Then $F_1(x) = 1 + x$ and for $n \geq 2$,

$$\begin{aligned} F_n(x) &= \sum_{m\geq 0} f(n,m)x^m = 1 + \sum_{m\geq 1}\left(f(n-1,m) + f(n-1,m-1)\right)x^m \\ &= 1 + \sum_{m\geq 1} f(n-1,m)x^m + \sum_{m\geq 1} f(n-1,m-1)x^m \\ &= F_{n-1}(x) + xF_{n-1}(x) = (1+x)F_{n-1}(x) = \cdots = (1+x)^n \end{aligned}$$

   as $F_1(x) = 1 + x$. Thus,

$$f(n,m) = \text{CF}[x^m, (1+x)^n] = \begin{cases} C(n,m) & \text{if } 0 \leq m \leq n \\ 0 & \text{if } m > n. \end{cases}$$

   Alternate. For $m \geq 1$, define $G_m(y) = \sum\limits_{n\geq 0} f(n,m)y^n = \sum\limits_{n\geq 1} f(n,m)y^n$. Then, $G_1(y) = \dfrac{y}{(1-y)^2}$ and for $m \geq 2$, Equation (5.10) gives

$$\begin{aligned} G_m(y) &= \sum_{n\geq 1} f(n,m)y^n = \sum_{n\geq 1}\left(f(n-1,m) + f(n-1,m-1)\right)y^n \\ &= \sum_{n\geq 1} f(n-1,m)y^n + \sum_{n\geq 1} f(n-1,m-1)y^n \\ &= yG_m(y) + yG_{m-1}(y). \end{aligned}$$

   Therefore, $G_m(y) = \dfrac{y}{1-y}G_{m-1}(y)$. As $G_1(y) = \dfrac{y}{(1-y)^2}$, one has $G_m(y) = \dfrac{y^m}{(1-y)^{m+1}}$. Thus,

$$f(n,m) = \text{CF}\left[y^n, \frac{y^m}{(1-y)^{m+1}}\right] = \text{CF}\left[y^{n-m}, \frac{1}{(1-y)^{m+1}}\right] = \begin{cases} C(n,m) & \text{if } 0 \leq m \leq n \\ 0 & \text{if } m > n. \end{cases}$$

4. Determine the sequence $\{S(n,m) \mid n, m \in \mathbb{N}_0\}$ which satisfy $S(0,0) = 1$, $S(n,m) = 0$ if either $m = 0$ or $n = 0$ but not both and

$$S(n,m) = mS(n-1,m) + S(n-1,m-1), \; (n,m) \neq (0,0). \tag{5.11}$$

Ans: For $n \geq 1$, define $G_m(y) = \sum\limits_{n \geq 0} S(n,m)y^n = \sum\limits_{n \geq 1} S(n,m)y^n$. Then, $G_1(y) = \frac{y}{1-y}$ and for $m \geq 1$, Equation (5.11) gives

$$\begin{aligned} G_m(y) &= \sum_{n\geq 0} S(n,m)y^n = \sum_{n \geq 1} \left(mS(n-1,m) + S(n-1,m-1)\right) y^n \\ &= m\sum_{n\geq 1} S(n-1,m)y^n + \sum_{n\geq 1} S(n-1,m-1)y^n \\ &= myG_m(y) + yG_{m-1}(y). \end{aligned}$$

Therefore, $G_m(y) = \dfrac{y}{1-my}G_{m-1}(y)$. As $G_1(y) = \dfrac{y}{1-y}$, one has

$$G_m(y) = \frac{y^m}{(1-y)(1-2y)\cdots(1-my)} = y^m \sum_{k=1}^{m} \frac{\alpha_k}{1-ky}, \tag{5.12}$$

where $\alpha_k = \dfrac{(-1)^{m-k}k^m}{k!\,(m-k)!}$, for $1 \leq k \leq m$. Thus,

$$\begin{aligned} S(n,m) &= \text{CF}\left[y^n, y^m \sum_{k=1}^{m} \frac{\alpha_k}{1-ky}\right] = \sum_{k=1}^{m} \text{CF}\left[y^{n-m}, \frac{\alpha_k}{1-ky}\right] \\ &= \sum_{k=1}^{m} \alpha_k k^{n-m} = \sum_{k=1}^{m} \frac{(-1)^{m-k}k^n}{k!\,(m-k)!} \qquad (5.13) \\ &= \frac{1}{m!}\sum_{k=1}^{m}(-1)^{m-k}k^n C(m,k) = \frac{1}{m!}\sum_{k=1}^{m}(-1)^k(m-k)^n C(m,k). \end{aligned}$$

Therefore, $S(n,m) = \dfrac{1}{m!}\sum\limits_{k=1}^{m}(-1)^k(m-k)^nC(m,k)$.

This identity is generally known as the **Stirling's Identity**.

Observation.

(a) Let us consider $H_n(x) = \sum\limits_{m \geq 0} S(n,m)x^m$. Then, verify that $H_n(x) = (x + xD)^n \cdot 1$ as $H_0(x) = 1$. Therefore, $H_1(x) = x$, $H_2(x) = x + x^2, \cdots$. Thus, we don't have a single expression for $H_n(x)$ which gives the value of $S(n,m)$'s. But, it helps in showing that $S(n,m)$, for fixed $n \in \mathbb{N}$, first increase and then decrease (commonly called *unimodal*).

The same holds for the sequence of binomial coefficients $\{C(n,m), m = 0,1,\ldots,n\}$.

(b) As there is no restriction on $n.m \in \mathbb{N}_0$, Equation (5.13) is also valid for $n < m$. But, we know that $S(n,m) = 0$, whenever $n < m$. Hence, we get the following identity,

$$\sum_{k=1}^{m} \frac{(-1)^{m-k}\;k^{n-1}}{(k-1)!\;(m-k)!} = 0 \text{ whenever } n < m.$$

5. For $n \in \mathbb{N}$, the n-th Bell number, denoted $b(n)$, is the number of partitions of $\{1,2,\ldots,n\}$. Thus, $b(n) = \sum\limits_{m=1}^{n} S(n,m)$, for $n \geq 1$ and $b(0) = 1$. Hence, for $n \geq 1$,

$$\begin{aligned} b(n) &= \sum_{m=1}^{n} S(n,m) = \sum_{m\geq 1} S(n,m) = \sum_{m \geq 1}\sum_{k=1}^{m} \frac{(-1)^{m-k}\;k^{n-1}}{(k-1)!\;(m-k)!} \\ &= \sum_{k\geq 1}\frac{k^n}{k!}\sum_{m \geq k}\frac{(-1)^{m-k}}{(m-k)!} = \frac{1}{e}\sum_{k\geq 1}\frac{k^n}{k!} = \frac{1}{e}\sum_{k\geq 0}\frac{k^n}{k!} \text{ as } 0^n = 0 \text{ for } n \neq 0. \qquad (5.14) \end{aligned}$$

Thus, Equation (5.14) is valid even for $n = 0$. As $b(n)$ has terms of the form $\dfrac{k^n}{k!}$, we compute its egf. Thus, if $B(x) = \sum\limits_{n\ge 0} b(n)\dfrac{x^n}{n!}$ then,

$$\begin{aligned}
B(x) &= 1 + \sum_{n\ge 1} b(n)\frac{x^n}{n!} = 1 + \sum_{n\ge 1}\left(\frac{1}{e}\sum_{k\ge 1}\frac{k^n}{k!}\right)\frac{x^n}{n!} \\
&= 1 + \frac{1}{e}\sum_{k\ge 1}\frac{1}{k!}\sum_{n\ge 1} k^n\frac{x^n}{n!} = 1 + \frac{1}{e}\sum_{k\ge 1}\frac{1}{k!}\sum_{n\ge 1}\frac{(kx)^n}{n!} \\
&= 1 + \frac{1}{e}\sum_{k\ge 1}\frac{1}{k!}\left(e^{kx} - 1\right) = 1 + \frac{1}{e}\sum_{k\ge 1}\left(\frac{(e^x)^k}{k!} - \frac{1}{k!}\right) \\
&= 1 + \frac{1}{e}\left(e^{e^x} - 1 - (e-1)\right) = e^{e^x - 1}. \qquad (5.15)
\end{aligned}$$

Recall that e^{e^x-1} is a valid formal power series (see Remark 5.3.5). Taking logarithm of Equation (5.15), we get $\log B(x) = e^x - 1$. Hence, $B'(x) = e^x B(x)$, or equivalently

$$B'(x) = \sum_{n\ge 1}\frac{b(n)x^{n-1}}{(n-1)!} = e^x\sum_{n\ge 0} b(n)\frac{x^n}{n!} = \sum_{m\ge 0}\frac{x^m}{m!}\cdot\sum_{n\ge 0} b(n)\frac{x^n}{n!}.$$

Thus,

$$\frac{b(n)}{(n-1)!} = \text{CF}\left[x^{n-1}, B'(x)\right] = \text{CF}\left[x^{n-1}, \sum_{m\ge 0}\frac{x^m}{m!}\cdot\sum_{n\ge 0} b(n)\frac{x^n}{n!}\right] = \sum_{m=0}^{n-1}\frac{1}{(n-1-m)!}\cdot\frac{b(m)}{m!}.$$

Hence, we get $b(n) = \sum\limits_{m=0}^{n-1} C(n-1, m)b(m)$, for $n \ge 1$, with $b(0) = 1$.

EXERCISE **5.5.4.** 1. *Find the number of binary words without having a subword* 00 *and* 111*.*

2. *Find the number of subsets of* $\{1, \ldots, n\}$ *not containing consecutive integers.*

3. *Let F_n be the nth Fibonacci number. Then, prove that F_n divides F_{nm} where n, m are positive integers.*

Objects-n distinct?	Places-r distinct?	Places nonempty?	Relate	Number
Y	Y	Y	Onto functions	$r!S(n,r) = \sum\limits_{i=0}^{r-1}(-1)^i C(r,i)(r-i)^n$
Y	Y	N	All functions	r^n
Y	N	Y	r-partition of a set	$S(n,r)$
Y	N	N	All partitions of a set	$b(n) = \sum\limits_{i=1}^{r} S(n,i)$
N	Y	Y	Positive integer solutions	$C(n-1, r-1)$
N	Y	N	Nonnegative integer solutions	$C(n+r-1, r-1)$
N	N	Y	r-partition of n	$\pi_n(r) = \text{CF}\left[x^{n-r}, \frac{1}{(1-x)(1-x^2)\cdots(1-x^r)}\right]$
N	N	N	Partitions of n of length $\le r$	$\sum\limits_{i=1}^{r}\pi_n(i)$

Exercise **5.5.5.** 1. *In a particular semester* 6 *students took admission in our PhD program. There were* 9 *professors who were willing to supervise these students. As a rule 'a student can have either one or two supervisors'. In how many ways can we allocate supervisors to these students if all the 'willing professors' are to be allocated? What if we have an additional condition that exactly one supervisor gets to supervise two students?*

2. (a) *Prove combinatorially that, for* $n \geq 2$, *we have* $D_n = (n-1)(D_{n-1} + D_{n-2})$.

   (b) *Use Part (a) to show that the exponential generating function of* D_n *is* $\dfrac{e^{-x}}{1-x}$.

3. *My friend says that he has* $n \geq 2$ *subsets of* $\{1, 2, \ldots, 14\}$ *each of which has size* 6. *Give a value of* n *so that we can guarantee 'some two of his subsets have* 3 *elements in common', without seeing his collection'? What is the smallest possible value of* n*?*

4. *Find the number of words of size* 12 *made using letters from* $\{A, B, C\}$ *in which 'BCA' does not appear (as a consecutive subword). For example:* $ABCABCCCCCBA$ *has an appearance of 'BCA' but* $BCCABCCABCCA$ *does not.*

5. *Find the number of* 8 *letter words made using alphabets from* $\{A, B, C, D\}$ *in which* 3 *consecutive letters are not allowed to be the same.*

6. *We have* 3 *blue bags,* 4 *red bags and* 5 *green bags. We have many balls of each of the colors blue, red and green. Fill in the blank with the smallest positive integer.*

   If we distribute _____ *balls (without seeing the colors) into these bags, then one of the following must happen:*

   (a) *a blue bag contains* 3 *blue balls or* 4 *red balls or* 5 *green balls*

   (b) *a red bag contains* 3 *blue balls or* 5 *red balls or* 7 *green balls*

   (c) *a green bag contains* 3 *blue balls or* 6 *red balls or* 9 *green balls*

7. *We have an integer polynomial* $f(x)$. *Fill in the blank with the smallest positive integer.*

   If $f(x) = 2009$ *has* _____ *many distinct integer roots, then* $f(x) = 9002$ *cannot have an integer root.*

8. (a) *In how many ways can one distribute* 10 *identical chocolates among* 10 *students?*

   (b) *In how many ways can one distribute* 10 *distinct chocolates among* 10 *students?*

   (c) *In how many ways can one distribute* 10 *distinct chocolates among* 10 *students so that each receives one?*

   (d) *In how many ways can one distribute* 15 *distinct chocolates among* 10 *students so that each receives at least one?*

   (e) *In how many ways can one distribute* 10 *out of* 15 *distinct chocolates among* 10 *students so that each receives one?*

   (f) *In how many ways can one distribute* 15 *distinct chocolates among* 10 *students so that each receives at most three?*

   (g) *In how many ways can one distribute* 15 *distinct chocolates among* 10 *students so that each receives at least one and at most three?*

   (h) *In how many ways can one distribute* 15 *identical chocolates among* 10 *students so that each receives at most three?*

9. (a) *In how many ways can one carry* 15 *distinct objects with* 10 *identical bags? Answer using* $S(n, r)$.

   (b) *In how many ways can one carry* 15 *distinct objects in* 10 *identical bags with no empty bag? Answer using* $S(n, r)$.

(c) *In how many ways can one carry* 15 *distinct objects in* 10 *identical bags with each bag containing at most three objects?*

(d) *In how many ways can one carry* 15 *identical objects in* 10 *identical bags?*

(e) *In how many ways can one carry* 15 *identical objects in* 10 *identical bags with no empty bag?*

(f) *In how many ways can one carry* 15 *identical objects in* 20 *identical bags?*

10. *What is the number of integer solutions of* $x + y + z = 10$*, with* $x \geq -1$*,* $y \geq -2$ *and* $z \geq -3$*?*

11. *Is the number of solutions of* $x+y+z = 10$ *in non-negative multiples of* $\frac{1}{2}$ *(*x, y, z *are allowed to be* $0, 1/2, 1, 3/2, \ldots$*) at most four times the number of non-negative integer solutions of* $x+y+z = 10$*?*

12. *How many words of length* 8 *can be formed using the English alphabets, where each letter can appear at most twice? Give answer using generating function.*

13. *Let* $p_1, \ldots, p_n$*,* $n \geq 2$ *be distinct prime numbers. Consider the set* $\{p_1, \ldots, p_n, p_1^2, \ldots, p_n^2\}$*. In how many ways can we partition the set into subsets of size two such that no prime is in the same subset containing its square?*

14. *What is the value of* $\sum\limits_{k=0}^{15} (-1)^k C(15, k)(15 - k)^5$*?*

15. *Give your answers using generating function.*

(a) *What is the number of partitions of* n *with entries at most* r*?*

(b) *What is the number of partitions of* n *with at most* r *parts?*

(c) *What is the number of partitions of* n *with exactly* r *parts (*$\pi_n(r)$*)?*

(d) *What is the number of partitions of* $n + C(r, 2)$ *with* r *distinct parts?*

(e) *What is the number of partitions of* n *with distinct entries?*

(f) *What is the number of partitions of* n *with entries odd?*

(g) *What is the number of partitions of* n *with distinct odd entries?*

(h) *What is the number of partitions of* n *which are self conjugate?*

16. *How many words of length* 15 *are there using the letters A,B,C,D,E such that each letter must appear in the word and A appears an even number of times? Give your answers using generating function.*

17. *The characteristic roots of a LHRRCC are* $2, 2, 2, 3, 3$*. What is the form of the general solution?*

18. *Consider the LNHRRCC* $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + 5^n$*. Give a particular solution.*

19. *Obtain the ogf for* a_n*, where* $a_n = 2a_{n-1} - a_{n-2} + 2^n$*,* $a_0 = 0$*,* $a_1 = 1$*.*

20. *Solve the recurrence relation* $a_n = 2a_{n-1} - a_{n-2} + 2^n + 5$*,* $a_0 = 0$*,* $a_1 = 1$*.*

21. *My class has* n *CSE,* m *MSC and* r *MC students. Suppose that* t *copies of the same book are to be distributed so that each branch gets at least* s*. In how many ways can this be done, if each student gets at most one? In how many ways can this be done, without the previous restriction? Answer only using generating function.*

EXERCISE **5.5.6.** 1. *My class has* n *CSE,* m *MSC and* r *MC students. Suppose that* t *distinct books are to be distributed so that each branch gets at least* s*. In how many ways can this be done, if each student gets at most one? In how many ways can this be done, without the previous restriction? Answer only using generating function.*

2. *My class has N students. Assume that, to conduct an exam, we have M identical answer scripts. In how many ways can we distribute the answer scripts so that each student gets at least* 2*. Answer only using generating function.*

3. *My class has N students. Assume that, for an exam, we have M questions; each student answers all the questions in an order decided by him/her (for example one can follow $1, 2, \cdots, M$ and another can follow $M, M-1, \cdots, 1$). In how many ways can it happen that some three or more students have followed the same order? Answer only using generating function.*

4. *When 'Freshers Welcome' was organized* 11 *teachers went to attend. There were* 4 *types of soft drinks available. In how many ways a total of* 18 *glasses of soft drinks can be served to them, in general? Answer only using generating function.*

Chapter 6

Introduction to Logic

6.1 Propositional Logic

We study logic to differentiate between valid and invalid arguments. An **argument** is a set of statements which has two parts: premise and conclusion. There can be many statements in the premise. Conclusion is just one statement. An argument has the structure

premise: Statement$_1$, ..., Statement$_k$; therefore conclusion: Statement$_c$.

Consider the following examples.

- Statement$_1$: If today is Monday, then Mr. X gets Rs. 5.
  Statement$_2$: Today is Monday.
  Statement$_c$: Therefore, Mr. X gets Rs. 5 (statement$_c$).

- Statement$_1$: If today is Monday, then Mr. X gets Rs. 5.
  Statement$_2$: Mr. X gets Rs. 5.
  Statement$_c$: Therefore, today is Monday.

- Statement$_1$: If today is Monday, then Mr. X gets Rs. 5.
  Statement$_2$: Today is Tuesday.
  Statement$_c$: Therefore, Mr. X gets Rs. 5.

- Statement$_1$: If today is Monday, then Mr. X gets Rs. 5.
  Statement$_2$: Today is Tuesday.
  Statement$_c$: Therefore, Mr. X does not get Rs. 5.

We understand that the first one is a valid argument, whereas the next three are not. In order to differentiate between valid and invalid argument, we need to analyze an argument. And in order to do that, we first have to understand 'what is a statement'. A simple statement is an expression which is either false or true but not both. We create complex statements from the old ones by using 'and', 'or' and 'not'.

For example, 'today is Monday' is a statement. 'Today is Tuesday' is also a statement. 'Today is Monday and today is Tuesday' is also a statement. 'Today is not Monday' is also a statement.

One way to analyze an argument is by writing it using symbols. The following definition captures the notion of a 'statement'.

Definition 6.1.1. 1. [**Atomic formulae and truth values**] Consider a nonempty finite set of symbols $\mathcal{F}$. We shall call an element of $\mathcal{F}$ as an **atomic formula** (also called **atomic variable**). (These are our simple statements). The **truth value** of each element in $\mathcal{F}$ is exactly one of T (for TRUE) and F (for FALSE). Normally, we use symbols $p, q, p_1, p_2, \ldots$ for atomic formulae.

2. [**Operations to create new formulae**] We use three symbols ‘$\vee$’ (called **disjunction/or**), ‘$\wedge$’ (called **conjunction/and**), and ‘$\neg$’ (called **negation**) to create new formulae. The way they are used and the way we attribute the truth value to such a new formula is described below.

If p and q are formulae, then $p \wedge q$, $p \vee q$, and $\neg p$ are formulae. The truth value of $p \wedge q$ is defined to be T when the truth values of both p and q are T. Its truth value is defined to be F in all other cases. The truth value of $p \vee q$ is defined to be T when the truth values of at least one of p and q are T. Its truth value is defined to be F when the truth values of both p and q are F. The truth value of $\neg p$ is defined to be T if the truth value of p is F. The truth value of $\neg p$ is defined to be F if the truth value of p is T.

Understanding $\vee$, $\wedge$ and $\neg$

The following tables describe how we attribute the truth values to $p \vee q$, $p \wedge q$ and $\neg p$.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	$\neg p$
T	F
F	T

How do we read these tables? Look at row 3 of the leftmost table (exclude the header). It tells that the formula $p \wedge q$ takes the truth value F if p takes truth value F and q takes T.

Remark 6.1.2. *We use brackets while creating new formulae to make the meaning unambiguous. For example, the expression $p \vee q \wedge r$ is ambiguous, where as $p \vee (q \wedge r)$ is unambiguous.*

Definition 6.1.3. 1. Sometimes we write ‘$f(p_1, \ldots, p_k)$ is a formula’ to mean that ‘f is a formula involving the atomic formulae $p_1, \ldots, p_k$’.

2. Let $f(p_1, \ldots, p_k)$ be a formula. Then, the truth value of f is determined based on the truth values of the atomic formulae $p_1, \ldots, p_k$. Since, there are 2 assignments for each $p_i, 1 \leq i \leq k$, there are 2^k ways of assigning truth values to these atomic formulae. An **assignment** of truth values to these atomic formulae is nothing but a function $A : \{p_1, \ldots, p_k\} \to \{T, F\}$.

3. By saying ‘TFT is an assignment to the atomic variables p, q, r’, we mean that the truth value of p is T, that of q is F and that of r is T. Keeping this in mind, all possible assignments to p, q, r are listed below. (Notice that, it is in the dictionary order, that is, ‘FFF appears before FFT in the list as if they are words in a dictionary’. The reader will notice that in the table given above, we have followed the reverse dictionary order while writing a truth table, which is natural to us. This should not create any confusion.)

p	q	r
F	F	F
F	F	T
F	T	F
F	T	T
T	F	F
T	F	T
T	T	F
T	T	T

4. A **truth table** for a formula $f(p_1, \ldots, p_k)$ is a table which systematically lists the truth values of f under every possible assignment of truth values to the involved atomic formulae. The following is a truth table for the formulae $p \vee (q \wedge r)$.

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$
F	F	F	F	F
F	F	T	F	F
F	T	F	F	F
F	T	T	T	T
T	F	F	F	T
T	F	T	F	T
T	T	F	F	T
T	T	T	T	T

5. In the previous table, if we fill the fourth column arbitrarily using T's and F's, will it be a truth table of some formula involving p, q and r? We shall talk about it later.

We have already noted that we use $\vee, \wedge$ and $\neg$ to create new formulae from old ones. Some of them will indeed be very important.

Definition 6.1.4. [**Conditional formulae**]

1. [p **implies** q] If p and q are formulae, then the formula $(\neg p) \vee q$ is denoted by $p \to q$ (read as p **implies** q). Its truth table is

p	q	$(\neg p) \vee q$
T	T	T
T	F	F
F	T	T
F	F	T

Observe

a) $p \to q$ takes the truth value F if and only if p takes the truth value T and q takes the truth value F.

b) If under some assignment '$p \to q$ takes the truth value T' and that 'in this assignment p is T', then it follows that in this assignment q must be T. This is why $p \to q$ is called 'if p then q'.

c) Other phrases used for 'if p then q' are 'p is sufficient for q' or 'p only if q' or 'q is a necessary condition for p'.

d) We sometimes use $p \leftarrow q$ to mean $q \to p$.

2. [p **if and only if** q] The formula $(p \leftrightarrow q)$ (called 'p if and only if q') means $(p \to q) \wedge (q \to p)$. Note that $(p \leftrightarrow q)$ takes the truth value 'T whenever p and q take the same truth values' and takes the truth value 'F whenever p and q take different truth values'. Its truth table is

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

3. [**Converse/Contrapositive**] The formula $q \to p$ is called the **converse** of $p \to q$ and the formula $\neg q \to \neg p$ is called the **contrapositive** of $p \to q$.

Discussion 6.1.5. [**Understanding a conditional formula**] When we assign different 'English statements' to the involved atomic formulae, we get an English statement corresponding to those formulae. For example, for the formula $p \to q$, consider the following statements:
p: you attend the class.
q: you understand the subject.
Then, $p \to q$ is the statement 'if you attend the class, then you understand the subject'. The formula $p \to q$ is true under the following three cases.

1. p is true and q is true: this means 'you attend the class and understand the subject'.
2. p is false and q is false: this means 'you do not attend the class and do not understand the subject'.
3. p is false and q is true: this means 'you do not attend the class but understand the subject'.

The formula $p \to q$ is false if 'p is true and q is false', which means 'you attend the class and do not understand the subject'.

Definition 6.1.6. [**Connectives**] The symbols $\vee, \wedge, \neg, \to$ and $\leftrightarrow$ are called **connectives**. The set of **well formed formulae (wff)** are defined inductively. Each atomic variable is a wff. If f and g are two wff, then $f \vee g$, $f \wedge g$, $\neg f$, $f \to g$, and $f \leftrightarrow g$ are wff. Brackets are used to avoid ambiguity.

Example 6.1.7. 1. $p \wedge \vee q$, $\vee q$, $p \vee q \wedge$ are not wff, as they do not make sense.

2. $p \vee q \wedge r$ is not a wff as it is not clear what it means. We use brackets to get $p \vee (q \wedge r)$ or $(p \vee q) \wedge r$ which are wff.
3. $(p \to q) \to r$, $(p \vee \neg q) \to \neg r$, $\neg(p \to q)$ are wff.

Did you notice?

The connectives $\vee, \wedge, \to$, and $\leftrightarrow$ always connect two old formulae to create a new one. This is why they are called 'binary connectives'. The connective $\neg$ is used on a single old formula to give a new one. So, it is called a 'unary connective'.

Definition 6.1.8. [**Truth function**] Let $\mathcal{A}$ be the set of assignments to the variables $p_1, \ldots, p_k$. A function $f : \mathcal{A} \to \{T, F\}$ is called a **truth function**. Since $|\mathcal{A}| = 2^k$, there are 2^{2^k} such truth functions.

Example 6.1.9. The table on the left describes a truth function f and that on the right describes the truth table for a particular formula.

p	q	f
T	T	F
T	F	T
F	T	T
F	F	F

p	q	$(p \wedge q) \vee (p \wedge (\neg q))$
T	T	T
T	F	T
F	T	F
F	F	F

EXERCISE **6.1.10.** *1. Draw a truth table for the formula* $p \wedge \big(\neg p \to (p \vee \neg q)\big)$.

2. Can both the formulae $p \to q$ *and* $q \to p$ *be false for some assignment on* p *and* q*?*

Definition 6.1.11. 1. [**Contradiction and tautology**] A **contradiction** (F) is a formula which takes truth value F under each assignment. For example, $p \wedge \neg p$. A **tautology** (T) is a formula which takes truth value T under each assignment. For example, $p \vee \neg p$.

2. [**Equivalence of formulae**] Two formulae f and g are said to be **equivalent**, denoted $f \equiv g$, if they have the same truth table involving all the atomic variables of both f and g. That is, if both f and g carry the same truth values under each assignment to the involved atomic variables.

Example 6.1.12. 1. Is $p \to q \equiv \neg q \to \neg p$? Yes, because they have the same truth tables.

p	q	$f = p \to q$	$g = \neg q \to \neg p$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

2. Is $p \equiv p \wedge (q \vee (\neg q))$? Yes, because they have the same truth tables.

p	q	$f = p$	$g = p \wedge (q \vee (\neg q))$
T	T	T	T
T	F	T	T
F	T	F	F
F	F	F	F

Remark 6.1.13. *1. There is another way to establish equivalence of two formulae f and g. We show that f has a truth value T (or F) if and only if g has the same truth value. For example, to show that $p \to q \equiv \neg q \to \neg p$, proceed in the following way.*

Step 1: Suppose that $p \to q$ has a truth value F for an assignment a. Then $a(p) = T$ and $a(q) = F$. But then, under that assignment, we have $\neg q$ is T and $\neg p$ is F. That is, under a, we have $\neg q \to \neg p$ is F.

Step 2: Suppose that $p \to q$ has a truth value T for an assignment a. Then $a \in \{TT, FT, FF\}$. Under TT, we have $\neg p$ is F and $\neg q$ is F, so that $\neg q \to \neg p$ is T. Under FT, we have $\neg p$ is T and $\neg q$ is F, so that $\neg q \to \neg p$ is T. Under FF, we have $\neg p$ is T and $\neg q$ is T, so that $\neg q \to \neg p$ is T.

Thus, both are equivalent.

2. Let $f(p_1, \ldots, p_k)$ be a formula and $q_1, \ldots, q_r$ be some new atomic variables. Then $f \equiv f \wedge (q_1 \vee (\neg q_1)) \wedge \cdots \wedge (q_r \vee (\neg q_r))$. This can be argued using induction. Thus f can be viewed as a formula involving atomic variables $p_1, \ldots, p_k, q_1, \ldots, q_r$.

3. We have seen that

(a) $p \to q \equiv \neg p \vee q$, and

(b) $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$.

Thus, the connectives $\vee, \wedge$ and $\neg$ are enough for writing a formula in place of the 5 connectives $\vee, \wedge, \neg, \to$ and $\leftrightarrow$.

4. Recall that a formula on variables p, q and r is a truth function. So there are exactly $2^{2^3} = 2^8$ nonequivalent formulae on variables p, q and r.

EXERCISE **6.1.14.** *Is $p \vee \neg p \equiv q \vee \neg q$?*

Definition 6.1.15. [**Substitution instance**] Suppose B is a formula which involves some variables including p. Then, substituting a formula A for each appearance of the variable p in B, gives us a new formula. This new formula is called a **substitution instance** of B. We may substitute more than one variables, simultaneously. Note that A may involve old and new variables.

Example 6.1.16. Let B: $(p \to q) \to p$. We substitute $p \to \neg q$ for p, and p for q, in B to obtain the following substitution instance of B.

$$\big((p \to \neg q) \to p\big) \to (p \to \neg q)$$

The following result is one of the most fundamental results of the subject.

Theorem 6.1.17. *Any substitution instance of a tautology is a tautology.*

Proof. Let $P(p_1, \ldots, p_k)$ be a tautology. Suppose that we replace each occurrence of p_1 by a formula f to obtain the formula R. Consider all the atomic variables involved in P and f. View P and R as formulae involving all these atomic variables. Let a be an assignment to these atomic variables.

If f takes the value T on a, then the value of R on a is nothing but the value of $P(T, p_2, \ldots, p_k)$ on a, which is T as P is a tautology.

If f takes the value F on a, then the value of R on a is nothing but the value of $P(F, p_2, \ldots, p_k)$ on a, which is T as P is a tautology. Thus, R takes the value T under each assignment. ■

Exercise **6.1.18.** *Show that any substitution instance of a contradiction is a contradiction.*

Definition 6.1.19. [**Functionally complete**] A subset S of connectives is called **functionally complete/adequate**, if each formula has an equivalent formula written only using the connectives in S.

Example 6.1.20. We already know that $S = \{\vee, \wedge, \neg\}$ is adequate.

Exercise **6.1.21.** *1. Determine which are adequate. (i) $\{\neg, \vee\}$ (ii) $\{\to, \neg\}$.*

2. Fill in the blanks to prove that '$f \equiv g$' if and only if '$f \leftrightarrow g$ is a tautology'.

Proof. Assume that $f \equiv g$. Let b be an assignment. Then, the value of f and g are ________ under b. Thus, the value of $f \leftrightarrow g$ is _ under b. As b is an ________ assignment, we see that $f \leftrightarrow g$ is a ________.

Therefore, if f is T under b, then g is T under b. That is, $f \to g$ and $g \to f$ are both T under b. Thus, $f \leftrightarrow g$ is T under the assignment b.

Conversely, suppose that $f \leftrightarrow g$ is a ________. Assume that $f \not\equiv g$. Then, there is ______________ under which _ and _ take different __________.

So, suppose that f takes T and g takes F under b. Then _____ is F under b and hence $f \leftrightarrow g$ takes F under b, a contradiction. A similar contradiction is obtained if f takes F and g takes T under b. ■

The proof of the next result is left as an exercise for the readers.

Proposition 6.1.22. [**Rules**] *If p, q, r are formulae, then*

1. $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$ *(commutative)*
2. $p \vee (q \vee r) \equiv (p \vee q) \vee r$, $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ *(associative)*
3. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ *(distributive)*
4. $\neg(p \vee q) \equiv \neg p \wedge \neg q$, $\neg(p \wedge q) \equiv \neg p \vee \neg q$ *(De Morgan's law)*
5. $p \vee p \equiv p$, $p \wedge p \equiv p$ *(idempotence)*
6. $\mathbf{F} \vee p \equiv p$, $\mathbf{F} \wedge p \equiv \mathbf{F}$

7. $\mathbf{T} \vee p \equiv \mathbf{T}$, $\mathbf{T} \wedge p \equiv p$

8. $\neg(\neg p) \equiv p$

9. $p \vee (p \wedge q) \equiv p$, $p \wedge (p \vee q) \equiv p$ *(absorption law)*

Proof. First six may be proved suing direct arguments and the rest by using the first six. ∎

EXERCISE **6.1.23.** *Does the absorption law imply $p \vee (p \wedge (\neg q)) \equiv p$ and $p \wedge (p \vee (\neg q)) \equiv p$?*

Discussion 6.1.24. The above rules can be used to simplify a formula or to show equivalence of formulae. For example,

$$\begin{aligned} p \to (q \to r) &\equiv \neg p \vee (\neg q \vee r) && \text{as } p \to p \equiv (\neg p) \vee q \\ &\equiv \neg p \vee \neg q \vee r && \text{Associativity} \\ &\equiv \neg(p \wedge q) \vee r && \text{De Morgan's law} \\ &\equiv (p \wedge q) \to r && \text{as } p \to p \equiv (\neg p) \vee q \end{aligned}$$

Did you notice?

There are 3 ways to prove $f \equiv g$.

1. Using truth table.
2. Arguing that f is false under an assignment (of the variables involved in both) if and only if g is false under the same assignment.
3. Using some of the above rules and by reducing f to g or g to f.

Experiment

Consider the variables p, q, r.
Give a formula which takes value T only on the assignment TTT.
Give a formula which takes value T only on the assignment TTF. $(p \wedge q \wedge (\neg r))$
Give a formula which takes value T only on the assignment FTF.
Give a formula which takes value T only on the assignments TTF and FTF.
Give a formula which takes value T only on the assignments TFT, TTF and TFF.
Give a formula f which takes value T only on the assignments FTF and FFF or whose truth table is the following

p	q	r	f
T	T	T	F
T	T	F	F
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

Lemma 6.1.25. *Let f be a truth function involving the variables $p_1, \ldots, p_k$. Then, there is a formula g involving $p_1, \ldots, p_k$, whose truth table is described by f.*

Proof. If $T \notin \mathsf{rng}\, f$, then write $q = p_1 \wedge \neg p_1 \wedge p_2 \wedge \cdots \wedge p_k$. Otherwise, collect all those assignments b such that $f(b) = T$. Call this set $\mathcal{A}_1$. For each $b \in \mathcal{A}_1$, define a formulae $q = r_1 \wedge r_2 \wedge \cdots \wedge r_k$, where for $1 \le j \le k$,

$$r_j = \begin{cases} p_j & \text{if } b(p_j) = T \\ \neg p_j & \text{otherwise.} \end{cases}$$

Then, the formulae q takes the value T only on the assignment b. Thus, taking the disjunctions of all such q's related to each $b \in \mathcal{A}_1$, we get the required result. ■

EXERCISE **6.1.26.** *Illustrate 6.1.25 with the truth function f*

p	q	f
T	T	T
T	F	T
F	T	F
F	F	F

Definition 6.1.27. [**Normal forms**] An atomic formula or it's negation is called a **literal**. We say that a formula f is in **disjunctive normal form** (in short, DNF) if it is expressed as a disjunction of conjunctions of literals. We say that a formula f is in **conjunctive normal form** (in short, CNF) if it is expressed as a conjunction of disjunctions of literals.

Example 6.1.28. p, $p \vee q$, $p \vee \neg q$, $(p \wedge \neg q) \vee \neg r$, $(p \wedge \neg q) \vee (q \wedge \neg r) \vee (r \wedge s)$ are in DNF. Write 5 formulae in CNF involving p, q, r.

Theorem 6.1.29. *Any formula is equivalent to a formulae in DNF. Similarly, Any formula is equivalent to a formulae in CNF.*

Proof. The proof of the first assertion follows from Lemma 6.1.25. For the second assertion, we can write one proof in a similar way.

An alternate proof: take f, consider $\neg f$, get a DNF P for $\neg f$, and consider $\neg P$. ■

EXERCISE **6.1.30.** *Write all the truth functions on two variables and write formulae for them.*

Definition 6.1.31. [**Principal connectives**] Let h be a formula. A **principal connective** in h is defined in the following way.

1. If h is expressed in a format $\neg f$, then $\neg$ is the principal connective of h.
2. If h is expressed in a format $f \vee g$, then $\vee$ is the principal connective of h.
3. If h is expressed in a format $f \wedge g$, then $\wedge$ is the principal connective of h.

EXERCISE **6.1.32.** *Use induction on the number of connectives to show that any formula is equivalent to a formulae in DNF and a formula in CNF.*

Definition 6.1.33. [**Dual**] The **dual** P^* of a formula P involving the connectives $\vee, \wedge, \neg$ is obtained by interchanging $\vee$ with $\wedge$ and the special variable $\mathbf{T}$ with the special variable $\mathbf{F}$.

Example 6.1.34. Note that the dual of $\neg(p \vee q) \wedge r$ is $\neg(p \wedge q) \vee r$.

Lemma 6.1.35. *Let $A(p_1, \ldots, p_k)$ be a formula in the atomic variables p_i involving connectives $\vee, \wedge$ and $\neg$. If $A(\neg p_1, \ldots, \neg p_k)$ is obtained by replacing p_i with $\neg p_i$ in A, then $A(\neg p_1, \ldots, \neg p_k) \equiv \neg A^*(p_1, \ldots, p_k)$.*

Proof. Use induction on the number of connectives. If $A = B \vee C$, then

$$\begin{aligned} A^* = B^* \wedge C^* &\equiv \neg B(\neg p_1, \ldots, \neg p_k) \wedge \neg C(\neg p_1, \ldots, \neg p_k) \\ &\equiv \neg(B \vee C)(\neg p_1, \ldots, \neg p_k) = \neg A(\neg p_1, \ldots, \neg p_k). \end{aligned}$$

The remaining parts are similar and hence left for the reader. ■

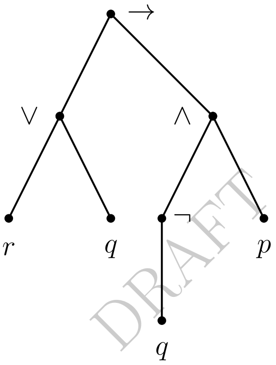
Theorem 6.1.36. *Let f, g be formulae using connectives $\vee, \wedge$ and $\neg$. If $f \equiv g$, then $f^* \equiv g^*$.*

Proof. By Lemma 6.1.35, we note that

$$f^*(\neg b) = \neg f(b) = \neg g(b) = g^*(\neg b) \text{ for any assignment } b.$$

Thus, $f^* \equiv g^*$. ■

Discussion 6.1.37. [**Tree representation**] A formula can be represented by a tree. For example, $(r \vee q) \to (\neg q \wedge p)$ has the following representation.



Definition 6.1.38. [**Polish notation**] A formula may be expressed using **Polish notation**. It is defined inductively as follows.

'Let $P(f)$ denote the Polish notation of f. Then $P(f \vee g)$ is $\vee P(f)P(g)$, $P(f \wedge g)$ is $\wedge P(f)P(g)$, and $P(\neg f)$ is $\neg P(f)$.'

This notation does not use brackets. Here the connectives are written in front of the expressions they connect. *Advantage:* it takes less space for storage. *Disadvantage:* it's complicated look.

Example 6.1.39. In Polish notation $(r \vee q) \to (\neg q \wedge p)$ becomes $\to \vee rq \wedge \neg qp$.

EXERCISE **6.1.40.** *Write a formula involving 8 connectives and the variables p, q, r. Draw it's tree. Write it's Polish notation.*

Definition 6.1.41.

1. [**Satisfiable**] A formula is **satisfiable** if it is not a contradiction.
2. [**Order of operations**] To reduce the use of brackets, we fix the **order of operations**: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$.

Discussion 6.1.42. There is another way of making a truth table for a formula. Consider $(p \vee q) \vee \neg r$. Draw a table like the following and give the truth values to the atomic formulae. Evaluate the connectives for the subformulae one by one. In this example, the sequence of column operations is: $5, 2, 4$.

$(p$	$\vee$	$q)$	$\vee$	$\neg$	r
T		T			T
T		T			F
T		F			T
T		F			F
F		T			T
F		T			F
F		F			T
F		F			F

$(p$	$\vee$	$q)$	$\vee$	$\neg$	r
T	T	T	T	F	T
T	T	T	T	T	F
T	T	F	T	F	T
T	T	F	T	T	F
F	T	T	T	F	T
F	T	T	T	T	F
F	F	F	F	F	T
F	F	F	T	T	F

Definition 6.1.43. [Inference] We say g is a **logical conclusion** of $\{f_1, \cdots, f_n\}$ if $(f_1 \wedge f_2 \wedge \cdots \wedge f_n) \rightarrow g$ is a tautology. We denote this by $\{f_1, \ldots, f_n\} \Rightarrow g$. At times, we write $f_1, \ldots, f_n \Rightarrow g$ to mean $\{f_1, \ldots, f_n\} \Rightarrow g$. Here, g is called the **conclusion** and $\{f_1, \ldots, f_n\}$ is called the **hypothesis/premise**.

Example 6.1.44. 1. Consider the following three statements.

A : if $x = 4$, then discrete math is bad;
B : discrete math is bad;
C : $x = 4$.

Does C logically follow from A, B?

Ans: No. Denote '$x = 4$' by p and 'discrete mathematics is bad' by q. Then, the above question is the same as asking whether $\{p \rightarrow q, q\} \Rightarrow p$ is true. That is, whether $P(p, q) := ((p \rightarrow q) \wedge q) \rightarrow p$ is a tautology.

To find that, suppose that there is an assignment for which P takes the value F. So, for that assignment, p must be F and $(p \rightarrow q) \wedge q$ must be true.

As $(p \rightarrow q) \wedge q$ is true, q must be T. So, the assignment must be FT. Notice that $p \rightarrow q$ has a value T with this assignment. Thus, $P(p, q)$ takes F under FT. Hence, it is not a tautology. So, C does not logically follow from A, B. □

2. Consider the following three statements.

A : 'if discrete math is bad, then $x = 4$';
B : 'discrete math is bad';
C : '$x = 4$'.

Does C logically follow from A, B?

Ans: Yes. Denote '$x = 4$' by p and 'discrete mathematics is bad' by q. Then, the above question is the same as asking whether $\{q \rightarrow p, q\} \Rightarrow p$ is true. That is, whether $P(p, q) := ((q \rightarrow p) \wedge q) \rightarrow p$ is a tautology.

To find that, suppose that there is an assignment for which P takes the value F. So, for that assignment, p must be F and $(q \rightarrow p) \wedge q$ must be true.

As $(q \rightarrow p) \wedge q$ is true, q must be T and $q \rightarrow p$ must be T. So, the assignment must be FT. But we see that $q \rightarrow p$ has a value F with this assignment. This is a contradiction.

Thus, there is no assignment for which $P(p, q)$ takes F. Hence, it is a tautology. So C logically follows from A, B. □

Definition 6.1.45. We write $f \Leftrightarrow g$ to mean '$f \Rightarrow g$ and $g \Rightarrow f$'.

Did you notice?

Let f, g, h be some formulae. Then $f, g \Rightarrow h$ means that 'whenever f and g are T, h is also T'. That is, 'if f and g are T under an assignment, then h is T under that assignment'. Thus '$f \Leftrightarrow g$' is the same as '$f \equiv g$'.

Example 6.1.46. 1. Show that $\{\alpha \to \beta, \beta \to \gamma, \gamma \to \delta\} \Rightarrow \alpha \to \delta$.

Ans: Suppose $\alpha \to \delta$ is F. Then α is T and δ is F. Assume that all the propositions in the hypothesis are true. As δ is F and $\gamma \to \delta$ is T, γ must be F. Continuing, we get α is F, a contradiction.

2. Determine validity of the argument.

The meeting can take place if all members are informed in advance and there is quorum (a minimum number of members are present). There is a quorum if at least 15 *members are present. Members would have been informed in advance if there was no postal strike. Therefore, if the meeting was canceled, then either there were fewer than* 15 *members present or there was a postal strike.*

A : Let us denote the different statements with symbols, say
m: the meeting takes place;
a: all members are informed;
f: at least fifteen members are present;
q: the meeting had quorum;
p: there was a postal strike.

So, we reformulate the problem: whether $\big\{(q \wedge a) \to m, f \to q, \neg p \to a\big\} \Rightarrow \neg m \to (\neg f \vee p)$?

From first two statements, we get $(f \wedge a) \to m$. Considering the third statement, we get $(f \wedge \neg p) \to m$. The conclusion is the contrapositive of this statement.

Alternate. Suppose that conclusion is F. This means that $\neg m \to (\neg f \vee p)$ takes the value F and $\big\{(q \wedge a) \to m, f \to q, \neg p \to a\big\}$ takes the value T.

The first one implies that $\neg f \vee p$ takes the value F and $\neg m$ takes the value T. Hence, we see that the variables m, f and p take values F, T and F, respectively.

The second one implies that all the three expressions $(q \wedge a) \to m$, $f \to q$, and $\neg p \to a$ take the value T. Since the second statement takes the value T and f has the value T, we see that q has to take the value T. Similarly, using the third statement, we see that a has to take the value T. So, we see that the first statement $(q \wedge a) \to m$ takes the value T with the assignment of both q and a being T. So, we must have m to have the value T, contradicting the value F taken by m in the previous paragraph.

EXERCISE **6.1.47.** *1. List all the nonequivalent formulae involving variables p and q which take truth value T on exactly half of the assignments.*

2. We assume $F \leq T$. Let f and g be two truth functions on the variables $p_1, \ldots, p_9$. Suppose that for each assignment a, we have $f(a) \leq g(a)$. Does this imply '$f \to g$ is a tautology'?

3. Let f and g be two formulae involving the variables $p_1, \ldots, p_k$. Prove that '$f \equiv g$' (the same truth table) if and only if '$f \leftrightarrow g$ is a tautology'.

4. Without using $\to$, write an equivalent simplified statement of $(p \to q) \to \big(p \to (q \to r)\big)$.

5. Determine which of the following are logically equivalent.

(a) $\big(p \to (r \vee s)\big) \wedge \big((q \wedge r) \to s\big)$.

(b) $\big((p \vee r) \vee (s \to p)\big) \wedge \big(p \to (s \to r)\big)$.

(c) $q \to s$.

(d) $\big(s \to (q \vee r)\big) \wedge \big((q \wedge s) \to r\big)$.

(e) $\big((p \vee s) \vee (q \to p)\big) \wedge \big(p \to (q \to s)\big)$.

6. *Let p be a formula written only using connectives $\wedge, \vee$ and $\to$ and involving the atomic variables $p_1, \cdots, p_k$, for some k. Show that the truth value of p is T under the assignment $f(p_i) = T$, for all i.*

7. *Is $\{\to, \vee, \wedge\}$ adequate?*

8. *Verify the following assertions.*

   (a) $P \wedge Q \Rightarrow P$

   (b) $P \Rightarrow P \vee Q$

   (c) $\neg P \Rightarrow P \to Q$

   (d) $\neg(P \to Q) \Rightarrow P$

   (e) $\neg P, P \vee Q \Rightarrow Q$

   (f) $P, P \to Q \Rightarrow Q$

   (g) $\neg Q, P \to Q \Rightarrow \neg P$

   (h) $P \to Q, Q \to R \Rightarrow P \to R$

   (i) $P \vee Q, P \to R, Q \to R \Rightarrow R$

   (j) $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$

   (k) $\{p \wedge q, p \vee q\} \Rightarrow q \to r$

   (l) $\{p \to q, \neg p\} \Rightarrow \neg q$

   (m) $\{p_0 \to p_1, p_1 \to p_2, \ldots, p_9 \to p_{10}\} \Rightarrow p_0 \vee p_5$.

   (n) $\big\{(\neg p \vee q) \to r, s \vee \neg q, \neg t, p \to t, (\neg p \wedge r) \to \neg s\big\} \Rightarrow \neg q$.

   (o) $\big\{p \to q, r \vee s, \neg s \to \neg t, \neg q \vee s, \neg s, (\neg p \wedge r) \to u, w \vee t\big\} \Rightarrow u \wedge w$.

9. *If H is a set of formulae, then $H \Rightarrow \alpha \to \beta$ if and only if $H \cup \{\alpha\} \Rightarrow \beta$.*

10. *Prove the equivalence of the following in three different ways (truth table, simplification, each is a logical consequence of the other): $p \to (q \vee r) \equiv (p \wedge \neg q) \to r$.*

11. *Determine which of the following conclusions are correct.*

    (a) *If the lecture proceeds, then either black board is used or the slides are shown or the tablet pc is used. If the black board is used, then students at the back bench are not comfortable in reading the black board. If the slides are shown, then students are not comfortable with the speed. If the tablet pc is used, then it causes lots of small irritating disturbances to the instructor. The lecture proceeds and the students are comfortable. So, it is deduced that the instructor faces disturbances.*

    (b) *There are three persons Mr X, Mr Y and Mr Z making statements. If Mr X is wrong, then Mr Y is right. If Mr Y is wrong, then Mr Z is right. If Mr Z is wrong, then Mr X is right. Therefore, some two of them are always right.*

12. *Consider the set S of all nonequivalent formulae written using two atomic variables p and q. For $f, g \in S$, define $f \leq g$ if $f \Rightarrow g$. Prove that this is a partial order on S. Draw it's Hasse diagram.*

13. *Consider the set S of all nonequivalent formulae written using three atomic variables p, q, r. For $f, g \in S$ define $f \leq g$ if $f \Rightarrow g$. Let f_1 and g_1 be two formulae having the truth tables*

p	q	r	f_1
T	T	T	T
T	T	F	F
T	F	T	T
T	F	F	T
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	F

p	q	r	g_1
T	T	T	T
T	T	F	F
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	T
F	F	F	F

How many nonequivalent formulae h are there such that $\{f_1, g_1\} \Rightarrow h$?

14. *How many assignments of truth values to p, q, r and w are there for which $\big((p \to q) \to r\big) \to w$ is true? Guess a formula in terms of the number of variables.*

15. *Check the validity of the argument. If discrete math is bad, then computer programming is bad. If linear algebra is good, then discrete math is good. If complex analysis is good, then discrete math is bad. If computer programming is good, then linear algebra is bad. Complex analysis is bad and hence, at least one more subject is bad.*

6.2 Predicate Logic*

Definition 6.2.1. [Predicate] A **k-place predicate** or **propositional function** $p(x_1, \ldots, x_k)$ is a statement involving the variables $x_1, \ldots, x_k$. A truth value can be assigned to a predicate $p(x_1, \cdots, x_k)$ for each assignment of $x_1, \ldots, x_k$ from their respective **universe of discourses** (in short, UD) (the set of values that x_i's can take is the i-th UD).

Example 6.2.2. Let $p(x)$ mean '$x > 0$'. Then $p(x)$ is a 1-place predicate on some UD. Let $p(x, y)$ mean '$x^2 + y^2 = 1$'. Then $p(x, y)$ is a 2-place predicate on some UD.

Definition 6.2.3. [Quantifiers] We call the symbols $\forall$ and $\exists$, the **quantifiers**. Formulae involving them are called quantified formulae. The statement $\forall x\, p(x)$ is true if for each x (in the UD) the property $p(x)$ is T. The statement $\exists x\, p(x)$ is T if $p(x)$ is T for some x in the UD.

Example 6.2.4. Let UD be the set of all human beings. Consider the 2-place predicate $F(x, y)$: 'x runs faster than y'. Then

1. $\forall x\, \forall y\, F(x, y)$ means 'each human being runs faster than every human being'.
2. $\forall x\, \exists y\, F(x, y)$ means 'for each human being there is a human being who runs slower'.
3. $\exists x\, \exists y\, F(x, y)$ means 'there is a human being who runs faster than some human being'.
4. $\exists x\, \forall y\, F(x, y)$ means 'there is a human being who runs faster than every human being '.

Definition 6.2.5. 1. **[Scope of quantifier]** In the quantified formulae $\forall x\, p(x)$ or $\exists x\, p(x)$ the formula $p(x)$ is called the **scope** of the quantifier (extent to which that quantification applies).

2. An **x-bound part** in a formula is a part of the form $\exists x\, p(x)$ or $\forall x\, q(x)$. Any occurrence of x in an x-bound part of the formula is a **bound** occurrence of x. Any other occurrence of x is a **free** occurrence of x.

Example 6.2.6. In $\exists x\, p(x, y)$ the occurrence of y is free and both the occurrences of x are bound. In $\forall y\, \exists x\, p(x, y)$ all the occurrences of x and y are bound.

Definition 6.2.7. 1. A quantified formulae is well formed if it is created using the following rules.

(a) Any **atomic formula** (of the form P, $P(x,y)$, $P(x,b,y)$) is a wff.

(b) If A and B are wffs, then $A \vee B$, $A \wedge B$, $A \to B$, $A \leftrightarrow B$, and $\neg A$ are wffs.

(c) If A is a wff and x is any variable, then $\forall x\, A$ and $\exists x\, A$ are wffs.

2. Let f be a formula. An **interpretation** (for f) means the process of specifying the UD, specifications of the predicates, and assigning values to the free variables from the UD. By an **interpretation of** f, we mean the formula f under a given interpretation.

Example 6.2.8. Consider the wff $\forall x\, p(x,y)$.

1. Take $\mathbb{N}$ as UD. Let $p(x,y)$ specify '$x > y$'. Let us assign 1 to the free variable y. Then, we get the interpretation 'each natural number is greater than 1' which has the truth value F.
2. Take $\mathbb{N}$ as UD. Let $p(x,y)$ mean '$x + y$ is an integer', and take $y = 2$. Then, we get an interpretation 'when we add 2 to each natural number we get an integer' which has a truth value T.

Discussion 6.2.9. [**Translation**] We expect to see that 'our developments on logic' help us in drawing appropriate conclusions. In order to do that, we must know how to translate an 'English statement' into a 'formal logical statement' that involves no English words. We may have to introduce appropriate variables and required predicates. We may have to specify the UD, but normally we use the most general UD.

Example 6.2.10. 1. Translate: 'each person in this class room is either a BTech student or an MSc student'.

A: Does the statement guarantee that there is a person in the room?
No. All it says is, if there is a person, then it has certain properties. Let $P(x)$ mean 'x is a person in this class room'; $B(x)$ mean 'x is a BTech student'; and $M(x)$ mean 'x is an MSc student'. Then, the formal expression is $\forall x \Big(P(x) \to \big(B(x) \vee M(x)\big)\Big)$.

2. Translate: 'there is a student in this class room who speaks Hindi or English'.

A: Does the statement guarantee that there is a student in the room?
Yes. Let $S(x)$ mean 'x is a student in this class room'; $H(x)$ mean 'x speaks Hindi'; and $E(x)$ mean 'x speaks English'. Then, the formal expression is $\exists x \Big(S(x) \wedge (H(x) \vee E(x))\Big)$.

Note that $\exists x \Big(S(x) \to (H(x) \vee E(x))\Big)$ is not the correct expression. Why?

Remember

$\exists x\,(S(x) \to T(x))$ never asserts $S(x)$ BUT $\exists x(S(x) \wedge T(x))$ asserts both $S(x)$ and $T(x)$.

Practice **6.2.11.** *Translate into formal logic.*

1. *Every natural number is either the square of a natural number or it's square root is irrational.*
2. *For every real number x there is a real number y such that $x + y = 0$.*
3. *A subset $S \subseteq \mathbb{R}^n$ is called compact, if '—write the formal statement here—'.*
4. *A function $f : \mathbb{R} \to \mathbb{R}$ is called continuous at a point a, if '—write the formal statement here—'.*
5. *A function $f : \mathbb{R} \to \mathbb{R}$ is called continuous, if '—write the formal statement here—'.*
6. *A function $f : \mathbb{R} \to \mathbb{R}$ is called uniformly continuous, if '—write the formal statement here—'.*

7. *A subset $S \subseteq \mathbb{R}^n$ is called connected, if '—write the formal statement here—'.*

8. *A set S is called a group, if '—write the formal statement here—'.*

9. *A subset $S \subseteq \mathbb{R}^n$ is called a subspace, if '—write the formal statement here—'.*

10. *A function $f : S \to T$ is called a bijection, if '—write the formal statement here—'.*

11. *A function $f : \mathbb{R}^n \to \mathbb{R}^k$ is called a linear transformation, if '—write the formal statement here—'.*

12. *A function $f : (S, \circ) \to (T, +)$ is called a group isomorphism, if '—write the formal statement here—'.*

13. *A function $f : \mathbb{V} \to \mathbb{W}$ is called a vector space isomorphism, if '— write the formal statement here—'.*

Definition 6.2.12. A quantified formula is called **valid** if every interpretation of it has truth value T. Two quantified formulae A and B are called **equivalent** ($A \equiv B$) if $A \leftrightarrow B$ is valid.

Example 6.2.13. 1. $\forall x\, P(x) \vee \exists x\, \neg P(x)$ is valid.

2. Is $\exists x\, \exists y\, p(x, y) \equiv \exists y\, \exists x\, p(x, y)$?

   A: Yes. Denote $\exists x\, \exists y\, p(x, y)$ by L and $\exists y\, \exists x\, p(x, y)$ by R. Suppose that $L \to R$ is F. This means, we have an interpretation in which L is T and R is F. As R is F, we see that $p(x, y)$ is F, for each x, y in the UD. In that case, L is F, a contradiction. So, $L \to R$ is T. Similarly, $R \to L$ is T.

3. $\forall x\, \forall y\, p(x, y) \equiv \forall y\, \forall x\, p(x, y)$. **!!**

4. $\exists x\, \forall y\, p(x, y) \not\equiv \forall y\, \exists x\, p(x, y)$. To see this take $p(x, y)$: $x > y$. □

Did you notice?

Two quantified formulae A and B are equivalent if and only if their interpretations under 'the same UD, the same specification of predicates, and the same values to the free variables' have the same truth value.

5. Is $\forall x\, \Big(r(x) \to \exists y\, \big(r(y) \wedge p(x, y)\big)\Big) \equiv \forall x \exists y \Big(r(x) \to \big(r(y) \wedge p(x, y)\big)\Big)$?

   A: We want to know if

   $$\forall x\, \Big(r(x) \to \exists y\, \big(r(y) \wedge p(x, y)\big)\Big) \leftrightarrow \forall x \exists y \Big(r(x) \to \big(r(y) \wedge p(x, y)\big)\Big)$$

   is valid. Let us see whether

   $$\forall x\, \Big(r(x) \to \exists y\, \big(r(y) \wedge p(x, y)\big)\Big) \to \forall x \exists y \Big(r(x) \to \big(r(y) \wedge p(x, y)\big)\Big)$$

   is valid. Suppose that this is invalid. So there is an interpretation such that Right hand side is F and Left hand side is T. As Right hand side is F, we see that $\exists x$, say x_0, for which $\exists y \Big(r(x) \to \big(r(y) \wedge p(x, y)\big)\Big)$ is F. That is, $\forall y$ the formula $r(x_0) \to \big(r(y) \wedge p(x_0, y)\big)$ is F. That is, $r(x_0)$ is T and for each y we see that $r(y) \wedge p(x_0, y)$ is F. That is, $r(x_0)$ is T and $\exists y(r(y) \wedge p(x_0, y))$ is F. That is, the formula $r(x_0) \to \exists y(r(y) \wedge p(x_0, y))$ is F. That is, $\forall x\, \Big(r(x) \to \exists y\, \big(r(y) \wedge p(x, y)\big)\Big)$ is F, a contradiction. The other part is an exercise.

   Alternate. Take $A := r(x) \to \exists y\, \big(r(y) \wedge p(x, y)\big)$ and $B := \exists y \Big(r(x) \to \big(r(y) \wedge p(x, y)\big)\Big)$.

Consider an x_0 in the UD. If $r(x_0)$ is F, Then A and B both have value T. If $r(x_0)$ is T. Then notice that $r(x_0) \to \exists y\,\big(r(y) \wedge p(x_0,y)\big)$ and $\exists y\Big(r(x_0) \to \big(r(y) \wedge p(x_0,y)\big)\Big)$ have the same truth value.

Thus $A \equiv B$. Hence $\forall x A \equiv \forall x B$.

6. Any student who appears in the exam and gets a score below 30, gets an F grade. Mr x_0 is a student who has not written the exam. Therefore, x_0 should get an F grade. Do you agree?

   A: Let $S(x)$ mean 'x is a student', $E(x)$ mean 'x writes the exam', $B(x)$ mean 'x gets a score below 30', and $F(x)$ mean 'x gets F grade'.

   We want to see whether $\Big\{\forall x[S(x) \wedge E(x) \wedge B(x) \to F(x)], S(x_0) \wedge \neg E(x_0)\Big\} \Rightarrow F(x_0)$?

   Take the following interpretation: $S(x)$ is 'x is a positive real number', $E(x)$ is 'x is a rational number', $B(x)$ is 'x is an integer', $F(x)$ is 'x is a natural number', and $x_0 = \sqrt{2}$.

   In this interpretation, statements in the premise mean 'every positive integer is a natural number' and '$\sqrt{2}$ is a positive real number which is not rational'. They both are true. Whereas the conclusion means '$\sqrt{2}$ is a natural number' which is false. So, the argument is incorrect.

7. Translate the following into formal statements.

   'All scientists are human beings. Therefore, all children of scientists are children of human beings.'

   A: Let Sx : 'x is a scientist'; Hx : 'x is a human being' and Cxy : x is a child of y.

   Let the hypothesis be $\forall x(Sx \to Hx)$. Then, the possible translations of the conclusion are the following.

   (a) $\forall x(\exists y(Sy \wedge Cxy) \to \exists z(Hz \wedge Cxz))$. It means 'for each x, if x has a scientist father, then x has a human father'.

   (b) $\forall x[\forall y(Sy \wedge Cxy) \to \forall z(Hz \wedge Cxz)]$. This is wrong, as the statement means 'for all x, if x is a common child of all scientists, then x is a common child of all human beings'.

   (c) $\forall x(Sx \to \forall y(Cyx \to \exists z(Hz \wedge Cyz)))$. This means 'for each x, if x is a scientist, then each child of x has a human father'.

   (d) $\forall x \forall y(Sx \wedge Cyx) \to \forall x \forall y(Hx \wedge Cxy)$. What? This means 'if each x is a scientist and each y is a child of x (including x it self!), then each x is a human being and each y is a child of x'.

EXERCISE **6.2.14.** *1. Write a formal definition of* $\lim\limits_{x\to a} f(x) \neq l$.

2. Is $\exists x\,[p(x) \wedge q(x)] \to \exists x\, p(x) \wedge \exists x\, q(x)$ *valid? Is it's converse valid?*

3. [**common ones**] *If* r *does not involve* x*, then establish the following assertions.*

   (a) $\neg\forall x\, p(x) \equiv \exists x\, \neg p(x)$*;* $\quad \neg\exists x\, p(x) \equiv \forall x\, \neg p(x)$

   (b) $\exists x\,\big(p(x) \vee q(x)\big) \equiv \exists x\, p(x) \vee \exists x\, q(x)$*;* $\quad \exists x\,\big(p(x) \wedge q(x)\big) \Rightarrow \exists x\, p(x) \wedge \exists x\, q(x)$.

   (c) $\forall x\,\big(p(x) \wedge q(x)\big) \equiv \forall x\, p(x) \wedge \forall x\, q(x)$*;* $\quad \forall x\,\big(p(x) \vee q(x)\big) \Leftarrow \forall x\, p(x) \vee \forall x\, q(x)$.

   (d) $\forall x\,\big(r \vee q(x)\big) \equiv r \vee \forall x\, q(x)$*;* $\quad \forall x\,\big(r \to q(x)\big) \equiv r \to \forall x\, q(x)$

   (e) $\exists x\,\big(r \wedge q(x)\big) \equiv r \wedge \exists x\, q(x)$*;* $\quad \exists x\,\big(r \to q(x)\big) \equiv r \to \exists x\, q(x)$.

   (f) $\forall x\, p(x) \to r \equiv \exists x\,\big(p(x) \to r\big)$*;* $\quad \exists x\, p(x) \to r \equiv \forall x\,\big(p(x) \to r\big)$.

4. Translate and check for validity of the following arguments.

   (a) Recall that the decimal representation of a rational number either terminates or begins to repeat the same finite sequence of digits, whereas that of an irrational number neither

terminates nor repeats. The square root of a natural number either has a decimal representation which is terminating or has a decimal representation which is non-terminating and non-repeating. The square root of all natural numbers which are squares have terminating decimal representation. Therefore, the square root of a natural number which is not a square is an irrational number.

(b) *For any two algebraic numbers* a *and* b, $a \neq 0, 1$ *and* b *irrational, we have that* a^b *is transcendental. The number* i *(imaginary unit) is irrational and algebraic. The number* i *is not equal to* 0 *or* 1. *Therefore, the number* i^i *is transcendental.*

5. (a) *Give an interpretation to show that* $\forall x \Big(r(x) \to \exists y \left(r(y) \wedge p(x,y)\right)\Big)$ *is not valid.*

   (b) *Give an interpretation to show the incorrectness of* $\forall x\big(p(x) \to q(x)\big) \Rightarrow \exists x\big(\neg p(x) \to \neg q(x)\big)$.

6. *Write a formal statement taking UD:= all students in all IIT's in India, for the following.*

   'For each student in IITG there is a student in IITG with more CPI.'

7. *Let UD=* $\mathbb{R}$, $p(x)$: x *is an integer, and* $q(x)$: x *is a rational number. Translate the following statements into English.*

   (a) $\forall x\big(p(x) \to q(x)\big)$

   (b) $\exists x\big(\neg p(x) \wedge q(x)\big)$

   (c) $\forall x\big(p(x) \wedge (x > 2)\big) \to \forall x\big(q(x) \wedge (x < 2)\big)$

   (d) $\exists \epsilon > 0\Big(\forall \delta > 0(0 < |x - a| < \delta \to |f(x) - l| < \epsilon)\Big)$

8. *Take the most general UD. Check whether the following conclusion is valid or not.*

   Each student writes the exam using blue ink or black ink. A student who writes the exam using black ink and does not write his/her roll number gets an F grade. A student who writes the exam using blue ink and does not have his/her ID card gets an F grade. A student who has his/her ID card has written the exam with black ink. Therefore, a student who passes the exam must have written his roll number.

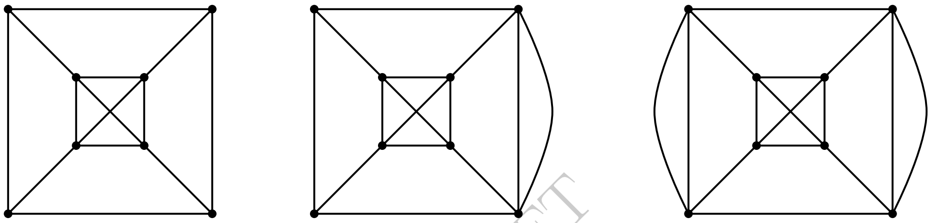
Chapter 7

Graphs

7.1 Basic Concepts

Experiment

'Start from a dot. Move through each line exactly once. Draw it.' Which of the following pictures can be drawn? What if we want the 'starting dot to be the finishing dot'?



Later, we shall see a theorem by Euler addressing this question.

Definition 7.1.1. A **pseudograph** or a general **graph** G is a pair (V, E) where V is a nonempty set and E is a multiset of unordered pairs of points of V. The set V is called the **vertex set** and its elements are called **vertices**. The set E is called the **edge set** and its elements are called **edges**.

Example 7.1.2. $G = \Big(\{1, 2, 3, 4\},\ \big\{\{1, 1\}, \{1, 2\}, \{2, 2\}, \{3, 4\}, \{3, 4\}\big\}\Big)$ is a pseudograph.

Discussion 7.1.3. A pseudograph can be represented in picture in the following way.

1. Put different points on the paper for vertices and label them.
2. If $\{u, v\}$ appears in E some k times, draw k distinct lines joining the points u and v.
3. A loop at u is drawn if $\{u, u\} \in E$.

Example 7.1.4. A picture for the pseudograph in Example 7.1.2 is given in Figure 7.1.

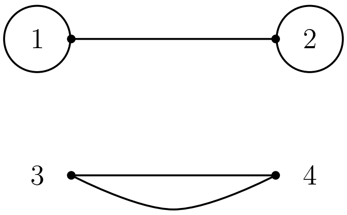


Figure 7.1: A pseudograph

Definition 7.1.5. 1. An edge $\{u, v\}$ is sometimes denoted uv. An edge uu is called a **loop**. The vertices u and v are called the **end vertices** of the edge uv. Let e be an edge. We say 'e is **incident** on u' to mean that 'u is an end vertex of e'.

2. A **multigraph** is a pseudograph without loops. A multigraph is a **simple graph** if no edge appears twice.
3. Henceforth, all graphs in this book are simple with a finite vertex set, unless stated otherwise.
4. We use $V(G)$ (or simply V) and $E(G)$ (or simply E) to denote the vertex set and the edge set of G, respectively. The number $|V(G)|$ is the **order** of the graph G. Sometimes it is denoted $|G|$. By $\|G\|$ we denote the number of edges of G. A graph with n vertices and m edges is called a (n, m) **graph**. The $(1, 0)$ graph is the **trivial graph**.
5. If uv is an edge in G, then we say 'u and v are **adjacent** in G' or 'u is a **neighbor** of v'. We write $u \sim v$ to denote that 'u is adjacent to v'. Two edges e_1 and e_2 are **adjacent** if they have a common end vertex.
6. A set of vertices or edges is said to be **independent** if no two of them are adjacent. The maximum size of an independent vertex set is called the **independence number**, denoted $\alpha(G)$, of G.
7. If $v \in V(G)$, by $N(v)$ or $N_G(v)$, we denote the set of neighbors of v in G and $|N(v)|$ is called the **degree** of v. It is usually denoted by $d_G(v)$ or $d(v)$. A vertex of degree 0 is called **isolated**. A vertex of degree one is called a **pendant** vertex.

Discussion 7.1.6. Note that a graph is an algebraic structure, namely, a pair of sets satisfying some conditions. However, it is easy to describe and carry out the arguments with a pictorial representation of a graph. Henceforth, the pictorial representations are used to describe graphs and to provide our arguments, whenever required. There is no loss of generality in doing this.

Example 7.1.7. Consider the graph G in Figure 7.2. The vertex 12 is an isolated vertex. We have $N(1) = \{2, 4, 7\}$, $d(1) = 3$. The vertices 1 and 6 are not adjacent. The set $\{9, 10, 11, 2, 4, 7\}$ is an independent vertex set. The set $\big\{\{1, 2\}, \{8, 10\}, \{4, 5\}\big\}$ is an independent edge set.

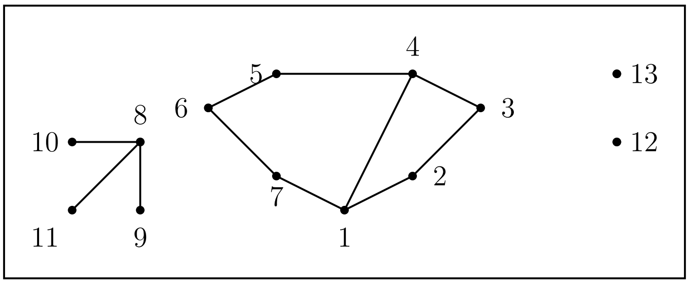


Figure 7.2: A graph G.

Definition 7.1.8. Let $G = (V, E)$ be a graph on n vertices, say $V = \{v_1, \ldots, v_n\}$. Then, G is said to be a

1. **Complete** graph, denoted K_n, if each pair of vertices in G are adjacent.
2. **Path graph**, denoted P_n, if $E = \{v_i v_{i+1} \mid 1 \le i \le n-1\}$.
3. **Cycle graph**, denoted C_n, if $E = \{v_i v_{i+1} \mid 1 \le i \le n-1\} \cup \{v_n v_1\}$.
4. **Bipartite graph** if $V = V_1 \cup V_2$ such that $|V_1|, |V_2| \ge 1$, $V_1 \cap V_2 = \emptyset$ and $e = \{u, v\} \in E$ if either $u \in V_1$ and $v \in V_2$ or $u \in V_2$ and $v \in V_1$.
5. **Complete bipartite graph**, denoted $K_{r,s}$ if $E = \{v_i v_j \mid 1 \le i \le r, r+1 \le j \le n\}$ with $r + s = n$.

The importance of the labels of the vertices depends on the context. At this point of time, even if we interchange the labels of the vertices, we still call them a complete graph or a path graph or a cycle or a complete bi-partite graph.

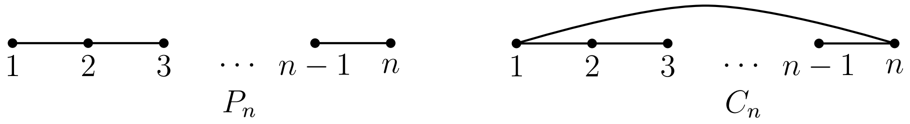


Figure 7.3: P_n and C_n.

Quiz **7.1.9.** *What is the maximum number of edges possible in a simple graph of order n?*[1]

Lemma 7.1.10. [Hand shaking lemma] *In any graph G, $\sum\limits_{v\in V} d(v) = 2|E|$. Thus, the number of vertices of odd degree is even.*

Proof. Each edge contributes 2 to the sum $\sum\limits_{v\in V} d(v)$. Hence, $\sum\limits_{v\in V} d(v) = 2|E|$. Note that

$$2|E| = \sum_{v\in V} d(v) = \sum_{v:d(v)\text{ is odd}} d(v) + \sum_{v:d(v)\text{ is even}} d(v)$$

is even. So, $\sum\limits_{v:d(v)\text{ is odd}} d(v)$ is even. Hence, the number of vertices of odd degree is even. ∎

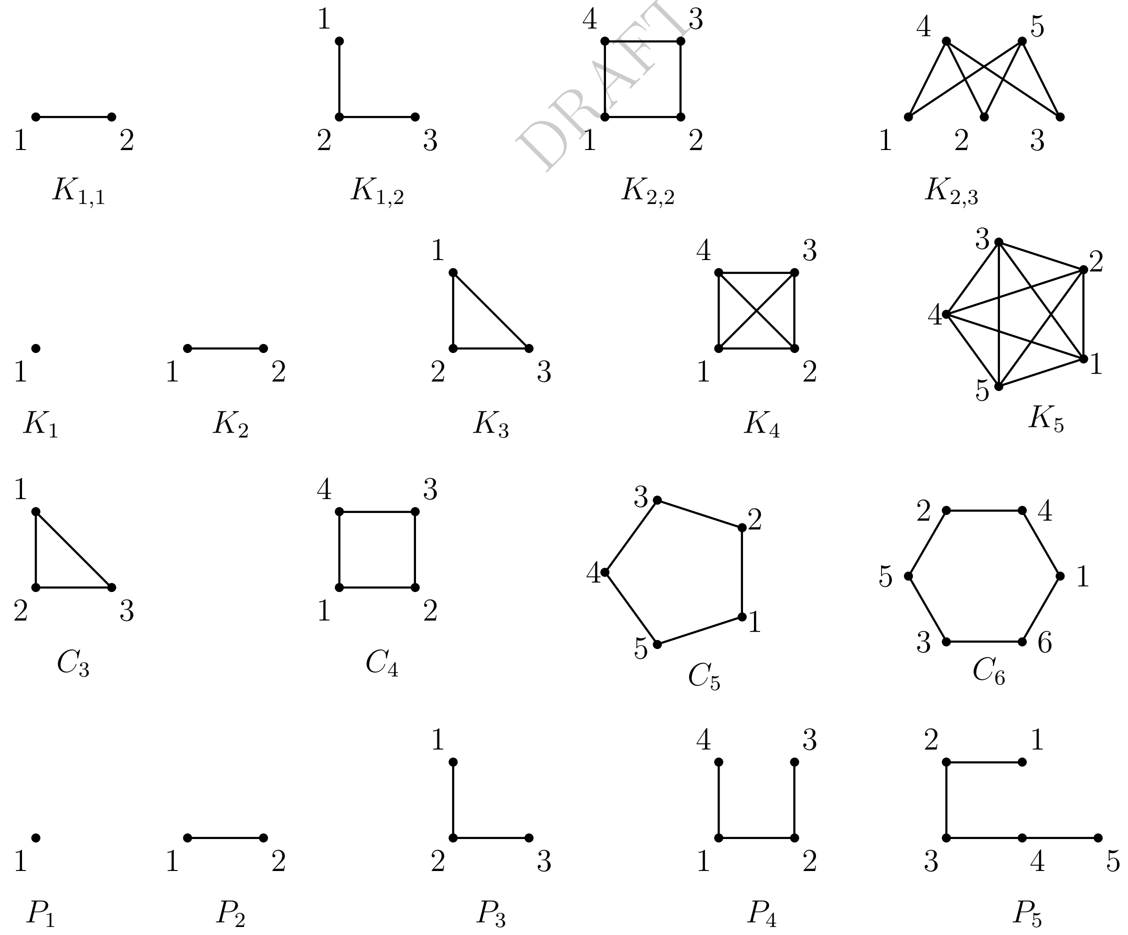


Figure 7.4: Some well known family of graphs

[1] $C(n,2)$.

Example 7.1.11. The graph in Figure 7.5 is called the **Petersen graph**. We shall use it as an example in many places.

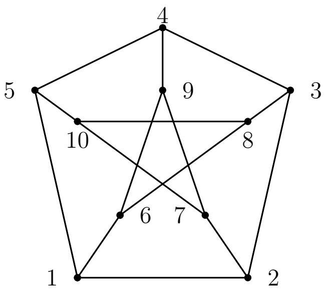


Figure 7.5: Petersen graphs

QUIZ **7.1.12.** *In a party of* 27 *persons, prove that someone must have an even number of friends (friendship is mutual).* [1]

Proposition 7.1.13. *In a graph G with $n = |G| \geq 2$, there are two vertices of equal degree.*

Proof. If G has two or more isolated vertices, we are done. So, suppose G has exactly one isolated vertex. Then, the remaining $n-1$ vertices have degree between 1 and $n-2$ and hence by PHP, the result follows. If G has no isolated vertex then G has n vertices whose degree lie between 1 and $n-1$. Now, again apply PHP to get the required result. ■

EXERCISE **7.1.14.**

1. *Let $X = (V, E)$ be a graph with a vertex $v \in V$ of odd degree. Then, prove that there exists a vertex $u \in V$ such that there is a path from v to u and* $\deg(u)$ *is also odd.*
2. *Let $X = (V, E)$ be a graph having exactly two vertices, say u and v, of odd degree. Then, prove that there is a path in X connecting u and v.*

Definition 7.1.15.

1. The **minimum degree** of a vertex in G is denoted $\delta(G)$ and the **maximum degree** of a vertex in G is denoted $\Delta(G)$.
2. A graph G is called k-**regular** if $d(v) = k$ for all $v \in V(G)$.
3. A 3-regular graph is called **cubic**.

Example 7.1.16.

1. The graph K_n is regular.
2. The graph K_4 is cubic.
3. The graph C_4 is 2-regular.
4. The graph P_4 is not regular.
5. The Petersen graph is cubic.
6. Consider the graph G in Figure 7.2. We have $\delta(G) = 0$ and $\Delta(G) = 3$.

QUIZ **7.1.17.** *Can we have a cubic graph on* 5 *vertices?*[2]

Definition 7.1.18. A graph H is a **subgraph** of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. If $U \subseteq V(G)$, then the subgraph of G **induced** by U is denoted by $\langle U \rangle = (U, E)$, where the edge set $E = \{uv \in E(G) \mid u, v \in U\}$. A subgraph H of G is a **spanning subgraph** if $V(G) = V(H)$. A k-regular spanning subgraph is called a k-**factor**.

Example 7.1.19.

1. Consider the graph G in Figure 7.2.

[1] Otherwise $\sum d(v)$ is odd.

[2] No, as $\sum d(v) = 15$, not even.

(a) Let H_1 be the graph with $V(H_1) = \{6, 7, 8, 9, 10, 12\}$ and $E(H_1) = \big\{\{6, 7\}, \{9, 10\}\big\}$. Then, H_1 is not a subgraph of G.

(b) Let H_2 be the graph with $V(H_2) = \{6, 7, 8, 9, 10, 12\}$ and $E(H_2) = \big\{\{6, 7\}, \{8, 10\}\big\}$. Then, H_2 is a subgraph but not an induced subgraph of G.

(c) Let H_3 be the induced subgraph of G on the vertex set $\{6, 7, 8, 9, 10, 12\}$. Then, verify that $E(H_3) = \big\{\{6, 7\}, \{8, 9\}, \{8, 10\}\big\}$.

(d) The graph G does not have a 1-factor.

2. A complete graph has a 1-factor if and only if it has an even order.

3. The Petersen graph has many 1-factors. One of them is obtained by selecting the edges $\{1, 6\}, \{2, 7\}, \{3, 8\}, \{4, 9\}$, and $\{5, 10\}$.

Quiz **7.1.20.** *Consider K_8 on the vertex set $\{1, 2, \ldots, 8\}$. How many 1-factors does it have?*[1]

Definition 7.1.21. Let G be a graph and v be a vertex. Then, the graph $G - v$, called the **vertex deleted subgraph**, is obtained by deleting v and all the edges that are incident with v. If $e \in E(G)$, then the graph $G - e = (V, E(G) \setminus \{e\})$ is called the **edge deleted subgraph**. If $u, v \in V(G)$ such that $u \nsim v$, then $G + uv = (V, E(G) \cup \{uv\})$ is called the **graph obtained by edge addition**.

Example 7.1.22. Consider the graph G in Figure 7.2. Let H_2 be the graph with $V(H_2) = \{6, 7, 8, 9, 10, 12\}$ and $E(H_2) = \big\{\{6, 7\}, \{8, 10\}\big\}$. Consider the edge $e = \{8, 9\}$. Then, $H_2 + e$ is the induced subgraph $\langle\{6, 7, 8, 9, 10, 12\}\rangle$ and $H_2 - 8 = \langle\{6, 7, 9, 10, 12\}\rangle$.

Definition 7.1.23. [**Complement graph**] The **complement** $\overline{G}$ of a graph G is defined as $(V(G), E)$, where $E = \{uv \mid u \neq v, uv \notin E(G)\}$.

Example 7.1.24. 1. See Figure 7.6 for two examples of complement graphs.

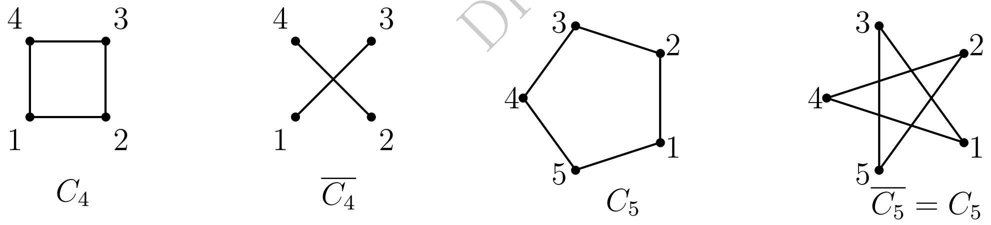


Figure 7.6: Complement graphs

2. The complement of K_3 contains 3 isolated points/vertices.

3. For any graph G, $\|G\| + \|\overline{G}\| = C(|G|, 2)$.

4. In any graph G of order n, $d_G(v) + d_{\overline{G}}(v) = n - 1$. Thus, $\Delta(G) + \Delta(\overline{G}) \geq n - 1$.

Quiz **7.1.25.** 1. *Characterize graphs G such that $\Delta(G) + \Delta(\overline{G}) = n - 1$.*[2]

2. *Can we have a graph G such that $\Delta(G) + \Delta(\overline{G}) = n$?*

3. *Show that a k-regular simple graph on n vertices exists if and only if kn is even and $n \geq k + 1$.*

Definition 7.1.26. The **intersection** of two graphs G and H, denoted $G \cap H$, is defined as $(V(G) \cap V(H), E(G) \cap E(H))$. The **union** of two graphs G and H, denoted $G \cup H$, is defined as $(V(G) \cup V(H), E(G) \cup E(H))$. A **disjoint union** of two graphs is the union while treating the vertex sets as disjoint sets.

[1] $8!/4!(2!)^4$.

[2] If $d_G(u) < d_G(v)$, then $d_{\overline{G}}(u) = n - 1 - d_G(u)$. Hence, $\Delta(G) + \Delta(\overline{G}) \geq d_G(v) + n - 1 - d_G(u) > d_G(v) + n - 1 - d_G(v) \geq n$. Thus, the answer is regular graphs.

Example 7.1.27. Two graphs G and H are shown below. The graphs $G \cup H$ and $G \cap H$ are also shown below.

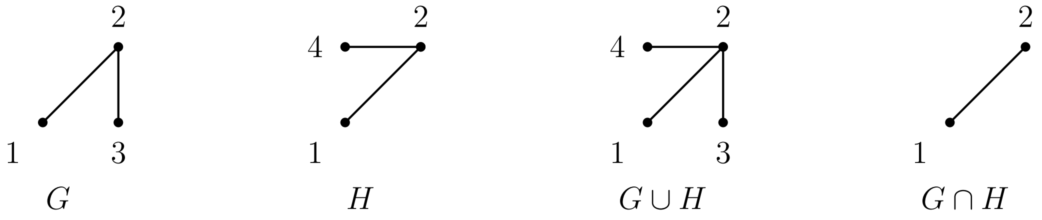


Figure 7.7: Disjoint union and join of graphs

The disjoint union of G and $G \cup H$ is G_1 in Figure 7.8.

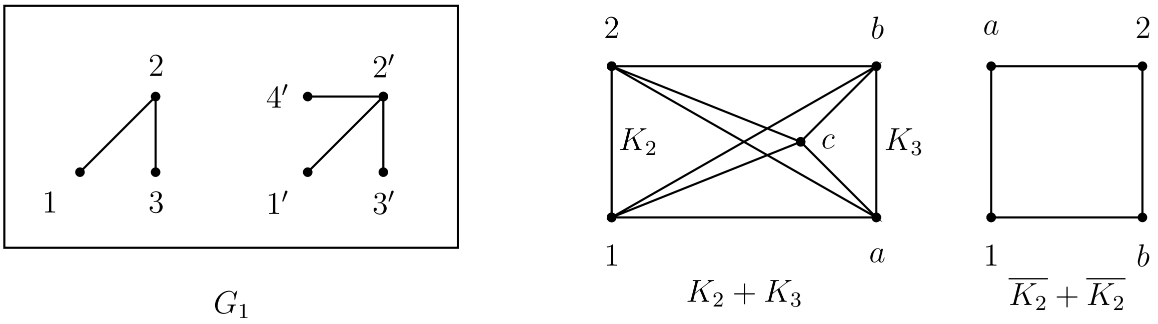


Figure 7.8: Disjoint union and join of graphs

Definition 7.1.28. If $V(G) \cap V(G') = \emptyset$, then the **join** $G + G'$ (here '+' represents join of two graphs) is defined as $G \cup G' + \{vv' : v \in V, v' \in V'\}$ (here '+' means adding a set of edges to a given graph).

Example 7.1.29. (a) $K_2 + K_3 = K_5$.

(b) $\overline{K_2} + \overline{K_2} = C_4$.

Quiz **7.1.30.** *1. What is the complement of the disjoint union of $\overline{G}$ and $\overline{H}$?*[1]

2. Is $K_{m,n} = \overline{K_m} + \overline{K_n}$?

Definition 7.1.31. Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. Then, the **Cartesian product** of G and G', denoted $G \times G' = (V_1, E_1)$, is a graph having $V_1 = V \times V'$ and whose edge set consists of all elements $\{(u_1, u_2), (v_1, v_2)\}$, where either $u_1 = v_1$ and $\{u_2, v_2\} \in E'$ or $u_2 = v_2$ and $\{u_1, v_1\} \in E$.

Example 7.1.32. See the graphs in Figure 7.9.

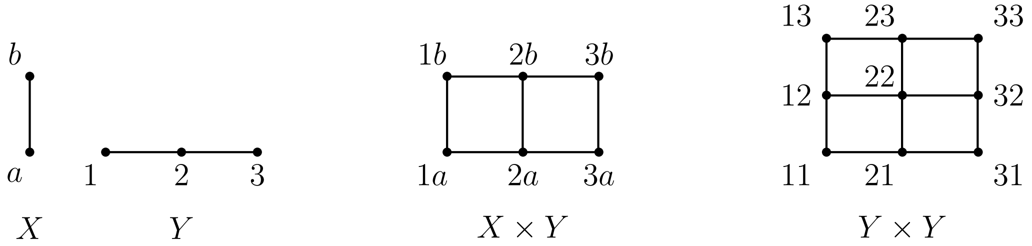


Figure 7.9: Cartesian product of graphs

[1] $G + H$.

7.2 Connectedness

Definition 7.2.1. An u-v **walk** in G is a finite sequence of vertices $[u = v_1, v_2, \cdots, v_k = v]$ such that $v_iv_{i+1} \in E$, for all $i = 1, \cdots, k-1$. The **length** of a walk is the number of edges on it. A walk is called a **trail** if edges on the walk are not repeated. A v-u walk is a called a **path** if the vertices involved are all distinct, except that v and u may be the same. A path can have length 0. A walk (trail, path) is called **closed** if $u = v$. A closed path is called a **cycle/circuit**. Thus, in a simple graph a cycle has length at least 3. A cycle (walk, path) of length k is also written as a k-cycle (k-walk, k-path). If P is an u-v path with $u \neq v$, then we sometimes call u and v as the **end vertices of** P and the remaining vertices on P as the **internal vertices**.

Example 7.2.2.

(a) Take $G = K_5$ with vertex set $\{1, 2, 3, 4, 5\}$.

- Then, $[1, 2, 3, 2, 1, 2, 5, 4, 3]$ is a 8-walk in G and $[1, 2, 2, 1]$ is not a walk.
- The walk $[1, 2, 3, 4, 5, 2, 4, 1]$ is a closed trail.
- The walk $[1, 2, 3, 5, 4, 1]$ is a closed path, that is, it is a 5-cycle.
- The maximum length of a cycle in G is 5 and the minimum length of a cycle in G is 3.
- There are $10 = C(5, 3)$ many 3-cycles in G.
- Verify that the number of 4-cycles in G is not $C(5, 4)$. Can it be $3 \times C(5, 4)$?

(b) Let G be the Petersen graph.

- There is a 9-cycle in G, namely, $[6, 8, 10, 5, 4, 3, 2, 7, 9, 6]$.
- There are no 10-cycles in G. We shall see this when we discuss the Eulerian graphs.

Proposition 7.2.3 (Technique). *Let G be a graph and $u, v \in V(G)$, $u \neq v$. Let $W = [u = u_1, \ldots, u_k = v]$ be a walk. Then, W contains an u-v-path.*

Proof. If no vertex on W repeats, then W is itself a path. So, let $u_i = u_j$ for some $i < j$. Now, consider the walk $W_1 = [u_1, \ldots, u_{i-1}, u_j, u_{j+1}, \ldots u_k]$. This is also an u-v walk but of shorter length. Thus, using induction on the length of the walk, the desired result follows. ■

Definition 7.2.4. The **distance** $d(u, v)$ between two vertices u and v in G is the shortest length of an u-v path in G. If no such path exists, the distance is taken to be ∞. The greatest distance between any two vertices in a graph G is called the **diameter** of G. We shall use $\mathsf{diam}(G)$ to denote the diameter of G. Let $dist_v = \max\limits_{u \in G} d(v, u)$. The **radius** is the $\min\limits_{v \in G} dist_v$ and the **center** consists of all vertices v for which $dist_v$ is the radius. The **girth**, denoted $g(G)$, of a graph G is the minimum length of a cycle contained in G. If G has no cycle, then we put $g(G) = \infty$.

Example 7.2.5. Let G be the Petersen graph. It has diameter 2. The radius is 2. Each vertex is in the center. Its girth is 5.

Practice **7.2.6.** *Determine the diameter, radius, center and girth of the following graphs: P_n, C_n, K_n and $K_{n,m}$.*

Exercise **7.2.7.** *Let G be a graph. Then, show that the distance function $d(u, v)$ is a metric on $V(G)$. That is, it satisfies*

1. *$d(u, v) \geq 0$ for all $u, v \in V(G)$ and $d(u, v) = 0$ if and only if $u = v$,*
2. *$d(u, v) = d(v, u)$ for all $u, v \in V(G)$ and*
3. *$d(u, v) \leq d(u, w) + d(w, u)$ for all $u, v, w \in V(G)$.*

Proposition 7.2.8 (Technique)**.** *Let G be a graph with $\|G\| \geq 1$ and $d(v) \geq 2$, for each vertex except one, say v_1. Then, G has a cycle.*

Proof. Consider a longest path $[v_1, \ldots, v_k]$ in G (as $V(G)$ is finite, such a path exists). As $d(v_k) \geq 2$, it must be adjacent to some vertex from $v_2, \ldots, v_{k-2}$, otherwise, we can extend it to a longer path. Let $i \geq 2$ be the smallest such that v_i is adjacent to v_k. Then, $[v_i, v_{i+1}, \ldots, v_k, v_i]$ is a cycle. ∎

Proposition 7.2.9 (Technique)**.** *Let P and Q be two different u-v paths in G. Then, $P \cup Q$ contains a cycle.*

Proof. Imagine a signal was sent from u to v via P and was returned back from v to u via Q. Call an edge 'dead' if signal has passed through it twice. Notice that each vertex receives the signal as many times as it sends the signal.

Is $E(P) = E(Q)$? No, otherwise both P and Q are the same paths.

So, there are some 'alive' edges. Get an alive edge $\overrightarrow{v_1v_2}$. There must be an alive edge $\overrightarrow{v_2v_3}$.[1] Similarly get $\overrightarrow{v_3v_4}$ and so on. Stop at the first instance of repetition of a vertex: $[v_1, v_2, \cdots, v_i, v_{i+1} \cdots, v_j = v_i]$. Then, $[v_i, v_{i+1} \cdots, v_j = v_i]$ is a cycle.

Alternate. Consider the graph $H = \big(V(P) \cup V(Q),\, E(P)\Delta E(Q)\big)$, where Δ is the symmetric difference. Notice that $E(H) \neq \emptyset$, otherwise $P = Q$. As the degree of each vertex in the multigraph $P \cup Q$ is even and H is obtained after deleting pairs of multiple edges, each vertex in H has even degree. Hence, by Proposition 7.2.8, H has a cycle. ∎

Proposition 7.2.10. *Every graph G containing a cycle satisfies $g(G) \leq 2\,\mathsf{diam}(G) + 1$.*

Proof. Let $C = [v_1, v_2, \ldots, v_k, v_1]$ be the shortest cycle and $\mathsf{diam}(G) = r$. If $k \geq 2r + 2$, then consider the path $P = [v_1, v_2, \ldots, v_{r+2}]$. Since the length of P is $r + 1$ and $\mathsf{diam}(G) = r$, there is a v_{r+2}-v_1 path R of length at most r. Note that P and R are different v_1-v_{r+2} paths. By Proposition 7.2.9, the closed walk $P \cup R$ of length at most $2r + 1$ contains a cycle. Hence, the length of this cycle is at most $2r + 1$, a contradiction to C having the smallest length $k \geq 2r + 2$. ∎

Definition 7.2.11. Let $C = [v_1, \ldots, v_k = v_1]$ be a cycle. An edge v_iv_j is called a **chord** of C if it is not an edge of C. A graph is called **chordal** if each cycle of length at least 4 has a chord. A graph is **acyclic** if it has no cycles.

Example 7.2.12. Complete graphs are chordal, so are the acyclic graphs. The Petersen graph is not chordal.

QUIZ **7.2.13.** 1. *How many acyclic graphs are there on the vertex set $\{1, 2, 3\}$?*[2]

2. *How many chordal graphs are there on the vertex set $\{1, 2, 3, 4\}$?*[3]

Definition 7.2.14. 1. A graph G is said to be **maximal** with respect to a property P if G has property P and no proper supergraph of G has the property P. We similarly define the term **minimal**.

> Notice!
>
> The class of all graphs with that property is the POSET here. So, the maximality and the minimality are defined naturally.

[1] Otherwise, v_2 is incident to just one alive edge and some dead edges. This means v_2 has received more signal than it has sent.

[2] 7: 3 edges can be put in 2^3 ways. One of them is a cycle.

[3] 61: 6 edges can be put in 2^6 ways. There are three 4-cycles.

2. A complete subgraph of G is called a **clique**. The maximum order of a clique is called the **clique number** of G. It is denoted $\omega(G)$.
3. A graph G is called **connected** if there is an u-v path, for each $u, v \in V(G)$.
4. A graph which is not connected is called **disconnected**. If G is a disconnected graph, then a maximal connected subgraph is called a **component** or sometimes a **connected component**.

Example 7.2.15. Consider the graph G shown in Figure 7.2. Then,

1. some cliques in G are $\langle\{8, 10\}\rangle$, $\langle\{2\}\rangle$. The first is a maximal cliques. Notice that every vertex is a clique. Similarly each edge is a clique. Here $\omega(G) = 2$.
2. the graph G is not connected. It has four connected components, namely, $\langle\{8, 9, 10, 11\}\rangle$, $\langle\{1, 2, 3, 4, 5, 6, 7\}\rangle$, $\langle\{12\}\rangle$ and $\langle\{13\}\rangle$.

Quiz **7.2.16.** *What is $\omega(G)$ for the Petersen graph?*[1]

Proposition 7.2.17. *If $\delta(G) \geq 2$, then G has a path of length $\delta(G)$ and a cycle of length at least $\delta(G) + 1$.*

Proof. Let $[v_1, \cdots, v_k]$ be a longest path in G. As $d(v_k) \geq 2$, v_k is adjacent to some vertex $v \neq v_{k-1}$. If v is not on the path, then we have a path that is longer than $[v_1, \cdots, v_k]$ path. A contradiction. Let i be the smallest positive integer such that v_i is adjacent to v_k. Thus,

$$\delta(G) \leq d(v_k) \leq |\{v_i, v_{i+1}, \cdots, v_{k-1}\}|.$$

Hence, the cycle $C = [v_i, v_{i+1}, \cdots, v_k, v_i]$ has length at least $\delta(G) + 1$ and the length of the path $P = [v_i, v_{i+1}, \cdots, v_k]$ is at least $\delta(G)$. ■

Definition 7.2.18. The **edge density**, denoted $\varepsilon(G)$, is defined to be the number $\frac{|E(G)|}{|V(G)|}$. Observe that $\varepsilon(G)$ is also a graph invariant.

Quiz **7.2.19.** 1. *When does 'deletion of a vertex' reduce edge density?*[2]

2. *Is $\frac{\delta(G)}{2}$ a lower bound for $\varepsilon(G)$?*[3]
3. *Suppose that $\varepsilon(G) \geq \delta(G)$. Should we have a vertex v with $\varepsilon(G) \geq d(v)$?*[4]

Proposition 7.2.20. *Let G be a graph with $\|G\| \geq 1$. Then, G has a subgraph H with $\delta(H) > \varepsilon(H) \geq \varepsilon(G)$.*

Proof. If $\varepsilon(G) < \delta(G)$, then we take $H = G$. Otherwise, there is a vertex v with $\varepsilon(G) \geq d(v)$. Put $G_1 = G - v$. Then, it can be easily verified that $\varepsilon(G_1) \geq \varepsilon(G)$.

If $\varepsilon(G_1) < \delta(G_1)$, then we take $H = G_1$. Otherwise, there is a vertex $v \in G_1$ with $\varepsilon(G_1) \geq d(v)$. Put $G_2 = G_1 - v$. Then, we again have $\varepsilon(G_2) \geq \varepsilon(G_1) \geq \varepsilon(G)$.

Continuing as above, we note that "Initially $\varepsilon(G) > 0$. At the i-th stage, we obtained the subgraph G_i satisfying $|V(G_i)| = |G| - i, \varepsilon(G_i) \geq \varepsilon(G_{i-1})$. That is, we have been reducing the number of vertices and the corresponding edge densities have been non-decreasing." Hence, this process must stop before we reach a single vertex, as its edge density is 0.

So, let us assume that the process stops at H. Then, '$\varepsilon(H) < \delta(H)$' must be true, or else, the process would not stop at H and hence the required result follows. ■

[1] 2.

[2] Put $H = G - v$. Then, $\|H\| = \varepsilon(G)n - d(v)$, so that $\varepsilon(H) = \frac{\varepsilon(G)n - d(v)}{n-1} = \varepsilon(G) + \frac{\varepsilon(G) - d(v)}{n-1}$. So, we should choose a vertex v with degree more that $\varepsilon(G)$.

[3] Yes.

[4] Yes. Otherwise, we have $\varepsilon(G) < d(v)$, for each v. In particular $\varepsilon(G) < \delta(G)$, a contradiction.

7.3 Isomorphism in Graphs

Definition 7.3.1. Two graphs $G = (V, E)$ and $G' = (V', E')$ are said to be **isomorphic** if there is a bijection $f : V \to V'$ such that $u \sim v$ in G if and only if $f(u) \sim f(v)$ in G', for each $u, v \in V$. In other words, an isomorphism is a bijection between the vertex sets which preserves adjacency. We write $G \cong G'$ to mean that G is isomorphic to G'.

Example 7.3.2. Consider the graphs in Figure 7.10. Then, note that

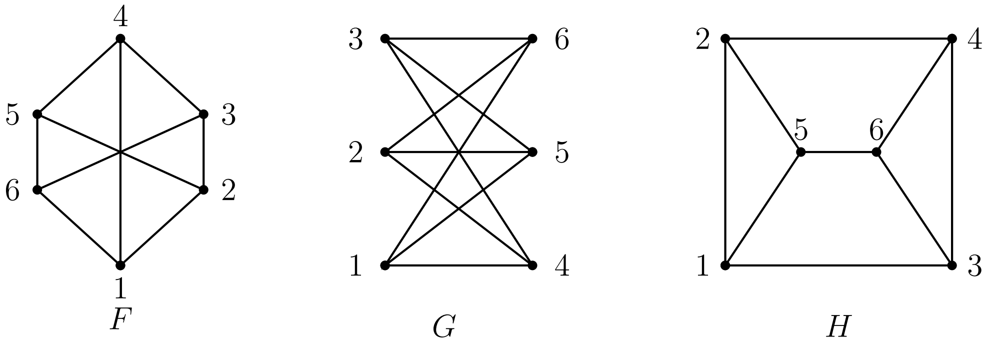


Figure 7.10: F is isomorphic to G but F is not isomorphic to H

1. the graph F is not isomorphic to H as $\alpha(F)$, the independence number of F is 3 whereas $\alpha(H) = 2$. Alternately, H has a 3-cycle, whereas F does not.
2. the graph F is isomorphic to G as the map $f : V(F) \to V(G)$ defined by $f(1) = 1$, $f(2) = 5$, $f(3) = 3$, $f(4) = 4$, $f(5) = 2$ and $f(6) = 6$ gives an isomorphism.

Check the adjacency

F	G
$1 \to 2, 4, 6$	$f(1) = 1 \to f(2) = 5, f(4) = 4, f(6) = 6$
$3 \to 2, 4, 6$	$f(3) = 3 \to f(2) = 5, f(4) = 4, f(6) = 6$
$5 \to 2, 4, 6$	$f(5) = 2 \to f(2) = 5, f(4) = 4, f(6) = 6$

All edges are covered, no need to check any further.

Discussion 7.3.3. [Isomorphism] Let F and G be isomorphic under $f : V(F) \to V(G)$. Take F. Relabel each vertex $v \in F$ as $f(v)$. Call the new graph F'. Then, $F' = G$. This is so, as $V(F') = V(G)$ and $E(F') = E(G)$ due to the isomorphic nature of the function f.

PRACTICE **7.3.4.** *Take the graphs F and G of Figure 7.10. Take the isomorphism $f(1) = 1$, $f(2) = 5$, $f(3) = 3$, $f(4) = 4$, $f(5) = 2$ and $f(6) = 6$. Obtain the F' as described in Discussion 7.3.3. List $V(F')$ and $E(F')$. List $V(G)$ and $E(G)$. Notice that they are the same.*

Definition 7.3.5. A graph G is called **self-complementary** if $G \cong \overline{G}$.

Example 7.3.6. Let G be a self-complementary graph on n vertices. Then $\|G\| = n(n-1)/4$. Thus, either $n = 4k$ or $n = 4k + 1$. Verify that

1. the path $P_4 = [0, 1, 2, 3]$ is self complimentary. An isomorphism from G to $\overline{G}$ is described by $f(i) = 2i \pmod 5$.
2. the cycle $C_5 = [0, 1, 2, 3, 4, 0]$ is self complimentary. An isomorphism from G to $\overline{G}$ is described by $f(i) = 2i \pmod 5$.

EXERCISE **7.3.7.** *1. Construct a self-complementary graph of order $4k$.*

2. *Construct a self-complementary graph of order $4k+1$.*

Definition 7.3.8. A **graph invariant** is a function which assigns the same value (output) to isomorphic graphs.

Example 7.3.9. Observe that some of the graph invariants are: $|G|$, $\|G\|$, $\Delta(G)$, $\delta(G)$, $\omega(G)$, $\alpha(G)$ and the multiset $\{d(v) : v \in V(G)\}$.

Exercise **7.3.10.** *How many graphs are there with vertex set $\{1,2,\ldots,n\}$? Do you find it easy if we ask for non-isomorphic graphs (try for $n=4$)?*

Proposition 7.3.11 (Technique)**.** *Let $f : G \to H$ be an isomorphism and $v \in V(G)$. Then, $G - v \cong H - f(v)$.*

Proof. Consider the bijection $g : V(G-v) \to V(H - f(v))$ described by $g = f_{V(G-v)}$. ■

Definition 7.3.12. An isomorphism of G to G is called an **automorphism**.

Example 7.3.13. 1. Identity map is always an automorphism on any graph.

2. Any permutation in S_n is an automorphism of K_n.

3. There are only two automorphisms of a path P_8. Is it true for P_n, for $n \geq 3$?

Proposition 7.3.14. *Let G be a graph and let $\Gamma(G)$ denote the set of all automorphisms of G. Then, $\Gamma(G)$ forms a group under composition of functions.*

Proof. Let $V(G) = \{1,2,\ldots,n\}$ and $\sigma, \mu \in \Gamma(G)$ be two automorphisms. Then,

$$ij \in E(G) \Leftrightarrow \mu(i)\mu(j) \in E(G) \Leftrightarrow (\sigma \circ \mu)(i)(\sigma \circ \mu)(j) \in E(G).$$

Thus, $\sigma \circ \mu$ is an automorphism. Moreover, μ^{-1}, σ^{-1} are indeed automorphisms. ■

Example 7.3.15. Determine $\Gamma(C_5)$.

Ans: Consider $C_5 = [1,\ldots,5,1]$. Note that $\sigma = (2,3,4,5,1)$ is an automorphism. Hence, $\{e,\sigma,\sigma^2,\ldots,\sigma^4\} \subseteq \Gamma(C_5)$ as $\sigma^5 = e$.

Now, let μ be an automorphism with $\mu(1) = i$. Put $\tau = \sigma^{6-i}\mu$. Then, τ is an automorphism with $\tau(1) = 1$. If $\tau(2) = 2$, then the adjacency structure implies that $\tau(j) = j$ for $j = 3,4,5$. Hence, in this case, $\sigma^{6-i}\mu = e$ and thus, $\mu = \sigma^{i-6} = \sigma^{i-1}$.

If $\tau(2) \neq 2$, then $\tau(2) = 5$, $\tau(3) = 4$ and so $\tau = (2,5)(3,4)$ is the reflection which fixes 1. Let us denote the permutation $(2,5)(3,4)$ by ρ. Then, $\Gamma(C_5)$ is the group generated by σ and ρ and hence $\Gamma(C_5)$ has 10 elements.

Example 7.3.16. Notice that $\Gamma(C_5)$ has a subgroup $\Gamma_1 = \{e,\sigma,\sigma^2,\sigma^3,\sigma^4\}$, with $\sigma^5 = e$, of order 5. Let G be a subgraph of C_5 obtained by deleting some (zero allowed) edges. If $\|G\| = 5$, then $|\Gamma(G)| = 10$. If $\|G\| = 0$, then $|\Gamma(G)| = |S_5| = 5!$. If $\|G\| = 4$, then $|\Gamma(G)| = 2$. If $\|G\| = 3$, then $|\Gamma(G)| = 2$ or 4. If $\|G\| = 2$, then $|\Gamma(G)| = 4$ or 8. If $\|G\| = 1$, then $|\Gamma(G)| = 2 \times 3!$. Thus, there is no subgraph of G whose automorphism group is Γ_1.

Exercise **7.3.17.** 1. *Determine the graphs G for which $\Gamma(G) = S_n$, the group of all permutations of $1,\ldots,n$.*

2. *Compute $\Gamma(G)$ for some graphs of small order.*

3. *Let G be a subgraph of H of the same order. Explore more about the relationship between $\Gamma(G)$ and $\Gamma(H)$.*

7.4 Trees

Definition 7.4.1. A connected acyclic graph is called a **tree**. A **forest** is a graph whose components are trees.

Proposition 7.4.2. *Let T be a tree and $u, v \in V(T)$. Then, there is a unique u-v-path in T.*

Proof. On the contrary, assume that there are two u-v-paths in T. Then, by Proposition 7.2.9, T has a cycle, a contradiction. ■

Proposition 7.4.3. *Let G be a graph with the property that 'between each pair of vertices there is a unique path'. Then, G is a tree.*

Proof. Clearly, G is connected. If G has a cycle $[v_1, v_2, \cdots, v_k = v_1]$, then $[v_1, v_2, \ldots, v_{k-1}]$ and $[v_1, v_{k-1}]$ are two v_1-v_{k-1} paths. A contradiction. ■

Definition 7.4.4. Let G be a connected graph. A vertex v of G is called a **cut vertex** if $G - v$ is disconnected. Thus, $G - v$ is connected if and only if v is not a cut vertex.

Proposition 7.4.5. *Let G be a connected graph with $|G| \geq 2$. If $v \in V(G)$ with $d(v) = 1$, then $G - v$ is connected. That is, a vertex of degree 1 is never a cut vertex.*

Proof. Let $u, w \in V(G - v)$, $u \neq w$. As G is connected, there is an u-w path P in G. The vertex v cannot be an internal vertex of P, as each internal vertex has degree at least 2. Hence, the path P is available in $G - v$. So, $G - v$ is connected. ■

Proposition 7.4.6 (Technique)**.** *Let G be a connected graph with $|G| \geq 2$ and let $v \in V(G)$. If $G - v$ is connected, then either $d(v) = 1$ or v is on a cycle.*

Proof. Assume that $G - v$ is connected. If $d_G(v) = 1$, then there is nothing to show. So, assume that $d(v) \geq 2$. We need to show that v is on a cycle in G.

Let u and w be two distinct neighbors of v in G. As $G - v$ is connected there is a path, say $[u = u_1, \ldots, u_k = w]$, in $G - v$. Then, $[u = u_1, \ldots, u_k = w, v, u]$ is a cycle in G containing v. ■

Quiz **7.4.7.** *Let G be a graph and v be a vertex on a cycle. Can $G - v$ be disconnected?*[1]

Definition 7.4.8. Let G be a graph. An edge e in G is called a **cut edge** or a **bridge** if $G - e$ has more connected components than that of G.

Proposition 7.4.9 (Technique)**.** *Let G be connected and $e = [u, v]$ be a cut edge. Then, $G - e$ has two components, one containing u and the other containing v.*

Proof. If $G - e$ is not disconnected, then by definition, e cannot be a cut edge. So, $G - e$ has at least two components. Let G_u (respectively, G_v) be the component containing the vertex u (respectively, v). We claim that these are the only components.

Let $w \in V(G)$. Then, G is a connected graph and hence there is a path, say P, from w to u. Moreover, either P contains v as its internal vertex or P doesn't contain v. In the first case, $w \in V(G_v)$ and in the latter case, $w \in V(G_u)$. Thus, every vertex of G is either in $V(G_v)$ or in $V(G_u)$ and hence the required result follows. ■

Proposition 7.4.10 (Technique)**.** *Let G be a graph and e be an edge. Then, e is a cut edge if and only if e is not on a cycle.*

[1] Yes. Take $G = (\{1, 2, 3, 4\},\ \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{3, 4\}\})$ and $v = 1$.

Proof. Suppose that $e = [u, v]$ is a cut edge of G. Let F be the component of G that contains e. Then, by Proposition 7.4.9, $F - e$ has two components, namely, F_u that contains u and F_v that contains v.

Let if possible, $C = [u, v = v_1, \ldots, v_k = u]$ be a cycle containing $e = [u, v]$. Then, $[v = v_1, \ldots, v_k = u]$ is an u-v path in $F - e$. Hence, $F - e$ is still connected. A contradiction. Hence, e cannot be on any cycle.

Conversely, let $e = [u, v]$ be an edge which is not on any cycle. Now, suppose that F is the component of G that contains e. We need to show that $F - e$ is disconnected.

Let if possible, there is an u-v-path, say $[u = u_1, \ldots, u_k = v]$, in $F-e$. Then, $[v, u = u_1, \ldots, u_k = v]$ is a cycle containing e. A contradiction to e not lying on any cycle.

Hence, e is a cut edge of F. Consequently, e is a cut edge of G. ■

Proposition 7.4.11. *Let T be a tree on n vertices. Then, T has $n - 1$ edges.*

Proof. We proceed by induction. Take a tree on $n \geq 2$ vertices and delete an edge e. Then, we get two subtrees T_1, T_2 of order n_1, n_2, respectively, where $n_1 + n_2 = n$. So, $E(T) = E(T_1) \cup E(T_2) \cup \{e\}$. By induction hypothesis $\|T\| = \|T_1\| + \|T_2\| + 1 = n_1 - 1 + n_2 - 1 + 1 = n_1 + n_2 - 1 = n - 1$. ■

Proposition 7.4.12. *Let G be a connected graph with n vertices and $n-1$ edges. Then, G is acyclic.*

Proof. On the contrary, assume that G has a cycle, say Γ. Now, select an edge $e \in \Gamma$ and note that $G-e$ is connected. We go on selecting edges from G that lie on cycles and keep removing them, until we get an acyclic graph H. Since the edges that are being removed lie on some cycle, the graph H is still connected. So, by definition, H is a tree on n vertices. Thus, by Proposition 7.4.11, $|E(H)| = n - 1$. But, in the above argument, we have deleted at least one edge and hence, $|E(G)| \geq n$. This gives a contradiction to $|E(G)| = n - 1$. ■

Proposition 7.4.13. *Let G be an acyclic graph with n vertices and $n-1$ edges. Then, G is connected.*

Proof. Let if possible, G be disconnected with components $G_1, \ldots, G_k, k \geq 2$. As G is acyclic, by definition, each G_i is a tree on, say $n_i \geq 1$ vertices, with $\sum\limits_{i=1}^{k} n_i = n$. Thus, $\|G\| = \sum\limits_{i=1}^{k} (n_i - 1) = n - k < n - 1 = \|G\|$, as $k \geq 2$. A contradiction. ■

Theorem 7.4.14. *Let G be a graph with $V(G) = \{1, 2, \ldots, n\}$. Then, the following are equivalent.*

1. *G is a tree.*
2. *G is a minimal connected graph on n vertices.*
3. *G is a maximal acyclic graph on n vertices.*

Proof. (a)⇒(b). Suppose that G is a tree. If it is not a minimal connected graph on n vertices, then there is an edge $[u, v]$ such that $G - [u, v]$ is connected. But then, by Theorem 7.4.10, $[u, v]$ is on a cycle in G. A contradiction.

(b)⇒(c). Suppose G is a minimal connected graph on n vertices. If G has a cycle, say Γ, then select an edge $e \in \Gamma$. Thus, by Theorem 7.4.10, $G-e$ is still connected graph on n vertices, a contradiction to the fact that G is a minimal connected graph on n vertices. Hence, G is acyclic. Since G is connected, for any new edge e, the graph $G + e$ contains a cycle and hence, G is maximal acyclic graph.

(c)⇒(a). Suppose G is maximal acyclic graph on n vertices. If G is not connected, let G_1 and G_2 be two components of G. Select $v_1 \in G_1$ and $v_2 \in G_2$ and note that $G + [v_1, v_2]$ is acyclic graph on n vertices. This contradicts that G is a maximal acyclic graph on n vertices. Thus, G is connected and acyclic and hence is a tree. ■

Theorem 7.4.15. *The following are Equivalent for a graph of order n.*

(a) G is a tree.

(b) G is minimal connected.

(c) G is maximal acyclic.

(d) G is acyclic with $\|G\| = n - 1$.

(e) G is connected with $\|G\| = n - 1$.

Proof. Left as an exercise.

Proposition 7.4.16. *The center of a tree always consists of a set of at most two vertices.*

Proof. Let T be a tree of radius k. Since the center contains at least one vertex, let u be a vertex in the center of T. Now, let v be another vertex in the center. We claim that u is adjacent to v.

Suppose $u \nsim v$. Then, there exists a path from u to v, denoted $P(u, v)$, with at least one internal vertex, say w. Let x be any pendant ($d(x) = 1$) vertex of T. Then, either $v \in P(x, w)$ or $v \notin P(x, w)$. In the latter case, check that $\|P(x, w)\| < \|P(x, v)\| \leq k$.

If $v \in P(x, w)$, then $u \notin P(x, w)$ and $\|P(x, w)\| < \|P(x, u)\| \leq k$. That is, the distance from w to any pendant vertex is less than k. Hence, k is not the radius, a contradiction. Thus, $uv \in T$.

We cannot have another vertex in the center, or else, we will have a C_3 in T, a contradiction. ■

EXERCISE **7.4.17.**

1. *Show that a graph G is a tree if and only if between each pair of vertices of G there is a unique path.*
2. *Draw a tree on 8 vertices. Label $V(T)$ as $1, \ldots, 8$ so that each vertex $i \geq 2$ is adjacent to exactly one element of $\{1, 2, \ldots, i - 1\}$.*

Proposition 7.4.18. *Let T be a tree. Then, any graph G with $\delta(G) \geq |T| - 1$ has a subgraph $H \cong T$.*

Proof. We prove the result by induction on $n = |T|$. The result is trivially true if $n = 1$ or 2. So, let the result be true for every tree on $n - 1$ vertices and take a tree T on n vertices. Also, suppose that G is any graph with $\delta(G) \geq |T| - 1$.

Let $v \in V(T)$ with $d(v) = 1$. Take $u \in V(T)$ such that $uv \in E(T)$. Now, consider the tree $T_1 = T - v$. Then, $\delta(G) \geq |T| - 1 = n - 1 > n - 2$. Hence, by induction hypothesis, G has a subgraph H such that $H \cong T_1$ under a map, say ϕ. Let $h \in V(H)$ such that $\phi(h) = u$. Since $\delta(G) \geq |T| - 1$, h has a neighbor, say h_1, such that h_1 is not a vertex in H but is a vertex in G. Now, map this vertex to v to get the required result. ■

EXERCISE **7.4.19.** *Let G be a graph on $n > 2$ vertices. If $\|G\| > C(n - 1, 2)$, is G necessarily connected? Give an 'if and only if' condition for the connectedness of a graph with exactly $C(n-1, 2)$ edges.*

Proposition 7.4.20. *A tree on $n \geq 2$ vertices has at least two pendant vertices.*

Proof. Let T be any tree on n vertices. Then, $\sum\limits_{v \in V(T)} d(v) = 2\|E(T)\| = 2(n - 1) = 2n - 2$. Hence, by PHP, T has at least two vertices of degree 1. ■

Definition 7.4.21. Let T be a tree on $n > 2$ vertices and labeled by n integers, say $\{1, 2, \ldots, n\}$. The **Prüfer code** P_T of T is a sequence X of size $n - 2$ created in the following way.

1. Find the largest pendant vertex, say v_1. Let u_1 be the neighbor of v_1. Put $X(1) = u_1$.
2. Let $T_1 = T - v_1$ and find $X(2)$.
3. Repeat the procedure to obtain $X(3), \ldots, X(n-2)$.

Example 7.4.22. For example, Consider the tree T in Figure 7.12.

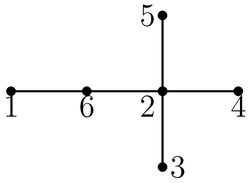


Figure 7.11: A tree T on 6 vertices

Then, the above process proceeds as follows.

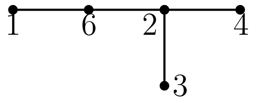
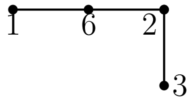
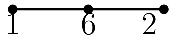
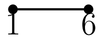
Step	**Pendant $\mathbf{v_i}$**	**Neighbor $\mathbf{u_i}$**	$\mathbf{P_T = X(1), X(2), \ldots}$	$\mathbf{T_i = T - v_i}$
1	5	2	2	
2	4	2	2,2	
3	3	2	2,2,2	
4	2	6	2,2,2,6	

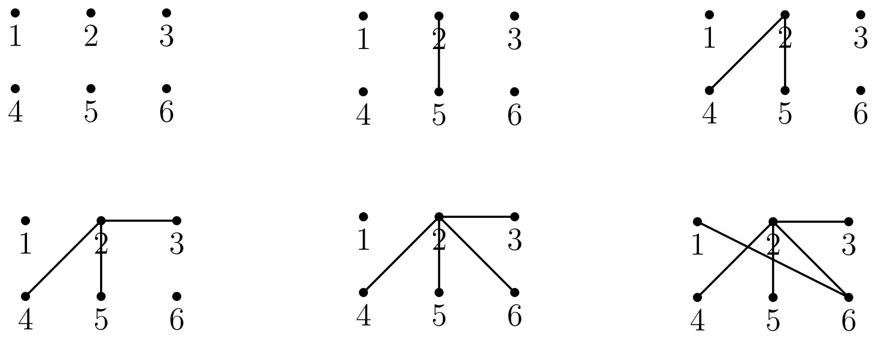
Figure 7.12: A tree T on 6 vertices

EXERCISE **7.4.23.** *In the above process, prove that $u_j = i$, for some j, if and only if $d(i) \geq 2$.*

Example 7.4.24. Can I get back the original tree T from the sequence $2, 2, 2, 6$? **Ans:** Yes. The process of getting back the original tree is as follows.

1. Plot points $1, 2, \ldots, 6$.
2. Since u_i is either 2 or 6, it implies that 2 and 6 are not the pendant vertices. Hence, the pendant vertices in T must be $\{1, 3, 4, 5\}$. Thus, the algorithm implies that the largest pendant 5 must be adjacent to (the first element of the sequence) 2.
3. At step 1, the vertex 5 was deleted. Hence, $V(T_1) = \{1, 2, 3, 4, 6\}$ with the given sequence $2, 2, 6$. So, the pendants in T_1 are $\{1, 3, 4\}$ and the vertex 4 (largest pendant) is adjacent to 2.
4. Now, $V(T_2) = \{1, 2, 3, 6\}$ with the sequence as $2, 6$. So, 3 is adjacent to 2.
5. Now, $V(T_3) = \{1, 2, 6\}$ with the sequence as 6. So, the pendants in the current T are $\{1, 2\}$ and 2 is adjacent to 6.
6. Lastly, $V(T_4) = \{1, 6\}$. As the process ends with K_2 and we have only two vertices left, they must be adjacent.

   The corresponding set of figures are as follows.



Proposition 7.4.25. *Let T be a tree on the vertex set $\{1, 2, \ldots, n\}$. Then, $d(v) \geq 2$ if and only if v appears in the Prüfer code P_T. Thus, $\{v : v \notin P_T\}$ are precisely the pendant vertices in T.*

Proof. Let $d(v) \geq 2$. Since the process ends with an edge, there is a stage, say i, where $d(v)$ decreases strictly. Thus, till the $(i-1)$-th stage, v was adjacent to a pendant vertex w and at the i-th stage w was deleted and thus, v appears in the sequence.

Conversely, let v appear in the sequence at k-th stage for the first time. Then, the tree T_k had a pendant vertex w of highest label that was adjacent to v. Note that $T_k - w$ is a tree with at least two vertices. Thus, $d(v) \geq d_{T_k}(v) \geq 2$. ■

Exercise **7.4.26.** *Prove that in the Prüfer code of T a vertex v appears exactly $d(v) - 1$ times. [Hint: Use induction and if v is the largest pendant adjacent to w and $T' = T - v$ then $P_T = w, P_{T'}$.]*

Proposition 7.4.27. *Let T and T' be two trees on the same vertex set of integers. If $P_T = P_{T'}$, then $T = T'$.*

Proof. The statement is trivially true for $|T| = 3$. Assume that the statement holds for $3 < |T| < n$. Now, let T and T' be two trees with vertex set $\{1, 2, \ldots, n\}$ and $P_T = P_{T'}$. As $P_T = P_{T'}$, T and T' have the same set of pendants. Further, the largest labeled pendant w is adjacent to the vertex $X(1)$ in both the trees. Thus, $P_{T-w} = P_{T'-w}$ and hence, by induction hypothesis $T - w = T' - w$. Thus, by PMI, $T = T'$. ■

Proposition 7.4.28. *Let S be a set of $n \geq 3$ integers and X be a sequence of length $n-2$ of elements from S. Then, there is a tree T with $V(T) = S$ and $P_T = X$.*

Proof. Verify the statement for $|T| = 3$. Now, let the statement hold for all trees T on $n > 3$ vertices and consider a set S of $n+1$ integers and a sequence X of length $(n-1)$ of elements of S.

Let $v = \max\{x \in S \,:\, x \notin X\}$, $S' = S - v$ and $X' = X(2), \ldots, X(n-1)$. By definition, note that $v \neq X(i)$, for $2 \leq i \leq n-1$. Thus, X' is a sequence of elements of S' of length $n-2$. As $|S'| = n$, by induction hypothesis, there is a tree T' with $P_{T'} = X'$.

Let T be the tree obtained by adding a new pendant v at the vertex $X(1)$ of T'. In T', the vertices $X(i)$, for $i \geq 2$, were not available as pendants and now in T the vertex $X(1)$ is also not available as a pendant (here some $X(i)$'s may be the same). Let $R' = \{x \in S' \,:\, x \notin X'\}$ be the pendants in T'. Then, the set of pendants in T is $(R' \cup \{v\}) \setminus \{X(1)\}$ which equals $\{x \in S \,:\, x \notin X\}$. Thus, v is the pendant of T of maximum label. Hence, $P_T = X$. ■

Theorem 7.4.29. [**A. Cayley,** 1889, **Quart. J. Math**] *Let $n \geq 3$. Then, there are n^{n-2} different trees with vertex set $\{1, 2, \ldots, n\}$.*

Proof. Let F be the class of trees on the vertex set $\{1, 2, \ldots, n\}$ and let G be the class of $(n-2)$-sequences of $\{1, 2, \ldots, n\}$. Note that the function $f : F \to G$ defined as $f(T) = P_T$, the Prüfer code, is a one-one and onto mapping. As $|G| = n^{n-2}$, the required result follows. ■

Exercise **7.4.30.** *1. Find out all non-isomorphic trees of order 7 or less.*

2. *Show that every automorphism of a tree fixes a vertex or an edge.*

3. *Give a class of trees T with $|\Gamma(T)| = 6$.*

4. *Let T be a tree, $\sigma \in \Gamma(T)$, $u \in V(T)$ such that $\sigma^2(u) \neq u$. Can we have an edge $[u, v] \in T$ such that $\sigma(u) = v$?*

5. *Let T be a tree with center $\{u\}$ and radius r. Let v satisfy $d(u, v) = r$. Show that r is a pendant.*

6. *Let T be a tree with $|T| > 2$. Let T' be obtained from T by deleting all the pendant vertices of T. Show that the center of T is the same as the center of T'.*

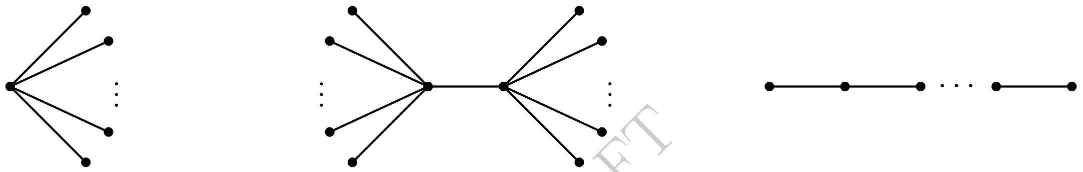
7. *Let T be a tree with center $\{u\}$ and $\sigma \in \Gamma(T)$. Show that $\sigma(u) = u$.*

8. *Is it possible to have a tree such that $|\Gamma(T)| = 7$?*

9. *Construct a tree T on vertices $S = \{1, 2, 3, 6, 7, 8, 9\}$ for which $P_T = 6, 3, 7, 1, 2$.*

10. *Practice with examples: get the Prüfer code from a tree; get the tree from a given code and a vertex set.*

11. *How many trees of the following forms are there on the vertex set $\{1, 2, \ldots, 100\}$?*



12. *Show that any tree has at least $\Delta(T)$ leaves (pendant edges).*

13. *Let T be a tree and T_1, T_2, T_3 be subtrees of T such that $T_1 \cap T_3 \neq \emptyset$, $T_2 \cap T_3 \neq \emptyset$ and $T_1 \cap T_2 \cap T_3 = \emptyset$. Show that $T_1 \cap T_2 = \emptyset$.*

14. *Let $\mathcal{T}$ be a set of subtrees of a tree T. Assume that the trees in $\mathcal{T}$ have nonempty pairwise intersection. Show that their overall intersection is nonempty. Is this true, if we replace T by a graph G?*

15. *Recall that a connected graph G is said to be unicyclic if G has exactly one cycle as it's subgraph. Prove that if G is connected and $|G| = \|G\|$, then G is a unicyclic graph.*

7.5 Connectivity

Proposition 7.5.1. *Let G be a connected graph on vertex set $\{1, 2, \ldots, n\}$. Then, its vertices can be labeled in such a way that the induced subgraph on the set $\{1, 2, \ldots, i\}$ is connected for $1 \leq i \leq n$.*

Proof. If $n = 1$, there is nothing to prove. Assume that the statement is true if $n < k$ and let G be a connected graph on the vertex set $\{1, 2, \ldots, k\}$. If G is a tree, pick any pendant vertex and label it k. If G has a cycle, pick a vertex on a cycle and label it k. In both the case $G - k$ is connected. Now, use the induction hypothesis to get the required result. ∎

Definition 7.5.2. Let G be a graph. Then, a set $X \subseteq V(G) \cup E(G)$ is called a **separating set** if $G - X$ has more connected components than that of G.

Let X be a separating set of G. Then, 'there exists $u, v \in V(G)$ that lie in the same component of G but lie in different components of $G - X$'. If $\{u\} \subseteq V(G)$ is a separating set of G, then u is a cut vertex. If $\{e\} \subseteq E(G)$ is a separating set of G, then it is a bridge/cut edge.

Example 7.5.3. 1. In a tree, each edge is a bridge and each non-pendant vertex is a cut vertex. Is it true for a forest?

2. The graph K_7 does not have a separating set of vertices. In K_7, a separating set of edges must contain at least 6 edges.

Definition 7.5.4. A graph G is said to be **k-connected** if $|G| > k$ and G is connected even after deletion of any $k-1$ vertices. The **vertex connectivity**, denoted by $\kappa(G)$, of a non trivial graph G is the largest k such that G is k-connected. Convention: $\kappa(K_1) = 0$.

Example 7.5.5. 1. Each connected graph of order more than one is 1-connected.

2. A 2-connected graph is also a 1-connected graph.

3. For a disconnected graph, $\kappa(G) = 0$ and for $n > 1$, $\kappa(K_n) = n - 1$.

4. The graph G in Figure 7.13 is 2-connected but not 3-connected. Thus, $\kappa(G) = 2$.

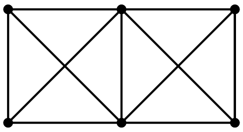


Figure 7.13: graph with vertex connectivity 2

5. The Petersen graph is 3-connected.

Definition 7.5.6. A graph G is called **l-edge connected** if $|G| > 1$ and $G - F$ is connected for every $F \subseteq E(G)$ with $|F| < l$. The greatest integer l such that G is l-edge connected is the **edge connectivity** of G, denoted $\lambda(G)$. Convention: $\lambda(K_1) = 0$.

Example 7.5.7. 1. Note that $\lambda(P_n) = 1, \lambda(C_n) = 2$ and $\lambda(K_n) = n - 1$, whenever $n > 1$.

2. Let T be a tree on $n \geq 2$ vertices. Then, $\lambda(T) = 1$.

3. For the graph G in Figure 7.13, $\lambda(G) = 3$.

4. For the Petersen graph G, $\lambda(G) = 3$.

EXERCISE **7.5.8.** *Let $|G| > 1$. Show that $\kappa(G) = |G| - 1$ if and only if $G = K_n$. Can we say the same for $\lambda(G)$?*

Theorem 7.5.9. [**H. Whitney,** 1932] *For any graph G, $\kappa(G) \leq \lambda(G) \leq \delta(G)$.*

Proof. If G is disconnected or $|G| = 1$, then we have nothing to prove. So, let G be connected graph and $|G| \geq 2$. Then, there is a vertex v with $d(v) = \delta(G)$. If we delete all edges incident on v, then the graph is disconnected. Thus, $\delta(G) \geq \lambda(G)$.

Suppose that $\lambda(G) = 1$ and $G - uv$ is disconnected with components C_u and C_v. If $|C_u| = |C_v| = 1$, then $G = K_2$ and $\kappa(G) = 1$. If $|C_u| > 1$, then we delete u to see that $\kappa(G) = 1$.

If $\lambda(G) = k \geq 2$, then there is a set of edges, say $e_1, \ldots, e_k$, whose removal disconnects G. Notice that $G - \{e_1, \ldots, e_{k-1}\}$ is a connected graph with a bridge, say $e_k = uv$. For each of $e_1, \ldots, e_{k-1}$ select an end vertex other than u or v. Deletion of these vertices from G results in a graph H with uv as a bridge of a connected component. Note that $\kappa(H) \leq 1$. Hence, $\kappa(G) \leq \lambda(G)$. ■

Exercise **7.5.10.** *Give a lower bound on the number of edges of a graph G on n vertices with vertex connectivity $\kappa(G) = k$.*

Theorem 7.5.11. [**Chartrand and Harary,** 1968] *For all integers a, b, c such that $0 < a \leq b \leq c$, there exists a graph with $\kappa(G) = a$, $\lambda(G) = b$ and $\delta(G) = c$.*

Proof. Omitted, as it is out of the scope of this book.

Theorem 7.5.12. [**Mader,** 1972] *Every graph G of average degree at least $4k$ has a k-connected subgraph.*

Proof. For $k = 1$, the assertion is trivial. So, let $k \geq 2$. Note that

$$\begin{aligned} n &= |G| \geq \Delta(G) \geq 4k \geq 2k-1 \text{ and} & (7.1)\\ m &= \|G\| \geq \frac{1}{2}(\text{average degree } \times n) \geq 2kn \geq (2k-3)(n-k+1)+1. & (7.2) \end{aligned}$$

We shall use induction to show that if G satisfies Equations (7.1) and (7.2), then G has a k-connected subgraph. If $n = 2k-1$, then $m \geq (2k-3)(n-k+1)+1 = (n-2)\frac{(n+1)}{2}+1 = \frac{n(n-1)}{2}$. So, G is a graph on n vertices with at least $\frac{n(n-1)}{2}$ edges and hence $G = K_n$. Thus, $K_{k+1} \subseteq K_n = G$.

Assume $n \geq 2k$. If v is a vertex with $d(v) \leq 2k-3$, then we apply induction hypothesis to $G - v$ to get the result. So, let $d(v) \geq 2k-2$, for each vertex v. If G is k-connected then, we have nothing to prove. Assume, if possible that G is not k-connected. Then, $G = G_1 \cup G_2$ with $|G_1 \cap G_2| < k$ and $|G_1|, |G_2| < n$. Thus, both $G_1 - V(G_2)$ and $G_2 - V(G_1)$ have at least one vertex and there is no edge between them as G is not k-connected. As the degree of these vertices is at least $2k-2$, we have $|G_1|, |G_2| \geq 2k-1$. Further,

$$|G_1| + |G_2| = |G_1 \cup G_2| + |G_1 \cap G_2| \leq n + (k-1) = n + k - 1. \quad (7.3)$$

If G_1 or G_2 satisfies Equation (7.2), using induction hypothesis, the result follows. Otherwise, $\|G_i\| \leq (2k-3)(|G_i| - k + 1)$, for $i = 1, 2$ and hence, using Equation (7.3)

$$m = \|G\| \leq \|G_1\| + \|G_2\| \leq (2k-3)(|G_1| + |G_2| - 2k + 2) \leq (2k-3)(n-k+1),$$

a contradiction to Equation (7.2) and hence the required result follows. ■

Theorem 7.5.13. [**Menger**] *A graph is k-edge-connected if and only if there are k edge disjoint paths between each pairs of vertices. A graph is k-connected if and only if there are k internally vertex disjoint paths between each pairs of vertices.*

Proof. Omitted.

7.6 Eulerian Graphs

Definition 7.6.1. Let G be a graph. Then, G is said to have an **Eulerian tour** if there is a closed walk, say $[v_0, v_1, \ldots, v_k, v_0]$, such that each edge of the graph appears exactly once in the walk. The graph G is said to be **Eulerian** if it has an Eulerian tour.

Note that by definition, a disconnected graph is not Eulerian. In this section, the graphs can have loops and multiple edges. The graphs that have a closed walk traversing each edge exactly once have been named "Eulerian graphs" due to the solution of the famous Königsberg bridge problem by Euler in 1736. The problem is as follows: The city Königsberg (the present day Kaliningrad) is divided into 4 land masses by the river Pregel. These land masses are joined by 7 bridges (see Figure 7.14). The question required one to answer "is there a way to start from a land mass that passes through all the seven bridges in Figure 7.14 and return back to the starting land mass"? Euler, rephrased the problem along the following lines: Let the four land masses be denoted by the vertices A, B, C and D of a graph and let the 7 bridges correspond to 7 edges of the graph. Then, he asked "does this graph have a closed walk that traverses each edge exactly once"? He gave a necessary and sufficient condition for a graph to have such a closed walk and thus giving a negative answer to Königsberg bridge problem.

One can also relate the above problem to the problem of "starting from a certain point, draw a given figure with pencil such that neither the pencil is lifted from the paper nor a line is repeated such that the drawing ends at the initial point".

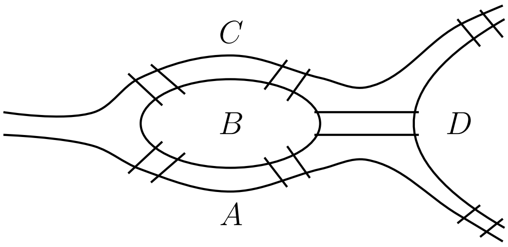


Figure 7.14: Königsberg bridge problem

Theorem 7.6.2. [**Euler,** 1736] *A connected graph G is Eulerian if and only if $d(v)$ is even, for each $v \in V(G)$.*

Proof. Let G have an Eulerian tour, say $W = [v_0, v_1, \ldots, v_k, v_0]$. Observe that whenever we arrive at a vertex v using an edge, say e, in W then we leave that vertex using an edge, say e' in W with $e \neq e'$. As each edge appears exactly once in W and each edge is traversed, $d(v) = 2r$, if $v \neq v_0$ and v appears r times in the tour. Also, $d(v_0) = 2(r-1)$, if v_0 appears r times in the tour. Hence, $d(v)$ is always even.

Conversely, let G be a connected graph with each vertex having even degree. Let $W = v_0 v_1 \cdots v_k$ be a longest walk in G without repeating any edge in it. As v_k has an even degree it follows that $v_k = v_0$, otherwise W can be extended. If W is not an Eulerian tour then there exists an edge, say $e' = v_i w$, with $w \neq v_{i-1}, v_{i+1}$. In this case, $W' = w v_i \cdots v_k (= v_0) v_1 \cdots v_{i-1} v_i$ is a longer walk compared to W, a contradiction. Thus, there is no edge lying outside W and hence W is an Eulerian tour. ■

Proposition 7.6.3. *Let G be a connected graph with exactly two vertices of odd degree. Then, there is an Eulerian walk starting at one of those vertices and ending at the other.*

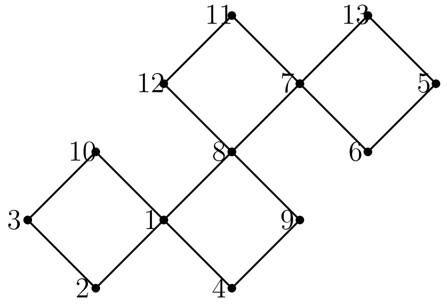
Proof. Let x and y be the two vertices of odd degree and let v be a symbol such that $v \notin V(G)$. Then, the graph H with $V(H) = V(G) \cup \{v\}$ and $E(H) = E(G) \cup \{xv, yv\}$ has each vertex of even degree and hence by Theorem 7.6.2, H is Eulerian. Let $\Gamma = [v, v_1 = x, \ldots, v_k = y, v]$ be an Eulerian tour. Then, $\Gamma - v$ is an Eulerian walk with the required properties. ■

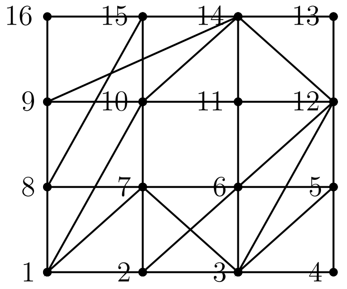
EXERCISE **7.6.4.** *Let G be a connected Eulerian graph and e be any edge. Show that $G - e$ is connected.*

How to find an Eulerian tour (algorithm)?

Start from a vertex v_0, move via edge that has not been taken and go on deleting them. Do not take an edge whose deletion creates a non trivial component not containing v_0.

EXERCISE **7.6.5.** *Find Eulerian tours for the following graphs.*





Theorem 7.6.6. [Finding Eulerian tour] *The previous algorithm correctly gives an Eulerian tour whenever, the given graph is Eulerian.*

Proof. Let the algorithm start at a vertex, say v_0. Now, assume that we are at u with H as the current graph and C as the only non trivial component of H. Thus, $d_H(u) > 0$. Assume that the deletion of the edge uv creates a non trivial component not containing v_0. Let C_u and C_v be the components of $C - uv$, containing u and v, respectively.

We first claim that $u \neq v_0$. In fact, if $u = v_0$, then H must have all vertices of even degree and $d_H(v_0) \geq 2$. So, C is Eulerian. Hence, $C - uv$ cannot be disconnected, a contradiction to $C - uv$ having two components C_u and C_v. Thus, $u \neq v_0$. Moreover, note that the only vertices of odd degree in C is u and v_0.

Now, we claim that C_u is a non trivial component. Suppose C_u is trivial. Then, $v_0 \in C_v$, a contradiction to the assumption that the deletion of the edge uv creates a nontrivial component not containing v_0. So, C_u is non trivial.

Finally, we claim that $v_0 \in C_v$. If possible, let $v_0 \in C_u$. Then, the only vertices in $C - uv$ of odd degree are $v \in C_v$ and $v_0 \in C_u$. Hence, $C - uv + v_0v$ is a connected graph with each vertex of even degree. So, by Theorem 7.6.2, the graph $C - uv + v_0v$ is Eulerian. But, this cannot be true as vv_0 is a bridge. Thus, $v_0 \in C_v$.

Hence, C_u is the newly created non trivial component not containing v_0. Also, each vertex of C_u has even degree and hence by Theorem 7.6.2, C_u is Eulerian. This means, we can take an edge e' incident on u and complete an Eulerian tour in C_u. So, at u if we take the edge e' in place of the edge e, then we will not create a non trivial component not containing v_0.

Thus, at each stage of the algorithm either $u = v_0$ or there is a path from u to v_0. Moreover, this is the only non trivial connected component. When the algorithm ends, we must have $u = v_0$. Because, as seen above, the condition $u \neq v_0$ gives the existence of an edge that is incident on u and that can be traversed (as $d_H(u)$ is odd). Hence, if $u \neq v_0$, the algorithm cannot stop. Thus, when algorithm stops $u = v_0$ and all components are trivial. ■

EXERCISE **7.6.7.** *Apply the algorithm to graphs of Exercise 7.6.5. Also, create connected graphs such that each of its vertex has even degree and apply the above algorithm.*

EXERCISE **7.6.8.** *1. Give a necessary and sufficient condition on m and n so that $K_{m,n}$ is Eulerian.*

2. Each of the 8 persons in a room has to shake hands with every other person as per the following rules:

(a) The handshakes should take place sequentially.

(b) Each handshake (except the first) should involve someone from the previous handshake.

(c) No person should be involved in 3 consecutive handshakes.

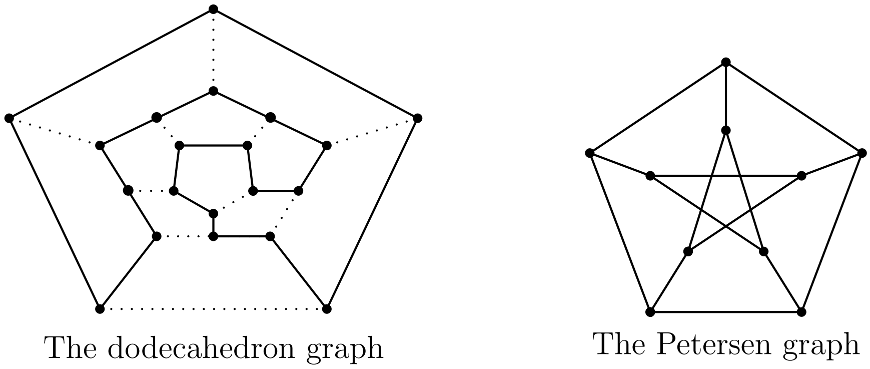
Is there a way to sequence the handshakes so that these conditions are all met?

3. *Let G be a connected graph. Then, G is an Eulerian graph if and only if the edge set of G can be partitioned into cycles.*

7.7 Hamiltonian Graphs

Definition 7.7.1. A cycle in G is said to be **Hamiltonian** if it contains all vertices of G. If G has a Hamiltonian cycle, then G is called a **Hamiltonian** graph. Finding a nice characterization of a Hamiltonian graph is an unsolved problem.

Example 7.7.2. 1. For each positive integer $n \geq 3$, the cycle C_n is Hamiltonian.



The dodecahedron graph

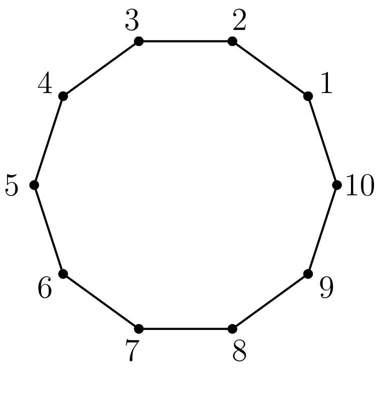
The Petersen graph

Figure 7.15: A Hamiltonian and a non-Hamiltonian graph

2. The graphs corresponding to all platonic solids are Hamiltonian.
3. The Petersen graph is a non-Hamiltonian Graph (the proof appears below).

Proposition 7.7.3. *The Petersen graph is not Hamiltonian.*

Proof. Suppose that the Petersen graph, say G, is Hamiltonian. So, G contains $C_{10} = [1, 2, 3, \ldots, 10, 1]$ as a subgraph. As each vertex of G has degree 3, $G = C_{10} + M$, where M is a set of 5 chords in which each vertex appears as an endpoint. Now, consider the vertices 1, 2 and 3.



Since, $g(G) = 5$, the vertex 1 can be adjacent to only one of the vertices $5, 6$ or 7. Hence, if 1 is adjacent to 5, then the possible third vertex that is adjacent to 10 will create cycles of length 3 or 4. Similarly, if 1 is adjacent to 7, then there is no choice for the possible third vertex that can be adjacent to 2. So, let 1 be adjacent to 6. Then, 2 must be adjacent to 8. In this case, note that there is no choice for the third vertex that can be adjacent to 3. Thus, the Petersen graph is non-Hamiltonian. ∎

Theorem 7.7.4. *Let G be a Hamiltonian graph. Then, for $S \subseteq V(G)$ with $S \neq \emptyset$, the graph $G - S$ has at most $|S|$ components.*

Proof. Note that by removing k vertices from a cycle, one can create at most k connected components. Hence, the required result follows. ■

Theorem 7.7.5. [**Dirac,** 1952] *Let G be a graph with $|G| = n \geq 3$ and $d(v) \geq n/2$, for each $v \in V(G)$. Then, G is Hamiltonian.*

Proof. Let is possible, G be disconnected. Then, G has a component, say H, with $|V(H)| = k \leq n/2$. Hence, $d(v) \leq k - 1 < n/2$, for each $v \in V(H)$. A contradiction to $d(v) \geq n/2$, for each $v \in V(G)$. Now, let $P = [v_1, v_2, \cdots, v_k]$ be a longest path in G. Since P is the longest path, all neighbors of v_1 and v_k are in P and $k \leq n$.

We claim that there exists an i such that $v_1 \sim v_i$ and $v_{i-1} \sim v_k$. Otherwise, for each $v_i \sim v_1$, we must have $v_{i-1} \nsim v_k$. Then, $|N(v_k)| \leq k - 1 - |N(v_1)|$. Hence, $|N(v_1)| + |N(v_k)| \leq k - 1 < n$, a contradiction to $d(v) \geq n/2$, for each $v \in V(G)$. So, the claim is valid and hence, we have a cycle $\tilde{P} := v_1 v_i v_{i+1} \cdots v_k v_{i-1} \cdots v_1$ of length k.

We now prove that $\tilde{P}$ gives a Hamiltonian cycle. Suppose not. Then, there exists $v \in V(G)$ such that v is outside P and v is adjacent to some v_j. Now, use $\tilde{P}, v$ and v_j to create a path whose length is larger than the length of P. Hence, P cannot be the path of longest length, a contradiction. Thus, the required result follows. ■

Theorem 7.7.6. [**Ore,** 1960] *Let G be a graph on $n \geq 3$ vertices such that $d(u) + d(v) \geq n$, for every pair of nonadjacent vertices u and v. Then, G is Hamiltonian.*

Proof. Exercise.

Exercise **7.7.7.** *Let u and v be two vertices such that $d(u) + d(v) \geq |G|$, whenever $uv \notin E(G)$. Prove that G is Hamiltonian if and only if $G + uv$ is Hamiltonian.*

Definition 7.7.8. The **closure** of a graph G, denoted $C(G)$, is obtained by repeatedly choosing pairs of nonadjacent vertices u, v such that $d(u) + d(v) \geq n$ and adding edges between them.

Proposition 7.7.9. *The closure of G is unique.*

Proof. Let K be a closure obtained by adding edges $e_1 = u_1v_1, \ldots, e_k = u_kv_k$ sequentially and F be a closure obtained by adding edges $f_1 = x_1y_1, \ldots, f_r = x_ry_r$ sequentially. Let e_i be the first edge in the e-sequence which does not appear in the f-sequence. Put $H = G + e_1 + \cdots + e_{i-1}$. Then, $e_i = u_iv_i$ implies that $e_i \notin E(H)$ and $d_H(u_i) + d_H(v_i) \geq n$. Also, H is a subgraph of F and hence, $d_F(u_i) + d_F(v_i) \geq n$. Moreover, $e_i = u_iv_i \notin F$ as e_i does not appear in the f-sequence. Thus, F cannot be a closure and therefore the required result follows. ■

Exercise **7.7.10.** *Let G be a graph on $n \geq 3$ vertices.*

1. *If G has a cut vertex, then prove that $C(G) \neq K_n$.*
2. *Now prove a generalization of Dirac's theorem: If the closure $C(G) \cong K_n$, then G is Hamiltonian.*

Theorem 7.7.11. *Let $d_1 \leq \cdots \leq d_n$ be the vertex degrees of G. Suppose that, for each $k < n/2$ with $d_k \leq k$, the condition $d_{n-k} \geq n - k$ holds. Then, prove that G is Hamiltonian.*

Proof. We show that under the above condition $H = C(G) \cong K_n$. On the contrary, assume that there exists a pair of vertices $u, v \in V(G)$ such that $uv \notin E(H)$ and $d_H(u) + d_H(v) \leq n - 1$. Among all such pairs, choose a pair $u, v \in V(G)$ such that $uv \notin E(H)$ and $d_H(u) + d_H(v)$ is maximum. Assume that $d_H(v) \geq d_H(u) = k$ (say). As $d_H(u) + d_H(v) \leq n - 1$, $k < n/2$.

Now, let $S_v = \{x \in V(H) \mid x \neq v, xv \notin E(H)\}$ and $S_u = \{w \in V(H) \mid w \neq u, wu \notin E(H)\}$. Therefore, the assumption that $d_H(u) + d_H(v)$ is the maximum among each pair of vertices u, v with

$uv \notin E(H)$ and $d_H(u) + d_H(v) \le n-1$ implies that $|S_v| = n-1-d_H(v) \ge d_H(u) = k$ and $d_H(x) \le d_H(u) = k$, for each $x \in S_v$. So, there are at least k vertices in H (elements of S_v) with degrees at most k.

Also, for any $w \in S_u$, note that the choice of the pair u, v implies that $d_H(w) \le d_H(v) \le n-1-d_H(u) = n-1-k < n-k$. As $d_H(u) = k$, $|S_u| = n-1-k$. Further, the condition $d_H(u)+d_H(v) \le n-1$, $d_H(v) \ge d_H(u) = k$ and $u \notin S_u$ implies that $d_H(u) \le n-1-d_H(v) \le n-1-k < n-k$. So, there are $n-k$ vertices in H with degrees less than $n-k$.

Therefore, if $d'_1 \le \cdots \le d'_n$ are the vertex degrees of H, then we observe that there exists a $k < n/2$ for which $d'_k \le k$ and $d'_{n-k} < n-k$. As $k < n/2$ and $d_i \le d'_i$, we get a contradiction to the given hypothesis. ■

EXERCISE **7.7.12.** *Complete an alternate proof of Theorem 7.7.11. Let R denote the property:*

R : 'If $d_k \le k$ then $d_{n-k} \ge n-k$, for each $k < n/2$'.

We know that G has this property.

1. *Let e be an edge not in G. Show that $G+e$ also has the property. What about the closure $H := C(G)$ of G?*
2. *Assume that $\max\{d(u)+d(v) : u, v \in H$ are not adjacent$\} \le n-2$. Let e be an edge not in H. Does $H+e$ have property R? Is $C(H+e) = H+e$?*
3. *In view of the previous observations assume that G is an edge maximal graph with property R which is not Hamiltonian. Do you have $C(G) = G$? Show that there are some k vertices having degree at most k and some $n-k$ vertices having degree less than $n-k$. Does that contradict R?*

Definition 7.7.13. The **line graph** H of a graph G is a graph with $V(H) = E(G)$ and $e_1, e_2 \in V(H)$ are adjacent in H if e_1 and e_2 share a common vertex/endpoint.

Example 7.7.14. Verify the following:

1. Line graph of C_5 is C_5.
2. Line graph of P_5 is P_4.
3. Line graph of any graph G contains a complete subgraph of size $\Delta(G)$.

EXERCISE **7.7.15.** 1. *Let G be a connected Eulerian graph. Then, show that the line graph of G is Hamiltonian. Is the converse true?*

2. *What can you say about the clique number of a line graph?*

Theorem 7.7.16. *A connected graph G is isomorphic to it's line graph if and only if $G = C_n$, for some $n \ge 3$.*

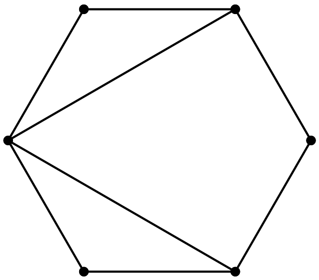
Proof. If G is isomorphic to its line graph, then $|G| = \|G\|$. Thus, G is a unicyclic graph. Let $[v_1, v_2, \ldots, v_k, v_{k+1} = v_1]$ form the cycle in G. Then, the line graph of G contains a cycle $P = [v_1v_2, v_2v_3, \ldots, v_kv_1]$. We now claim that $d_G(v_i) = 2$.

Suppose not and let $d_G(v_1) \ge 3$. So, there exists a vertex $u \notin \{v_2, \ldots, v_k\}$ such that $u \sim v_1$. In that case, the line graph of G contains the triangle $T = [v_1v_2, v_1v_k, v_1u]$ and $P \ne T$. Thus, the line graph is not unicyclic, a contradiction. ■

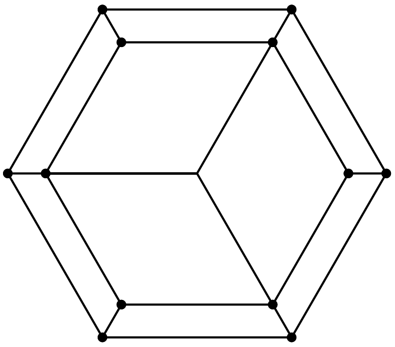
EXERCISE **7.7.17.** *Consider the graphs shown below.*

1. *Determine the closure of G.*

2. *Show that H is not Hamiltonian.*



G



H

3. *Give a necessary and sufficient condition on $m, n \in \mathbf{N}$ so that $K_{m,n}$ is Hamiltonian.*

4. *Show that any graph G with $|G| \geq 3$ and $\|G\| \geq C(n-1, 2) + 2$ is Hamiltonian.*

5. *Show that for any $n \geq 3$ there is a graph H with $\|G\| = C(n-1, 2) + 1$ that is not Hamiltonian. But, prove that all such graphs H admit a Hamiltonian path (a path containing all vertices of H).*

7.8 Bipartite Graphs

Definition 7.8.1. A graph is said to be **2-colorable** if it's vertices can be colored with two colors in a way that adjacent vertices get different colors.

Lemma 7.8.2. *Let P and Q be two v-w-paths in G such that length of P is odd and length of Q is even. Then, G contains an odd cycle.*

Proof. If P, Q have no inner vertex (a vertex other than v, w) in common then $P \cup Q$ is an odd cycle in G.

So, suppose P, Q have an inner vertex in common. Let x be the first common inner vertex when we walk from v to w. Then, one of $P(v, x), P(x, w)$ has odd length and the other is even. Let $P(v, x)$ be odd. If length of $Q(v, x)$ is even then $P(v, x) \cup P(x, v)$ is an odd cycle in G. If length of $Q(v, x)$ is odd then the length of $Q(x, w)$ is also odd and hence we can consider the x-w-paths $P(x, w)$ and $Q(x, w)$ and proceed as above to get the required result. ■

Theorem 7.8.3. *Let G be a connected graph with at least two vertices. Then, the following statements are equivalent.*

1. *G is 2-colorable.*

2. *G is bipartite.*

3. *G does not have an odd cycle.*

Proof. Part 1 ⇒ Part 2. Let G be 2-colorable. Let V_1 be the set of red vertices and V_2 be the set of blue vertices. Clearly, G is bipartite with partition V_1, V_2.

Part 2 ⇒ Part 1. Color the vertices in V_1 with red color and that of V_2 with blue color to get the required 2 colorability of G.

Part 2 ⇒ Part 3. Let G be bipartite with partition V_1, V_2. Let $v_0 \in V_1$ and suppose $\Gamma = v_0 v_1 v_2 \cdots v_k = v_0$ is a cycle. It follows that $v_1, v_3, v_5 \cdots \in V_2$. Since, $v_k \in V_1$, we see that k is even. Thus, Γ has an even length.

Part 3 ⇒ Part 2. Suppose that G does not have an odd cycle. Pick any vertex v. Define $V_1 = \{w \mid$ there is a walk of even length from v to $w\}$ and $V_2 = \{w \mid$ there is a walk of odd length from v to $w\}$. Clearly, $v \in V_1$. Also, G does not have an odd cycle implies that $V_1 \cap V_2 = \emptyset$ (use Lemma 7.8.2. As G is connected each w is either in V_1 or in V_2.

Let $x \in V_1$. Then, there is an even path $P(v, x)$ from v to x. If $xy \in E(G)$, then we have a v-y-walk of odd length. Deleting all cycles from this walk, we have an odd v-y-path. Thus, $y \in V_2$. Similarly, if $x \in V_2$ and $xy \in E$, then $y \in V_1$. Thus, G is bipartite with parts V_1, V_2. ■

Exercise **7.8.4.** *1. There are 15 women and some men in a room. Each man shook hands with exactly 6 women and each woman shook hands with exactly 8 men. How many men are there in the room?*

2. How do you test whether a graph is bipartite or not?

3. Prove that every tree is a bipartite graph.

4. Prove that the Petersen graph is not bipartite.

5. Let G and H be two bipartite graphs. Prove that $G \times H$ is also a bipartite graph.

7.9 Matching in Graphs

Definition 7.9.1. A **matching** in a graph G is an independent set of edges. A **maximum matching** is a matching with maximum number of edges. A vertex v is **saturated by a matching** M if there is an edge $e \in M$ incident on v. A matching is a **perfect matching** if every vertex is saturated.

Example 7.9.2. 1. In Figure 7.16, $M_1 = \{u_1u_2\}$ is a matching. So, is $M_2 = \{e\}$, where e is any edge. The set $M_3 = \{u_3u_2, u_4u_7\}$ is also a matching. The set $M_4 = \{u_1u_2, u_4u_5, u_6u_7\}$ is also a matching and it is maximum (why?). Can you give another maximum matching?

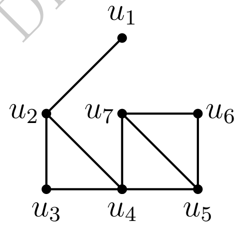


Figure 7.16: A graph

2. Any non trivial graph G has a maximum matching.
3. Vertices that are saturated for M_3 are $\{u_2, u_3, u_4, u_7\}$.
4. Any graph with a perfect matching must have even order as each edge saturates two vertices. The Figure 7.16 cannot have a perfect matching.

Definition 7.9.3. Let M be a matching in G. A path P is called M**-alternating** if its edges are alternately from M and from $G - M$. An M-alternating path with two unmatched vertices as end points (of the alternating path) is called M**-augmenting**. Convention: Each path of length 1 in M is M-alternating.

Example 7.9.4. Consider Figure 7.16 and Example 7.9.2.

1. The path $[u_1, u_2]$ is M_1-alternating. The only path of length 2 which is M_1-alternating is $[u_1, u_2, u_3]$.
2. The path $[u_1, u_2, u_4, u_7]$ is not M_3-alternating. But, $[u_2, u_3, u_4, u_7]$ is M_3-alternating.

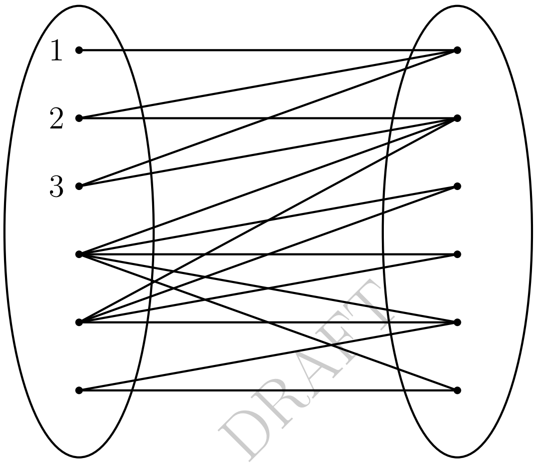
3. The path $P = [u_1, u_2, u_3, u_4, u_7, u_6]$ is M_3-alternating and M_3-augmenting. This gives us a way to get a larger (in size) matching M_5 using M_3: throw away the even edges of P from M_3 and add the odd edges; *i.e.*, $M_5 = M_3 - \{u_2u_3, u_4u_7\} + \{u_1u_2, u_3u_4, u_7u_6\}$.

Theorem 7.9.5. [**Berge,** 1957] *A matching M is maximum if and only if there is no M-augmenting path in G.*

Proof. Let $M = \{u_1v_1, \ldots, u_kv_k\}$ be a maximum matching. If there is an M-augmenting path P, then $(P \setminus M) \cup (M \setminus P)$ is a larger matching, a contradiction. Conversely, suppose that M is not maximum. Let M^* be a maximum matching. Consider the graph $H = (V, M \cup M^*)$. Note that $d_H(v) \leq 2$, for each vertex in H. Thus, H is a collection of isolated vertices, paths and cycles. Since a cycle contains equal number of edges of M and M^*, there is a path P which contains more number of edges of M^* than that of M. Then, P is an M-augmenting path. A contradiction. ■

Exercise **7.9.6.** *How do we find a maximum matching in a graph G.*

Example 7.9.7. Can we find a matching that saturates all vertices in the graph given below?



Ans: No. Let X be the given graph and take $S = \{1, 2, 3\}$. If there is a matching that saturates S then $|N(S)| \geq |S|$. But this is not the case with this graph.

Question: What if $|N(S)|$ were at least $|S|$, for each $S \subseteq X$?

Theorem 7.9.8. [**Hall,** 1935] *Let $G = (X \cup Y, E)$ be a bipartite graph. Then, there is a matching that saturates all vertices in X if and only if for all $S \subseteq X$, $|N(S)| \geq |S|$.*

Proof. If there is such a matching, then obviously $|S| \leq |N(S)|$, for each subset S of X. Conversely, suppose that $|N(S)| \geq |S|$, for each $S \subseteq X$. Let if possible, M^* be a maximum matching that does not saturate $x \in X$.

As $|N(\{x\})| \geq |\{x\}|$, there is a $y \in Y$ such that $xy \notin M^*$. Since M^* cannot be extended, y must have been matched to some $x_1 \in X$.

Now consider $N(\{x, x_1\})$. It has a vertex y_1 which is adjacent to either x or x_1 or both by an edge not in M^*. Again the condition that M^* cannot be extended implies that y_1 must have been matched to some $x_2 \in X$. Continuing as above, we see that this process never stops and thus, G has infinitely many vertices, which is not true. Hence, M^* saturates each $x \in X$. ■

Corollary 7.9.9. *Let G be a k-regular ($k \geq 1$) bipartite graph. Then, G has a perfect matching.*

Proof. Let X and Y be the two parts. Since G is k-regular $|X| = |Y|$. Let $S \subseteq X$ and E be the set of edges with an end vertex in S. Then $k|S| = |E| \leq \sum\limits_{v \in N(S)} d(v) = k|N(S)|$. Hence, we see that for each $S \subseteq X$, $|S| \leq |N(S)|$ and thus, by Hall's theorem the required result follows. ■

Definition 7.9.10. Let G be a graph. Then, $S \subseteq V(G)$ is called a **covering** of G if each edge has at least one end vertex in S. A **minimum covering** of G is a covering of G that has minimum cardinality.

Exercise **7.9.11.** *1. Show that for any graph G the size of a minimum covering is $n - \alpha(G)$.*

2. Characterize G in terms of it's girth if the size of a minimum covering is $|G| - 2$.

Proposition 7.9.12. *Let G be a graph. If M is a matching and K is a covering of G, then $|M| \leq |K|$. If $|M| = |K|$, then M is a maximum matching and K is a minimum covering.*

Proof. By definition, the proof of the first statement is trivial. To prove the second statement, suppose that $|M| = |K|$ and M is not a maximum matching. Let M^* be a matching of G with $|M^*| \geq |M|$. Then, using the first statement, we have $|K| \geq |M^*|$. Hence, $|K| \geq |M^*| > |M| = |K|$. Thus, M is maximum. As each covering must have at least $|M|$ elements, we see that K is a minimum covering.■

Exercise **7.9.13.** *Let $G = K_n$, $n \geq 3$. Then, determine*

1. the cardinality of a maximum matching?

2. the cardinality of a minimum covering?

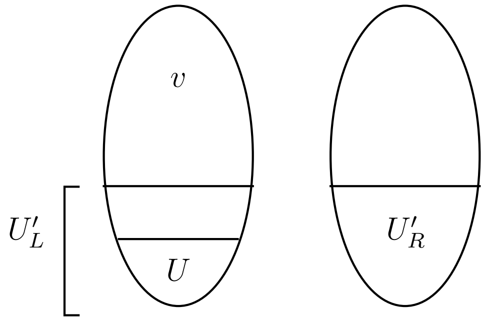
Is the converse of Proposition 7.9.12 necessarily true? Can you guess the class of graphs for which the converse of Proposition 7.9.12 is true?

Theorem 7.9.14. **[Konig,** 1931] *Let M be a maximum matching in a bipartite graph G and let K be a minimum covering. Then, $|M| = |K|$.*

Proof. Let $V = X \cup Y$ be the bipartition of V and let M be a maximum matching. Let U be the vertices in X that are not saturated by M and let Z be the set of vertices reachable from U by an M-alternating path.

Put $S = Z \cap X$, $T = Z \cap Y$ and $K = T \cup (X \setminus S)$. Then, $U \subseteq Z \subseteq X \cup Y$ and every element of $X \setminus S$ is saturated. Also, every vertex in T is saturated by M (as M is a maximum matching) and $N(S) = T$ (else there will be M-augmenting path starting from $u \in U$). Further, a vertex $v \in X \setminus S$ is matched to some vertex $y \notin T$. Thus, $|K| = |T \cup (X \setminus S)| \leq |M|$. If K is not a covering, then there is an edge $xy \in G$ with $x \in S$ and $y \notin T$, a contradiction to $N(S) = T$. Thus, K is a covering and hence, using $|K| \leq |M|$ and Proposition 7.9.12, we get $|K| = |M|$. Furthermore, by Proposition 7.9.12, we also see that K is a minimum covering. ■

Alternate proof: Let (L, R) (L for left and R for right) be the bipartition of V and let M be a maximum matching. Let U be the set of unmatched vertices on the left.



Let U' be the set of vertices reachable from U by alternating paths (with respect to M). Then U' has two parts : one one the left, say U'_L and the other on the right, say U'_R. Note that the vertices of U are reachable from themselves. Hence, we have $U \subseteq U'_L$. We have a few observations.

a) If $v \in L$ is a left vertex not in U_L', then it is not in U, and so it must be matched to some right vertex, say w. Can $w \in U_R'$? No. Because, if $w \in U_R'$, then we have an alternating path from u to w and as $[w, u]$ is a matching edge, we see that v is reachable from u by an alternating path. Then v should have been in U_L', a contradiction. Thus every vertex from $L \setminus U_L'$ is matched to a vertex in $R \setminus U_R'$.

b) Is every vertex in U_R' matched (saturated)? Yes. To see it, suppose that $w \in U_R'$ is not matched. As $w \in U_R'$, it must be reachable from a vertex $u \in U$ via an alternating path. But, this alternating path is an augmenting path. This means M is not a maximum matching, a contradiction.

c) The above two points imply that $|M| = |L \setminus U_L'| + |U_R'|$.

d) Is there any edge from a vertex in U_L' to a vertex in $R \setminus U_R'$? No. To see this note that, each vertex in $U_L' \setminus U$ is reached from some vertex of U via an alternating path and the last edge of this path must be a matching edge. Thus, each vertex in $U_L' \setminus U$ is matched to some vertex in U_R'. This means, if there an edge from a vertex in U_L' to a vertex in $w \in R \setminus U_R'$, it must be a nonmatching edge. But then, this makes w reachable from U via an alternating path. So w should have been in U_R', a contradiction.

e) The previous point means that $(L \setminus U_L') \cup U_R'$ is covering. This is a minimum covering, as any covering must contain at least $|M|$ many vertices by Proposition 7.9.12. ∎

EXERCISE **7.9.15.** *How many perfect matchings are there in a labeled K_{2n}?*

7.10 Ramsey Numbers

Recall that in any group of 6 or more persons either we see 3 mutual friends or we see 3 mutual strangers. Expressed using graphs it reads 'let $G = (V, E)$ be a graph with $|V| \geq 6$. Then, either $K_3 \subseteq G$ or $\overline{K}_3 \subseteq G$.'

Definition 7.10.1. The **Ramsey number** $r(m, n)$ is the smallest natural number k such that any graph G on k vertices either has a K_m or a $\overline{K}_n$ as it's subgraph.

Example 7.10.2. As C_5 does not have K_3 or $\overline{K}_3$ as it's subgraph, $r(3, 3) > 5$. But, using the first paragraph of this section, we get $r(3, 3) \leq 6$ and hence, $r(3, 3) = 6$. It is known that $r(3, 4) = 9$ (see the text by Harary for a table).

Proposition 7.10.3. *Let G be a graph on 9 vertices. Then, either $K_4 \subseteq G$ or $\overline{K}_3 \subseteq G$.*

Proof. Assume that $|V| = 9$. Then, we need to consider three cases.

Case I. There is a vertex a with $d(v) \leq 4$. Then, $|N(a)'| = |V \setminus N(a)| \geq 4$. If all vertices in $N(a)'$ are pairwise adjacent, then $K_4 \subseteq G$. Otherwise, there are two nonadjacent vertices, say $b, c \in N(a)'$. In that case a, b, c induces the graph $\overline{K}_3$.

Case II. There is a vertex a with $d(a) \geq 6$. If $\langle N(a) \rangle$ has a $\overline{K}_3$, we are done. Otherwise, $r(3, 3) = 6$ implies that $\langle N(a) \rangle$ has a K_3 with vertices, say, b, c, d. In that case a, b, c, d induces the graph K_4.

Case III. Each vertex has degree 5. This case is not possible as $\sum d(v)$ should be even. ∎

EXERCISE **7.10.4.** *Can you draw a graph on 8 vertices*

1. *which does not have $K_3, \overline{K}_4$ in it?*
2. *which does not have $K_4, \overline{K}_3$ in it?*
3. *Consider the graph $C_8 = [1, 2, \ldots, 8, 1]$ with 10 extra edges $13, 14, 17, 26, 27, 35, 36, 48, 57, 58$. Does this graph has a K_4 or the complement of C_3?*

Theorem 7.10.5. [**Erdos & Szekeres,** 1935] *Let $m, n \in \mathbb{N}$. Then,*

$$r(m,n) \leq r(m-1,n) + r(m,n-1).$$

Proof. Let $p = r(m-1,n)$ and $q = r(m,n-1)$. Now, take any graph G on $p+q$ vertices and take a vertex a. If $d(a) \geq p$, then $\langle N(a) \rangle$ has either a subgraph K_{m-1} (and K_{m-1} together with a gives K_m) or a subgraph $\overline{K_n}$. Otherwise, $|N(a)'| \geq q$. In this case, $\langle N(a)' \rangle$ has either a subgraph K_m or a subgraph $\overline{K}_{n-1}$ ($\overline{K}_{n-1}$ together with a gives $\overline{K}_n$). ■

7.11 Degree Sequence

Definition 7.11.1. The **degree sequence** of a graph of order n is the tuple $(d_1, \ldots, d_n)$ where $d_1 \leq \cdots \leq d_n$. A non-decreasing sequence $d = (d_1, \ldots, d_n)$ of non-negative integers is **graphic** if there is a graph whose degree sequence is d.

Exercise **7.11.2.** *Show that* $(1,1,3,3)$ *is not graphic.*

Theorem 7.11.3. *Fix $n \geq 1$ and the natural numbers $d_1 \leq \cdots \leq d_n$. Then, $d = (d_1, \ldots, d_n)$ is the degree sequence of a tree on n vertices if and only if $\sum d_i = 2n-2$.*

Proof. If $d = (d_1, \ldots, d_n)$ is the degree sequence of a tree on n vertices then $\sum d_i = 2|E(T)| = 2(n-1) = 2n-2$.

Conversely, let $d_1 \leq \cdots \leq d_n$ be a sequence of natural numbers with $\sum d_i = 2n-2$. We use induction to show that $d = (d_1, \ldots, d_n)$ is the degree sequence of a tree on n vertices. For $n = 1, 2$, the result is trivial. Let the result be true for all $n < k$ and let $d_1 \leq \cdots \leq d_k, k > 2$, be natural numbers with $\sum d_i = 2k-2$. Since, $\sum d_i = 2k-2$, we must have $d_1 = 1$ and $d_k > 1$. Then, we note that $d_2' = d_2, \cdots, d_{k-1}' = d_{k-1}$ and $d_k' = d_k - 1$ are natural numbers such that $\sum d_i' = 2(k-1)-2$. Hence, by induction hypothesis, there is a tree T' on vertices $2, \cdots, k-1, k$ with degrees d_i''s. Now, introduce a new vertex 1 and add the edge $\{1, k\}$ to get a tree T that has the required degree sequence. ■

Theorem 7.11.4. [**Havel-Hakimi,** 1962] *The degree sequence $d = (d_1, \ldots, d_n)$ is graphic if and only if the sequence $d_1, d_2, \ldots, d_{n-d_n-1}, d_{n-d_n} - 1, \ldots, d_{n-1} - 1$ is graphic.*

Proof. If the later sequence is graphic then we introduce a new vertex and make it adjacent to the vertices whose degrees are $d_{n-d_n} - 1, \ldots, d_{n-1} - 1$. Hence, the sequence $d = (d_1, \ldots, d_n)$ is graphic.

Now, assume that d is graphic and G is a graph with degree sequence d. Let $d_n = k$ and let $N_G(n) = \{i_1, i_2, \ldots, i_k\}$ with $d_{i_1} \leq d_{i_2} \leq \cdots \leq d_{i_k}$. If $d_{i_1} \geq d_v$ for all $v \in V(G) \setminus N_G(n)$ then $\{d_{i_1}, d_{i_2}, \ldots, d_{i_k}\} = \{d_{n-d_n}, d_{n-d_n+1}, \ldots, d_{n-1}\}$ and hence $G - n$ is the required graph.

If $d_{i_1} < d_{v_0}$ for some $v_0 \in V(G) \setminus N_G(n)$ then, we construct another graph, say G', such that G and G' have the same degree sequence but

$$\sum_{v \in N_{G'}(n)} d_v \geq \sum_{u \in N_G(n)} d_u. \tag{7.4}$$

As, $v_0 \not\sim n$, the vertex v_0 has a neighbor $v \neq i_1$ with $v \not\sim i_1$. Now, consider the graph $G' = G - \{v_0, v\} + \{n, v_0\} + \{i_1, v\} - \{i_1, n\}$. Then, G' also has d as it's degree sequence with $N_{G'}(n) = \{v_0, i_2, \ldots, i_k\}$. Thus, we see that Equation (7.4) holds. This process will end after a finite number of steps by producing a graph in which the vertex n has degree d_n and has neighbors with degrees $d_{n-d_n}, d_{n-d_n+1}, \ldots, d_{n-1}$ and hence the required result follows. ■

Exercise **7.11.5.**

1. *How many different degree sequences are possible on a graph with* 5 *vertices? List all the degree sequences and draw a graph for each one. (Include connected and disconnected graphs.)*

2. *Which of the sequences below are graphic? Draw the graph or supply an argument.*
   (a) $(2, 2, 3, 4, 4, 5)$
   (b) $(1, 2, 2, 3, 3, 4)$
   (c) $(2^2, 3^6, 4^2) = (2, 2, 3, 3, 3, 3, 3, 3, 4, 4)$
3. *If two graphs have the same degree sequence, are they necessarily isomorphic?*
4. *If two graphs are isomorphic, is it necessary that they have the same degree sequence?*

7.12 Planar Graphs

Definition 7.12.1. A graph is said to be **embedded** on a surface S when it is drawn on S so that no two edges intersect. A graph is said to be **planar** if it can be embedded on the plane. A **plane graph** is a graph which can be embedded on the plane.

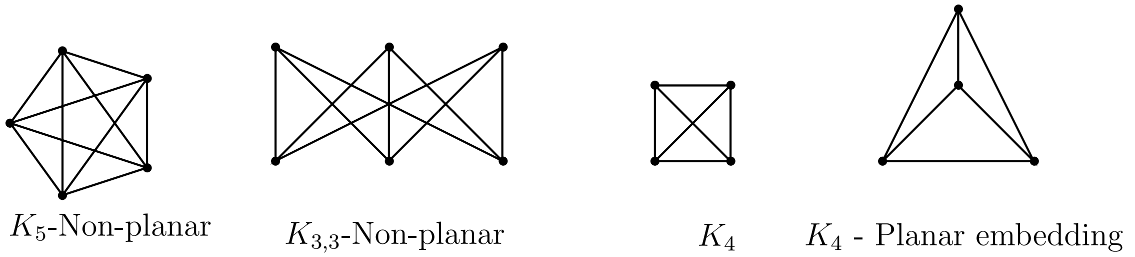


Figure 7.17: Planar and non-planar graphs

Example 7.12.2. 1. A tree is embeddable on a plane and when it is embedded we have only one face, the exterior face.

2. Any cycle C_n, $n \geq 3$ is planar and any plane representation of C_n has two faces.
3. The planar embedding of K_4 is given in Figure 7.17.
4. Draw a planar embedding of $K_{2,3}$.
5. Draw a planar embedding of the three dimensional cube.
6. Draw a planar embedding of $K_5 - e$, where e is any edge.
7. Draw a planar embedding of $K_{3,3} - e$, where e is any edge.

Definition 7.12.3. Consider a planar embedding of a graph G. The regions on the plane defined by this embedding are called **faces/regions** of G. The unbounded face/region is called the exterior face (see Figure 7.18).

Example 7.12.4. Consider the following planar embedding of the graphs X_1 and X_2.

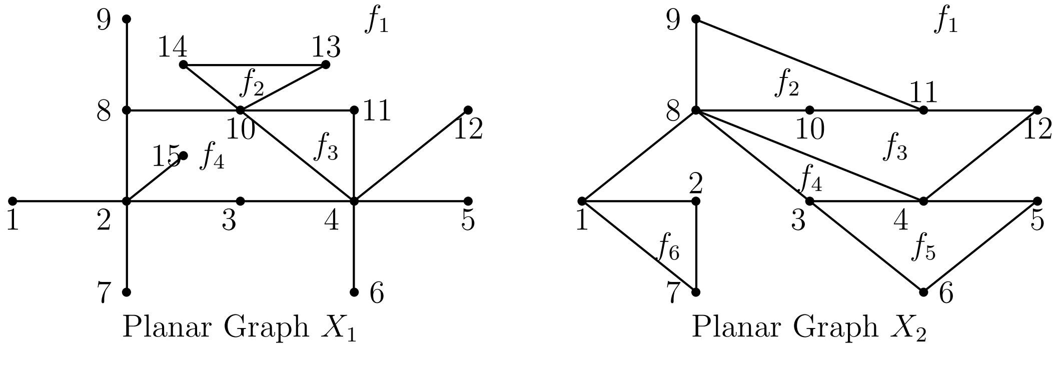


Figure 7.18: Planar graphs with labeled faces to understand the Euler's theorem

1. The faces of the planar graph X_1 and their corresponding edges are listed below.

Face	Corresponding Edges
f_1	$\{9,8\},\{8,9\},\{8,2\},\{2,1\},\{1,2\},\{2,7\},\{7,2\},\{2,3\},\{3,4\},\{4,6\},\{6,4\},\{4,5\},$ $\{5,4\},\{4,12\},\{12,4\},\{4,11\},\{11,10\},\{10,13\},\{13,14\},\{14,10\},\{10,8\},\{8,9\}$
f_2	$\{10,13\},\{13,14\},\{14,10\}$
f_3	$\{4,11\},\{11,10\},\{10,4\}$
f_4	$\{2,3\},\{3,4\},\{4,10\},\{10,8\},\{8,2\},\{2,15\},\{15,2\}$

2. Determine the faces of the planar graph X_2 and their corresponding edges.

From the table, we observe that each edge of X_1 appears in two faces. This can be easily observed for the faces that don't have pendant vertices (see the faces f_2 and f_3). In faces f_1 and f_4, there are a few edges which are incident with a pendant vertex. Observe that the edges that are incident with a pendant vertex, *e.g.*, the edges $\{2,15\},\{8,9\}$ and $\{1,2\}$ etc., appear twice when traversing a particular face. This observation leads to the proof of Euler's theorem for planar graphs which is the next result.

Theorem 7.12.5. **[Euler formula]** *Let G be a connected plane graph with f as the number of faces. Then,*

$$|G| - \|G\| + f = 2. \tag{7.5}$$

Proof. We use induction on f. Let $f = 1$. Then, G cannot have a subgraph isomorphic to a cycle. For if, G has a subgraph isomorphic to a cycle then in any planar embedding of G, $f \geq 2$. Therefore, G is a tree and hence $|G| - \|G\| + f = n - (n-1) + 1 = 2$.

So, assume that Equation (7.5) is true for all plane connected graphs having $2 \leq f < n$ and let G be a connected planar graph with $f = n$. Now, choose an edge that is not a cut-edge, say e. Then, $G - e$ is still a connected graph. Also, the edge e is incident with two separate faces and hence it's removal will combine the two faces and thus $G - e$ has only $n - 1$ faces. Thus,

$$|G| - \|G\| + f = |G-e| - (\|G-e\| + 1) + n = |G-e| - \|G-e\| + (n-1) = 2$$

using the induction hypothesis. Hence, the required result follows. ∎

Lemma 7.12.6. *Let G be a plane bridgeless graph with $\|G\| \geq 2$. Then, $2\|G\| \geq 3f$. Further, if G has no cycle of length 3 then, $2\|G\| \geq 4f$.*

Proof. For each edge put two dots on either side of the edge. The total number of dots is $2\|G\|$. If G has a cycle then each face has at least three edges. So, the total number of dots is at least $3f$. Further, if G does not have a cycle of length 3, then $2\|G\| \geq 4f$. ∎

Theorem 7.12.7. *The complete graph K_5 and the complete bipartite graph $K_{3,3}$ are not planar.*

Proof. If K_5 is planar, then consider a plane representation of it. By Equation (7.5), $f = 7$. But, by Lemma 7.12.6, one has $20 = 2\|G\| \geq 3f = 21$, a contradiction.

If $K_{3,3}$ is planar, then consider a plane representation of it. Note that it does not have a C_3. Also, by Euler's formula, $f = 5$. Hence, by Lemma 7.12.6, one has $18 = 2\|G\| \geq 4f = 20$, a contradiction. ∎

Definition 7.12.8. Let G be a graph. Then, a **subdivision** of an edge uv in G is obtained by replacing the edge by two edges uw and wv, where w is a new vertex. Two graphs are said to be **homeomorphic** if they can be obtained from the same graph by a sequence of subdivisions.

For example, for each $m, n \in \mathbf{N}$, the paths P_n and P_m are homeomorphic. Similarly, all the cyclic graphs are homeomorphic to the cycle C_3 if our study is over simple graphs. In general, one can say that all cyclic graphs are homeomorphic to the graph $G = (V, E)$, where $V = \{v\}$ and $E = \{e, e\}$ (*i.e.*, a graph having exactly one vertex and a loop). Also, note that if two graphs are isomorphic then they are also homeomorphic. Figure 7.19 gives examples of homeomorphic graphs that are different from a path or a cycle.

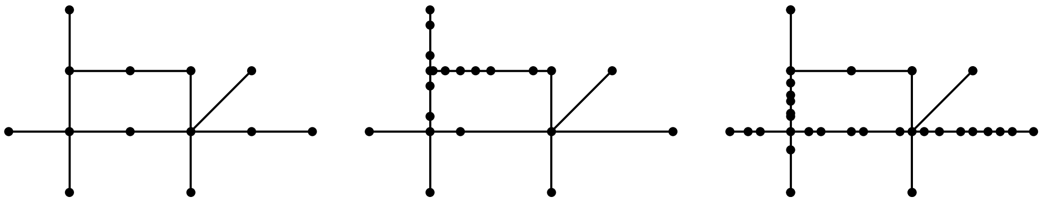


Figure 7.19: Homeomorphic graphs

Theorem 7.12.9. [**Kuratowski,** 1930] *A graph is planar if and only if it has no subgraph homeomorphic K_5 or $K_{3,3}$.*

Proof. Omitted.

We have the following observations that directly follow from Kuratowski theorem.

Remark 7.12.10. *1. Among all simple connected non-planar graphs*

(a) the complete graph K_5 has minimum number of vertices.

(b) the complete bipartite graph $K_{3,3}$ has minimum number of edges.

2. If Y is a non-planar subgraph of a graph X then X is also non-planar.

Definition 7.12.11. Let G be a graph. Define a relation on the edges of G by $e_1 \sim e_2$ if either $e_1 = e_2$ or there is a cycle containing both these edges. Note that this is an equivalence relation. Let E_i be the equivalence class containing the edge e_i. Also, let V_i denote the endpoints of the edges in E_i. Then, the induced subgraphs $\langle V_i \rangle$ are called the **blocks** of G.

Proposition 7.12.12. *A graph G is planar if and only if each of its blocks are planar.*

Proof. Omitted.

Definition 7.12.13. A graph is called **maximal planar** if it is planar and addition of any more edges results in a non-planar graph. A maximal plane graph is necessarily connected.

Proposition 7.12.14. *If G is a maximal planar graph with $|G| \geq 3$ vertices, then every face is a triangle and $\|G\| = 3|G| - 6$.*

Proof. Suppose there is a face, say f, described by the cycle $[u_1, \ldots, u_k, u_1]$, $k \geq 4$. Then, we can take a curve joining the vertices u_1 and u_3 lying totally inside the region f, so that $G + u_1u_3$ is planar. This contradicts the fact that G is maximal planar. Thus, each face is a triangle. It follows that $2\|G\| = 3f$. As $|G| - \|G\| + f = 2$, we have $2\|G\| = 3f = 3(2 - |G| + \|G\|)$ or $\|G\| = 3|G| - 6$. ■

Exercise **7.12.15.** *1. Suppose that G is a plane graph such that each face is a 4-cycle. What is the number of edges in G?*

2. Show that the Petersen graph has a subgraph homeomorphic to $K_{3,3}$.

3. Show that a plane graph on ≥ 3 vertices can have at most $2|G| - 5$ bounded faces.

4. *Let G be a plane graph with f faces and k components. Prove that $|G| - \|G\| + f = k + 1$ (use induction).*
5. *If G is a plane graph without 3-cycles, then show that $\delta(G) \leq 3$.*
6. *Is it necessary that a plane graph G should contain a vertex of degree less than 5?*
7. *Show that any plane graph on ≥ 4 vertices has a vertex of degree at most five.*
8. *Show that any plane graph on ≥ 4 vertices has at least four vertices of degree at most five.*
9. *Produce a planar embedding of the graph G that appears in Figure 7.20.*

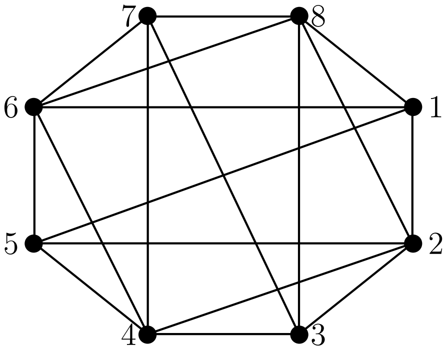


Figure 7.20: A graph on 8 vertices

7.13 Vertex Coloring

Definition 7.13.1. A graph G is said to be **k-colorable** if the vertices can be assigned k colors in such a way that adjacent vertices get different colors. The **chromatic number** of G, denoted $\chi(G)$, is the minimum k such that G is k-colorable.

Exercise **7.13.2.** *Every connected bipartite graph on ≥ 2 vertices has chromatic number 2.*

Theorem 7.13.3. *For every graph G, $\chi(G) \leq \Delta(G) + 1$.*

Proof. If $|G| = 1$, the statement is trivial. Assume that the result is true for $|G| = n$ and let G be a graph on $n+1$ vertices. Let $H = G - 1$. As H is $(\Delta(G)+1)$-colorable and $d(1) \leq \Delta(G)$, the vertex 1 can be given a color other than its neighbors. ■

Theorem 7.13.4. [**Brooks,** 1941] *Every non complete graph which is not an odd cycle has $\chi(G) \leq \Delta(G)$.*

Theorem 7.13.5. [**5-color Theorem**] *Every Planar graph is 5-colorable.*

Proof. Let G be a minimal planar graph on $n \geq 6$ vertices and m edges, such that G is not 5-colorable. Then, by Proposition 7.12.14, $m \leq 3n - 6$. So, $n\delta(G) \leq 2m \leq 6n - 12$ and hence, $\delta(G) \leq 2m/n \leq 5$. Let v be a vertex of degree 5. Note that by the minimality of G, $G - v$ is 5-colorable. If neighbors of v use at most 4 colors, then v can be colored with the 5-th color to get a 5-coloring of G. Else, take a planar embedding in which the neighbors $v_1, \ldots, v_5$ of v appear in clockwise order.

Let $H = G[V_i \cup V_j]$ be the graph spanned by the vertices colored i or j. If v_i and v_j are in different connected components of H, then we can swap colors i and j in a component that contains v_i, so that the vertices $v_1, \ldots, v_5$ use only 4 colors. Thus, as above, in this case the graph G is 5-colorable. Otherwise, there is a $1,3$-colored path between v_1 and v_3 and similarly, a $2,4$-colored path between v_2 and v_4. But this is not possible as the graph G is planar. Hence, every planar graph is 5-colorable. ■

7.14 Representing graphs with Matrices

Definition 7.14.1. Let $G = (V, E)$ be a simple (undirected) graph on vertices $1, \ldots, n$. Then, the **adjacency matrix** $A(G)$ of G (or simply A) is described by

$$a_{ij} = \begin{cases} 1 & \text{if } \{i,j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Let H be the graph obtained by relabeling the vertices of G. Then, note that $A(H) = S^{-1}A(G)S$, for some permutation matrix S (recall that for a permutation matrix $S^t = S^{-1}$). Hence, we talk of the adjacency matrix of a graph and do not worry about the labeling of the vertices of G.

Example 7.14.2. The adjacency matrices of the 4-cycle C_4 and the path P_4 on 4 vertices are given below.

$$A(C_4) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \quad A(P_4) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Exercise **7.14.3.**

1. *A graph G is not connected if and only if there exists a permutation matrix P such that $A(G) = \begin{bmatrix} A_{11} & 0 \\ 0 & A_{22} \end{bmatrix}$, for some matrices A_{11} and A_{22}.*
2. *Two graphs G and H are isomorphic if and only if $A(G) = P^tA(H)P$, for some permutation matrix P.*

Theorem 7.14.4. *The (i,j) entry of $B = A(G)^k$ is the number of i-j-walks of length k.*

Proof. Note that by the definition of matrix product

$$b_{ij} = \sum_{i_1, \ldots, i_{k-1}} a_{ii_1} a_{i_1 i_2} \cdots a_{i_{k-1} i_k}.$$

Thus, $b_{ij} = r$ if and only if we have r sequences $i_1, \ldots, i_{k-1}$ with $a_{ii_1} = \cdots = a_{i_{k-1}i_k} = 1$. That is, $b_{ij} = r$ if and only if we have r walks of length k between i and j. ■

Theorem 7.14.5. *Let G be a graph of order n. Then, G is connected if and only if $\big[I + A(G)\big]^{n-1}$ is entrywise positive.*

Proof. Put $B = I + A$ and let G be connected. If P is an i-j-path of length $n-1$, then $B_{ij}^{n-1} \geq A_{ij}^{n-1} \geq 1$. If $P = [i, i_1, \ldots, i_k = j]$ is an i-j-path of length $k < n-1$, then $b_{ii} \ldots b_{ii} b_{ii_1} \ldots b_{i_{k-1}j} = 1$, where b_{ii} is used $n-1-k$ times. Thus, $B_{ij}^{n-1} > 0$.

Conversely, let $B_{ij}^{n-1} > 0$. Then, the corresponding summand $b_{ii_1} \ldots b_{i_{n-1}j}$ is positive. By throwing out entries of the form b_{ii}, for $1 \leq i \leq n$, from this expression, we have an expression which corresponds to an i-j-walk of length at most $n-1$. As B^{n-1} is entrywise positive, it follows that G is connected. ■

Exercise **7.14.6.** *Let G be a simple, undirected graph with adjacency matrix A.*

1. *Then the eigenvalues of A are all real.*
2. *The eigenvectors can be chosen to form an orthonormal basis of $\mathbb{R}^n$.*
3. *If A has a rational eigenvalue then it has to be an integer.*
4. *If G be the complete graph K_n then $A = J - I$, where J is the matrix with each entry 1. Further, in this case $n-1$ is an eigenvalues with multiplicity 1 and -1 as an eigenvalue repeated $n-1$ times.*

5. *Let $\overline{G}$ be the complement graph of G. Then, $A(\overline{G}) = J - I - A$.*

6. *If G is k-regular then k is an eigenvalue of A with the vector of all 1's as an eigenvector. Further,*

   (a) *$n - k - 1$ is an eigenvalue of $\overline{G}$.*

   (b) *if λ is an eigenvalue of A then $-1 - \lambda$ is an eigenvalue of $A(\overline{G})$.*

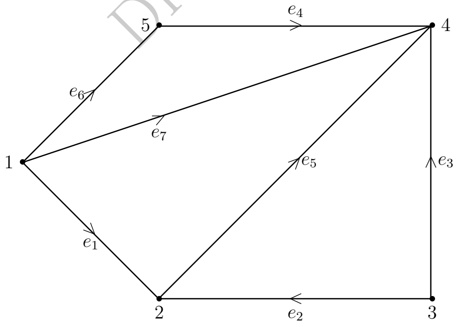
7. *If G is bipartite then there exists a permutation matrix P such that $B = P^tAP = \begin{bmatrix} \mathbf{0} & B_1 \\ B_1^t & \mathbf{0} \end{bmatrix}$. Further, prove that λ is an eigenvalue of A if and only if $-\lambda$ is an eigenvalue of A.*

Definition 7.14.7. Let G be a graph with $V(G) = \{1, 2, \ldots, n\}$ and $E(G) = \{e_1, e_2, \ldots, e_m\}$. Let us arbitrarily give an orientation to each edge of G. For this fixed orientation, the **vertex-edge incidence matrix** or in short, incidence matrix, $Q(G) = [q_{ij}]$ of G is a $n \times m$ matrix whose (i, e_j)-entry is described by

$$q_{ij} = \begin{cases} 1 & \text{if edge } e_j \text{ originates at } i, \\ -1 & \text{if edge } e_j \text{ terminates at } i, \\ 0 & \text{if edge } e_j \text{ is not incident with } i. \end{cases}$$

Example 7.14.8. Consider the graph given below. It has $V(G) = \{1, 2, 3, 4, 5\}$ and $E(G) = \{e_1, e_2, \ldots, e_7\}$. Thus, its incidence matrix

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 \end{bmatrix}.$$



Exercise **7.14.9.** *Let G be a graph on n vertices and m edges.*

1. *Prove that $Q^tQ = diag(d_1, d_2, \ldots, d_n) - A$, where $diag(d_1, d_2, \ldots, d_n)$ is the diagonal matrix of d_i's the degrees of different vertices.*

2. *Prove that $QQ^t = 2I - A(L(G))$, where $A(L(G))$ is the adjacency matrix of the line graph, $L(G)$ of G.*

3. *Let e be a vector of all 1's. Then $e^tQ = \mathbf{0}^t$.*

4. *If G is connected then $rank(Q) = n - 1$.*

5. *Prove that determinant of any square submatrix of Q lies in $\{-1, 0, 1\}$ (Q is unimodular).*

7.14.1 More Exercises

Exercise **7.14.10.** 1. *Can there be a graph in which the size of a minimum covering is $|G|$?*

2. *Characterize G if the size of a minimum covering is $|G| - 1$.*

3. *What relationship is there between the size of a minimum covering and* $\alpha(G)$*?*

4. *Is it necessary that a plane graph* G *should contain a vertex of degree at most* 5*?*

5. *Is* $K_5 - e$ *planar, where* e *is any edge?*

6. *Is* $K_{3,3} - e$ *planar, where* e *is any edge?*

7. *Is it true that any group of* 7 *persons there are* 3 *mutual friends or* 4 *mutual strangers?*

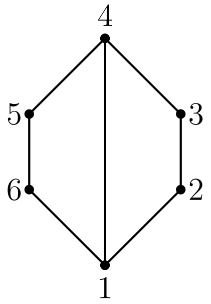
8. *Prove/disprove: A two colorable graph is necessarily planar.*

9. *Draw the tree on the vertex set* $\{1, 2, \ldots, 12\}$ *whose Prüfer code is* 9954449795.

10. *How many chordal graphs are there on the vertex set* $\{1, 2, 3, 4\}$*?*

11. *Count with diameter: how many non-isomorphic trees are there of order* 7*?*

12. *List the automorphisms of the following graph.*



Bibliography

[1] G. Agnarson and R. Greenlaw, *Graph Theory: Modelling, Applications and Algorithm*, Pearson Education.

[2] R. B. Bapat, *Graphs and Matrices*, Hindustan Book Agency, New Delhi, 2010.

[3] J. Cofman, "Catalan Numbers for the Classroom?", *Elem. Math.*, 52 (1997), 108 - 117.

[4] D. M. Cvetkovic, Michael Doob and Horst Sachs, *Spectra of Graphs: theory and applications*, Academic Press, New York, 1980.

[5] D. I. A. Cohen, *Basic Techniques of Combinatorial Theory*, John Wiley and Sons, New York, 1978.

[6] William Dunham, *Euler: The Master of Us All*, Published and Distributed by The Mathematical Association of America, 1999.

[7] F. Harary, *Graph Theory*, Addison-Wesley Publishing Company, 1969.

[8] Victor J Katz, A history of mathematics, an intro, Harper Collins College Publishers, New York, 1993.

[9] G. E. Martin, *Counting: The Art of Enumerative Combinatorics*, Undergraduate Texts in Mathematics, Springer, 2001.

[10] R. Merris, *Combinatorics, 2^{th} edition*, Wiley-Interscience, 2003.

[11] J. Riordan, *Introduction to Combinatorial Analysis*, John Wiley and Sons, New York, 1958.

[12] R. P. Stanley, *Enumerative Combinatorics, vol. 2*, Cambridge University Press, 1999.

[13] H. S. Wilf, *Generatingfunctionology*, Academic Press, 1990.

Index