Lecture Notes on Discrete Mathematics

July 30, 2019

Contents

Chapter 1

Basic Set Theory

The following notations will be followed throughout the book.

1. The empty set, denoted $\varnothing$, 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. $\mathbb{Z} := \{0, 1, -1, 2, -2, \ldots\}$, 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.

This chapter will be devoted to understanding set theory, relations, functions. We start with the basic set theory.

1.1 Sets

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 of sets happened only in the 19-th century due to the German mathematician Georg Cantor. He was solely responsible in ensuring that sets 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 two types of transfinite numbers, namely, transfinite ordinals and transfinite cardinals. 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. We only give an informal description of sets and then proceed to establish their properties.

A "well-defined collection" of distinct objects can be considered to be a set. Thus, the principal property of a set is that of "membership" or "belonging". Well-defined, in this context, would enable us to determine whether a particular object is a member of a set or not.

Members of the collection comprising the set are also referred to as elements of the set. Elements of a set can be just about anything from real physical objects to abstract mathematical objects. An important feature of a set is that its elements are "distinct" or "uniquely identifiable."

A set is typically expressed by curly braces, $\{\ \}$ enclosing its elements. If A is a set and a is an element of it, we write $a \in A$. The fact that a is not an element of A is written as $a \notin A$. For instance, if A is the set $\{1, 4, 9, 2\}$, then $1 \in A$, $4 \in A$, $2 \in A$ and $9 \in A$. But $7 \notin A$, $\pi \notin A$, the English word 'four' is not in A, etc.

Example 1.1.1. 1. Let $X = \{\text{apple}, \text{tomato}, \text{orange}\}$. Here, 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 $\{\text{digits in the number } 12321\}$ 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 the list of digits $1, 2, 1, 4, 2$. Is it a set?

2. 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. The set S that contains no element is called the **empty set** or the **null set** and is denoted by $\{\ \}$ or $\varnothing$. A set that has only one element is called a **singleton set**.

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. $X = \{x : 0 < x \le 10, x \text{ is an even integer }\}$, or
      ii. $X = \{x : 1 < x < 11, x \text{ is an even integer }\}$, or
      iii. $x = \{x : 2 \le x \le 10, x \text{ is an even integer }\}$ etc.

   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 specified by
   (a) $4 \in X$,
   (b) whenever $x \in X$, then $x + 2 \in X$, and
   (c) every element of X satisfies the above two rules.

In the recursive definition of a set, 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. Let X and Y be two sets.

1. Suppose X is the set such that whenever $x \in X$, then $x \in Y$ as well. Here, X is said to be a **subset** of the set Y, and is denoted by $X \subseteq Y$. When there exists $x \in X$ such that $x \notin Y$, then we say that X is not a subset of Y; and we write $X \not\subseteq Y$.
2. If $X \subseteq Y$ and $Y \subseteq X$, then X and Y are said to be **equal**, and is denoted by $X = Y$.
3. If $X \subseteq Y$ and $X \neq Y$, then X is called a **proper subset** of Y.

   Thus, X is a proper subset of Y if and only if $X \subseteq Y$ and $X \neq Y$.

Example 1.1.5. 1. For any set X, we see that $X \subseteq X$. Thus, $\varnothing \subseteq \varnothing$. Also, $\varnothing \subseteq X$. Hence, the empty set is a subset of every set. It thus follows that there is only one empty 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 $\varnothing \notin \varnothing$.
4. Let $X = \{a, b, c\}$. Then $a \in X$ but $\{a\} \subseteq X$. Also, $\{\{a\}\} \not\subseteq X$.
5. Notice that $\{\{a\}\} \not\subseteq \{a\}$ and $\{a\} \not\subseteq \{\{a\}\}$; though $\{a\} \in \{a, \{a\}\}$ and also $\{a\} \subseteq \{a, \{a\}\}$.

We now mention some set operations that enable us in generating new sets from existing ones.

1.2 Operations on sets

Definition 1.2.1. *Let X and Y be two sets.*

1. *The* **union** *of X and Y, denoted by $X \cup Y$, is the set that consists of all elements of X and also all elements of Y. More specifically, $X \cup Y = \{x | x \in X \text{ or } x \in Y\}$.*
2. *The* **intersection** *of X and Y, denoted by $X \cap Y$, is the set of all common elements of X and Y. More specifically, $X \cap Y = \{x | x \in X \text{ and } x \in Y\}$.*
3. *The sets X and Y are said to be* **disjoint** *if $X \cap Y = \varnothing$.*

Example 1.2.2. 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 $X = \{\{b, c\}, \{\{b\}, \{c\}\}, b\}$ and $Y = \{a, b, c\}$. Then

$$X \cap Y = \{b\} \text{ and } X \cup Y = \{a, b, c, \{b, c\}, \{\{b\}, \{c\}\}\ \}.$$

We now state a few properties related to the union and intersection of sets.

Lemma 1.2.3. *Let R, S and T be sets. Then,*

1. *(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) *$S \cup \varnothing = S$, $S \cap \varnothing = \varnothing$.*

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

Proof. 2*a*. Let $x \in R \cup (S \cap T)$. Then, $x \in R$ or $x \in S \cap T$. If $x \in R$ then, $x \in R \cup S$ and $x \in R \cup T$. Thus, $x \in (R \cup S) \cap (R \cup T)$. If $x \notin R$, then $x \in S \cap T$. So, $x \in S$ and $x \in T$. Here, $x \in R \cup S$ and $x \in R \cup T$. Thus, $x \in (R \cup S) \cap (R \cup T)$. In other words, $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$.

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 $y \in R \cup (S \cap T)$. 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 thereby proving the first distributive law. The remaining proofs are left as exercises. ∎

Exercise **1.2.4.** 1. *Complete the proof of Lemma 1.2.3.*

2. *Prove the following:*

   (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 $S \cup T \neq \varnothing$ then either $S \neq \varnothing$ or $T \neq \varnothing$.*

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

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

Definition 1.2.5. Let X and Y 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 set $(X \setminus Y) \cup (Y \setminus X)$, denoted by $X \Delta Y$, is called the **symmetric difference** of X and Y.

Example 1.2.6. 1. Let $A = \{1, 2, 4, 18\}$ and $B = \{x \in \mathbb{Z} : 0 < x \leq 5\}$. 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 $T = \{x \in \mathbb{R} : 0.5 \leq x < 7\}$. Then,

$$S \setminus T = \{x \in \mathbb{R} : 0 \leq x < 0.5\} \text{ and } T \setminus S = \{x \in \mathbb{R} : 1 < x < 7\}.$$

3. Let $X = \{\{b, c\}, \{\{b\}, \{c\}\}, b\}$ and $Y = \{a, b, c\}$. Then

$$X \setminus Y = \{\{b, c\}, \{\{b\}, \{c\}\}\}, Y \setminus X = \{a, c\} \text{ and } X \Delta Y = \{a, c, \{b, c\}, \{\{b\}, \{c\}\}\}.$$

In naive set theory, all sets are essentially defined to be subsets of some reference set, referred to as the universal set, and is denoted by U. We now define the complement of a set.

Definition 1.2.7. Let U be the universal set and $X \subseteq U$. Then, the **complement** of X, denoted by X^c, is defined by $X^c = \{x \in U : x \notin X\}$.

We state more properties of sets.

Lemma 1.2.8. *Let U be the universal set and $S, T \subseteq U$. Then,*

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

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.

Exercise **1.2.9.** *Let S and T be subsets of a universal set U.*

1. *Then prove Lemma 1.2.8.*
2. *Suppose that $S \Delta T = T$. Is $S = \varnothing$?*

Definition 1.2.10. Let X be a set. 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 1.2.11.

1. Let $X = \varnothing$. Then $\mathcal{P}(\varnothing) = \mathcal{P}(X) = \{\varnothing, X\} = \{\varnothing\}$.
2. Let $X = \{\varnothing\}$. Then $\mathcal{P}(\{\varnothing\}) = \mathcal{P}(X) = \{\varnothing, X\} = \{\varnothing, \{\varnothing\}\}$.
3. Let $X = \{a, b, c\}$. Then $\mathcal{P}(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
4. Let $X = \{\{b, c\}, \{\{b\}, \{c\}\}\}$. Then $\mathcal{P}(X) = \{\varnothing, \{\{b, c\}\}, \{\{\{b\}, \{c\}\}\}, \{\{b, c\}, \{\{b\}, \{c\}\}\}\ \}$.

1.3 Relations

In this section, we introduce the set theoretic concepts of relations and functions. We will use these concepts to relate different sets. This method also helps in constructing new sets from existing ones.

Definition 1.3.1. Let X and Y be two sets. Then their Cartesian product, denoted by $X \times Y$, is defined as $X \times Y = \{(a, b) : a \in X, b \in Y\}$. The elements of $X \times Y$ are also called **ordered pairs** with the elements of X as the first entry and elements of Y as the second entry. 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 1.3.2.

1. Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$. Then

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

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

3. By convention, $\varnothing \times Y = X \times \varnothing = \varnothing$. In fact, $X \times Y = \varnothing$ if and only if $X = \varnothing$ or $Y = \varnothing$.

Remark 1.3.3. Let X and Y be two nonempty sets. Then, $X \times Y$ can also be defined as follows: Let $x \in X$ and $y \in Y$ and think of (x, y) as the set $\{\{x\}, \{x, y\}\}$, *i.e.*, we have a new set in which an element (a set formed using the first element of the ordered pair) is a subset of the other element (a set formed with both the elements of the ordered pair). Then, with the above understanding, the ordered pair (y, x) will correspond to the set $\{\{y\}, \{x, y\}\}$. As the two sets $\{\{x\}, \{x, y\}\}$ and $\{\{y\}, \{x, y\}\}$ are not the same, the ordered pair $(x, y) \neq (y, x)$.

EXERCISE **1.3.4.** *Let X, Y, Z and W be nonempty sets. Then, prove the following statements:*

1. *The product construction can be used on sets several times, e.g.,*

$$X \times Y \times Z = \{(x, y, z) : x \in X, y \in Y, z \in Z\} = (X \times Y) \times Z = X \times (Y \times Z).$$

2. $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$.
3. $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$.
4. $(X \times Y) \cap (Z \times W) = (X \cap Z) \times (Y \cap W)$.
5. $(X \times Y) \cup (Z \times W) \subseteq (X \cup Z) \times (Y \cup W)$. *Give an example to show that the converse need not be true.*
6. *Is it possible to write the set $T = \{(x, x, y) : x, y \in \mathbb{N}\}$ as Cartesian product of 3 sets? What about the the set $T = \{(x, x^2, y) : x, y \in \mathbb{N}\}$?*

A relation can be informally thought of as a property which either holds or does not hold between two objects. For example, x is taller than y can be a relation. However, if x is taller than y, then y cannot be taller than x.

Definition 1.3.5. Let X and Y be two nonempty sets. A **relation** R from X to Y is a subset of $X \times Y$, *i.e.*, it is a collection of certain ordered pairs. We write xRy to mean $(x, y) \in R \subseteq X \times Y$. Thus, for any two sets X and Y, the sets $\varnothing$ and $X \times Y$ are always relations from X to Y. A relation from X to X is called a **relation on** X.

Example 1.3.6.

1. Let X be any nonempty set and consider the set $\mathcal{P}(X)$. 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 $A = \{a, b, c, d\}$. Some 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) $R = \{(a,a),(a,b),(b,a),(a,c),(c,a),(c,c),(b,b)\}$.

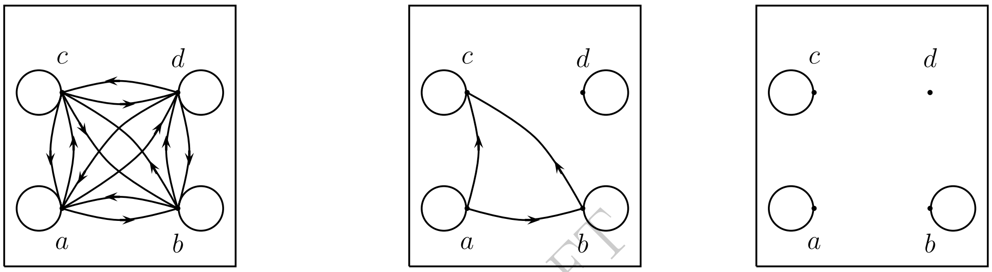
(f) $R = \{(a,b),(b,c),(a,c),(d,d)\}$.

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

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

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

Sometimes, we draw pictures to have a better understanding of different relations. For example, to draw pictures for relations on a set X, we first put a node for each element $x \in X$ and label it x. Then, 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 pictures for some of the relations is given in Figure 1.1.



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

Figure 1.1: Pictorial representation of some relations from Example 2

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]

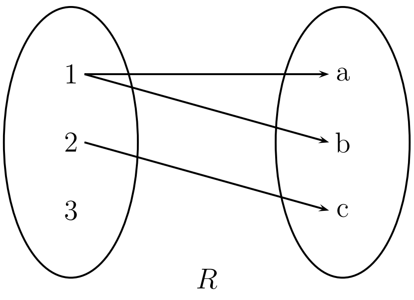


Figure 1.2: Pictorial representation of the relation in Example 3

4. Let $R = \{(x,y) : x,y \in \mathbb{Z} \text{ and } y = x + 5m \text{ for some } m \in \mathbb{Z}\}$ is a relation on $\mathbb{Z}$. If we try to draw a picture for this relation then there is no arrow between any two elements of $\{1,2,3,4,5\}$.

5. Fix $n \in \mathbb{N}$. 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 between any two elements of $\{1,2,3,\ldots,n\}$.

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

Definition 1.3.7. Let X and Y be two nonempty sets and let R be a relation from X to Y. Then, the **inverse relation**, denoted by R^{-1}, is a relation from Y to X, defined by $R^{-1} = \{(y,x) \in Y \times X : (x,y) \in R\}$. So, for all $x \in X$ and $y \in Y$

$$(x,y) \in R \text{ if and only if } (y,x) \in R^{-1}.$$

Example 1.3.8.
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 $R^{-1} = \{(b,a),(c,b),(c,a)\}$ is also a relation on A.

Let R be a relation from X to Y. Consider an element $x \in X$. It is natural to ask if there exists $y \in Y$ such that $(x,y) \in R$. This gives rise to the following three possibilities:

1. $(x,y) \notin R$ for all $y \in Y$.
2. There is a unique $y \in Y$ such that $(x,y) \in R$.
3. There exists at least two elements $y_1, y_2 \in Y$ such that $(x,y_1),(x,y_2) \in R$.

One can ask similar questions for an element $y \in Y$. To accommodate all these, we introduce a notation in the following definition.

Definition 1.3.9. Let R be a nonempty relation from X to Y. Then,
1. the set $\mathsf{dom}\, R := \{x : (x,y) \in R\}$ is called the **domain of** R[1], and
2. the set $\mathsf{rng}\, R := \{y \in Y : (x,y) \in R\}$ is called the **range of** R.

Notation 1.3.10. Let R be a nonempty relation from X to Y. Then,
1. for any set Z, one writes $R(Z) := \{y : (z,y) \in R \text{ for some } z \in Z\}$.
2. for any set W, one writes $R^{-1}(W) := \{x \in X : (x,w) \in R \text{ for some } w \in W\}$.

Example 1.3.11. Let a, b, c, and d be distinct symbols and let $R = \{1,a),(1,b),(2,c)\}$. Then,
1. $\mathsf{dom}\, R = \{1,2\}$, $\mathsf{rng}\, R = \{a,b,c\}$,
2. $R(\{1\}) = \{a,b\}$, $R(\{2\}) = \{c\}$, $R(\{1,2\}) = \{a,b,c\}$, $R(\{1,2,3\}) = \{a,b,c\}$, $R(\{4\}) = \varnothing$.
3. $\mathsf{dom}\, R^{-1} = \{a,b,c\}$, $\mathsf{rng}\, R^{-1} = \{1,2\}$,
4. $R^{-1}(\{a\}) = \{1\}$, $R^{-1}(\{a,b\}) = \{1\}$, $R^{-1}(\{b,c\}) = \{1,2\}$, $R^{-1}(\{a,d\}) = \{1\}$, $R^{-1}(\{d\}) = \varnothing$.

The following is an immediate consequence of the definition, but we give the proof of a few parts for the sake of better understanding.

Proposition 1.3.12. *Let R be a nonempty relation from X to Y, and let Z be any set.*
1. $R(Z) = R(X \cap Z) \subseteq Y$, $R^{-1}(Z) = R^{-1}(Z \cap Y) \subseteq X$.
2. $\mathsf{dom}\, R = R^{-1}(Y) = \mathsf{rng}\, R^{-1} \subseteq X$, $\mathsf{rng}\, R = R(X) = \mathsf{dom}\, R^{-1} \subseteq Y$.
3. $R(Z) \neq \varnothing$ *if and only if* $\mathsf{dom}\, R \cap Z \neq \varnothing$.
4. $R^{-1}(Z) \neq \varnothing$ *if and only if* $\mathsf{rng}\, R \cap Z \neq \varnothing$.

Proof. We prove the last two parts. The proof of the first two parts is left as an exercise.
3. Let $f(S) \neq \varnothing$. There exist $a \in S \cap A$ and $b \in B$ such that $(a,b) \in f$. It implies that $a \in \mathsf{dom}\, f \cap S$ $(a \in S)$. Converse is proved in a similar way.

4. Let $\mathsf{rng}\, f \cap S \neq \varnothing$. There exist $b \in \mathsf{rng}\, f \cap S$ and $a \in A$ such that $(a,b) \in f$. Then $a \in f^{-1}(b) \subseteq f^{-1}(S)$. Similarly, the converse follows. ■

[1]In some texts, the set X is referred to as the domain set of R and it should not be confused with $\mathsf{dom}\, R$.

1.4 Functions

Definition 1.4.1. Let X and Y be nonempty sets and let f be a relation from X to Y.

1. f is called a **partial function** from X to Y, denoted by $f : X \rightharpoonup Y$, if for each $x \in X$, $f(\{x\})$ is either a singleton or $\varnothing$.

2. For an element $x \in X$, if $f(\{x\}) = \{y\}$, a singleton, we write $f(x) = y$. Hence, y is referred to as the **image** of x under f; and x is referred to as the **pre-image** of y under f.

   $f(x)$ is said to be undefined at $x \in X$ if $f(\{x\}) = \varnothing$.

3. If f is a partial function from X to Y such that for each $x \in X$, $f(\{x\})$ is a singleton then f is called a **function** and is denoted by $f : X \to Y$.

Observe that for any partial function $f : X \rightharpoonup Y$, the condition $(a, b), (a, b') \in f$ implies $b = b'$. Thus, if $f : X \rightharpoonup Y$, then for each $x \in X$, either $f(x)$ is undefined, or there exists a unique $y \in Y$ such that $f(x) = y$. Moreover, if $f : X \to Y$ is a function, then $f(x)$ exists for each $x \in X$, *i.e.*, there exists a unique $y \in Y$ such that $f(x) = y$.

It thus follows that a partial function $f : X \rightharpoonup Y$ is a function if and only if $\mathsf{dom}\, f = X$, *i.e.*, domain set of f is X.

Example 1.4.2. Let $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ and $X = \{3, 4, b, c\}$.

1. Consider the relation $R_1 = \{(a, 1), (b, 1), (c, 2)\}$ from A to B. The following are true.
   (a) R_1 is a partial function.
   (b) $R_1(a) = 1$, $R_1(b) = 1$, $R_1(c) = 2$. Also, $R_1(\{d\}) = \varnothing$; thus $R_1(d)$ is undefined.
   (c) $R_1(X) = \{1, 2\}$.
   (d) $R_1^{-1} = \{(1, a), (1, b), (2, c)\}$. So, $R_1^{-1}(\{1\}) = \{a, b\}$ and $R_1^{-1}(2) = c$. For any $x \in X$, $R_1^{-1}(x) = \varnothing$. Therefore, $R_1^{-1}(x)$ is undefined.

2. $R_2 = \{(a, 1), (b, 4), (c, 2), (d, 3)\}$ is a relation from A to B. The following are true.
   (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, $R_2^{-1}(X) = \{b, d\}$.

Convention:

Let $p(x)$ be a polynomial in the variable 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 $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x^2$ corresponds to the set $\{(a, a^2) : a \in \mathbb{Z}\}$.

Example 1.4.3. 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. The following relations $f : \mathbb{Z} \to \mathbb{Z}$ are indeed functions.
   (a) $f = \{(x, 1) : x \text{ is even}\} \cup \{(x, 5) : x \text{ is odd}\}$.
   (b) $f = \{(x, -1) : x \in \mathbb{Z}\}$.
   (c) $f = \{(x, 1) : x < 0\} \cup \{(0, 0)\} \cup \{(x, -1) : x > 0\}$.

3. Define $f : \mathbb{Q}^+ \to \mathbb{N}$ by $f = \{(\frac{p}{q}, 2^p 3^q) : p, q \in \mathbb{N}, q \neq 0, p$ and q are coprime$\}$. Then, f is a function.

Remark 1.4.4. 1. If $X = \varnothing$, then by convention, one assumes that there is a function, called the empty function, from X to Y.

2. If $Y = \varnothing$ and $X \neq \varnothing$, then by convention, we say 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 $X = \{-1, 0, 1\}$. Then, the functions $f, g, h : X \to X$ 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 X.
4. A function is also called a map.
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.

Some important functions are now defined.

Definition 1.4.5. Let X be a nonempty set.

1. The relation $\mathbf{Id} := \{(x, x) : x \in X\}$ is called the **identity** relation on X.
2. 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. 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 **1.4.6.** *1. Do the following relations represent functions? Why?*

(a) $f : \mathbb{Z} \to \mathbb{Z}$ defined by
   i. $f = \{(x, 1) : 2$ divides $x\} \cup \{(x, 5) : 3$ divides $x\}$.
   ii. $f = \{(x, 1) : x \in S\} \cup \{(x, -1) : x \in S^c\}$, where $S = \{n^2 : n \in \mathbb{Z}\}$ and $S^c = \mathbb{Z} \setminus S$.
   iii. $f = \{(x, x^3) : x \in \mathbb{Z}\}$.

(b) $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f = \{(x, \pm\sqrt{x}) : x \in \mathbb{R}^+\}$, where $\mathbb{R}^+$ is the set of all positive real numbers.

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

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

(e) $f : \mathbb{R}^- \to \mathbb{R}$ defined by $f = \{(x, \log_e |x|) : x \in \mathbb{R}^-\}$, where $\mathbb{R}^-$ is the set of all negative real numbers.

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

2. Let $f : X \to Y$ be a function. Then f^{-1} is a relation from Y to X. Show that the following results hold for f^{-1} :

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

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

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

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

(e) $f^{-1}(Y \setminus B) = X \setminus \big(f^{-1}(B)\big)$ for each $B \subseteq Y$.

3. Let $S = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1, x \geq 0\}$. It is a relation from $\mathbb{R}$ to $\mathbb{R}$. Draw a picture of the inverse of this relation.

Definition 1.4.7. A function $f : X \to Y$ is said to be **injective** (also called **one-one** or an **injection**) if for all $x, y \in X$, $x \neq y$ implies $f(x) \neq f(y)$. Equivalently, f is one-one if for all $x, y \in X$, $f(x) = f(y)$ implies $x = y$.

Example 1.4.8.
1. Let X be a nonempty set. Then, the identity map **Id** on X is one-one.
2. Let X be a nonempty proper subset of Y. Then $f(x) = x$ is a one-one map from X to Y.
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 1.4.9. Let $f : X \to Y$ be a function. Let $A \subseteq X$ and $A \neq \varnothing$. The **restriction of f to A**, denoted by f_A, is the function $f_A = \{(x, y) : \ (x, y) \in f, x \in A\}$.

Example 1.4.10. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 0$ if x is rational, and $f(x) = 1$ if x is irrational. Then, $f_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ is the zero function.

Proposition 1.4.11. *Let $f : X \to Y$ be a one-one function and let Z be a nonempty subset of X. Then f_Z is also one-one.*

Proof. Suppose $f_Z(x) = f_Z(y)$ for some $x, y \in Z$. Then $f(x) = f(y)$. As f is one-one, $x = y$. Thus, f_Z is one-one. ∎

Definition 1.4.12. A function $f : X \to Y$ is said to be **surjective** (also called **onto** or a **surjection**) if $f^{-1}(\{b\}) \neq \varnothing$ for each $b \in Y$. Equivalently, $f : X \to Y$ is onto if there exists a pre-image under f, for each $b \in Y$.

Example 1.4.13.
1. Let X be a nonempty set. Then the identity map on X is onto.
2. Let X be a nonempty proper subset of Y. Then the identity map $f : X \to Y$ is not onto.
3. There are 6 onto functions from $\{a, b, c\}$ to $\{a, b\}$. For example, $f(a) = a, f(b) = b$, and $f(c) = b$ is one such function.
4. Let X be a nonempty subset of Y. Fix an element $a \in X$. Define $g : Y \to X$ by
$$g(y) = \begin{cases} y, & \text{if } y \in X, \\ a, & \text{if } y \in Y \setminus X. \end{cases}$$
Then g is an onto function.
5. There does not exist any onto function from the set $\{a, b\}$ to its proper superset $\{a, b, c\}$.
6. There exist onto functions from the set $\{2, 3, \ldots\}$ to its proper superset $\mathbb{N}$. An example of such a function is $f(n) = n - 1$ for all $n \geq 2$.

Definition 1.4.14. Let X and Y be sets. A function $f : X \to Y$ is said to be **bijective** (also call a **bijection**) if f is both one-one and onto. The set X is said to be **equinumerous**[1] with the set Y if there exists a bijection $f : X \to Y$.

[1] If X is equinumerous with Y then X is also said to be *equivalent* to Y.

Clearly, if a set X is equinumerous with a set Y then Y is also equinumerous with X. Hence, X and Y are said to be equinumerous sets.

Example 1.4.15. 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, $f^{-1} : \{a,b,c\} \to \{1,2,3\}$ is a bijection; and the set $\{a,b,c\}$ is equinumerous with $\{1,2,3\}$.

2. Let X be a nonempty set. Then the identity map on X is a bijection. Thus, the set X is equinumerous with itself.

3. The set $\mathbb{N}$ is equinumerous with $\{2,3,\ldots\}$. 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 **1.4.16.** *1. Let $f : X \to Y$ be a bijection. Then, for every choice of pairs x, y with $x \in X$ and $y \in Y$ there exists a bijection, say $h : X \to Y$, such that $h(x) = y$.*

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

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

4. Let X be a nonempty set. Give a one-one function from X to $\mathcal{P}(\mathcal{P}(\mathcal{P}(X)))$.

5. For a fixed $n \in \mathbb{N}$, let A_n and B_n be nonempty 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.

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

1.5 Composition of functions

Definition 1.5.1. 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

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

Notice that the composition of two relations in the above definition is a relation. In case, both f and g are functions, $g \circ f$ is also a function, and $(g \circ f)(x) = g(f(x))$ 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 1.5.2. Let $f = \{(\beta, a), (3, b), (3, c)\}$ 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 1.5.3. **[Algebra of composition of functions]** *Let $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ be functions.*

1. Then, $(h \circ g) \circ f : Z \to W$ and $h \circ (g \circ f) : X \to W$ are functions. Moreover, $(h \circ g) \circ f = h \circ (g \circ f)$ (associativity holds).

2. If f and g are injections then $g \circ f : X \to Z$ is an injection.

3. If f and g are surjections then $g \circ f : X \to Z$ is a surjection.

4. If f and g are bijections then $g \circ f : X \to Z$ is a bijection.

5. [**Extension**] *If* $\mathsf{dom}\, f \cap \mathsf{dom}\, h = \varnothing$ *and* $\mathsf{rng}\, f \cap \mathsf{rng}\, h = \varnothing$ *then the function* $f \cup h$ *from* $X \cup Z$ *to* $Y \cup W$ *defined by* $f \cup h = \{(a, f(a)) : a \in X\} \cup \{(c, h(c)) : c \in Z\}$ *is a bijection.*

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

Theorem 1.5.4. [**Properties of the identity function**] *Let* X *and* Y *be two nonempty sets and* $\mathbf{Id}$ *be the identity function on* X. *Then, for any two functions* $f : X \to Y$ *and* $g : Y \to X$,

$$f \circ \mathbf{Id} = f \quad \text{and} \quad \mathbf{Id} \circ g = g.$$

Proof. By definition, $(f \circ \mathbf{Id})(x) = f(\mathbf{Id}(x)) = f(x)$, for all $x \in X$. Hence, $f \circ \mathbf{Id} = f$. Similarly, the other equality follows. ∎

We now give a very important bijection principle.

Theorem 1.5.5. [**Bijection principle**] *Let* $f : X \to Y$ *and* $g : Y \to X$ *be functions such that* $(g \circ f)(x) = x$ *for each* $x \in X$. *Then* f *is one-one and* g *is onto.*

Proof. To show that f is one-one, suppose $f(a) = f(b)$ for some $a, b \in X$. Then

$$a = (g \circ f)(a) = g\left(f(a)\right) = g\left(f(b)\right) = (g \circ f)(b) = b.$$

Thus, f is one-one.

To show that g is onto, let $a \in X$. Write $b = f(a)$. Now, $a = (g \circ f)(a) = g(f(a)) = g(b)$. That is, we have found $b \in Y$ such that $g(b) = a$. Hence, g is onto. ∎

Exercise **1.5.6.**

1. *Let* $f, g : \mathbb{W} \to \mathbb{W}$ *be defined by* $f = \{(x, 2x) : x \in \mathbb{W}\}$ *and* $g = \{\left(x, \frac{x}{2}\right) : x \text{ is even}\} \cup \{(x, 0) : x \text{ is odd}\}$. *Verify that* $g \circ f$ *is the identity function on* $\mathbb{W}$, *whereas* $f \circ g$ *maps even numbers to even numbers and odd numbers to* 0.

2. *Let* $f : X \to Y$ *be a function. 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 let* $A \subseteq X$. *Is* $f(X \setminus A) = Y \setminus f(A)$*?*

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

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

   (b) $(g \circ f)(x) = x$ *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?*

1.6 Equivalence relation

We look at some relations that are of interest in mathematics.

Definition 1.6.1. Let A be a nonempty set. Then, a relation R on A is said to be

1. **reflexive** if for each $a \in A$, $(a, a) \in R$.
2. **symmetric** if for each pair of elements $a, b \in A$, $(a, b) \in R$ implies $(b, a) \in R$.
3. **transitive** if for each triple of elements $a, b, c \in A$, $(a, b), (b, c) \in R$ imply $(a, c) \in R$.

Exercise **1.6.2.** *For relations defined in Example 1.3.6, determine which of them are*

1. *reflexive.*
2. *symmetric.*
3. *transitive.*

Definition 1.6.3. Let A be a nonempty set. A relation on A is called an **equivalence relation** if it is reflexive, symmetric and transitive. It is customary to write a supposed equivalence relation as $\sim$ rather than R. The **equivalence class** of the equivalence relation $\sim$ containing an element $a \in A$ is denoted by $[a]$, and is defined as $[a] := \{x \in A : x \sim a\}$.

Example 1.6.4. 1. Consider the relations on A of Example 1.3.6.

(a) The relation in Example 1.3.6.1 is not an equivalence relation; it is not symmetric.

(b) The relation in Example 1.3.6.2a is an equivalence relation with $[a] = \{a, b, c, d\}$ as the only equivalence class.

(c) Other relations in Example 1.3.6.2 are not equivalence relations.

(d) The relation in Example 1.3.6.4 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) The relation in Example 1.3.6.5 is an equivalence relation with the equivalence classes as

$$\begin{aligned}
&[0] = \{\ldots, -3n, -2n, -n, 0, n, 2n, \ldots\}.\\
&[1] = \{\ldots, -3n+1, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}.\\
&[2] = \{\ldots, -3n+2, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\}.\\
&\quad\vdots\\
&[n-2] = \{\ldots, -2n-2, -n-2, -2, n-2, 2n-2, 3n-2, \ldots\}.\\
&[n-1] = \{\ldots, -2n-1, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}.
\end{aligned}$$

2. Consider the relation $R = \{(a, a), (b, b), (c, c)\}$ on the set $A = \{a, b, c\}$. Then R is an equivalence relation with three equivalence classes, namely $[a] = \{a\}$, $[b] = \{b\}$ and $[c] = \{c\}$.

3. The relation $R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$ is an equivalence relation on $A = \{a, b, c\}$. It has two equivalence classes, namely $[a] = [c] = \{a, c\}$ and $[b] = \{b\}$.

Proposition 1.6.5. [Equivalence relation divides a set into disjoint classes] *Let $\sim$ be an equivalence relation on a nonempty set X. Then,*

1. *any two equivalence classes are either disjoint or identical;*
2. *the set X is equal to the union of all equivalence classes of $\sim$.*

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

Proof. 1. Let $a, b \in X$ be distinct elements of X. If the equivalence classes $[a]$ and $[b]$ are disjoint, then there is nothing to prove. So, assume that there exists $c \in X$ such that $c \in [a] \cap [b]$. That is, $c \sim a$ and $c \sim b$. By symmetry of $\sim$ it follows that $a \sim c$ and $b \sim c$. We will show that $[a] = [b]$.

For this, let $x \in [a]$. Then $x \sim a$. Since $a \sim c$ and $\sim$ is transitive, we have $x \sim c$. Again, $c \sim b$ and transitivity of $\sim$ imply that $x \sim b$. Thus, $x \in [b]$. That is, $[a] \subseteq [b]$. A similar argument proves that $[b] \subseteq [a]$. Thus, whenever two equivalence classes intersect, they are indeed equal.

2. Notice that for each $x \in X$, the equivalence class $[x]$ is well defined, $x \in [x]$ and $[x] \subseteq X$. Thus, if we take the union of the equivalence classes over all $x \in X$, we get $X = \bigcup\limits_{x \in X} [x]$. ∎

EXERCISE **1.6.6.** *Determine the equivalence relation among the relations given below. Further, for each equivalence relation, determine its equivalence classes.*

1. $R = \{(a, b) \in \mathbb{Z}^2 : a \leq b\}$ *on* $\mathbb{Z}$.
2. $R = \{(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^* : a$ *divides* $b\}$ *on* $\mathbb{Z}^*$, *where* $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.
3. *Recall the greatest integer function* $f : \mathbb{R} \to \mathbb{Z}$ *given by* $f(x) = [x]$ *and let* $R = \{(a, b) \in \mathbb{R} \times \mathbb{R} : [a] = [b]\}$ *on* $\mathbb{R}$.
4. *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) $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : x_1^2 + x_2^2 = y_1^2 + y_2^2\}$.
   (b) $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : \mathbf{x} = \alpha\mathbf{y}$ *for some* $\alpha \in \mathbb{R}^*\}$.
   (c) $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : 4x_1^2 + 9x_2^2 = 4y_1^2 + 9y_2^2\}$.
   (d) $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : \mathbf{x} - \mathbf{y} = \alpha(1, 1)$ *for some* $\alpha \in \mathbb{R}^*\}$.
   (e) *Fix* $c \in \mathbb{R}$. *Now, define* $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : y_2 - x_2 = c(y_1 - x_1)\}$.
   (f) $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : |x_1| + |x_2| = \alpha(|y_1| + |y_2|)\}$, *for some number* $\alpha \in \mathbb{R}^+$.
   (g) $R = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^2 \times \mathbb{R}^2 : x_1 x_2 = y_1 y_2\}$.
5. *For* $\mathbf{x} = (x_1, x_2), \mathbf{y} = (y_1, y_2) \in \mathbb{R}^2$, *let* $S = \{\mathbf{x} \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}$. *Then, are the relations given below an equivalence relation on* S?
   (a) $R = \{(\mathbf{x}, \mathbf{y}) \in S \times S : x_1 = y_1, x_2 = -y_2\}$.
   (b) $R = \{(\mathbf{x}, \mathbf{y}) \in S \times S : \mathbf{x} = -\mathbf{y}\}$.

Definition 1.6.7. Let X be a nonempty set. Then a **partition** of X is a collection of disjoint, nonempty subsets of X whose union is X.

Example 1.6.8. Let $X = \{a, b, c, d, e\}$.

1. Then $\{\{a, b\}, \ \{c, e\}, \ \{d\}\}$ is a partition of X.

   Consider the relation $R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (c, e), (e, c)\}$ on X. The equivalence classes of R are $[a] = [b] = \{a, b\}$, $[c] = [e] = \{c, e\}$ and $[d] = \{d\}$, which constitute the said partition of X.
2. Consider the partition $\{\{a\}, \ \{b, c, d\}, \ \{e\}\}$ of X. Verify that the relation

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

   is an equivalence relation on X with equivalence classes $[a] = \{a\}$, $[b] = \{b, c, d\}$ and $[e] = \{e\}$.

Given a partition of a nonempty set X, does there exists an equivalence relation on X such that the disjoint equivalence classes are exactly the elements of the partition? Recall that the elements of a partition are subsets of the given set.

Proposition 1.6.9. **[Constructing equivalence relation from equivalence classes]** *Let* $\mathcal{P}$ *be a partition of a nonempty set* X. *Let* $\sim$ *be the relation on* X *defined by*

> *for each pair of elements* $x, y \in X$, $x \sim y$ *if and only if both* x *and* y *are elements of the same subset* A *in* $\mathcal{P}$.

Then the set of equivalence classes of $\sim$ is equal to $\mathcal{P}$.

Proof. The construction of $\sim$ says that if A and B are two distinct elements of $\mathcal{P}$, then all elements of A are related to each other by $\sim$, all elements of B are related to each other by $\sim$, but no element of A is related to any element of B by $\sim$.

Let $x \in X$. Since $\mathcal{P}$ is a partition, $x \in A$ for some $A \in \mathcal{P}$. Then $x \sim x$. So, $\sim$ is reflexive.

Let $x, y \in X$ such that $x \sim y$. Then, there exists $A \in \mathcal{P}$ such that $x, y \in A$. So, $y \sim x$. Hence $\sim$ is symmetric.

Let $x, y, z \in X$ such that $x \sim y$ and $y \sim z$. Then there exists $A \in \mathcal{P}$ such that $x, y \in A$ and $y, z \in A$. It follows that $x \sim z$. That is, $\sim$ is transitive.

To complete the proof, we show that

1. Each equivalence class of $\sim$ is an element of $\mathcal{P}$.
2. each element of $\mathcal{P}$ is an equivalence class of $\sim$.

1. Let $[x]$ be an equivalence class of $\sim$ for some $x \in X$. This x is in some $A \in \mathcal{P}$. Now, $y \in [x] \Leftrightarrow x \sim y \Leftrightarrow y \in A$. Then $[x] = A$.

2. Similarly, let $B \in \mathcal{P}$. Take $x \in B$. Now $y \in B \Leftrightarrow y \sim x \Leftrightarrow y \in [x]$. Then $[x] = B$. ∎

Exercise **1.6.10.**
1. *Let X and Y be two nonempty sets and f be a relation from X to Y. 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. *In addition to the data in (1), suppose 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 $X \neq \varnothing$. Is $X \times X$ an equivalence relation on X? If yes, what are the equivalence classes?*
4. *On a nonempty set X, 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)?*
5. *Supply the equivalence relation on $\mathbb{R}$ whose equivalence classes are $\{[m, m+1) : m \in \mathbb{Z}\}$.*

---

6. *A relation on a nonempty set may or may not be reflexive, symmetric, or transitive. Thus there are 8 types of relations. With $X = \{1, 2, 3, 4, 5\}$, give one example for each type of such relations.*
7. *What is the number of all relations on $\{1, 2, 3\}$?*
8. *What is the number of relations f from $\{1, 2, 3\}$ to $\{a, b, c\}$ such that $\mathsf{dom}\, f = \{1, 3\}$?*
9. *What is the number of relations f on $\{1, 2, 3\}$ such that $f = f^{-1}$?*
10. *What is the number of partial functions on $\{1, 2, 3\}$? How many of them are functions?*
11. *What is the number of functions from $\{1, 2, 3\}$ to $\{a_1, a_2, \ldots, a_n\}$?*
12. *What is the number of equivalence relations on $\{1, 2, 3, 4, 5\}$?*
13. *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.*

14. *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) $f \cup g^c$ *is necessarily an equivalence relation.* $(g^c = (\mathbb{R} \times \mathbb{R}) \setminus g)$

Chapter 2

The Natural Number System

Proofs are to mathematics what spelling is to poetry. Mathematical works do consist of proofs, just as poems do consist of words - V. Arnold.

2.1 Peano Axioms

In this section, the set of natural numbers is defined axiomatically. These axioms are credited to the Italian mathematician G. Peano and the German mathematician J. W. R. Dedekind. The goal in these axioms is to first establish the existence of one natural number and then define a function, called the successor function, to generate the remaining natural numbers. Each of these axioms, listed **P1** to **P3** below, is crucial to the properties that the set of natural numbers enjoy.

P1. $1 \in \mathbb{N}$, *i.e.*, 1 is a natural number.

P1 guarantees the existence of one natural number. We now generate more natural numbers using the successor function. So, we assume the existence of a successor function S defined on $\mathbb{N}$. The existence of the successor function is a property unique to the set of natural numbers.

P2. There exists an injective function $S : \mathbb{N} \to \mathbb{N} \setminus \{1\}$.

Here, for each $x \in \mathbb{N}, S(x)$ is called the successor of x.

Axiom **P2** implies that 1 is not the successor of any natural number. As $S(1) \neq 1$, denote $S(1)$ by 2. Now $S(S(1))$, which is $S(2)$, is different from both 1 and 2. Denote $S(2)$ by 3. By a similar argument, denote $S(3)$ to be 4, $S(4)$ to be 5, etc. From this argument each of the elements of the set $\{1, 2, 3, \ldots\}$ is also an element of $\mathbb{N}$. Thus, the axiomatic/formal definition of $\mathbb{N}$ includes all the usual elements, *i.e.*, $1, 2, 3, \ldots$.

Further, to exclude versions of $\mathbb{N}$ that are 'too large', the last axiom, called the **Axiom of Induction** is stated next.

P3. [**Axiom of Induction**] Let $X \subseteq \mathbb{N}$ be such that

1. $1 \in X$, and
2. for each $x \in X$, $S(x) \in X$.

Then $X = \mathbb{N}$.

Axioms **P1** and **P2** ensure that $\{1, 2, \ldots\} \subseteq \mathbb{N}$. Further, as $1 \in \{1, 2, \ldots\}$ and for each $n \in \{1, 2, \ldots\}$, $S(n) \in \{1, 2, \ldots, \}$, Axiom **P3** ensures that that $\mathbb{N} = \{1, 2, \ldots\}$.

The next result ensures that any natural number different from 1 has to be a successor of some other natural number. This, in effect, re-emphasizes the Axioms **P2** and **P3**.

Lemma 2.1.1. *If $n \in \mathbb{N}$ and $n \neq 1$, then there exists $m \in \mathbb{N}$ such that $S(m) = n$.*

Proof. Let $X = \{x \in \mathbb{N} : x = 1 \text{ or } \exists\, y \in \mathbb{N} \text{ such that } x = S(y)\}$. By the definition of X, both 1 and $S(1)$ belong to X, *i.e.*, $X \setminus \{1\} \neq \emptyset$.

So, for any $x \in X \setminus \{1\}$, there must exist $y \in \mathbb{N}$ such that $x = S(y)$. Observe that $S(y) \in \mathbb{N}$. Therefore, $S(x) = S(S(y))$ implies that $S(x) \in X$. Thus, by the induction axiom, **P3** $X = \mathbb{N}$. ∎

The existence of the set of natural numbers has been established axiomatically. So, we now discuss the arithmetic on $\mathbb{N}$, an important property of the set of natural numbers. The arithmetic in $\mathbb{N}$ that touches every aspect of our lives is clearly addition and multiplication. So, depending solely on the Peano axioms, we define the operation of addition on $\mathbb{N}$. 1 is always a natural number by Axiom **P1**. First, we establish what it means to add 1 to a natural number n. Here, we define $n + 1 = S(n)$.

We now wish to add any two natural numbers n and m. Without loss of generality assume that $m \neq 1$. From Lemma 2.1.1, there exists $k \in \mathbb{N}$ such that $m = S(k)$. So, to define $n+m$, it is sufficient to define $n + S(k)$. We do this by using the following recursive definition: $n + S(k) = S(n + k)$.

For example, suppose we wish to compute $1+2$. By the paragraph after Axiom **P2**, $2 = S(1)$. So, $1 + 2 = 1 + S(1)$. By the above definition, $1 + S(1) = S(1 + 1)$ and $1 + 1 = S(1)$, which is 2 by the paragraph after Axiom **P2**. Thus, $1 + S(1) = S(1 + 1) = S(2) = 3$. An iteration of this process will generate the usual addition on $\mathbb{N}$. In short, the definition for addition is:

Definition 2.1.2. We define addition as follows.

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

Using a similar argument, axiomatic multiplication "$\cdot$" can be defined. First, set $n \cdot 1$ to be n. The multiplication of arbitrary natural numbers is now defined in a recursive manner. The formal definition is:

Definition 2.1.3. The multiplication of two natural numbers is defined as follows.

1. For all $n \in \mathbb{N}$, $n \cdot 1 := n$, and
2. for all $m, n \in \mathbb{N}$, $n \cdot S(m) := (n \cdot m) + n$.

We follow the usual convention of writing $(n \cdot m) + k$ as $n \cdot m + k$.

Using the above axiomatic definitions of both addition and multiplication, we derive the properties of the set of natural numbers $\mathbb{N}$.

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

   Let $n, m \in \mathbb{N}$. As

$$\begin{aligned} n + (m + 1) &= n + S(m) && \text{(Definition 2.1.2.1)} \\ &= S(n + m) && \text{(Definition 2.1.2.2)} \\ &= (n + m) + 1, && \text{(Definition 2.1.2.1)} \end{aligned}$$

   we get $1 \in X$. Now, let $z \in X$ and let us show that $S(z) \in X$. As $z \in X$, by definition of X

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

Therefore, using the definition of X 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 the induction axiom, Axiom **P3**, $X = \mathbb{N}$. ■

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

   To show $1 \in X$, we define the set Y to be $Y = \{n \in \mathbb{N} : n + 1 = 1 + n, \text{ for all } n \in \mathbb{N}\}$ and prove that $Y = \mathbb{N}$.

   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 **P3**, $Y = \mathbb{N}$. Therefore, we 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 $n \in \mathbb{N}$. Thus, using $1 \in X$, $n + z = z + n$, for all $n \in \mathbb{N}$ 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 **P3**, $X = \mathbb{N}$. ■

3. [**Distributive law**] For every $n, m, k \in \mathbb{N}$, $n \cdot (m + k) = n \cdot m + n \cdot k$.
   Proof. Let $X = \{k \in \mathbb{N} : \text{ for all } m, n \in \mathbb{N}, n \cdot (m + k) = n \cdot m + n \cdot k\}$. We 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 **P3**, $X = \mathbb{N}$. ■

EXERCISE **2.1.4.** *Prove the following using only the above properties:*

1. [**Uniqueness of addition**] *For every $m, n, k \in \mathbb{N}$, if $m = n$ then $m + k = n + k$.*
2. [**Additive cancellation**] *For every $x, y \in \mathbb{N}$, if $x + z = y + z$ for some $z \in \mathbb{N}$ then $x = y$.*
3. [**Associativity of 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 $x = y$.*

2.2 Other forms of Principle of Mathematical Induction

Mathematical Induction is an important and useful technique used for proofs in Mathematics. This in a sense is a reformulation of the Axiom of Induction. We discuss this principle now.

Let $P(n)$ be a statement which may or may not be true for any natural number n. Consider the set $X = \{n \in \mathbb{N} : P(n) \text{ is true }\}$. The axiom of induction states that if $1 \in X$ and $n \in X$ implies $n + 1 = S(n) \in X$, for all $n \in \mathbb{N}$ then $X = \mathbb{N}$. In other words, if $P(1)$ is true and $P(n)$ is true implies $P(n + 1)$ is true for all $n \in \mathbb{N}$ then one concludes that $P(n)$ is true for all $n \in \mathbb{N}$. The formal description is given below.

[Principle of Mathematical Induction (PMI)] Let $P(n)$ be a statement (proposition) dependent on a natural number $n \in \mathbb{N}$ such that the following hold:

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 $n \in \mathbb{N}$.

We give an analogy, to the above principle.

Observation.

Imagine a ladder with n rungs, where n can be very large. Suppose I wish to climb the ladder. The strategy that I would like to adopt is:

1. I step onto the first rung of the ladder.
2. When I am on the k-th rung of the ladder, I know how to climb to the $(k + 1)$-th rung.

Here, observe that if $k = 1$, then I am on the first rung and using 2, I climb to the second rung. When $k = 2$, by 2, I can climb to the third rung. In short, using 1, I step onto the ladder and then using 2 repeatedly, I ascend up the ladder. This is the essence of mathematical induction.

Stepping onto the ladder is referred to as the base step and the process of moving to the $(k + 1)$-th step from the k-th step is referred to as the inductive step. The above idea is formalized as the principle of mathematical induction. We now state and prove it using Peano axioms.

We now present three simple examples to illustrate this.

Example 2.2.1. 1. Compute the sum of the first n natural numbers.

Let $P(n)$ be the statement that $\sum\limits_{i=1}^{n} i = \dfrac{n(n + 1)}{2}$.

(a) Base step: $n = 1 \Rightarrow \sum\limits_{i=1}^{1} i = 1 = \dfrac{1 \cdot 2}{2}$.

(b) Induction hypothesis: Let us assume that $P(k)$ holds and show that $P(k + 1)$ holds. Here,

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k + 1) = \frac{k(k + 1)}{2} + (k + 1) = \frac{(k + 1)(k + 2)}{2}.$$

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

2. Prove that 6 divides $n^3 + 5n$ for all natural numbers.

Let $P(n)$ be the statement that 6 divides $n^3 + 5n$.

(a) Base step: $n = 1 \Rightarrow 1^3 + 5 \cdot 1 = 6$, which is clearly divisible by 6.

(b) Induction hypothesis: Let us assume that $P(k)$ holds and show that $P(k+1)$ holds. Note that the properties of addition and multiplication implies that $(k+1)^3 = k^3+3k^2+3k+1$. Thus,

$$(k+1)^3 + 5(k+1) = k^3 + 3k^2 + 3k + 1 + 5k + 5 = (k^3 + 5k) + 3k(k+1) + 6.$$

By induction hypothesis, 6 divides k^3+5k; 6 divides 6 and 6 also divides $3k(k+1)$ as either k or $k+1$ is even for all natural number k.

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

3. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then prove that $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, for all $n \geq 1$.

For $n \geq 1$, let $P(n)$ be the statement that $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. Then,

(a) $P(1) = A = A^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ holds true.

(b) So, let us assume that $P(k)$ is true and show that $P(k+1)$ holds. Here, $P(k)$ holds true implies that $A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$. Thus,

$$A^{k+1} = A^k A = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}.$$

Thus, by PMI $P(n)$ is true for all $n \geq 1$.

There is another form of the principle of mathematical induction, generally called the principle of strong induction, wherein the difference is in the induction step.

Theorem 2.2.2. **[Principle of strong induction (PSI)]** *Let $P(n)$ be a statement dependent on $n \in \mathbb{N}$ such that the following hold:*

1. **Base step:** $P(1)$ *is true.*
2. **Induction step:** *For each $n \in \mathbb{N}$, $P(1),\ P(2), \ldots,\ P(n)$ are all true implies $P(n+1)$ is true.*

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

Proof. Let $X = \{n \in \mathbb{N} : P(1)$ and $P(2)$ and $\ldots$ and $P(n)$ hold true$\}$. Since $P(1)$ is assumed true, $1 \in X$. Let $n \in X$. Then all of $P(1),\ P(2),\ \ldots,\ P(n)$ are true. By the induction step, $P(n+1)$ is true. That is, $n+1 = S(n) \in X$. Thus, X is an inductive set and hence by Axiom **P3**, $X = \mathbb{N}$. Therefore, $P(n)$ is true for all $n \in \mathbb{N}$. ∎

As expected, PSI is equivalent to PMI. We now prove this equivalence.

Theorem 2.2.3. **[Equivalence of PMI and PSI]** *Let $P(n)$ be a statement dependent on $n \in \mathbb{N}$. Suppose that P means the statement '$P(n)$ is true for each $n \in \mathbb{N}$.' Then 'P can be proved using PMI' if and only if 'P can be proved using PSI'.*

Proof. Let us assume that P has been proved using PMI. Hence, $P(1)$ is true. Further, whenever $P(n)$ is true, we are able to establish that $P(n+1)$ is true. Therefore, we can recursively establish that $P(n+1)$ is true if $P(1), \ldots, P(n)$ are true. Hence, P can be proved using PSI.

So, now let us assume that P has been proved using PSI. Define $Q(n)$ to mean '$P(\ell)$ holds for $\ell = 1, 2, \ldots, n$.' Notice that $Q(1)$ is true. Suppose that $Q(n)$ is true, *i.e.*, $P(\ell)$ is true for

$\ell = 1, 2, \ldots, n$. But, by hypothesis, we know that P has been proved using PSI. Thus, $P(n+1)$ is true whenever $P(\ell)$ is true for $\ell = 1, 2, \ldots, n$. This, in turn, means that $Q(n+1)$ is true. Hence, by PMI, $Q(n)$ is true for all $n \in \mathbb{N}$ using PMI. Thus, P can be proved using PMI. ∎

There are many variations of PMI and PSI. One useful formulation considers the set $\mathbb{N} \setminus \{1, 2, \ldots, n_0\}$ (for some fixed $n_0 \in \mathbb{N}$) instead of $\mathbb{N}$. We formulate and prove one such version of PMI below.

Theorem 2.2.4. **[Another form of PMI]** *Let $n_0 \in \mathbb{N}$. Let $P(n)$ be a statement dependent on $n \in \mathbb{N}$ such that the following hold:*

1. *$P(n_0 + 1)$ is true.*
2. *For each $n \geq n_0 + 1$, $P(n)$ is true implies $P(n+1)$ is true.*

Then, $P(n)$ is true for each $n \geq n_0 + 1$.

Proof. Since $n_0 \in \mathbb{N}$, for each $n \in \mathbb{N}$, $n + n_0 \in \mathbb{N}$. Consider the statement $Q(n) := P(n + n_0)$. Then $Q(1) = P(n_0 + 1)$.

Let $n \geq n_0 + 1$. Then, $n = n_0 + \ell$, for some $\ell \in \mathbb{N}$ with $\ell \geq 1$. Let us now assume that $Q(\ell)$ is true. Then, by definition $P(\ell + n_0) = P(n)$ holds true as $Q(\ell) = P(\ell + n_0)$. Therefore, using the second assumption and the commutativity of addition, $P(n+1) = P(\ell + n_0 + 1) = P(\ell + 1 + n_0)$ holds true. Thus, $Q(\ell + 1) = P(\ell + 1 + n_0)$ holds true. Hence, we have shown the following:

1. $Q(1)$ is true.
2. Further, for each $\ell \in \mathbb{N}, \ell \geq 1$ the assumption $Q(\ell)$ is true implies that $Q(\ell + 1)$ is true.

Hence, by PMI, it follows that for each $m \in \mathbb{N}$, $Q(m)$ is true. However, $m \geq 1$ implies $n \geq n_0 + 1$. Therefore, for each $n \geq n_0 + 1$, $P(n)$ is true. ∎

Exercise **2.2.5.** *Prove the following variations of PSI and PMI.*

1. Variation of PSI*: Let $n_0 \in \mathbb{N}$ be fixed. Let $P(n)$ be a statement dependent on $n \in \mathbb{N}$ such that the following hold:*

   $P(n_0 + 1)$ is true.
   For each $n \geq n_0 + 1$, $P(n_0 + 1), P(n_0 + 2), \ldots, P(n)$ are true implies $P(n+1)$ is true.

   Then for each $n \geq n_0 + 1$, $P(n)$ is true.

2. Variation of PMI*: Let $n_0 \in \mathbb{N}$ and let $\mathbb{N}_0 = \{n_0 + 1, n_0 + 2, \ldots\}$. Let $X \subseteq \mathbb{N}_0$ be such that $n_0 + 1 \in X$, and for each $n \in \mathbb{N}_0$, $n_0 + 1, n_0 + 2, \ldots, n \in X$ implies $S(n) \in X$. Then $X = \mathbb{N}_0$.*

As an application, we now prove the following result.

Example 2.2.6. Every natural number greater than or equal to 2 is a product of primes.[1]
Let $P(n)$ be the statement that any natural number $n \geq 2$ can be written as a product of primes.

1. **Base step:** Let $n = 2$. As 2 is prime, $P(2)$ is true.
2. **Induction step:** Assume that $P(1)$, $P(2), \ldots,$ $P(k)$ are all true.

   Consider the natural number $k + 1$. Then, we consider the following two cases:

   (a) If $k + 1$ is prime then $P(k+1)$ holds.

[1] Refer to Definition 4.1.11 for prime numbers.

(b) $k+1$ is not a prime. In this case, there exists $p, q \in \{2, 3, \ldots, k\}$ such that $p \cdot q = k+1$. Since $p, q \leq k$, by PSI we already know that each of p and q can be written as product of primes, say $p = p_1 \cdots p_s$ and $q = q_1 \cdots q_t$. Thus, $k+1 = (p_1 \cdots p_s) \cdot (q_1 \cdots q_t)$. Therefore, $P(k+1)$ holds.

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

2.3 Applications of Principle of Mathematical Induction

Example 2.3.1. **[Triangular numbers]**

1. Show that for each $x \in \mathbb{N}$, $x \geq 2$, there exists a unique $t \in \mathbb{N}$ such that $1 + 2 + \cdots + t < x \leq 1 + 2 + \cdots + t + (t+1)$.
2. Let $S_0 = 0$[1] and let $S_t = 1 + 2 + \cdots + t$ for $t \in \mathbb{N}$. Show that for each $x \in \mathbb{N}$, there exists a unique $t \in \mathbb{W} = \mathbb{N} \cup \{0\}$ such that $S_t < x \leq S_{t+1}$.

The base steps in PMI and PSI are important, and overlooking these may result in spurious arguments. See the following example.

Example 2.3.2. **[Wrong use of PSI]** 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. ■

The following result enables us to define a function on $\mathbb{N}$ inductively.

Theorem 2.3.3. **[Inductive definition of function]** *Let f be a relation from $\mathbb{N}$ to a nonempty set X satisfying*

1. *$f(\{1\})$ is a singleton, and*
2. *for each $n \in \mathbb{N}$, if $f(\{n\})$ is a singleton implies $f(\{S(n)\})$ is a singleton.*

Then, f is a function $\mathbb{N}$ to X.

Proof. By the hypothesis, f is already a partial function. Now, let $A = \mathsf{dom}\, f$. Note that $1 \in A$ and $n \in A$ implies $S(n) \in A$. So, by the induction axiom $A = \mathbb{N}$. Thus, f is a function. ■

In the following exercises, assume the usual properties of x^n where $x \in \mathbb{C}$ and $n \in \mathbb{N} \cup \{0\}$.

EXERCISE **2.3.4.**

1. *Let $a, a+d, a+2d, \ldots, a+(n-1)d$ be the first n terms of an arithmetic progression, with $a, d \in \mathbb{C}$. Then* $\displaystyle\sum_{i=0}^{n-1} (a + id) = a + (a+d) + \cdots + (a + (n-1)d) = \frac{n}{2}\left(2a + (n-1)d\right).$
2. *Let $a, ar, ar^2, \ldots, ar^{n-1}$ be the first n terms of a geometric progression, with $a, r \in \mathbb{C}$, $r \neq 1$. Then* $\displaystyle\sum_{i=0}^{n-1} ar^i = a + ar + \cdots + ar^{n-1} = a\frac{r^n - 1}{r - 1}.$
3. *Prove that*

[1] The reader may refer to Section 2.6 for the construction of the set of integers.

(a) *6 divides* $n^3 - n$, *for all* $n \in \mathbb{N}$.

(b) *12 divides* $n^4 - n^2$, *for all* $n \in \mathbb{N}$.

(c) *7 divides* $n^7 - n$, *for all* $n \in \mathbb{N}$.

(d) *3 divides* $2^{2n} - 1$, *for all* $n \in \mathbb{N}$.

(e) *9 divides* $2^{2n} - 3n - 1$, *for all* $n \in \mathbb{N}$.

(f) *10 divides* $n^9 - n$, *for all* $n \in \mathbb{N}$.

(g) *12 divides* $2^{2n+2} - 3n^4 + 3n^2 - 4$, *for all* $n \in \mathbb{N}$.

(h) $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

4. *Find a formula for* $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n$ *and prove it.*

5. *Find 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.*

6. *Find a formula for* $1 \cdot 3 \cdot 5 + 2 \cdot 4 \cdot 6 + \cdots + n \cdot (n+2) \cdot (n+4)$ *and prove it.*

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

8. *Prove by induction that* 2^n *divides* $(n+1)(n+2)\cdots(2n)$.

9. **[AM-GM inequality]**

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

$$\frac{a_1 + a_2}{2} + \frac{a_1 + a_2}{2} + a_3 + \cdots + a_9 = 5, \quad a_1 \cdots a_9 \leq \left(\frac{a_1 + a_2}{2}\right)^2 a_3 \cdots a_9.$$

(b) *Among two pairs of non-negative real numbers with equal sum, the pair with least difference has the largest product.*

(c) *The product of* $n \geq 2$ *non-negative real numbers is maximum when all numbers are equal.*

(d) *Let* $a_1, \ldots, a_n$ *be non-negative real numbers. Show that* $[(a_1 + \cdots + a_n)/n]^n \geq a_1 \cdots a_n$; *and equality is achieved, when* $a_1 = \cdots = a_n$.

---

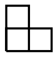
10. *For all* $n \geq 32$, *there exist non-negative integers* x *and* y *such that* $n = 5x + 9y$.

11. *Prove that, for all* $n \geq 40$, *there exist non-negative integers* x *and* y *such that* $n = 5x + 11y$.

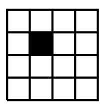
12. *Prove that for* $\mu > 0$,

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

13. *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 tiled with L-shaped pieces.*

14. *Use* $(k+1)^5 - k^5 = 5k^4 + 10k^3 + 10k^2 + 5k + 1$ *to get a closed form expression for* $\sum_{k=1}^{n} k^4$. *Then use PMI to prove your answer.*

2.4 Well Ordering Property of Natural Numbers

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

Definition 2.4.1. Let $m, n \in \mathbb{N}$. Then, the natural number n is said to be **strictly less than** the natural number m, denoted by $n < m$, (in word, n is less than m) if there exists a $k \in \mathbb{N}$ such that $m = n + k$. Further, $n \leq m$ will imply that either $n = m$ or $n < m$. When $n < m$, we also write $m > n$ and read it as m is greater than n.

We prove some properties of $\mathbb{N}$ with the ordering $<$.

Lemma 2.4.2. [**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 $k, \ell \in \mathbb{N}$. Since the sum of two natural numbers is a natural number, we conclude from Definition 2.4.1 that $x < z$. ∎

Exercise **2.4.3.** *Let $x, y, z \in \mathbb{N}$. Then prove the following:*

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

Lemma 2.4.4. *For all $m, n \in \mathbb{N}$, $m \neq m + n$.*

Proof. Suppose there exist $m, n \in \mathbb{N}$ such that $m = m + n$. Then $m + 1 = m + n + 1 = m + S(n)$. By additive cancellation (Exercise 2.1.4.2), $1 = S(n)$, contradicting Axiom **P2**. ∎

Lemma 2.4.5. [**Law of trichotomy**] *For all $m, n \in \mathbb{N}$, exactly one of the following is true:*

$$n < m, \quad n = m, \quad n > m.$$

Proof. As a first step, we show that no two of the above can hold together. For, suppose $n < m$ and $n = m$. Then $n = m + k$ for some $k \in \mathbb{N}$ and $n = m$. That is, $m = m + k$, which contradicts Lemma 2.4.4. As another possibility, assume that $n < m$ and $n > m$. Then there exist $k, \ell \in \mathbb{N}$ such that $n = m + k$ and $m = n + \ell$. So that $n = m + k = n + (\ell + k)$, which again contradicts Lemma 2.4.4. Similarly, other possibilities can be ruled out and is left as an exercise for the reader.

To complete the proof, fix $n \in \mathbb{N}$, and define $X = \{m \in \mathbb{N} : n < m \text{ or } n = m \text{ or } n > m\}$. We show that $X = \mathbb{N}$.

First, we need to 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, $1 < n$ or $n > 1$. Thus, $1 \in X$.

Next, in order to apply Axiom **P3**, assume that $m \in X$. Then either $n < m$ or $n = m$ or $n > m$. We will consider all three cases and in each case show that $S(m) \in X$.

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, $S(m) \in X$.

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

If $n > m$ 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,

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

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

Thus, by Axiom **P3**, $X = \mathbb{N}$. ■

As an application of the law of trichotomy, we show that there does not exist any natural number between n and $S(n)$. Or equivalently, if $n \leq m < n + 1$, then it is necessarily true that $n = m$. Observe that this fact is a consequence of the following result.

Lemma 2.4.6. *For all $m, n \in \mathbb{N}$, $m \leq n$ if and only if $m < n + 1$.*

Proof. Let $m, n \in \mathbb{N}$. Suppose $m \leq n$. Clearly, $n < n + 1$. So, if $m = n$, then $n < n + 1$ implies that $m < n + 1$. If $m < n$, then $n < n + 1$ again implies that $m < n + 1$. Thus, in any case, $m < n + 1$.

Conversely, suppose $m < n + 1$. If $m \not\leq n$, then by the law of trichotomy, $m > n$. That is, there exists $\ell \in \mathbb{N}$ such that $m = n + \ell$. It follows that $n + \ell < n + 1$ for some $\ell \in \mathbb{N}$. Thus, using Additive Cancellation (Exercise 2.1.4.2), one has $\ell < 1$. However, either $\ell = 1$ or $\ell = S(k)$ for some $k \in \mathbb{N}$. The first case implies $1 < 1$ and the second case implies that 1 is a successor of some natural number; giving us a contradiction in either case. Hence $m \leq n$. ■

We are now in a position to state an important principle, namely the well ordering principle.

Theorem 2.4.7. [Well Ordering Principle in $\mathbb{N}$] *Every nonempty subset X of $\mathbb{N}$ contains its least element.*

Proof. By definition, a least element of a set is an element of the set. We thus need to show that every nonempty subset of $\mathbb{N}$ has a least element. On the contrary, suppose A is a nonempty subset of $\mathbb{N}$ that has no least element. Let $B = \mathbb{N} \setminus A$. If $1 \in A$, then 1 will be the least element of A. Thus $1 \notin A$ so that $1 \in B$.

Suppose $1, 2, \ldots, m \in B$. Then, none of $1, 2, \ldots, m$ is in A. If $S(m) \in A$, then $S(m)$ would be the least element of A. Thus, $S(m) \notin A$ and hence $S(m) \in B$.

Hence, by the strong form of induction, $B = \mathbb{N}$. Then, $B = \mathbb{N} \setminus A$ implies $A = \varnothing$, a contradiction. ■

Exercise **2.4.8. [Variation of well ordering principle]** *Let $n_0 \in \mathbb{N}$ and let X be a nonempty subset of $\{n_0 + 1, n_0 + 2, \ldots, \}$. Then prove that X contains its least element.*

2.5 Recursion Theorem

Recall how we defined addition and multiplication in $\mathbb{N}$. For any fixed $n \in \mathbb{N}$, we defined addition by declaring that $n + 1 := S(n)$ and $n + S(m) := S(n + m)$. Due to induction, we remarked that for each $m \in \mathbb{N}$, these two conditions defined $n + m$. This intuitive work requires a formal justification. Notice that $+$ is a binary operation on $\mathbb{N}$, that is, $+$ is a function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. We need to derive rigorously from our axioms that a function satisfying the properties $n + 1 := S(n)$ and $n + S(m) := S(n + m)$ exists, and that such a function is unique. Similarly, multiplication is to be tackled. We rather present a more general result, and view the definitions of addition and multiplication as special cases. The following result provides this general framework in $\mathbb{N}$.

Theorem 2.5.1. **[Recursion Theorem]** *Let $f : \mathbb{N} \to \mathbb{N}$ be a function. Then, for any fixed natural number α, there exists a unique function $g : \mathbb{N} \to \mathbb{N}$ such that*

$$g(1) = \alpha \text{ and } g(S(x)) = f(g(x)) \text{ for each } x \in \mathbb{N}. \tag{2.3}$$

Proof. Define $g \subseteq \mathbb{N} \times \mathbb{N}$ as follows

1. $(1, \alpha) \in g$, and
2. $(x, y) \in g$ implies $(S(x), f(y)) \in g$.

As 1 is not a successor of any natural number, $g(\{1\}) = \{\alpha\}$, is a singleton. Assume that $g(\{x\}) = \{y\}$. Then, $g(\{S(x)\}) = \{f(y)\}$, a singleton as f is a function. So, by Theorem 2.3.3, g is a function.

To show the uniqueness of the function g, we consider two functions $g_1, g_2 : \mathbb{N} \to \mathbb{N}$, satisfying Equation (2.3). Now, define

$$V = \{n \in \mathbb{N} : g_1(n) = g_2(n)\}.$$

From Equation (2.3), $g_1(1) = g_2(1) = \alpha$. So, $1 \in V$.

Let $n \in V$. Here, $g_1(n) = g_2(n)$. Therefore, $g_1(S(n)) = f(g_1(n)) = f(g_2(n)) = g_2(S(n))$. Thus, $S(n) \in V$. By Axiom **P3**, $V = \mathbb{N}$. Therefore, $g_1 = g_2$. ■

Using the recursion theorem, we now show that the definitions of addition and multiplication are indeed well defined.

Example 2.5.2. 1. **[Addition function]** Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined by $f(x) = S(x)$, for all $x \in \mathbb{N}$. Fix any element $y \in \mathbb{N}$. By the recursion theorem, there exists a unique function

$$g : \mathbb{N} \to \mathbb{N} \text{ such that } g(1) = S(y) \text{ and } f(g(x)) = g(S(x)), \text{ for all } x \in \mathbb{N}. \tag{2.4}$$

Define

$$\text{for all } x \in \mathbb{N}, \quad y + x := g(x) \tag{2.5}$$

When $x = 1$, from Equation (2.5), we get $y + 1 = g(1)$. As $g(1) = S(y)$, we get $y + 1 = S(y)$.

Further, for any $x \in \mathbb{N}$, we see that

$$\begin{aligned} y + S(x) &= g(S(x)) && \text{(using Equation (2.5))} \\ &= f(g(x)) && \text{(using } f(g(x)) = g(S(x))) \\ &= S(g(x)) && \text{(using } f(x) = S(x)) \\ &= S(y + x). && \text{(using } g(x) = y + x) \end{aligned}$$

Thus, for all $y,\ x \in \mathbb{N}$, $y + S(x) = S(y + x)$. Hence, both the rules of addition stated in stated in Definition 2.1.2 are satisfied.

2. **[Multiplication function]** Fix an element $y \in \mathbb{N}$ and consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + y$. (Observe that this is well defined by Part 1.)

   Then, by the recursion theorem, there exists a unique function $h : \mathbb{N} \to \mathbb{N}$, such that $h(1) = y$ and $f(h(x)) = h(S(x))$, for all $x \in \mathbb{N}$. Now, define $y \cdot x := h(x)$, for all $x \in \mathbb{N}$.

   Then, for $x = 1$, we get $y \cdot 1 = h(1) = y$. Further, for any $x \in \mathbb{N}$, we see that

   $$y \cdot S(x) = h(S(x)) = f(h(x)) = f(y \cdot x) = y \cdot x + y,$$

   thereby, proving both the rules of multiplication stated in Definition 2.1.3.

3. **[Power function]** Fix an element $m \in \mathbb{N}$ and consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x \cdot m$. (Part 2 allows us to define such a function.)

   Then, by the recursion theorem, there exists a unique function $p : \mathbb{N} \to \mathbb{N}$, such that $p(1) = m$ and $f(p(x)) = p(S(x))$, for all $x \in \mathbb{N}$. Now, define $m^x := p(x)$, for all $x \in \mathbb{N}$.

   Then, for $x = 1$, we get $m^1 = p(1) = m$. Further, for any $x \in \mathbb{N}$, $S(x) = x + 1$ gives

$$m^{x+1} = m^{S(x)} = p(S(x)) = f(p(x)) = p(x) \cdot m = (m^x) \cdot m.$$

   Hence, we have obtained the required power function.

Remark 2.5.3. Recall that in Example 2.5.2.1, it was easy to show that $y + S(x) = S(y + x)$, for all $y, x \in \mathbb{N}$. What is more difficult to prove is that $S(y) + x = S(y + x)$, for all $x, y \in \mathbb{N}$ which together with Example 2.5.2.1 gives us commutativity of addition.

So, we take $X = \{x \in \mathbb{N} \ : \ S(y) + x = S(y + x)\}$ and prove that X is an inductive set.

By the recursion theorem, there exists a unique function $t : \mathbb{N} \to \mathbb{N}$ such that $t(1) = S(S(y))$ and $f(t(x)) = t(S(x))$, for all $x \in \mathbb{N}$. Define

$$S(y) + x := t(x) \text{ for all } x \in \mathbb{N}. \tag{2.6}$$

As $g(1) = S(y)$ (see Example 2.5.2.1) and $g(1) = y + 1$ (Equation (2.5)), we see that for $x = 1$, $S(y) + 1 = t(1) = S(S(y)) = S(g(1)) = S(y + 1)$. This implies that $1 \in X$.

To show that $X = \mathbb{N}$, we assume that $x \in X$. Now, consider $S(y) + S(x)$. Then, using Example 2.5.2.1, $S(y) + S(x) = S(S(y) + x)$. As $x \in X$, $S(y) + x = S(y + x)$ and hence

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

where the last equality also follows from Example 2.5.2.1.

Therefore, $S(x) \in X$, whenever $x \in X$. Therefore, by Axiom **P3**, $X = \mathbb{N}$.

2.6 Construction of Integers

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. In this section and the succeeding one, we will discuss how to construct the integers and rational numbers from the natural numbers.

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

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 $m \in \mathbb{N}$, $[(S(m), 1)] = \{(m + n, n) : \text{ for all } n \in \mathbb{N}\}$.

Further, $\mathbb{Z}$ consists of all equivalence classes of the above forms. That is,

$$\mathbb{Z} = \{[(1,1)]\} \cup \{[(1,S(m))] : m \in \mathbb{N}\} \cup \{[(S(m),1)] : m \in \mathbb{N}\}.$$

Definition 2.6.1. Let $[\mathbf{x}] = [(x_1,x_2)], [\mathbf{y}] = [(y_1,y_2)] \in \mathbb{Z}$ for some $x_1,x_2,y_1,y_2 \in \mathbb{N}$. Define

$$[\mathbf{x}] \oplus [\mathbf{y}] = [(x_1,x_2)] \oplus [(y_1,y_2)] = [(x_1+y_1, x_2+y_2)]. \tag{2.7}$$

The map $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, defined above is called the **addition** in $\mathbb{Z}$.

Note that addition, i.e., the function $\oplus$ maps a pair of two nonempty sets, say $[(x_1,x_2)]$ and $[(y_1,y_2)]$ to the set $[(x_1+y_1,x_2+y_2)]$. 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 2.6.2. *The map $\oplus$ defined in Equation (2.7) 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

$$[(u_1,u_2)] \oplus [(x_1,x_2)] = [(u_1+x_1,u_2+x_2)], \quad [(v_1,v_2)] \oplus [(y_1,y_2)] = [(v_1+y_1,v_2+y_2)].$$

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 $u_1+v_2 = u_2+v_1$ 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. ■

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

Definition 2.6.3. 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

$$[\mathbf{x}] \odot [\mathbf{y}] = [(x_1,x_2)] \odot [(y_1,y_2)] = [(x_1y_1+x_2y_2, x_1y_2+x_2y_1)]. \tag{2.8}$$

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 that multiplication is well-defined. Further, the following properties of of addition and multiplication in $\mathbb{Z}$ can be proved by using the corresponding properties of natural numbers and hence is left as an exercise for the readers.

Exercise **2.6.4.** 1. *Show that the multiplication defined in Equation* (2.8) *is well-defined.*

2. *Let $[\mathbf{x}],[\mathbf{y}],[\mathbf{z}] \in \mathbb{Z}$. Write $[\mathbf{0}] = [(1,1)]$. Prove the following:*
   (a) **[Associativity of addition]** $([\mathbf{x}]+[\mathbf{y}])+[\mathbf{z}] = [\mathbf{x}]+([\mathbf{y}]+[\mathbf{z}])$.
   (b) **[Commutativity of addition]** $[\mathbf{x}]+[\mathbf{y}] = [\mathbf{y}]+[\mathbf{x}]$.
   (c) **[Existence of the zero element]** $[\mathbf{x}]+[\mathbf{0}] = [\mathbf{x}]$.
   (d) **[Cancellation property]** *If $[\mathbf{x}]+[\mathbf{y}] = [\mathbf{x}]+[\mathbf{z}]$ then $[\mathbf{y}] = [\mathbf{z}]$. This implies that the zero element is unique.*

(e) **[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. So, the equivalence class* $-[\mathbf{x}]$ *is called the* **additive inverse** *of* $[\mathbf{x}]$.

(f) **[Distributive laws]** $([\mathbf{x}] + [\mathbf{y}]) \odot [\mathbf{z}] = [\mathbf{x}] \odot [\mathbf{z}] \oplus [\mathbf{y}] \odot [\mathbf{z}]$.

(g) **[Associativity of multiplication]** $([\mathbf{x}] \odot [\mathbf{y}]) \odot [\mathbf{z}] = [\mathbf{x}] \odot ([\mathbf{y}] \odot [\mathbf{z}])$.

(h) **[Commutativity of multiplication]** $[\mathbf{x}] \odot [\mathbf{y}] = [\mathbf{y}] \odot [\mathbf{x}]$.

(i) **[Existence of the identity element]** $[\mathbf{x}] \odot [\mathbf{1}] = [\mathbf{x}]$*, where* $[\mathbf{1}] = [(S(1), 1)]$.

(j) **[Cancellation property]** *If* $[\mathbf{x}] \odot [\mathbf{y}] = [\mathbf{x}] \odot [\mathbf{z}]$ *with* $[\mathbf{x}] \neq [\mathbf{0}]$ *then* $[\mathbf{y}] = [\mathbf{z}]$.

(k) $[\mathbf{x}] \odot [\mathbf{0}] = [\mathbf{0}]$.

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

Lemma 2.6.5. *Define* $f : \mathbb{N} \to \mathbb{Z}$ *by* $f(n) = [(S(n), 1)]$ *for all* $n \in \mathbb{N}$*. Then the following are true:*

1. f *is one-one.*
2. *For all* $a, b \in \mathbb{N}$, $f(a + b) = f(a) \oplus f(b)$.
3. *For all* $a, b \in \mathbb{N}$, $f(a \cdot b) = f(a) \odot f(b)$.

Proof. 1. Suppose $f(a) = f(b)$ for some $a, b \in \mathbb{N}$. By definition, $[(S(a), 1)] = [(S(b), 1)]$ or equivalently, $S(a) + 1 = S(b) + 1$. By the cancellation law in $\mathbb{N}$, we get $S(a) = S(b)$. Since S is one-one, we have $a = b$.

2. Let $a, b \in \mathbb{N}$. By definition, $f(a + b) = [(S(a + b), 1)]$. So

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

3. Let $a, b \in \mathbb{N}$. Now, $f(a \cdot b) = [(S(a \cdot b), 1)]$. So

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

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

We have shown that $f(\mathbb{N}) \subseteq \mathbb{Z}$. Further, the map f commutes with the addition operation and the multiplication operation. Thus, we identify $f(\mathbb{N})$ inside $\mathbb{Z}$ as a copy of $\mathbb{N}$. 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 2.6.6. 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, $v_1 + y_2 < y_1 + v_2$. As $[(u_1, u_2)] = [(v_1, v_2)]$ and $[(x_1, x_2)] = [(y_1, y_2)]$, one has $u_1 + v_2 = v_1 + u_2$ and $x_1 + y_2 = y_1 + x_2$. Thus, $u_1 + v_2 + y_1 + x_2 = v_1 + u_2 + x_1 + y_2$. Hence,

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

as $u_1 + x_2 < x_1 + u_2$. Therefore, by the order property in $\mathbb{N}$ (see Exercise 2.4.3), $v_1 + y_2 < y_1 + v_2$. Thus, the above definition is well-defined. At this stage, one would like to verify that the function f defined in Lemma 2.6.5 preserves the order as well.

Lemma 2.6.7. *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 2.4.3, $a < b$ 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 2.6.8. 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 $[\mathbf{0}] \le [\mathbf{x}]$. In general, we write $[\mathbf{x}] > [\mathbf{0}]$ to mean $[\mathbf{x}]$ is positive and $[\mathbf{x}] \ge [\mathbf{0}]$ for $[\mathbf{x}]$ being non-negative.

Lemma 2.6.9. *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 2.4.3, one obtains $[(x_1, x_2)] > [(1, 1)]$ if and only if $x_1 > x_2$. ■

Exercise **2.6.10.** 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 need not worry about well-definedness. Let us now discuss the "absolute value function", namely the modulus function.

Definition 2.6.11. A function $g : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is called an **absolute/modulus** function if

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

This function is denoted by $|\cdot|$. Thus, $|m| = m$, if $m \ge 0$ and $-m$, if $m < 0$. Further, by Exercise 2.6.10.1, observe that $|m| \ge 0$ for all $m \in \mathbb{Z}$.

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

Lemma 2.6.12. *For any $x \in \mathbb{Z}$, $-|x| \le x \le |x|$. Further, if $x \ge 0$ and $-x \le y \le x$ for some $y \in \mathbb{Z}$, then $|y| \le x$.*

Proof. Let $x \ge 0$. Then, by definition $|x| = x$ and hence $x \le |x|$. As $|x| = x$, the other inequality $-|x| \le x$ reduces to $-x \le x$. Or equivalently, we need to show that $0 = x + (-x) \le x + x = 2x$, which is indeed true. If $x < 0$ then we see that $|x| > 0 > x$ and hence $x \le |x|$. Note that the condition $-|x| \le x$ is equivalent to the condition $|x| + x \ge 0$ (use Exercise 2.6.10.2) which is indeed true as by definition $x + |x| = x + (-x) = 0$.

For the second part, we again consider two cases, namely, $y \ge 0$ and $y < 0$. If $y \ge 0$ then $|y| = y$ and hence the condition $y \le x$ implies $|y| \le x$. If $y < 0$ then $|y| = -y$. Further, using Exercise 2.6.10.2, the condition $-x \le y$ is equivalent to the condition $0 \le y + x$ which in turn is equivalent to $-y \le x$. Hence $|y| = -y \le x$. Thus, the required result follows. ∎

As a direct application of Lemma 2.6.12, one obtains the triangle inequality.

Lemma 2.6.13. **[Triangle inequality in $\mathbb{Z}$]** *Let $x, y \in \mathbb{Z}$. Then $|x + y| \le |x| + |y|$.*

Proof. Using Lemma 2.6.12, 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 2.6.12. ∎

This finishes most of the results on the basic operations related to integers. As a last note, we make the following remark.

Remark 2.6.14. Even though the well ordering principle and its extension (Exercise 2.4.8) is valid for subsets of $\mathbb{N}$, it can be generalized to $\mathbb{W}$, the set of whole numbers. Furthermore, if we fix an integer $z \in \mathbb{Z}$ and take $S = \{z, z+1, z+2, \ldots\}$ then it can also be shown that every nonempty subset X of S contains its least element. Or equivalently, every nonempty subset X of $\mathbb{Z}$ which is bounded below satisfies the well ordering principle.

2.7 Construction of Rational Numbers

We will describe the construction of rational numbers in brief, and and prove a few properties, such as addition, multiplication, subtraction and division by nonzero elements.

We write $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ and define 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. Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$. Then, **addition** in $\mathbb{Q}$, denoted as $\oplus$, is defined by

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

2. Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$. Then, **multiplication** in $\mathbb{Q}$, denoted as $\odot$, is defined by

$$[\mathbf{x}] \odot [\mathbf{y}] = [(x_1, x_2)] \odot [(y_1, y_2)] = [(x_1 \cdot y_1, x_2 \cdot y_2)].$$

The readers are advised to verify that the above operations in $\mathbb{Q}$ are well-defined. Further, the map $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(a) = [(a, 1)]$, is one-one and it preserves addition and multiplication. Thus, $\mathbb{Z}$ is seating inside $\mathbb{Q}$ as $f(\mathbb{Z})$. As earlier, we replace the symbols '$\oplus$' and '$\odot$' by '$+$' and '$\cdot$'. Sometimes, $x \cdot y$ is simply written as xy. 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 $[(x_1, x_2)] \neq 0$ implies that $x_1 \neq 0$. Verify that for each $[(x_1, x_2)] \in \mathbb{Q}$ with $x_1 \neq 0$, 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 2.7.1. Let $[\mathbf{x}] = [(x_1, x_2)], [\mathbf{y}] = [(y_1, y_2)] \in \mathbb{Q}$ with $y_1 \neq 0$. Then, the **division** in $\mathbb{Q}$, denoted as $/$, is defined by

$$[\mathbf{x}]/[\mathbf{y}] = [(x_1, x_2)]/[(y_1, y_2)] = [(x_1 y_2, x_2 y_1)].$$

Note that $x_2 y_1 \in \mathbb{Z}^*$ as $x_2, y_1 \neq 0$.

The readers are advised to verify that division is well-defined. Before proceeding further with other important properties of rational numbers, the readers should verify all the properties related with addition, subtraction, multiplication, and division by a nonzero element. The next result helps in defining order in $\mathbb{Q}$.

Lemma 2.7.2. **[Representation of an Element of $\mathbb{Q}$]** *Let $[\mathbf{x}] \in \mathbb{Q}$. Then $[\mathbf{x}] = [(y_1, y_2)]$ for some $y_1, y_2 \in \mathbb{Z},\ y_2 > 0$.*

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 2.6.10.1, we know that $-x_2 > 0$. Then, by the definition of equivalence class we have $[\mathbf{x}] = [(x_1, x_2)] = [(-x_1, -x_2)]$. Hence the required result follows. ∎

Definition 2.7.3. 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 $x_1 y_2 > x_2 y_1$.

One should verify that the order in $\mathbb{Q}$ is indeed well-defined. Notice that as earlier, $[\mathbf{x}] \geq [\mathbf{y}]$ means either $[\mathbf{x}] = [\mathbf{y}]$ or $[\mathbf{x}] > [\mathbf{y}]$. Further, it may be seen that $\mathbb{Q}$ is an *ordered field*, that is, the following are satisfied for all $a, b, c \in \mathbb{Q}$:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. $a + 0 = a$.
4. There exists an element, written as $-a$ such that $a + (-a) = 0$.
5. $a \cdot b = b \cdot a$.
6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
7. $a \cdot 1 = a$.
8. Corresponding to a, there exists an element, written as $1/a \in \mathbb{Q}$ such that $a \cdot (1/a) = 1$.
9. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
10. Exactly one of the conditions $a < b$ or $a = b$ or $b < a$ is true.
11. If $a < b$ and $b < c$, then $a < c$.
12. If $a < b$, then $a + c < b + c$.
13. If $a < b$ and $0 < c$, then $a \cdot c < b \cdot c$.

As a final result of this section, we prove the following result.

Lemma 2.7.4. **[Existence of a Rational between two Rationals]** *Let $[\mathbf{x}], [\mathbf{y}] \in \mathbb{Q}$ with $[\mathbf{x}] < [\mathbf{y}]$. Then there exists $[\mathbf{z}] \in \mathbb{Q}$ 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 $[\mathbf{z}] = [(x_1 y_2 + x_2 y_1, 2x_2 y_2)]$. It can be easily verified that $[\mathbf{x}] < [\mathbf{z}] < [\mathbf{y}]$ as $x_2, y_2 \in \mathbb{Z}$ and using the multiplicative cancellation (Exercise 2.1.4.8) in $\mathbb{Z}$. ∎

Chapter 3

Countable and Uncountable Sets

In this chapter, we discuss the size of sets. Intuitively, the number of elements in a set may be considered as its size. For instance, the sets $\{1\}$ has size 1 and the set $\{a, b\}$ has size 2. We will be concerned about size of sets of various kinds.

3.1 Finite and infinite sets

We first show that the intuitive notion of 'number of elements in a set' is a well defined notion, at least for finite sets. Since the set $\{1, 2, \ldots, m\}$ will be used often, we give a notation for this set.

Notation: $[m] = \{1, 2, \ldots, m\}$ for $m \in \mathbb{N}$.

We hope that this notation will not conflict with the notation of an equivalence class induced by an equivalence relation; the context will clarify which one is used.

Lemma 3.1.1. *Let $n \in \mathbb{N}$. There exists no one-one function from $[n]$ to any of its proper subsets.*

Proof. We use PMI to prove this result. For each $n \in \mathbb{N}$, let $P(n)$ be the statement that there exists no one-one function from $[n]$ to any of its proper subsets.

The statement $P(1)$ holds as there exists no one-one function from $[1]$ to $\varnothing$. Assume the induction hypothesis that for an $m \in \mathbb{N}$, $P(m)$ holds. We show that $P(m+1)$ holds.

On the contrary, suppose there exists one-one function $f : [m+1] \to A$, where A is a proper subset of $[m+1]$. We consider two cases depending on whether $m+1 \in \mathsf{rng}\, f$ or not.

Case 1: $m+1 \in \mathsf{rng}\, f$.

(a) If $f(m+1) = m+1$, then the restriction function $f_{[m]}$ is a one-one function from $[m]$ to $A \setminus \{m+1\}$, which is a proper subset of $[m]$. This contradicts the induction hypothesis.

(b) If $f(m+1) \neq m+1$, then there exist $k, \ell \in [m]$ such that $f(k) = m+1$ and $f(m+1) = \ell$. Define the function $g : [m] \to A \setminus \{m+1\}$ by

$$g(k) = \ell, \quad g(x) = f(x) \;\text{ for } x \neq k.$$

Observe that g is one-one and $A \setminus \{m+1\}$ is a proper subset of $[m]$. This contradicts the induction hypothesis.

Case 2: $m+1 \notin \mathsf{rng}\, f$.

In this case, $f(m+1) \in [m]$. Then the restriction function $f_{[m]}$ is a one-one function from $[m]$ to $A \setminus \{f(m+1)\}$, which is a proper subset of $[m]$. Again, it contradicts the induction hypothesis.

Hence, there exists no one-one function from $[m+1]$ to any of its proper subsets so that $P(m+1)$ holds. ■

As an application of Lemma 3.1.1, we prove the following result.

Lemma 3.1.2. *Let $m, n \in \mathbb{N}$. Then the following are true:*

1. **[Injection]** *There exists a one-one function from $[m]$ to $[n]$ if and only if $m \le n$.*
2. **[Bijection]** *There exists a bijection from $[m]$ to $[n]$ if and only if $m = n$.*

Proof. (1) Suppose $m \le n$. Then the function $\mathbf{Id} : [m] \to [n]$ given by $\mathbf{Id}(x) = x$ is a one-one function. Conversely, let $f : [m] \to [n]$ be a one-one function. If $m > n$, then $[n]$ is a proper subset of $[m]$. Now, f is one-one function from $[m]$ to a proper subset of $[m]$ contradicting Lemma 3.1.1. Hence $m \le n$.

(2) Assume that $m = n$. Then the identity function on $[n]$, given by $\mathbf{Id}(x) = x$ is a bijection. Conversely, suppose that $g : [m] \to [n]$ is a bijection. Then both g and $g^{-1} : [n] \to [m]$ are one-one functions. By (1), $m \le n$ and $n \le m$. Therefore, $m = n$. ■

Recall that two sets are said to be equinumerous if there is a bijection between them, and that the composition of two bijections is a bijection. Thus, if $m, n \in \mathbb{N}$, $m \ne n$ and A is a set equinumerous with $\{1, 2, \ldots, m\}$, then A cannot be equinumerous with $\{1, 2, \ldots, n\}$, *i.e.*, such a set A has a definite number of elements. This idea provides a mathematical justification of the fact that if two persons count all English words in this page correctly, then they will arrive at the same number.

Taking cue from the above results, we define the notions of finite sets, infinite sets, and the number of elements, or the cardinality of a finite set as follows.

Definition 3.1.3. 1. A set X is called **finite** if either $X = \varnothing$ or there exists a bijection from X to $[m]$ for some $m \in \mathbb{N}$; this number m is called the **cardinality** of X and is denoted by $|X|$. We write $|\varnothing| = 0$.

2. A set which is not finite is called an **infinite** set.

For instance, $[m]$ is a finite set for any $m \in \mathbb{N}$. Moreover, $|[m]| = m$. For any $m \in \mathbb{N}$, if $a_1, \ldots, a_m$ are distinct objects, then $A := \{a_1, \ldots, a_m\}$ is a finite set since $f : A \to [m]$ defined by $f(a_j) = j$ is a bijection; and, $|A| = m$.

If $\mathbb{N}$ is a finite set, then there is a bijection $f : \mathbb{N} \to [n]$ for some $n \in \mathbb{N}$. In that case, the restriction function $f_{[n+1]} : [n+1] \to [n]$ is one-one. It contradicts Lemma 3.1.1. Therefore, $\mathbb{N}$ is an infinite set.

We give some characterization of finite and infinite sets, where the requirements are seemingly weaker than those mentioned in their definitions.

Theorem 3.1.4. *1. A nonempty set X is finite if and only if there exists a one-one function $f : X \to [m]$ for some $m \in \mathbb{N}$.*

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

3. A set X is infinite if and only if there exists a bijection from X to one of its proper subsets.

4. A set X is infinite if and only if there exists a one-one function from X to one of its proper subsets.

Proof. (1) Let X be a nonempty set. If X is finite, then there is a bijection $f : A \to [n]$ for some $n \in \mathbb{N}$. Now, f itself is a one-one function.

Conversely, let $g : X \to [m]$ be a one-one function for some $m \in \mathbb{N}$. We show by PMI on m that X is finite. For $m = 1$, if $g : X \to \{1\}$ is one-one, then g is onto, and hence a bijection. So, by definition

X is finite. Assume that the statement is true for $m = k$ and let $g : X \to [k+1]$ be one-one function. If g is onto, then g is a bijection with $n = k+1$ so that , *i.e.*, X is equinumerous with $[k+1]$ and hence by definition, X is finite. So, assume that g is not onto.

If $k+1 \notin \operatorname{rng} g$, then $g : X \to [k]$ is one-one, and the induction hypothesis implies that X is finite. Otherwise, there exist $x_0 \in X$ and $\ell \leq k$ such that $g(x_0) = k+1$ and $\ell \notin \operatorname{rng} g$. Define $h : X \to [k]$ by

$$h(t) = \begin{cases} g(t), & \text{if } t \notin x_0 \\ \ell, & \text{if } t = x_0. \end{cases}$$

Then $h : X \to [k]$ is one-one. By the induction hypothesis, X is finite.

(2) Let X be an infinite set. Since $X \neq \varnothing$, there exists at least one element, say, $a_1 \in X$. We show by induction that for each $n \geq 2$, there exists $a_n \in X$ different from $a_1, \ldots, a_{n-1}$. Now that a_1 has been chosen, consider the set $X \setminus \{a_1\}$. If this set is empty, then $X = \{a_1\}$, which is a finite set. As X is infinite, $X \setminus \{a_1\}$ is nonempty. So, let $a_2 \in X \setminus \{a_1\}$. This proves the basis case. So, suppose $a_1, \ldots, a_m \in X$ have been chosen corresponding to the numbers $1, 2, \ldots, m$. The set $X \setminus \{a_1, a_2, \ldots, a_m\}$ is nonempty, since otherwise $X = \{a_1, a_2, \ldots, a_m\}$ would be a finite set. So, let $a_{m+1} \in X \setminus \{a_1, a_2, \ldots, a_m\}$. This proves the induction step.

Hence, corresponding to 1, there exists $a_1 \in X$, and for each $n \geq 2$, there exists $a_n \in X$ different from all of $a_1, a_2, \ldots, a_{n-1}$. Define the function $f : \mathbb{N} \to X$ by $f(n) = a_n$. Then f is a one-one function. (Notice that for different choices of a_ns, we get different functions f.)

Conversely, let $f : \mathbb{N} \to X$ be one-one. If X is finite, then there exists a one-one function $g : X \to [m]$ for some $m \in \mathbb{N}$. Then $g \circ f : \mathbb{N} \to [m]$ is one-one. The restriction of $g \circ f$ to $[n+1]$ is a one-one function from $[n+1]$ to $[n]$. It contradicts Lemma 3.1.1. Therefore, X is infinite.

(3) Let X be an infinite set. By (2), there is a one-one function $f : \mathbb{N} \to X$. Now define the function $g : X \to X \setminus \{f(1)\}$ by

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

Then g is a bijection. So, we have a bijection from X to one of its proper subsets.

Conversely, Let $g : X \to Y$ be a bijection, where Y is a proper subset of X. On the contrary, assume that X is a finite set. Then, there is a bijection $f : X \to [m]$ for some $m \in \mathbb{N}$. Since Y is a proper subset of X, $f(Y)$ is a proper subset of $f(X)$. As $f(X) = [m]$, the function $f \circ g \circ f^{-1} : [m] \to f(Y)$ is a bijection from $[m]$ to a proper subset of $[m]$. This contradicts Lemma 3.1.1.

(4) Let X be an infinite set. By (3) there exists a bijection from X to one of its proper subsets. This bijection is itself a one-one function from X to that subset. Conversely, suppose that $h : X \to Y$ is one-one, where Y is a proper subset of X. Let $Z = \operatorname{rng} h$. We see that Z is also a proper subset of X and $h : X \to Z$ is a bijection. ∎

Observe that Theorem 3.1.4.3 implies that a set X is finite if and only if there is no bijection from X to any of its proper subsets, if and only if, there is no one-one function from X to any of its proper subsets.

Exercise **3.1.5.**

1. *A subset of a finite set is finite.*
2. *If X and Y are disjoint sets with $|X| = m$ and $|Y| = n$, then $|X \cup Y| = m + n$. In particular, if X and Y are disjoint finite sets, then $X \cup Y$ is finite.*
3. *Let X and Y be finite sets. Then $X \cup Y$ is finite.*

4. *Let X be a nonempty set with $|X| = n$. For any $x \in X$, $|X \setminus \{x\}| = n - 1$.*
5. *A superset of an infinite set is infinite.*
6. *Let X be an infinite set and let Y be a finite set. Then $X \setminus Y$ is an infinite set.*
7. Let X and Y be nonempty finite sets. Then $|X| \leq |Y|$ if and only if there exists a one-one function $f : X \to Y$.
8. Let X and Y be nonempty finite sets. Then $|X| = |Y|$ if and only if there is a bijection from X to Y.
9. *Let X be a finite nonempty set and let α be a fixed symbol. Let $Y = \{(a, \alpha) : a \in X\}$. Then $|X| = |Y|$.*
10. *Let X be a nonempty finite set. Then, for any set Y, $|X| = |X \setminus Y| + |X \cap Y|$.*
11. *Let X and Y be two finite sets. Then $|X \cup Y| = |X| + |Y| - |X \cap Y|$.*
12. *Let A and B be finite sets. Show that $A \times B$ is a finite set, and $|A \times B| = |A| \times |B|$.*
13. *Let $f : A \to B$ be a function, where both A and B are finite sets. If $\operatorname{rng} f = \{b_1, \ldots, b_n\}$ then show that $|A| = \sum\limits_{j=1}^{n} |f^{-1}(b_j)|$. In particular, if $|f^{-1}(b_j)| = k$ for $j = 1, 2, \ldots, n$, then $|A| = nk$.*

3.2 Families of sets

In this section, we extend the notation of operations on sets to sets of sets.

Definition 3.2.1. Let I be a set. For each $\alpha \in I$, take a set A_α. The set

$$\{A_\alpha\}_{\alpha \in I} := \{A_\alpha : \alpha \in I\}$$

is called a **family of sets** indexed by elements of I. In this case, the set I is called an index set. The family of sets $\{A_\alpha : \alpha \in I\}$ is called a **nonempty family** when the index set I is nonempty.

Let $\{Y_\alpha\}_{\alpha \in I}$ be a nonempty family of sets. We define the union and intersection of the sets in the family as follows:

1. **union** : $\bigcup\limits_{\alpha \in I} Y_\alpha = \{y : y \in Y_\alpha \text{ for some } \alpha \in I\}$;
2. **intersection** : $\bigcap\limits_{\alpha \in I} Y_\alpha = \{y : y \in Y_\alpha \text{ for all } \alpha \in I\}$.

[**Convention**] The union of sets in an empty family is $\varnothing$. The intersection of sets in an empty family of subsets of a set S is S.[1]

Unless otherwise mentioned, we assume that the index set for a family of sets is nonempty so that the family is a nonempty family.

Example 3.2.2.

1. Take $A = \{1, 2, 3\}$, $B_1 = \{1, 2\}$, $B_2 = \{2, 3\}$ and $B_3 = \{4, 5\}$. Then the family

$$\{B_\alpha : \alpha \in A\} = \{B_1, B_2, B_3\} = \{\{1, 2\}, \{2, 3\}, \{4, 5\}\}.$$

Thus, $\bigcup\limits_{\alpha \in A} B_\alpha = \{1, 2, 3, 4, 5\}$ and $\bigcap\limits_{\alpha \in A} B_\alpha = \varnothing$.

[1]Consider the family $\{A_\alpha\}_{\alpha \in I}$, where each A_α is a subset of a set S. Let $x \in S$. If $x \notin \bigcap\limits_{\alpha \in I} A_\alpha$, then there exists an $\alpha \in I$ such that $x \notin A_\alpha$. However, such an α does not exist since I is empty. Therefore, each such $x \in \bigcap\limits_{\alpha \in I} A_\alpha$.

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

$$\{B_\alpha : \alpha \in A\} = \{B_1, B_2, \ldots\} = \{\{1,2,\ldots\}, \{2,3,\ldots\}, \ldots\}.$$

Thus, $\bigcup_{\alpha\in A} B_\alpha = \mathbb{N}$ and $\bigcap_{\alpha\in A} B_\alpha = \varnothing$.

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

Proposition 3.2.3. *Let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of subsets of X and let B be any set. For any subset Y of X, write $Y^c = X \setminus Y$. Then*

1. $B \cup \left(\bigcap_{\alpha\in I} A_\alpha\right) = \bigcap_{\alpha\in I} (B \cup A_\alpha)$,
2. $B \cap \left(\bigcup_{\alpha\in I} A_\alpha\right) = \bigcup_{\alpha\in I} (B \cap A_\alpha)$,
3. $\left(\bigcup_{\alpha\in I} A_\alpha\right)^c = \bigcap_{\alpha\in I} A_\alpha^c$, *and*
4. $\left(\bigcap_{\alpha\in I} A_\alpha\right)^c = \bigcup_{\alpha\in I} A_\alpha^c$.

Proof. (1) Let $x \in B \cup \left(\bigcap_{\alpha\in I} A_\alpha\right)$. Then $x \in B$ or $x \in \bigcap_{\alpha\in I} A_\alpha$. If $x \in B$, then $x \in B \cup A_\alpha$ for each $\alpha \in I$. So, $x \in \bigcap_{\alpha\in I}(B \cup A_\alpha)$. If $x \in \bigcap_{\alpha\in I} A_\alpha$, then for each $\alpha \in I$, $x \in A_\alpha$ so that $x \in B \cup A_\alpha$. Then $x \in \bigcap_{\alpha\in I}(B \cup A_\alpha)$. In any case, $x \in \bigcap_{\alpha\in I}(B \cup A_\alpha)$.

Conversely, suppose $x \in \bigcap_{\alpha\in I}(B \cup A_\alpha)$. Then for each $\alpha \in I$, $x \in B \cup A_\alpha$. If $x \in B$, then $x \in B \cup \left(\bigcap_{\alpha\in I} A_\alpha\right)$. If $x \notin B$ but $x \in B \cup A_\alpha$ for each $\alpha \in I$, then $x \in A_\alpha$ for each $\alpha \in I$. So that $x \in \bigcap_{\alpha\in I} A_\alpha$. Then $x \in B \cup \left(\bigcap_{\alpha\in I} A_\alpha\right)$.

(3) Notice that both the sets are subsets of X. So, let $x \in X$. Now,

$$x \in \left(\bigcup_{\alpha\in I} A_\alpha\right)^c \Leftrightarrow x \notin \bigcup_{\alpha\in I} A_\alpha \Leftrightarrow \text{ for each } \alpha \in I,\ x \notin A_\alpha \Leftrightarrow \text{ for each } \alpha \in I,\ x \in A_\alpha^c \Leftrightarrow x \in \bigcap_{\alpha\in I} A_\alpha^c.$$

Proof of (2) and (4) are similar to those of (1) and (3), respectively. ∎

Practice **3.2.4.**

1. *Consider $\{A_x\}_{x\in\mathbb{R}}$, where $A_x = [x, x+1]$. What is $\bigcup_{x\in\mathbb{R}} A_x$ and $\bigcap_{x\in\mathbb{R}} A_x$?*
2. *For $x \in [0,1]$ write $\mathbb{Z}x := \{zx : z \in \mathbb{Z}\}$ and $A_x = \mathbb{R} \setminus \mathbb{Z}x$. What is $\bigcup_{x\in[0,\,1]} A_x$ and $\bigcap_{x\in[0,\,1]} A_x$?*
3. *Write the closed interval $[1,2]$ as $\bigcap_{n\in\mathbb{N}} I_n$ for suitable open intervals I_n.*

Proposition 3.2.5. *Let X and Y be nonempty sets and let f be a relation from X to Y. Let $\{A_\alpha\}_{\alpha\in I}$ be a family of subsets of X. Then*

$$f\big(\bigcup_{\alpha\in I} A_\alpha\big) = \bigcup_{\alpha\in I} f(A_\alpha) \quad \text{and} \quad f\big(\bigcap_{\alpha\in I} A_\alpha\big) \subseteq \bigcap_{\alpha\in I} f(A_\alpha).$$

Proof. For the equality,

$$\begin{aligned} y \in f\big(\bigcup_{\alpha\in I} A_\alpha\big) &\Leftrightarrow (x,y) \in f \text{ for some } x \in \bigcup_{\alpha\in I} A_\alpha \Leftrightarrow (x,y) \in f \text{ where } x \in A_\alpha \text{ for some } \alpha \in I \\ &\Leftrightarrow y \in f(A_\alpha) \text{ for some } \alpha \in I \Leftrightarrow y \in \bigcup_{\alpha\in I} f(A_\alpha). \end{aligned}$$

For the containment, the case $\bigcap_{\alpha\in I} A_\alpha = \varnothing$ is obvious. So, assume that $\bigcap_{\alpha\in I} A_\alpha \neq \varnothing$. Then

$$\begin{aligned} y \in f\big(\bigcap_{\alpha\in I} A_\alpha\big) &\Leftrightarrow (x,y) \in f \text{ for some } x \in \bigcap_{\alpha\in I} A_\alpha \Leftrightarrow (x,y) \in f \text{ with } x \in A_\alpha \text{ for all } \alpha \in I \\ &\Rightarrow y \in f(A_\alpha) \text{ for all } \alpha \in I \Leftrightarrow y \in \bigcap_{\alpha\in I} f(A_\alpha). \end{aligned}$$

∎

Remark 3.2.6. Observe that in the proof of the containment in Proposition 3.2.5, if $y \in f(A_\alpha)$ for each $\alpha \in I$, then for each $\alpha \in I$, we can find some $x_\alpha \in A_\alpha$ such that $(x_\alpha, y) \in f$. However, such an x_α need not be the same for each α. Thus the containment need not be an equality. To see that it is indeed the case, consider the function $f : \{1,2,3,4\} \to \{a,b\}$ where $f = \{(1,a),(2,a),(2,b),(3,b),(4,b)\}$. Take $A_1 = \{1,3\}$ and $A_2 = \{1,2,4\}$ and verify that $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$.

To define the product of sets in a family, we first rewrite the product of two sets in an equivalent way. Let A_1 and A_2 be nonempty sets and let $a_1 \in A_1,\ a_2 \in A_2$. The ordered pair (a_1, a_2) may be thought of as the function $f : \{1,2\} \to A_1 \cup A_2$ with $f(1) = a_1$ and $f(2) = a_2$. Therefore, $A_1 \times A_2$ is identified with the set of all functions $f : \{1,2\} \to A_1 \cup A_2$ with $f(1) \in A_1$ and $f(2) \in A_2$. Generalizing this observation leads to the following definition.

Definition 3.2.7. Let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of sets. Assume that A_α is nonempty for each $\alpha \in I$. The **product** of the sets in the family is defined as

$$\prod_{\alpha\in I} A_\alpha = \big\{f : f \text{ is a function from } I \text{ to } \bigcup_{\alpha\in I} A_\alpha \text{ with } f(\alpha) \in A_\alpha \text{ for each } \alpha \in I\big\}.$$

In case $A_\alpha = \varnothing$ for some $\alpha \in I$, we define the product $\prod_{\alpha\in I} A_\alpha := \varnothing$.

Example 3.2.8. Take $I = \mathbb{N}$ and $A_\alpha = \{0,1\}$ for each $\alpha \in \mathbb{N}$. Then the product $\prod_{\alpha\in I} A_\alpha$ is the set of all functions $f : \mathbb{N} \to \{0,1\}$. In other words, the product is the set of all 0-1 sequences.

Exercise **3.2.9.**

1. *Write $\mathbb{R}$ as a union of infinite number of pairwise disjoint infinite sets.*
2. *Write the set $\{1,2,3,4\}$ as the intersection of infinite number of infinite sets.*
3. *Prove Parts 2 and 4 of Proposition 3.2.3.*
4. *Let $f : X \to Y$ be a partial function, $A \subseteq X$, $B \subseteq Y$ and let $\{B_\beta\}_{\beta\in I}$ be a nonempty family of subsets of Y. Show the following.*
   (a) $f^{-1}\big(\bigcap_{\beta\in I} B_\beta\big) = \bigcap_{\beta\in I} f^{-1}(B_\beta)$.
   (b) $f^{-1}(B^c) = \mathsf{dom}\, f \setminus f^{-1}(B)$.
   (c) $f\left(f^{-1}(B) \cap A\right) = B \cap f(A)$.
   (d) $f^{-1}\big(\bigcup_{\beta\in I} B_\beta\big) = \bigcup_{\beta\in I} f^{-1}(B_\beta)$.

   Also, show that in (a)-(c), equality may fail if f is a relation but not a partial function. Observe that (d) is a special case of Proposition 3.2.5.
5. *Let $f : X \to Y$ be a one-one function and let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of subsets of X. Is it true that $f\big(\bigcap_{\alpha\in I} A_\alpha\big) = \bigcap_{\alpha\in I} f(A_\alpha)$?*
6. *Show that each set can be written as a union of finite sets.*
7. *Give an example of an equivalence relation on $\mathbb{N}$ for which there are 7 equivalence classes, out of which exactly 5 are infinite.*
8. *Show that the union of finitely many finite sets is a finite set.*
9. *Let $I = A_1 = A_2 = A_3 = \{1,2,3\}$. Is the set $\prod_{\alpha\in I} A_\alpha$ equal to the set of all functions from $\{1,2,3\}$ to $\{1,2,3\}$? Give reasons for your answer.*
10. *Give sets A_n, $n \in \mathbb{N}$, such that $\prod_{n\in\mathbb{N}} A_n$ has 6 elements. Give another.*[1]

[1] When we ask for more than one example, we encourage the reader to get examples of different types, if possible.

3.3 Constructing bijections

Though we have discussed criteria for classifying a set as finite or infinite through injections, the definitions demand creating bijections. If $f : X \to Y$ is one-one, then $f : X \to \mathsf{rng}\, f$ is a bijection. Besides this, we now discuss some general techniques to create bijections.

Experiment 1: Make a horizontal list of the elements of $\mathbb{N}$ using only dots instead of writing the numbers themselves. Also write $\mathbb{Z}$ using dots horizontally below the list for $\mathbb{N}$. Draw arrows connecting the dots on the top list to dots on the bottom list to supply a bijection from $\mathbb{N}$ to $\mathbb{Z}$. Can you supply another bijection by changing the arrows?

Experiment 2: Consider an open interval (a, b). Its center is $c = \frac{a+b}{2}$, length is $\ell = b - a$, and the distance of the center from each end-point is $\frac{\ell}{2}$. View the open interval as a line segment on the real line. Stretch (a, b) uniformly without disturbing the center and make its length equal to L. Use this information to answer the following:

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

   Using these information, find a bijection from (a, b) to (s, t). [Hint: First, fix the center.]

Practice **3.3.1.**

1. *Construct two bijections from* $(1, \infty)$ *to* $(5, \infty)$.
2. *Construct two bijections from* $(0, 1)$ *to* $(1, \infty)$.
3. *Construct two bijections from* $(-1, 1)$ *to* $(-\infty, \infty)$.
4. *Construct two bijections from* $(0, 1)$ *to* $\mathbb{R}$.
5. *Construct two bijections from* $(0, 1) \times (0, 1)$ *to* $\mathbb{R} \times \mathbb{R}$.

Experiment 3: Let $P = (0, 1)$, $T = (3, 5)$ and $f : P \to T$ be a bijection. Imagine elements of P as 'persons' and elements of T as 'seats' in a train. So, f assigns 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?

It leads to the following result, which you can prove easily.

Theorem 3.3.2. **[Train Seat Argument]** *Let X be a set with $\{a_1, a_2, \ldots, \} \subseteq X$ and let $f : X \to Y$ be a bijection.*

1. *If $c_1, \ldots, c_k$ are distinct objects not in X, then the function*

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

   is a bijection from $X \cup \{c_1, \ldots, c_k\}$ to Y.

2. *If $c_1, c_2, \ldots$ are distinct objects not in X, then the function*

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

   is a bijection from $X \cup \{c_1, c_2, \ldots\}$ to Y.

Example 3.3.3. In each of the following cases, give a bijection from X to Y:

1. $X = [0, 1)$ and $Y = (0, 1)$.

   Ans: Map $\{0, 1/2, 1/3, \ldots\}$ onto $\{1/2, 1/3, \ldots\}$ and each of the rest to itself. That is, define $f : X \to Y$ by $f(x) = \begin{cases} 1/2 & \text{if } x = 0 \\ 1/(n+1) & \text{if } x = 1/n \text{ with } n \in \{2, 3, \ldots\} \\ x & \text{if } x \notin \{1/2, 1/3, 1/4, \cdots\}. \end{cases}$

2. $X = (0, 1)$ and $Y = \mathbb{R} \setminus \mathbb{N}$.

   Ans: $f : X \to \mathbb{R}$ given by $f(x) = \tan(\pi(x - 1/2))$ is a bijection. Define $g : \mathbb{R} \to Y$ by

$$g(x) = \begin{cases} x & \text{if } \; x \in \mathbb{R} \setminus \mathbb{Z} \\ -2x & \text{if } \; x \in \mathbb{N} \cup \{0\} \\ -2x + 1 & \text{if } \; -x \in \mathbb{N}. \end{cases}$$

   That is, g maps each x in $\mathbb{R} \setminus \mathbb{Z}$ to itself by the identity map, and then it maps $0, -1, 1, -2, 2, -3, 3, \ldots$ to $0, -1, -2, -3, -4, -5, -6, \ldots$ in that order. Clearly, g is a bijection. Hence $g \circ f : X \to Y$ is a bijection.

Exercise **3.3.4.** *In each of the following, use Theorem 3.3.2 to give a bijection from X to Y.*

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

3.4 Cantor-Schröder-Bernstein Theorem

Let A and B be finite sets with $|A| = m$ and $|B| = n$. Suppose there exists a one-one function from A to B. Then we know that $m \leq n$. In addition, if there exists a one-one function from B to A, then $n \leq m$ so that $m = n$. It then follows that there is a bijection from A to B. Does the same result hold good for infinite sets? That is, given one-one functions $f : A \to B$ and $g : B \to A$ does there exist a bijection from A to B?

Experiment : *Creating a Bijection from Injections*
Let $X = Y = \mathbb{N}$. Take one-one functions $f : X \to Y$ and $g : Y \to X$ defined by $f(x) = x + 2$ 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.

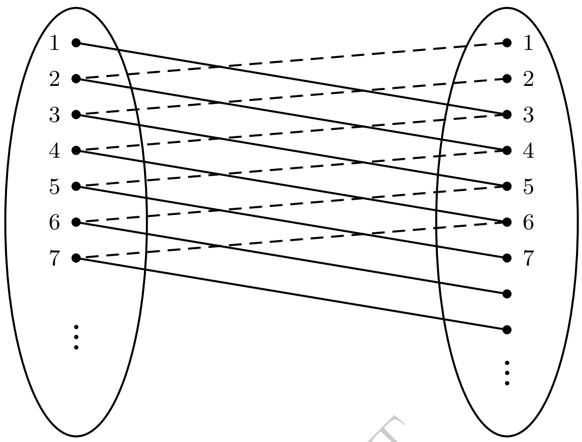


Figure 3.1: Graphic representation of functions f and g

We want to create a bijection h from X to Y by erasing some of these lines. Initially, we keep all solid lines and look at $\operatorname{rng} f$. Since f is not an onto function, there are elements in $Y \setminus \operatorname{rng} f$. Each one of these elements must be connected by a dotted line to some element in X. So, we keep all those pairs $(y, x) \in g$ such that $y \notin \operatorname{rng} f$. We follow the heuristic of keeping as many pairs in f as possible; and then keep a pair $(y, x) \in g$ if no pair $(z, y) \in f$ has been kept.

1. The elements $1, 2 \in Y$ but are not in $\operatorname{rng} f$. So, the dotted lines connecting them to elements in X must stay. That is, the pairs $(1, 2), (2, 3) \in g$ must be kept.
2. Then the pairs $(2, 4), (3, 5) \in f$ must be deleted.
3. Now, $(1, 3) \in f$; it is kept, and then $(3, 4) \in g$ must be deleted.
4. The pair $(4, 5) \in g$ is kept; so $(5, 7) \in f$ must be deleted.
5. The pair $(4, 6) \in f$ is kept, and then $(6, 7) \in g$ must be deleted.
6. The pair $(7, 8) \in g$ is kept; so $(8, 10) \in f$ must be deleted.

Continue this scheme to realize what is happening. Then the bijection $h : X \to Y$ is given by

$$h(x) = \begin{cases} f(x) & \text{if } \ x = 3n - 2, n \in \mathbb{N} \\ g^{-1}(x) & \text{otherwise.} \end{cases}$$

Practice **3.4.1.** *Construct bijections using the given injections $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$.*

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 $g(x) = 2x$.*

We use this heuristic method of constructing a bijection in proving the following theorem.

Theorem 3.4.2. [Cantor-Schröder-Bernstein (CSB)] *Let X and Y be nonempty sets and let $f : X \to Y$ and $g : Y \to X$ be one-one functions. Then there exists a bijection $h : X \to Y$.*

Proof. If f is onto, then f itself is a bijection. So, assume that f is not onto. Then $f(X)$ is a proper subset of Y. Write $B = Y \setminus f(X)$, $\phi = f \circ g$, and $A = B \cup \phi(B) \cup \phi^2(B) \cup \cdots = B \cup \bigcup\limits_{n=1}^{\infty} \phi^n(B)$. Then $A \subseteq Y$ and

$$\phi(A) = \phi(B) \cup \bigcup_{n=2}^{\infty} \phi^n(B) = \bigcup_{n=1}^{\infty} \phi^n(B).$$

Hence $A = B \cup \phi(A)$. Notice that $f(X) = Y \setminus B$, $\phi(A) = f(g(A)) \subseteq Y$, and f is one-one. Hence

$$f(X \setminus g(A)) = f(X) \setminus f(g(A)) = [Y \setminus B] \setminus \phi(A) = Y \setminus [B \cup \phi(A)] = Y \setminus A.$$

Thus, the restriction of f to $X \setminus g(A)$ is a bijection onto $Y \setminus A$. As g is one-one, its restriction to A is a bijection onto $g(A)$. That is, $g^{-1} : g(A) \to A$ is a bijection. Therefore, the function $h : X \to Y$ defined by

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

is a bijection. ∎

Alternate. If g is onto, we have nothing to prove. So, assume that g is not onto. Then $O := X \setminus g(Y) \neq \varnothing$. Write $\psi = g \circ f$ and $E = O \cup \psi(O) \cup \psi^2(O) \cup \cdots = O \cup \bigcup\limits_{n=1}^{\infty} \psi^n(O)$. Observe that $O \subseteq E \subseteq X$, $\psi : X \to X$ is one-one, and g does not map any element of Y to any element of O. Hence

$$\psi(E) = \psi\Big(O \cup \bigcup_{n=1}^{\infty} \psi^n(O)\Big) = \bigcup_{n=1}^{\infty} \psi^n(O) = E \setminus O.$$

Thus the restriction of ψ to E is a bijection from E onto $E \setminus O$. Define the function $\tau : X \to X \setminus O$ by

$$\tau(x) = \begin{cases} x, & \text{if } x \in X \setminus E, \\ \psi(x), & \text{if } x \in E. \end{cases}$$

Then τ is a bijection. Write $h := \tau^{-1} \circ g$. Then h is one-one and $h(Y) = \tau^{-1}(g(Y)) = \tau^{-1}(X \setminus O) = X$. Therefore, h is a bijection from Y to X. ∎

Alternate. Consider the family $\mathcal{F} = \{T \subseteq X : g\left(f(T)^c\right) \subseteq T^c\}$ of subsets of X. Here, $T^c = X \setminus T$ and $f(T)^c = Y \setminus f(T)$.

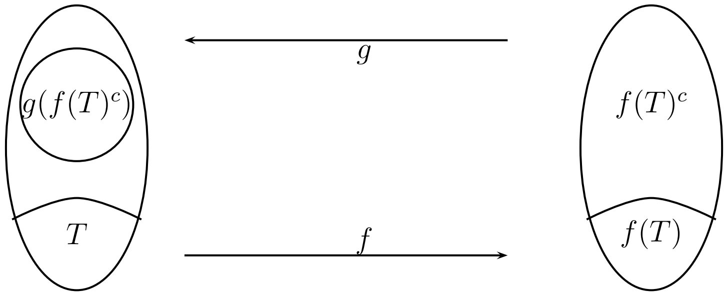


Figure 3.2: Depiction of CSB-theorem

Note that $\varnothing \in \mathcal{F}$. Put $U = \underset{T\in\mathcal{F}}{\cup} T$. Then

$$g\big(f(U)^c\big) = g\Big(\big[f\big(\underset{T\in F}{\cup} T\big)\big]^c\Big) = g\Big(\big[\underset{T\in F}{\cup} f(T)\big]^c\Big) = g\Big(\underset{T\in F}{\cap} f\,(T)^c\Big) = \underset{T\in F}{\cap} g\,(f\,(T)^c) \subseteq \underset{T\in F}{\cap} T^c = U^c.$$

Thus, $U \in \mathcal{F}$; and hence U is the maximal element of $\mathcal{F}$. Now that $g\,(f(U)^c) \subseteq U^c$, we want to show that $g\,(f(U)^c) = U^c$. On the contrary, assume that $U^c \neq g\,(f(U)^c)$. Then we have an element $x \in U^c \setminus g\,(f(U)^c)$. Write $V = U \cup \{x\}$. Then $g\big(f(U)^c\big) \subseteq U^c \cap \{x\}^c$ and $f(U) \subseteq f(V)$. Thus, $f(V)^c \subseteq f(U)^c$ and

$$g\big(f(V)^c\big) \subseteq g\big(f(U)^c\big) \subseteq U^c \cap \{x\}^c = V^c.$$

This contradicts the maximality of U in $\mathcal{F}$. So, $g\big(f(U)^c\big) = U^c$. Hence f is a bijection from U to $f(U)$ and g is a bijection from $f(U)^c$ to U^c. Define $h : X \to Y$ by

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

Then h is a bijection. ■

We apply CSB-theorem to prove the following important result. Also, we give different proofs of this fact.

Theorem 3.4.3. *The set* $\mathbb{N} \times \mathbb{N}$ *is equinumerous with* $\mathbb{N}$.

Proof. We already know that the function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ given by $f(n) = (n, 1)$ is one-one. Define the function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $g(m, n) = 2^m 3^n$. Note that $g(m, n) = g(r, s)$, implies that $2^{m-r} = 3^{s-n}$. Since one is a power of 2 and the other is a power of 3, their equality ensures that the indices are 0. Hence $m = r$ and $s = n$; that is, $(m, n) = (r, s)$, and thus f is one-one. By CSB-theorem, there exists a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. ■

Alternate. Define the function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $h(x, y) = 2^{x-1}(2y - 1)$. Suppose $h(x, y) = h(m, n)$. Then, $2^{x-1}(2y - 1) = 2^{m-1}(2n - 1)$. Let $x > m$. Then $2^{x-m}(2y - 1) = 2n - 1$ implies that the left hand side is an even number whereas the right hand side is an odd number; this is a contradiction. Similarly, $x < m$ leads to a contradiction. Hence $x = m$. Then the equality implies $2y - 1 = 2n - 1$ so that $y = n$. Thus, $(x, y) = (m, n)$ and hence h is a one-one function. Further, each $x \in \mathbb{N}$ can be uniquely written as $x = 2^{r-1}(2n - 1)$, for some $r, n \geq 1$. So, h is an onto function. ■

Alternate. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m, n) = (m + n - 1)(m + n - 2)/2 + n$. Since $m \geq 1, n \geq 1$, $(m + n - 1)(m + n - 2)/2 + n \geq 1$. Hence f is well defined. Write $S_0 = 0$; and for any $r \in \mathbb{N}$, write $1 + 2 + \cdots + r = S_r$. Notice that $f(m, n) = S_{m+n-2} + n$. In Example 2.3.1.2, we have shown that corresponding to each $x \in \mathbb{N}$, there exists a unique $t \in \mathbb{N} \cup \{0\}$ such that $S_t < x \leq S_{t+1}$. The existence of such a t shows that f is onto, and its uniqueness shows that f is one-one. The details are as follows.

Suppose $f(k, \ell) = f(m, n)$ for some choice of $k, \ell, m, n \in \mathbb{N}$, *i.e.*, $x := S_{k+\ell-2} + \ell = S_{m+n-2} + n$. Since $\ell \leq k + \ell - 1$ and $n \leq m + n - 1$, we have $S_{k+\ell-2} < x \leq S_{k+\ell-1}$ and $S_{m+n-2} < x \leq S_{m+n-1}$. By the uniqueness of t corresponding to x it follows that $k + \ell - 2 = m + n - 2$. Therefore $S_{k+\ell-2} = S_{m+n-2}$ and $\ell = x - S_{k+\ell-2} = x - S_{m+n-2} = n$. This, along with $k + \ell - 2 = m + n - 2$ implies that $k = m$. Hence, $(k, \ell) = (m, n)$ and consequently, f is one-one.

To show that f is onto, let $x \in \mathbb{N}$. Then there exists $t \in \mathbb{N}$ such that $S_t < x \leq S_{t+1}$. Take $n = x - S_t$. The inequality $S_t < x \leq S_{t+1}$ implies that $1 \leq n \leq t + 1$. So, take $m = t + 2 - n$. Then note that for m, n chosen as above $m \geq 1, n \geq 1, t = m + n - 2$ and $f(m, n) = S_{m+n-2} + n = S_t + n = x$. Therefore, f is an onto function. ■

The function $f(m, n)$ in the above proof is called *Cantor's pairing function.* Till now it is not known whether there exists another polynomial in m and n which is a bijection.

Example 3.4.4. We show that $\mathbb{Q}$ is equinumerous with $\mathbb{N}$. For this, write $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$, where

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

1. Prove that $\mathbb{Q}^+$ is equinumerous with $\mathbb{N}$.

   Proof. Let $p_1, p_2, \ldots$ be the infinite list of prime numbers arranged in an increasing order, that is, $p_1 = 2, p_2 = 3, p_3 = 5$, etc. The *prime factorization theorem* asserts that each $n \in \mathbb{N}$ can be written uniquely as $n = p_1^{a_1} p_2^{a_2} \cdots$, where $a_i \in \mathbb{N}$ only for a finite number of p_i's, and the rest of a_i's are 0. Hence each $q \in \mathbb{Q}^+$ can be written uniquely as $q = p_1^{b_1} p_2^{b_2} \cdots$, where $b_i \in \mathbb{Z} \setminus \{0\}$ only for a finite number of p_i's, and the rest of b_i's are 0. Let $f : \mathbb{N} \to \mathbb{Z}$ be a bijection such as $f(n) = -n/2$ if n is even, and $f(n) = (n+1)/2$ if n is odd. Define $g : \mathbb{N} \to \mathbb{Q}^+$ by $g(n) = p_1^{f(a_1)} p_2^{f(a_2)} \cdots$ for $n = p_1^{a_1} p_2^{a_2} \cdots$. Then g is a bijection.

2. Use the above to conclude that $\mathbb{Q}^-$ is equinumerous with $\mathbb{N}$.

   Ans: The function $h : \mathbb{Q}^+ \to \mathbb{Q}^-$ given by $h(q) = -q$ is a bijection. Using Part 1, we see that $h \circ g : \mathbb{N} \to \mathbb{Q}^-$ is a bijection.

3. Use the above two parts to conclude that $\mathbb{Q}$ is equinumerous with $\mathbb{N}$.

   Ans: Let $A = \{2n : n \in \mathbb{N}\}$, $B = \{2n+1 : n \in \mathbb{N}\}$. Then $\mathbb{N} = A \cup B \cup \{1\}$. Define $\phi_1 : A \to \mathbb{N}$ by $\phi_1(n) = n/2$, and $\phi_2 : B \to \mathbb{N}$ by $\phi_2(n) = (n-1)/2$. Let $g : \mathbb{N} \to \mathbb{Q}^+$ and $h : \mathbb{Q}^+ \to \mathbb{Q}^-$ be the bijections given in Parts 1 and 2. Then $g \circ \phi_1$ is a bijection from A to $\mathbb{Q}^+$, and $h \circ g \circ \phi_2$ is a bijection from B to $\mathbb{Q}^-$. We see that the following function $\psi : \mathbb{N} \to \mathbb{Q}$ is a bijection:

$$\psi(x) = \begin{cases} (g \circ \phi_1)(x) & \text{if } x \in A \\ (h \circ g \circ \phi_2)(x) & \text{if } x \in B \\ 0 & \text{if } x = 1. \end{cases}$$

Exercise **3.4.5.**

1. *For each of the exercises in Exercise 3.3.4, give injections. Then use the CSB-theorem to prove that all the sets are equinumerous.*

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

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

   Show that f is one-one. Apply CSB-theorem to prove that $\mathbb{Q}$ is equinumerous with $\mathbb{N}$.

3. *Let $X = \{(x,y) \in \mathbb{N} \times \mathbb{N} : y \le x\}$.*

   (a) *Define a function $f : \mathbb{N} \times \mathbb{N} \to X$ by $f(x,y) = (x+y-1, y)$. Prove that f is a bijection.*

   (b) *Further, define $g : X \to \mathbb{N}$ by $g(x,y) = \frac{x(x-1)}{2} + y$. Prove that g is a bijection.*

   Note that $g \circ f$ is a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. Is this function the same as Cantor's pairing function?

3.5 Countable and uncountable sets

As we have seen $\mathbb{N} \times \mathbb{N}$ and $\mathbb{Q}$ are equinumerous with $\mathbb{N}$. By induction it follows that $\mathbb{N}^k$, that is the product of $\mathbb{N}$ with itself taken k times, for any natural number k, is also equinumerous with $\mathbb{N}$. Does it mean that every infinite set is equinumerous with $\mathbb{N}$? With the hope of discovering an answer to this question, we introduce some related notions.

Definition 3.5.1. 1. A set which is equinumerous with $\mathbb{N}$ is called a **denumerable** set. A denumerable set is also called a **countably infinite** set.

2. A set which is either finite or denumerable is called a **countable** set.
3. A set which is not countable is called an **uncountable** set.

Since the identity function on $\mathbb{N}$ is a bijection, it follows that $\mathbb{N}$ is denumerable. Each finite set such as $\varnothing$ and $[m]$, for some $m \in \mathbb{N}$, are countable; so is $\mathbb{N}$.

Example 3.5.2.

1. Define $f : \mathbb{N} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{N}$, respectively by

$$f(x) = \begin{cases} -x/2 & \text{if } x \text{ is even} \\ (x-1)/2 & \text{if } x \text{ is odd,} \end{cases} \qquad g(x) = \begin{cases} -2z & \text{if } z \text{ is negative} \\ 1+2z & \text{if } z \text{ is non-negative.} \end{cases}$$

   Then, we see that $g \circ f$ and $f \circ g$ are identity functions on their respective domains. Hence f is a bijection. Therefore, $\mathbb{Z}$ is denumerable; and also countable.

2. By Theorem 3.4.3, there is a bijection from $\mathbb{N} \times \mathbb{N}$ onto $\mathbb{N}$. Thus, $\mathbb{N} \times \mathbb{N}$ is denumerable, and countable.
3. By Example 3.4.4, $\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{Q}$ are denumerable, and countable.

Before exploring other examples, we will give simpler characterizations of these notions.

Theorem 3.5.3. *Let X be a nonempty set.*

1. *X is countable if and only if there exists a one-one function $f : X \to \mathbb{N}$.*
2. *X is denumerable if and only if there exist one-one functions $f : X \to \mathbb{N}$ and $g : \mathbb{N} \to X$.*

Proof. 1. Let X be a countable set. If X is finite, then there exists a bijection $f : X \to [m]$ for some $m \in \mathbb{N}$. This bijection gives a one-one function $f : X \to \mathbb{N}$. Else, X is denumerable, so that there is a bijection $g : X \to \mathbb{N}$. In this case, the function g is one-one. Conversely, suppose there exists a one-one function $f : X \to \mathbb{N}$. If X is finite, then it is countable. So, suppose that X is infinite. Then, by Theorem 3.1.4.2, there exists a one-one function $g : \mathbb{N} \to X$. By CSB-theorem, there exists a bijection $h : X \to \mathbb{N}$. Hence X is denumerable; thus countable.

2. Let X be a denumerable set. By definition there is a bijection $f : X \to \mathbb{N}$. Thus, $f : X \to \mathbb{N}$ and $f^{-1} : \mathbb{N} \to X$ are one-one functions. Conversely, suppose there exist one-one functions $f : X \to \mathbb{N}$ and $g : \mathbb{N} \to X$. Then, by CSB-theorem, there exists a bijection $h : X \to \mathbb{N}$. Hence X is denumerable. ■

Definition 3.5.4.

1. Let X be a denumerable set. Then, there is a bijection $f : \mathbb{N} \to X$. So, we can list all the elements of X as $f(1), f(2), \ldots$. This list is called an **enumeration** of the elements of X.
2. Let X be a nonempty set. An infinite **sequence** of elements of X is a function $f : \mathbb{N} \to X$. Writing $f(i) = x_i$, such a sequence is represented by $(x_i)_{i \in \mathbb{N}} = (x_1, x_2, \ldots)$, where $x_i \in X$.

In the proof of Theorem 1, Part 2, we have essentially extracted an infinite sequence from the infinite set X.

Since $\mathbb{Z}$ is denumerable, its elements can be enumerated. For example, $0, 1, -1, 2, -2, 3, -3, \ldots$ is an enumeration of $\mathbb{Z}$. Similarly, all rational numbers can be enumerated; and sometimes we write such an enumeration of $\mathbb{Q}$ by $r_1,\ r_2,\ r_3,\ \ldots$. It says that there is a sequence $\big(r_1, r_2, r_3, \ldots\big)$ in which each rational number occurs exactly once. This is what an enumeration means. If X is a countable set, then its elements can be enumerated in a sequence; but the sequence can be finite or infinite.

By a denumerable family of sets, we mean a family of sets which is denumerable. A denumerable family of sets can be indexed by $\mathbb{N}$ and we may write such a family as $\{A_i\}_{i\in\mathbb{N}}$. We also use the same notation for a countable family, where possibly only a finite number of sets A_i are nonempty. The union of sets in a countable family will be referred to as *a countable union* of sets.

Notice that a countable infinite set is denumerable. Besides this, some more facts about countable sets are listed in the following proposition.

Proposition 3.5.5. **[Facts about countable sets]**

1. *Each subset of a denumerable set is countable.*
2. *Each infinite subset of a denumerable set is denumerable.*
3. *A set is infinite if and only if it has a denumerable subset.*
4. *Any subset of a countable set is countable; and any superset of an uncountable set is uncountable.*
5. *A countable union of countable sets is countable.*
6. *For any $k \in \mathbb{N}$, the Cartesian product $\mathbb{N}^k$ is denumerable.*
7. *A finite product of countable sets is countable.*

Proof. (1) Let $X \subseteq Y$, where Y is denumerable. There exists a bijection $f : Y \to \mathbb{N}$. The identity function $\mathbf{Id} : X \to Y$ is one-one. So, $f \circ \mathbf{Id} : X \to \mathbb{N}$ is one-one.

(2) Let X be an infinite subset of a denumerable set. By (1), X is countable. So, X is countably infinite, same as denumerable.

(3) Let X be an infinite set. Then, by Theorem 3.5.3, there is a one-one function $f : \mathbb{N} \to X$. Thus, $f : \mathbb{N} \to \mathsf{rng}\, f$ is a bijection. Hence, $\mathsf{rng}\, f$ is a denumerable subset of X.

Conversely, let X be a set and let $Y \subseteq X$ be denumerable. There exists a bijection $f : Y \to \mathbb{N}$. The function $f^{-1} : \mathbb{N} \to X$ is one-one. By Theorem 3.1.4, X is an infinite set.

(4) Let X be a countable set and let $Y \subseteq X$. If $Y = \varnothing$, then it is finite, thus countable. So, suppose that $Y \neq \varnothing$. As X is countable, by Theorem 3.5.3, there exists a one-one function $f : X \to \mathbb{N}$. The restriction of f to Y is also a one-one function from Y to $\mathbb{N}$. Hence Y is countable.

Let X be an uncountable set and let $Y \supseteq X$. If X is countable, then by what we have just proved, X would be countable. Hence, Y is uncountable.

(5) Let $\{A_i\}_{i\in\mathbb{N}}$ be a countable family of sets, where each A_i is a countable set. Write $X = \underset{i\in\mathbb{N}}{\cup} A_i$. We show that X is countable.

If X is finite, then it is countable. So, let X be infinite. By Theorem 3.1.4.2, there is a one-one function $f : \mathbb{N} \to X$. Now, let $x \in X$. Then, there exists at least one $i \in \mathbb{N}$ such that $x \in A_i$. Further, since A_i is countable, we may assume that A_i has been enumerated. So, suppose x appears at the kth position in this enumeration of A_i. Thus, corresponding to each $x \in X$, we have a unique pair (i, k) of natural numbers. Define $g : X \to \mathbb{N}$ by $g(x) = 2^i 3^k$, where i is the smallest natural number 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. Therefore, by

CSB-theorem, A is equinumerous with $\mathbb{N}$.

(6) For $k = 1$, the result is obvious. Suppose the result is true for $k = m$. That is, there exists a bijection $f : \mathbb{N}^m \to \mathbb{N}$. From Theorem 3.4.3, we have a bijection $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Define $h : \mathbb{N}^{m+1} \to \mathbb{N}$ by $h(x_1, \ldots, x_m, x_{m+1}) = g\big(f(x_1, \ldots, x_m), x_{m+1}\big)$. Then h is a bijection. Thus, by the PMI the result holds.

Alternate. The function $f : \mathbb{N} \to \mathbb{N}^k$ given by $f(m) = (m, 1, \ldots, 1)$ is one-one. Next, let $p_1, \ldots, p_k$ be the first k number of primes, *i.e.*, $p_1 = 2, p_2 = 3$, etc. Define $g : \mathbb{N}^k \to \mathbb{N}$ by $g(m_1, \ldots, m_k) = p_1^{m_1-1} p_2^{m_2-1} \cdots p_k^{m_k-1}$. The prime factorization theorem implies that g is one-one. So, by CSB-theorem, there exists a bijection from $\mathbb{N}^k \to \mathbb{N}$.

(7) Let $A_1, \ldots, A_k$ be countable sets. We need to show that $X := A_1 \times \cdots \times A_k$ is countable. If any $A_i = \varnothing$, then $X = \varnothing$; thus it is countable. So, assume that each A_i is nonempty. Since A_i is countable, there exists a one-one function $f_i : A_i \to \mathbb{N}$. Then the function $f : X \to \mathbb{N}^k$ defined by $f(x_1, \ldots, x_k) = \big(f_1(x_1), \ldots, f_k(x_k)\big)$ is one-one. Let $g : \mathbb{N}^k \to \mathbb{N}$ be the one-one function given in (6). Then $g \circ f : X \to \mathbb{N}$ is a one-one function. ■

We now address the question whether all infinite sets are denumerable or not. Its answer is hidden in Cantor's experiment, which we present in the following. Recall that if X is a set, then its power set $\mathcal{P}(X)$ denotes the set of all subsets of X.

Cantor's experiment: Take a blank sheet of 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 larger 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 $Y = \{i \,:\, i \notin f(i)\}$. Locate this set on the right.
4. It is guaranteed that you do not have a directed line touching Y. Why?

Theorem 3.5.6. **[Cantor]** *There exists no surjection from a set to its power set.*

Proof. On the contrary, let X be a set and let $f : X \to \mathcal{P}(X)$ be an onto function. For each $x \in X$, $f(x) \subseteq X$. Consider the set $Y = \{x \in X : x \notin f(x)\}$. Since $Y \in \mathcal{P}(X)$ and f is onto, there exists $s \in X$ with $f(s) = Y$.

If $s \in Y$, then s satisfies the defining property of Y, *i.e.*, $s \notin f(s)$. As $f(s) = Y$, $s \notin Y$.

If $s \notin Y$, then $f(s) = Y$ gives $s \notin f(s)$. So, s satisfies the defining property of Y, and hence $s \in Y$.

We thus see that $s \in Y$ if and only if $s \notin Y$. This is a contradiction. ■

Remark 3.5.7. Cantor's theorem implies that one cannot have a bijection between a set and its power set. In particular, the sets $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ cannot be equinumerous. However, $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ given by $f(x) = \{x\}$ is one-one. Thus the set $\mathcal{P}(\mathbb{N})$ is infinite but not denumerable, *i.e.*, by Definition 3.5.1, $\mathcal{P}(\mathbb{N})$ is an uncountable set. It follows that any set equinumerous with $\mathcal{P}(\mathbb{N})$ is uncountable. In general, the following result holds.

Theorem 3.5.8. *The power set of any infinite set is uncountable.*

Proof. Let X be an infinite set. By Theorem 3.1.4, there exists a one-one function $f : \mathbb{N} \to X$. Define the function $g : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(X)$ by

$$g(A) = \{f(i) : i \in A\} \text{ for each } A \in \mathcal{P}(\mathbb{N}).$$

Then, g is one-one. As Remark 3.5.7 shows, $\mathcal{P}(\mathbb{N})$ is uncountable. Thus $g\big(\mathcal{P}(\mathbb{N})\big)$ is uncountable. The set $\mathcal{P}(X)$, being a superset of $g\big(\mathcal{P}(\mathbb{N})\big)$, is uncountable. ∎

Example 3.5.9.

1. Let X be the family of all functions $x : \mathbb{N} \to \{0, 1\}$. Equivalently, let

$$X = \big\{x : x = (x_1, x_2, \ldots),\ x_i \in \{0, 1\} \text{ for each } i \in \mathbb{N}\big\},$$

   the set of all 0-1 sequences. Define $f : X \to \mathcal{P}(\mathbb{N})$ by

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

   Then f is a bijection. Hence, X is uncountable.

2. Let $Y = \big\{.a_1a_2a_3\cdots : a_i \in \{0, 1\} \text{ for each } i \in \mathbb{N}\big\}$. It follows from (1) that X is uncountable. We give another proof by Cantor.

   Cantor's diagonalization: On the contrary, suppose Y is countable. Clearly Y is not finite. So, let $x_1, x_2, \cdots$ be an enumeration of Y. Let $x_n = .x_{n1}x_{n2}\cdots$, where $x_{ni} \in \{0, 1\}$. We construct the numbers y_n as follows:

   If $x_{nn} = 0$, then take $y_n = 1$; otherwise, take $y_n = 0$.

   Now, consider the number $y = .y_1y_2\cdots \in X$. Notice that for each n, $y \neq x_n$, *i.e.*, $y \in Y$ but it is not in the enumeration of Y. This is a contradiction.

   Recall that every real number in the interval $[0, 1)$ has a unique non-terminating binary representation, and also a non-terminating decimal representation. Thus we have shown that $[0, 1)$ is an uncountable set.

Theorem 3.5.10. *The set $\mathcal{P}(\mathbb{N})$ is equinumerous with $[0, 1)$ and also with $\mathbb{R}$.*

Proof. By Example 3.5.9, there exists a one-one function $f : \mathcal{P}(\mathbb{N}) \to [0, 1)$. Let $r \in (0, 1)$. Consider the non-terminating binary representation of r. Denote by F_r the set of positions of 1 in this representation. Define $g : [0, 1) \to \mathcal{P}(\mathbb{N})$ by $g(0) = \varnothing$, and $g(r) = F_r$ if $r \neq 0$. Then g is one-one. Therefore, by CSB-theorem, $\mathcal{P}(\mathbb{N})$ is equinumerous with $[0, 1)$.

The next statement follows as $[0, 1)$ is equinumerous with $(0, 1)$ (see Exercise 3.3.4.1) and $(0, 1)$ is equinumerous with $\mathbb{R}$ (see Practice 3.3.1.4). ∎

Exercise **3.5.11.**

1. *Let X be a nonempty set. Prove by two methods that there is no injection from $\mathcal{P}(X)$ to X; once by using CSB-theorem and once without using it.*
2. *Give a bijection from $\mathbb{R}$ to $\mathbb{R} \setminus \mathbb{Q}$.*
3. *Write $\mathbb{R}$ as a union of pairwise disjoint sets of size 5.*
4. *Supply a bijection from $(0, 1)$ to $(1, 2) \cup (3, 4) \cup (5, 6) \cup (7, 8) \cup \cdots$.*
5. *Show using CSB-theorem that $(0, 1)$ is equinumerous with $(0, 1]$.*

6. *Show that* $(0, 1)$ *is equinumerous with* $(0, 1) \times (0, 1)$*; and that* $\mathbb{R} \times \mathbb{R}$ *is equinumerous with* $\mathbb{R}$.

7. *Let* $A_1, A_2, \ldots$ *be an infinite sequence of nonempty sets such that* A_k *is a proper superset of* A_{k+1} *for each* $k \in \mathbb{N}$*. Show that* A_1 *is an infinite set.*

8. *Let* X *be a set such that* $f : \mathbb{N} \to X$ *is an onto function. Then prove that* X *is countable.*

9. *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* $x_{k+1} = x_{k+2} = \cdots$*'. Is* S *countable?*

10. *Let* S *be the set of all decreasing*[1] *sequences made with natural numbers. Is* S *countable?*

11. *Let* S *be the set of all increasing sequences made with natural numbers. Is* S *uncountable?*

12. *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*?*

13. *A complex number is called* **algebraic** *if it is a root of a polynomial equation with integer coefficients. All other complex numbers are called* **transcendental**.
    (a) *Show that the set of algebraic numbers is countable.*
    (b) *Show that the set of transcendental numbers is uncountable.*

14. *Fix an* $n \in \mathbb{N}$ *and let* T_n *be the set of all functions from* $\{1, 2, \ldots, n\}$ *to* $\mathbb{N}$.
    (a) *Is* T_n *a countable set?*
    (b) *Is the set* $\bigcup_{n=1}^{\infty} T_n$ *countable?*

15. *Let* X *be the set of all functions from* $\mathbb{N}$ *to* $\mathbb{N}$.
    (a) *Is* X *uncountable? Justify your answer.*
    (b) *A function* $f \in X$ *is said to be* **eventually constant** *if there exist* $m, N \in \mathbb{N}$ *such that* $f(n) = m$ *for all* $n \geq N$*. Let* $S \subseteq X$ *be the set all eventually constant functions. Is* S *countable?*

[1] A sequence (x_n) is called decreasing if $x_{m+1} \leq x_m$ for each $m \in \mathbb{N}$; increasing if $x_{m+1} \geq x_m$ for each $m \in \mathbb{N}$; strictly decreasing if $x_{m+1} < x_m$ for each $m \in \mathbb{N}$; and it is called strictly increasing if $x_{m+1} > x_m$ for each $m \in \mathbb{N}$.

Chapter 4

Elementary Number Theory

4.1 Division algorithm and its applications

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

Lemma 4.1.1. [**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 $0 \leq r < b$. The integer q is called the* **quotient** *and r, the* **remainder**.

Proof. Existence: Take $S = \{a + bx | x \in \mathbb{Z}\} \cap \mathbb{W}$. Then $a + |a|b \in S$. Hence, S is a nonempty subset of $\mathbb{W}$. Therefore, by the well ordering principle, S contains its minimum, say s_0. So, $s_0 = a + bx_0$, for some $x_0 \in \mathbb{Z}$. Since $s_0 \in \mathbb{W}, s_0 \geq 0$.

If $s_0 \geq b$ then $0 \leq s_0 - b = a + b(x_0 - 1) \in S$. This contradicts the minimality of s_0. Hence $0 \leq s_0 < b$. Take $q = -x_0$ and $r = s_0$. Then $qb + r = -x_0 b + s_0 = -x_0 b + a + bx_0 = a$, *i.e.*, 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 $a = q_1 b + r_1$, $0 \leq r_1 < b$, $a = q_2 b + r_2$, and $0 \leq r_2 < b$. Suppose $r_1 < r_2$. Then $0 < r_2 - r_1 < b$. Notice that $r_2 - r_1 = (q_1 - q_2)b$. So, $0 < (q_1 - q_2)b < b$. This is a contradiction since $(0, b)$ does not contain any integer which is a multiple of b. Similarly, $r_2 < r_1$ leads to a contradiction. Therefore, $r_1 = r_2$. Then, $0 = r_1 - r_2 = (q_1 - q_2)b$ and $b \neq 0$ imply that $q_1 = q_2$. ■

Definition 4.1.2. 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** a and we write $b|a$ (read as b divides a.) When $b|a$, we also say that b is a **divisor** of a, and that a is a **multiple** of b.

Remark 4.1.3. Let a be a nonzero integer. If b is a positive divisor of a, then $1 \leq b \leq |a|$. Hence the set of all positive divisors of a nonzero integer is a nonempty finite set.

Further, if a is a positive integer and b is a positive divisor of a, then $a = kb$ for some $k \in \mathbb{N}$ so that $b \leq a$. It then follows that if $a, b \in \mathbb{N}$ such that $a|b$ and $b|a$, then $a = b$.

Definition 4.1.4.

1. 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 by $\gcd(a, b)$. The gcd is also called the **highest common factor**.

2. An integer a is said to be **relatively prime** to an integer b if $\gcd(a, b) = 1$. In this case, we also say that the integers a and b are **coprimes**.

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

Theorem 4.1.5. **[Bézout's identity]** *Let a and b be two nonzero integers and let $d = \gcd(a, b)$. Then there exist integers x_0, y_0 such that $d = ax_0 + by_0$.*

Proof. Consider the set $S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Then, either $a \in S$ or $-a \in S$. Thus, S is a nonempty subset of $\mathbb{N}$. By the 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 show that $d = \gcd(a, b)$.

By the division algorithm, there exist integers q and r such that $a = dq + r$, with $0 \le r < d$. If $r > 0$, then

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

In this case, r is a positive integer in S which is strictly less than d. This contradicts the choice of d as the least element of S. Thus, $r = 0$. Consequently, $d|a$. Similarly, $d|b$. Hence $d \le \gcd(a, b)$.

Now, $\gcd(a, b)|a$ and $\gcd(a, b)|b$. Since $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$, we have $\gcd(a, b)|d$. That is, $d = k \times \gcd(a, b)$ for some integer k. However, both $\gcd(a, b)$ and d are positive. Thus k is a positive integer. Hence $d \ge \gcd(a, b)$.

Therefore, $d = \gcd(a, b)$. ∎

We prove three useful corollaries to Bézout's identity.

Corollary 4.1.6. *Let $a, b \in \mathbb{Z}$ and let $d \in \mathbb{N}$. Then, $d = \gcd(a, b)$ if and only if $d|a$, $d|b$, and each common divisor of a and b divides d.*

Proof. Suppose $d = \gcd(a, b)$. Then $d|a$ and $d|b$. By Bézout's identity, $d = ak + bm$ for some $k, m \in \mathbb{Z}$. Thus, any common divisor of a and b divides $d = \gcd(a, b)$.

Conversely, suppose $d|a$, $d|b$ and each common divisor of a and b divides d. Since d is a common divisor of a and b, by what we have just proved, $d|\gcd(a, b)$. Further, $\gcd(a, b)$ is a common divisor of a and b; so, by assumption $\gcd(a, b)|d$. By Remark 4.1.3, $d = \gcd(a, b)$. ∎

Corollary 4.1.7. *Let a, b be nonzero integers. Then $\gcd(a, b) = 1$ if and only if there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$.*

Proof. If $\gcd(a, b) = 1$, then by Bézout's identity, there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. Conversely, suppose there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. If $\gcd(a, b) = k$, then k is a positive integer such that $k|1$. It follows that $k \le 1$; consequently, $k = 1$. ∎

Corollary 4.1.8. *Let $n_1, \ldots, n_k$ be positive integers which are pairwise coprimes. If $a \in \mathbb{Z}$ is such that $n_1|a, \ldots, n_k|a$, then $n_1 \cdots n_k|a$.*

Proof. The positive integers $n_1, \ldots, n_k$ are pair wise coprimes means that if $i \ne j$, then $\gcd(n_i, n_j) = 1$. Let $a \in \mathbb{Z}$ be such that $n_1|a, \ldots, n_k|a$. We show by induction that $n_1 \cdots n_k|a$. For $k = 2$, it is given that $n_1|a$, $n_2|a$ and $\gcd(n_1, n_2) = 1$. By Bézout's identity, there exist $x, y \in \mathbb{Z}$ such that $n_1x + n_2y = 1$. Multiplying by a, we have $a = an_1x + an_2y = n_1n_2\big(x(\frac{a}{n_2}) + y(\frac{a}{n_1})\big)$.
Since $n_2|a$ and $n_1|a$, we see that $\frac{a}{n_2}$, $\frac{a}{n_1} \in \mathbb{Z}$ so that $\big(x(\frac{a}{n_2}) + y(\frac{a}{n_1})\big) \in \mathbb{Z}$. Hence $n_1n_2|a$.

Assume the induction hypothesis that the statement is true for $k = m$. Let each of $n_1, \ldots, n_{m+1}$ divide a and that they are pairwise coprimes. Let $n_1 \cdots n_m = \ell$. Then $\gcd(\ell, n_{m+1}) = 1$. By the induction hypothesis, $\ell|a$. By the basis case, ($k = 2$ as proved), we conclude that $\ell\, n_{m+1}|a$. That is, $n_1 \cdots n_{m+1}|a$. ∎

The division algorithm helps to algorithmically compute the greatest common divisor of two nonzero integers, commonly known as the Euclid's algorithm.

Let a, and b be nonzero integers. By the division algorithm, there exists integers q and r with $0 \le r < |b|$ such that $a = |b|q + r$. We apply our observation that a common divisor of two integers divides their gcd.

Now, $\gcd(|b|, r)$ divides both $|b|$ and r; hence it divides a. Again, $\gcd(|b|, r)$ divides both a and $|b|$. Hence $\gcd(|b|, r) \mid \gcd(a, |b|)$.

Similarly, with $r = a - |b|q$, we see that $\gcd(a, |b|)$ divides both a and $|b|$; hence $\gcd(a, |b|) | r$. Consequently, $\gcd(a, |b|) \mid \gcd(|b|, r)$.

Further, the gcd of any two integers is positive. Thus, $\gcd(a, b) = \gcd(a, |b|)$. So, we obtain

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

Euclid's algorithm applies this idea repeatedly to find the greatest common divisor of two given nonzero integers, which we now present.

Euclid's algorithm

Input: Two nonzero integers a and b; Output: $\gcd(a, b)$.

$$\begin{array}{lcllr}
a & = & b\,q_0 + r_0 & \text{with} & 0 \le r_0 < b \\
b & = & r_0\,q_1 + r_1 & \text{with} & 0 \le r_1 < r_0 \\
r_0 & = & r_1\,q_2 + r_2 & \text{with} & 0 \le r_2 < r_1 \\
r_1 & = & r_2\,q_3 + r_3 & \text{with} & 0 \le r_3 < r_2 \\
 & \vdots & & & \\
r_{\ell-1} & = & r_\ell\,q_{\ell+1} + r_{\ell+1} & \text{with} & 0 \le r_{\ell+1} < r_\ell \\
r_\ell & = & r_{\ell+1}\,q_{\ell+2}. & & \\
\gcd(a, b) & = & r_{\ell+1} & &
\end{array}$$

The process will take at most $b - 1$ steps as $0 \le r_0 < b$. Also, note that $r_{\ell+1}$ can be expressed in the form $r_{\ell+1} = a\,x_0 + b\,y_0$ for integers x_0, y_0 using backtracking. That is,

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

Example 4.1.9. We apply Euclid's algorithm for computing $\gcd(155, -275)$ as follows.

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

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 $d = ax + by$.

Exercise **4.1.10.** *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 dependent on 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. *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 4.1.11. 1. The integer 1 is called the **unity** (or the **unit** element) of $\mathbb{Z}$.

2. An integer $p > 1$ is called a **prime**, if p has exactly two positive divisors, namely, 1 and p.

3. An integer $r > 1$ is called **composite** if r is not a prime.

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

Lemma 4.1.12. **[Euclid's Lemma]** *Let $a, b \in \mathbb{Z}$ and let p be a prime. If $p|ab$ then $p|a$ or $p|b$.*

Proof. Suppose $p|ab$. If $p|a$, then there is nothing to prove. So, assume that $p \nmid a$. As p is a prime, $\gcd(p, a) = 1$. Thus there exist integers x, y such that $1 = ax + py$. Then $b = abx + pby$. Since $p|ab$ and $p|pb$, we see that $p|b$. ∎

One also has the following result.

Proposition 4.1.13. *Let $a, b, n \in \mathbb{Z}$ be such that $n|ab$. If $\gcd(n, a) = 1$, then $n|b$.*

Proof. Suppose $\gcd(n, a) = 1$. There exist $x_0, y_0 \in \mathbb{Z}$ such that $nx_0 + ay_0 = 1$. Then $b = aby_0 + nbx_0$. Since $n|ab$ and $n|nb$, we have $n|b$. ∎

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 4.1.14. **[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 $i \in \{1, \ldots, k\}$, $p_i = q_i$ and $s_i = t_i$.*

Proof. See Example 2.2.6 for a proof. ∎

Theorem 4.1.15. **[Euclid: Infinitude of primes]** *The number of primes is infinite.*

Proof. On the contrary assume that the number of primes is finite, say $p_1 = 2, p_2 = 3, \ldots, p_k$. Consider the positive integer $N = p_1 p_2 \cdots p_k + 1$. We see that none of the primes $p_1, p_2, \ldots, p_k$ divides N. This contradicts Theorem 4.1.14. ∎

Proposition 4.1.16. **[Primality testing]** *Let $n \in \mathbb{N}$ with $n \geq 2$. If no prime $p \leq \sqrt{n}$ divides n, then n is prime.*

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

EXERCISE **4.1.17.** 1. *Prove that there are infinitely many primes of the form $4n - 1$.*

2. *Fix $N \in \mathbb{N}, N \ge 2$. Then, there exists a consecutive set of N natural numbers that are composite.*

Definition 4.1.18. The **least common multiple** of integers a and b, denoted as $\mathsf{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

Lemma 4.1.19. *Let $a, b \in \mathbb{Z}$ and let $\ell \in \mathbb{N}$. Then, $\ell = \mathsf{lcm}(a, b)$ if and only if $a|\ell$, $b|\ell$ and ℓ divides each common multiple of a and b.*

Proof. Let $\ell = \mathsf{lcm}(a, b)$. Clearly, $a|\ell$ and $b|\ell$. Let x be a common multiple of both a and b. If $\ell \nmid x$, then by the division algorithm, $x = \ell \cdot q + r$ for some integer q and some r with $0 < r < \ell$. Notice that $a|x$ and $a|\ell$. So, $a|r$. Similarly, $b|r$. That is, r is a positive common multiple of both a and b which is less than $\mathsf{lcm}(a, b)$. This is a contradiction. Hence, $\ell = \mathsf{lcm}(a, b)$ divides each common multiple of a and b.

Conversely, suppose $a|\ell$, $b|\ell$ and ℓ divides each common multiple of a and b. By what we have just proved, $\mathsf{lcm}(a, b)|\ell$. Further, $\mathsf{lcm}(a, b)$ is a common multiple of a and b. Thus $\ell|\,\mathsf{lcm}(a, b)$. By Remark 4.1.3, we conclude that $\ell = \mathsf{lcm}(a, b)$. ∎

Theorem 4.1.20. *Let $a, b \in \mathbb{N}$. Then $\gcd(a, b) \cdot \mathsf{lcm}(a, b) = ab$. In particular, $\mathsf{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.*

Proof. Let $d = \gcd(a, b)$. Then $a = a_1 d$ and $b = b_1 d$ for some $a_1, b_1 \in \mathbb{N}$. Further,

$$ab = a_1 d\, b_1 d = (a_1 b_1 d) \cdot \gcd(a, b).$$

Thus, it is enough to show that $\mathsf{lcm}(a, b) = a_1 b_1 d$.

Towards this, notice that $a_1 b_1 d = a b_1 = a_1 b$, that is, $a|a_1 b_1 d$ and $b|a_1 b_1 d$. Let $c \in \mathbb{N}$ be any common multiple of a and b. Then $\frac{c}{a}, \frac{c}{b} \in \mathbb{Z}$. Further, by Bézout's identity, $d = as + bt$ for some $s, t \in \mathbb{Z}$. So,

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

Hence $a_1 b_1 d | c$. That is, $a_1 b_1 d$ divides each common multiple of a and b. By Lemma 4.1.19, $a_1 b_1 d = \mathsf{lcm}(a, b)$. ∎

4.2 Modular arithmetic

Definition 4.2.1. Fix a positive integer n. Let $a, b \in \mathbb{Z}$. If n divides $a - b$, we say that a is **congruent** to b modulo n, and write $a \equiv b \pmod{n}$.

Example 4.2.2. 1. Notice that $2|(2k - 2m)$ and also $2|[(2k - 1) - (2m - 1)]$. Therefore, any two even integers are congruent modulo 2; and any two odd integers are congruent modulo 2.

2. The numbers ± 10 and 22 are congruent modulo 4 as $4|(22 - 10)$ and $4|(22 - (-10))$.

3. Let n be a fixed positive integer. Recall the notation $[n - 1] := \{0, 1, 2, \ldots, n - 1\}$.

   (a) Then, by the division algorithm, for any $a \in \mathbb{Z}$ there exists a unique $b \in [n - 1]$ such that $a \equiv b \pmod{n}$. The number b is called the **residue** of a modulo n.

(b) Further $\mathbb{Z} = \bigcup\limits_{a=0}^{n-1} \{a + kn : k \in \mathbb{Z}\}$, *i.e.*, every integer is congruent to an element of $[n-1]$. The set $[n-1]$ is taken as the **standard representative** for the set of residue classes modulo n.

Theorem 4.2.3. *Fix $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$. Then the following are true:*

1. *If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*
2. *If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$, $a - c \equiv b - c \pmod{n}$ and $ac \equiv bc \pmod{n}$.*
3. *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$ and $ac \equiv bd \pmod{n}$. In particular, $a \equiv b \pmod{n}$ implies $a^m \equiv b^m \pmod{n}$ for all $m \in \mathbb{N}$.*
4. *If $ac \equiv bc \pmod{n}$ for nonzero a, b, c, and $d = \gcd(c, n)$, then $a \equiv b \pmod{n/d}$. In particular, if $ac \equiv bc \pmod{n}$ for nonzero a, b, c, and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.*

Proof. We will only prove two parts. The readers should supply the proof of other parts.
3. Note that $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$. Thus, $n|ac - bd$, whenever $n|a - b$ and $n|c - d$. 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 $m \in \mathbb{N}$.

4. Let $\gcd(c, n) = d$. Then, there exist nonzero $c_1, n_1 \in \mathbb{Z}$ with $c = c_1 d, n = n_1 d$. Then $n|ac - bc$ implies $n_1 d | c_1 d(a - b)$, which implies $n_1 | c_1(a - b)$. By Proposition 4.1.13, $n_1 | a - b$, *i.e.*, $\frac{n}{\gcd(c,n)} | a - b$. ∎

Example 4.2.4. 1. Note that $3 \cdot 9 + 13 \cdot (-2) \equiv 1 \pmod{13}$. If x satisfies $9x \equiv 4 \pmod{13}$ then

$$\begin{aligned} x \equiv x \cdot 1 \equiv x \cdot (3 \cdot 9 + 13 \cdot (-2)) & & \text{as } 3 \cdot 9 + 13 \cdot (-2) \equiv 1 \pmod{13} \\ \equiv 3 \cdot 9x & & \text{as } 13 \equiv 0 \pmod{13} \\ \equiv 3 \cdot 4 & & \text{as } 9x \equiv 4 \pmod{13} \\ \equiv 12 \pmod{13}. & & \end{aligned}$$

To verify, if $x \equiv 12 \pmod{13}$, then $9x \equiv 108 \equiv (13 \times 8 + 4) \equiv 4 \pmod{13}$. Therefore, the congruence equation $9x \equiv 4 \pmod{13}$ has solution $x \equiv 12 \pmod{13}$.

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

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

3. Verify that the equation $3x \equiv 15 \pmod{30}$ has solutions $x = 5, 15, 25$; where as the equation $7x = 15 \pmod{30}$ has only one solution $x = 15$; and that the equation $3x \equiv 5 \pmod{30}$ has no solution.

Theorem 4.2.5. **[Linear Congruence]** *Let n be a positive integer and let a, b be nonzero integers. Then the congruence equation $ax \equiv b \pmod{n}$ has at least one solution if and only if $\gcd(a, n)|b$. Moreover, if $d = \gcd(a, n)|b$, then $ax \equiv b \pmod{n}$ has exactly d number of solutions $r_1, \ldots, r_d \in \{0, 1, 2, \ldots, n-1\}$, where $r_i \equiv r_j \pmod{n/d}$ for all $i, j = 1, 2, \ldots, d$.*

Proof. Write $d = \gcd(a, n)$. 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, $b = ax_0 - nq$. Since $d|a$ and $d|n$, we have $d|ax_0 - nq = b$.

Conversely, suppose $d|b$. Then, $b = b_1 d$, for some $b_1 \in \mathbb{Z}$. By Bézout's identity, there exist $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + ny_0 = d$. Hence,

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

That is, $x_0 b_1$ is a solution of $ax \equiv b \pmod{n}$. This proves the first statement.

To proceed further, assume that $d|b$. By what we have just proved, there exists a solution x_1 of $ax \equiv b \pmod{n}$. By the division algorithm, there exist $p, r \in \mathbb{Z}$ with $0 \le r < n$ such that $x_1 = pn + r$. Now, $ar \equiv a(x_1 - pn) \equiv ax_1 \equiv b \pmod{n}$. Thus, r is also a solution of $ax \equiv b \pmod{n}$, *i.e.*, there exists $r \in \{0, 1 \ldots, n-1\}$ satisfying $ar \equiv b \pmod{n}$.

If $x_2 \in \{0, 1, \ldots, n-1\}$ is any other solution of $ax \equiv b \pmod{n}$, then $ax_2 \equiv b \equiv ar \pmod{n}$. Thus, by Theorem 4.2.3.4, $x_2 \equiv r \pmod{n/d}$. Conversely, if $x_2 \equiv r \pmod{n/d}$, then $x_2 = r + m(n/d)$ for some $m \in \mathbb{Z}$. Then $ax_2 = ar + am(n/d) = ar + mn(a/d)$. as $d|a$, the number a/d is an integer. Hence, $ax_2 \equiv ar \pmod{n}$ so that x_2 is a solution of $ax \equiv b \pmod{n}$.

Therefore, all solutions of $ax \equiv b \pmod{n}$ in $\{0, 1, \ldots, n-1\}$ are of the form $r + k(n/d)$ for $k \in \mathbb{Z}$. However, there are exactly d number of integers in $\{0, 1, \ldots, n-1\}$ which are congruent to r modulo (n/d). Hence there are d number of solutions of $ax \equiv b \pmod{n}$ in $\{0, 1, \ldots, n-1\}$. ■

Remark 4.2.6. Observe that a solution of the congruence $ax \equiv b \pmod{n}$ is a number in $\{0, 1, \ldots, n-1\}$. This set is not to be confused with the congruence class $[n-1]$. When $d = \gcd(a, n)$, we may write the distinct solutions in $[n-1]$ in increasing order as $r_1 = r, r_2 = r + n/d, r_3 = r + 2n/d, \ldots, r_d = r + (d-1)n/d$. It means that the solutions are $x_i \equiv r_i \pmod{n}$ for $i = 1, 2, \ldots, d$.

Exercise **4.2.7.**

1. *Complete the proof of Theorem 4.2.3.*
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. *Consider the congruence pair* $3x \equiv 4 \pmod{28}$ *and* $4x \equiv 2 \pmod{27}$.
   (a) *Prove that the given pair is equivalent to the pair* $x \equiv 20 \pmod{28}$ *and* $x \equiv 14 \pmod{27}$.
   (b) *Prove that solving the congruence pair in (a) is equivalent to solving one of the congruences* $20 + 28k \equiv 14 \pmod{27}$ *or* $14 + 27k \equiv 20 \pmod{28}$ *for the unknown quantity* k.
   (c) *Verify that* $k = 21$ *is the solution for the first case in (b) and* $k = 22$ *for the second case.*
   (d) *Conclude that* $x = 20 + 28 \cdot 21 = 14 + 27 \cdot 22$ *is a solution for the given congruence pair.*
6. *Prove that if* p *is a prime, then* $p|C(p,k) := \dfrac{p!}{k!(p-k)!}$ *for* $1 \le k \le p-1$.

---

7. *Let* p *be a prime. Write* $\mathbb{Z}_p := \{0, 1, 2, \ldots, p-1\}$ *and* $\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\} = \mathbb{Z}_p \setminus \{0\}$. *Show that* $\mathbb{Z}_p$ *has the following properties:*
   (a) *For all* $a, b \in \mathbb{Z}_p$, $a + b \pmod{p} \in \mathbb{Z}_p$.
   (b) *For all* $a, b \in \mathbb{Z}_p$, $a + b = b + a \pmod{p}$.
   (c) *For all* $a, b, c \in \mathbb{Z}_p$, $a + (b + c) \equiv (a + b) + c \pmod{p}$.
   (d) *For all* $a \in \mathbb{Z}_p$, $a + 0 \equiv a \pmod{p}$.
   (e) *For all* $a \in \mathbb{Z}_p$, $a + (p - a) \equiv 0 \pmod{p}$.
   (f) *For all* $a, b \in \mathbb{Z}_p^*$, $a \cdot b \pmod{p} \in \mathbb{Z}_p^*$.
   (g) *For all* $a, b \in \mathbb{Z}_p^*$, $a \cdot b = b \cdot a \pmod{p}$.
   (h) *For all* $a, b, c \in \mathbb{Z}_p^*$, $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{p}$.
   (i) *For all* $a \in \mathbb{Z}_p^*$, $a \cdot 1 \equiv a \pmod{p}$.
   (j) *For each* $a \in \mathbb{Z}_p^*$, *there exists* $b \in \mathbb{Z}_p^*$ *such that* $a \cdot b \equiv 1 \pmod{p}$.

(k) *For all* $a, b, c \in \mathbb{Z}_p$, $a \cdot (b + c) \equiv (a \cdot b) + (a \cdot c) \pmod{p}$.

Any nonempty set containing at least two elements such as 0 and 1, in which 'addition' and 'multiplication' can be defined in such a way that the above properties are satisfied, is called a **field**. So, $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is an example of a field. The well known examples of fields are:

(a) $\mathbb{Q}$, the set of rational numbers.

(b) $\mathbb{R}$, the set of real numbers.

(c) $\mathbb{C}$, the set of complex numbers.

8. *Let p be an odd prime. Prove the following:*
   (a) *The equation $x^2 \equiv 1 \pmod{p}$ has exactly two solutions in $\mathbb{Z}_p$.*
   (b) *Corresponding to any $a \in \{2, 3, \ldots, p-2\}$, if there exists $b \in \mathbb{Z}_p^*$ such that $a \cdot b \equiv 1 \pmod{p}$, then $b \in \{2, 3, \ldots, p-2\}$ and $b \neq a$.*
   (c) *If $a, b, c, d \in \{2, 3, \ldots, p-2\}$ satisfy $a \neq c$, $a \cdot b \equiv 1 \pmod{p}$ and $c \cdot d \equiv 1 \pmod{p}$, then $b \neq d$.*
   (d) *Let $p > 3$. Write $q = (p-3)/2$. There exist two-element sets $\{a_1, b_1\}, \{a_2, b_2\}, \ldots, \{a_q, b_q\}$ that are pairwise disjoint satisfying $a_i \cdot b_i \equiv 1 \pmod{p}$ for $1 \leq i \leq q$, and $\bigcup\limits_{i=1}^{q} \{a_i, b_i\} = \{2, 3, \ldots, p-2\}$.*
   (e) *If $p > 3$, then $2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}$.*

9. **[Wilson's Theorem]** *If p is any prime, then $(p-1)! \equiv -1 \pmod{p}$.*

10. **[Primality Testing]** *Any integer $n > 1$ is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$.*

4.3 Chinese Remainder Theorem

Theorem 4.3.1. [Chinese remainder theorem] *Fix a positive integer m. Let $n_1, n_2, \ldots, n_m$ be pairwise coprime positive integers. Write $M = n_1 n_2 \cdots n_m$. Then, the system of congruences*

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

has a unique solution modulo M.

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 $1 \leq k \leq m$. Let $1 \leq i, j \leq m$. Then

$$M_i x_i \equiv M_i x_i + n_i y_i \equiv 1 \pmod{n_i}; \quad i \neq j \Rightarrow n_i | M_j \Rightarrow M_j x_j \equiv 0 \pmod{n_i}.$$

Now, $x_0 := \sum\limits_{k=1}^{m} M_k x_k a_k \equiv M_i x_i a_i \equiv 1 \cdot a_i \equiv a_i \pmod{n_i}$. That is, x_0 is a solution to the given system of congruences.

If y_0 is any solution to the system of congruences, then for each integer k with $0 \leq k \leq m$, we have $y_0 \equiv a_k \pmod{n_k}$ so that $y_0 - x_0 \equiv a_k - a_k \equiv 0 \pmod{n_k}$. Since $n_1, \ldots, n_k$ are pairwise coprimes and their product is M, Corollary 4.1.8 implies that $y_0 - x_0 \equiv 0 \pmod{M}$. Therefore, x_0 is the unique solution of the system of congruences module M. ■

Example 4.3.2. Consider the system of congruences $x \equiv 20 \pmod{28}$ and $x \equiv 14 \pmod{27}$ in Exercise 4.2.7.5. In this case, $a_1 = 20,\ a_2 = 14,\ n_1 = 28$ and $n_2 = 27$ so that $M = 28 \cdot 27 = 756, M_1 = 27$ and $M_2 = 28$. Then, $x_1 = -1$ and $x_2 = 1$ show that $M_1x_1 + M_2x_2 = 27 \cdot -1 + 28 \cdot 1 = 1$. Hence

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

EXERCISE **4.3.3.** 1. *Find the smallest positive integer which when divided by* 4 *leaves a remainder* 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 $n \equiv 4 \pmod{14}$ and $n \equiv 6 \pmod{18}$? Give reasons for your answer. What if we replace* 6 *or* 4 *with an odd number?*

---

4. *Let n be a positive integer. Show that the set $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ has the following properties:*

   (a) *For all $a, b \in \mathbb{Z}_n$, $a + b \pmod{n} \in \mathbb{Z}_n$.*
   (b) *For all $a, b \in \mathbb{Z}_n$, $a + b = b + a \pmod{n}$.*
   (c) *For all $a, b, c \in \mathbb{Z}_n$, $a + (b + c) \equiv (a + b) + c \pmod{n}$.*
   (d) *For all $a \in \mathbb{Z}_n$, $a + 0 \equiv a \pmod{n}$.*
   (e) *For all $a \in \mathbb{Z}_n$, $a + (n - a) \equiv 0 \pmod{n}$.*
   (f) *For all $a, b \in \mathbb{Z}_n$, $a \cdot b \pmod{n} \in \mathbb{Z}_n$.*
   (g) *For all $a, b \in \mathbb{Z}_n$, $a \cdot b = b \cdot a \pmod{n}$.*
   (h) *For all $a, b, c \in \mathbb{Z}_n$, $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{n}$.*
   (i) *For all $a \in \mathbb{Z}_n$, $a \cdot 1 \equiv a \pmod{n}$.*
   (j) *For all $a, b, c \in \mathbb{Z}_n$, $a \cdot (b + c) \equiv (a \cdot b) + (a \cdot c) \pmod{n}$.*

   Any set, say $\mathcal{R}$, with $0, 1 \in \mathcal{R},\ 0 \neq 1$, in which 'addition' and 'multiplication' can be defined in such a way that the above properties are satisfied, 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. The well known examples of commutative ring with unity are:

   (a) $\mathbb{Z}$, the set of integers.
   (b) $\mathbb{Q}$, the set of rational numbers.
   (c) $\mathbb{R}$, the set of real numbers.
   (d) $\mathbb{C}$, the set of complex numbers.

5. *Let m and n be two coprime positive integers. By Exercise 4.3.3.4, the sets $\mathbb{Z}_m, \mathbb{Z}_n$, and $\mathbb{Z}_{mn}$ are commutative rings with unity. Now, define addition and multiplication in $\mathbb{Z}_m \times \mathbb{Z}_n$ componentwise. Also, define the function*

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

   Then, prove the following:

   (a) *$\mathbb{Z}_m \times \mathbb{Z}_n$ is a commutative ring with unity. What are the 0 and 1 here?*
   (b) *For all $x, y \in \mathbb{Z}_{mn}$, $f(x + y) = f(x) + f(y)$.*

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

(d) *For each* $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ *there exists a unique* $x \in \mathbb{Z}_{mn}$ *such that* $x \equiv a \pmod{m}$ *and* $x \equiv b \pmod{n}$*.*

(e) $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_{mn}| = mn$*.*

Such a function f is called a ring isomorphism, and thus, the two rings $\mathbb{Z}_m \times \mathbb{Z}_n$ and $\mathbb{Z}_{mn}$ are isomorphic.

Chapter 5

Combinatorics - I

Combinatorics can be traced back more than 3000 years to India and China. For many centuries, it primarily comprised the solving of problems relating to the permutations and combinations of objects. The use of the word "combinatorial" can be traced back to Leibniz in his dissertation on the art of combinatorial in 1666. Over the centuries, combinatorics evolved in recreational pastimes. These include the Königsberg bridges problem, the four-colour map problem, the Tower of Hanoi, the birthday paradox and Fibonacci's 'rabbits' problem. In the modern era, the subject has developed both in depth and variety and has cemented its position as an integral part of modern mathematics. Undoubtedly part of the reason for this importance has arisen from the growth of computer science and the increasing use of algorithmic methods for solving real-world practical problems. These have led to combinatorial applications in a wide range of subject areas, both within and outside mathematics, including network analysis, coding theory, and probability.

5.1 Addition and multiplication rules

We first consider some questions.

1. How many possible crossword puzzles are there?
2. Suppose we have to select 4 balls from a bag of 20 balls numbered 1 to 20. How often do two of the selected balls have consecutive numbers?
3. How many ways are there of rearranging the letters in the word ALPHABET?
4. Can we construct a floor tiling from squares and regular hexagons?

We observe various things about the above problems. A priori, unlike many problems in mathematics, there is hardly any abstract or technical language. Despite the initial simplicity, some of these problems will be frustratingly difficult to solve. Further, we notice that despite these problems appearing to being diverse and unrelated, they principally involve selecting, arranging, and counting objects of various types. We will first address the problem of counting. Clearly, we would like to be able to count without actually counting. In other words, can we figure out how many things there are with a given property without actually enumerating each of them. Quite often this entails deep mathematical insight. We now introduce two standard techniques which are very useful for counting without actually counting. These techniques can easily be motivated through the following examples.

Example 5.1.1.

1. Let the cars in New Delhi have license plates containing 2 alphabets followed by two numbers. What is the total number of license plates possible?

   Ans: Here, we observe that there are 26 choices for the first alphabet and another 26 choices for the second alphabet. After this, there are two choices for each of the two numbers in the license plate. Hence, we have a maximum of $26 \times 26 \times 10 \times 10 = 67,600$ license plates.

2. Let the cars in New Delhi have license plates containing 2 alphabets followed by two numbers with the added condition that "in the license plates that start with a vowel the sum of numbers should always be even". What is the total number of license plates possible?

   Ans: Here, we need to consider two cases.
   Case 1: The license plate doesn't start with a vowel. Then using the previous example, the number of license plates equals $21 \times 26 \times 10 \times 10 = 54600$.

   Case 2: The license plate starts with a vowel. Then the number of license plates equals $5 \times 26 \times (5 \times 5 + 5 \times 5) = 6500$.

   Hence, we have a maximum of $54600 + 6500 = 61100$ license plates.

Generalization of the first example leads to what is referred to as the rule of product and that of the second leads to the rule of addition. To understand these rules, we explain the involved ideas.

Suppose we have a task to complete and that the task has some parts (subtasks). Assume that each of the parts can be completed on their own and completion of one part does not result in the completion of any other part. We say the parts are compulsory to mean that each of the parts must be completed to complete the task. We say the parts are alternative to mean that exactly one of the parts must be completed to complete the task. With this setting we state the two basic rules of combinatorics.

Discussion 5.1.2. [Basic counting rules] Let $n, m_1, \ldots, m_n \in \mathbb{N}$.

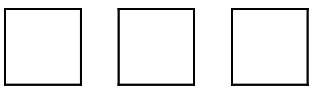
1. [**Multiplication/Product rule**] If a task consists of n *compulsory* parts and the i-th part can be completed in m_i ways, $i = 1, 2, \ldots, n$, then the task can be completed in $m_1 m_2 \cdots m_n$ ways.

2. [**Addition rule**] If a task consists of n *alternative* parts, and the i-th part can be completed in m_i ways, $i = 1, \ldots, n$, then the task can be completed in $m_1 + m_2 + \cdots + m_n$ ways.

To illustrate these rules once again let us consider the following examples.

Example 5.1.3. 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 of forming a three digit number can be viewed as filling three boxes kept in a horizontal row. Our 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:** $9 \times 10 \times 10$.

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 digits using digits from $\{1,3,5,7,9\}$. Part 2: form a three digit number with distinct digits using digits from $\{2,4,6,8\}$. Observe that Part 1 is a task having three compulsory subparts. Using multiplication rule, we see that Part 1 can be done in $5 \times 4 \times 3$ ways. Part 2 is a task having three compulsory subparts. So, it can be done in $4 \times 3 \times 2$ ways. Since our task has alternative parts, addition rule applies. **Ans:** 84.

Remark 5.1.4. There is another way to formulate the above rules. Let A_i be the set of all possible ways in which the i-th part can be completed. In this setting, the multiplication rule can be re-written as: *if $A_1, A_2, \ldots, A_n$ are nonempty finite sets, then $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$.*
For the addition rule, note that, as the completion of one part does not result in the completion of any other part, $A_1, A_2, \ldots, A_n$ are disjoint. Thus, the addition rule can be re-written as: *if $A_1, A_2, \ldots, A_n$ are disjoint, nonempty finite sets, then $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.*

5.2 Permutations and combinations

This section is primarily devoted to introduce some very common combinatorial objects and development of methods to count them using the addition rule and multiplication rule.

5.2.1 Counting words made with elements of a set S

The first fundamental combinatorial object one commonly studies is a function $f : [k] \to S$. The set of all functions from A to B will be denoted by $\mathsf{Map}(A, B)$.

Discussion 5.2.1. 1. Let $k \in \mathbb{N}$ and let $f \in \mathsf{Map}([k], S)$. Then, we may view f as the ordered k-tuple $(f(1), \ldots, f(k))$. Thus f is an element of $S^k = S \times S \times \cdots \times S$, k times.

2. Consider an ordered k-tuple $(x_1, x_2, \ldots, x_k)$ of elements of X. If we remove the brackets and the commas, then what we get is $x_1 x_2 \ldots x_k$, which is called a **word** of length k made with elements of X. Thus, the word corresponding to the tuple (a, a, b) is aab.

3. Consider a function $f : [3] \to \{a, b, \ldots, z\}$, defined by $f(1) = a, f(2) = a$ and $f(3) = b$. Technically, $f = \{(1, a), (2, a), 3, b)\}$ and the ordered tuple it gives is (a, a, b) and the word related to it is aab. Because of this natural one-one correspondence, people use them interchangeably.

Theorem 5.2.2. *Let $n, r \in \mathbb{N}$ be fixed. Then $|\mathsf{Map}([n], [r])| = r^n$.*

Proof. Forming such a function is a task with n compulsory parts, where each part can be done in r many ways. So, by the product rule, the number of such functions is r^n. ∎

Example 5.2.3. 1. How many functions are there from [9] to [12]?

Ans: 12^9. This task has 9 compulsory parts, where is each part can be done in 12 ways.

2. Determine the number of words of length 9 made with alphabets from $\{a, b, \ldots, z\}$?

Ans: 26^9. This task has 9 compulsory parts, where each part can be done in 26 many ways.

3. Suppose 3 distinct coins are tossed and the possible outcomes, namely H and T, are recorded. For example, the word TTH means that the first two coins have shown T and the third coin has shown H. Determine the number of possible outcomes.

Ans: It is the same as the number of words of length 3 made using T and H. So, it is 2^3.

Practice **5.2.4.** *1. Let $n, r \in \mathbb{N}$. In how many ways can r distinct balls be placed into n distinct boxes?*

2. How many ways are there to make 5-letter words (words of length 5) using the ENGLISH alphabet such that the vowels do not appear at even positions?

3. Determine the number of possible outcomes if three distinct coins and five distinct dice are tossed?

Discussion 5.2.5. **[Use of complements]** A simple technique which is used very frequently is counting the complement of a set, when we know the size of the whole set. For example, consider the following question.

How many 5-letter words can be made using the letters A, B, C, D that do not contain the string "ADC"? For example, $ADCDD, BADCB$ are not counted but $DACAD$ is counted.

Ans: Let X be the set of all 5-letter words that can be made using A, B, C, D. Then $|X| = 4^5$. Consider the sets $A = \{\text{words in } X \text{ of the form } ADC**\}$, $B = \{\text{words in } X \text{ of the form } *ADC*\}$, and $C = \{\text{words in } X \text{ of the form } **ADC\}$. We see that $|A| = |B| = |C| = 4^2$. As the sets A, B, C are disjoint, we see that $|A \cup B \cup C| = 3 \times 4^2$. Hence our answer to the original question is $4^5 - 3 \times 4^2$.

Practice **5.2.6.** *1. Determine the number of functions $f : [6] \to [5]$ satisfying $f(i) \neq i$ for at least two values of i?*

2. How many 5 digit natural numbers are there that do not have the digit 9 appearing exactly 4 times?

5.2.2 Counting words with distinct letters made with elements of a set S

We now discuss the next combinatorial object namely the one-one functions. For $n \in \mathbb{N}$, the term n**-set** is used for 'a set of size n'. Further, $n! = 1 \cdot 2 \cdot \cdots \cdot n$ and by convention, $0! = 1$.

Discussion 5.2.7. **[Injections]** Let $n, r \in \mathbb{N}$ and X be a non-empty set.

1. An injection $f : [r] \to X$ can be viewed as an ordered r-tuple of elements of X with distinct entries. It can also viewed as a word of length r with distinct letters made with elements of X. The set of all injections from A to B will be denoted by $\mathsf{Inj}(A, B)$.

2. If $|X| = r$, then a bijection $f : X \to X$ is called a **permutation** of X. If $X = \{x_1, \ldots, x_r\}$, then $f(x_1), \ldots, f(x_r)$ is just a rearrangement of elements of X.

3. We define $\mathbf{P(n, r)} := |\mathsf{Inj}([r], [n])|$. As a convention, $P(n, 0) = 1$ for $n \geq 0$.

Example 5.2.8. How many one-one maps $f : [4] \to \{A, B, \ldots, Z\}$ are there?

Ans: The task of forming such a one-one map has 4 compulsory parts: selecting $f(1)$, $f(2)$, $f(3)$ and $f(4)$. Further, $f(2) \neq f(1)$, $f(3) \neq f(1), f(2)$ and so on. So, by the product rule, the number of one-one map equals $26 \cdot 25 \cdot 24 \cdot 23 = \frac{26!}{22!}$.

Theorem 5.2.9. **[Number of injections $f : [r] \to S$]** *Let $n, r \in \mathbb{N}$ and $|S| = n$. Then the number $P(n, r) = \frac{n!}{(n-r)!}$.*

Proof. The task is to from an r-tuple $(f(1), \ldots, f(r))$ of distinct elements. It has r compulsory parts, namely selecting $f(1)$, $f(2)$, $\ldots$, $f(r)$ with the condition that $f(k) \notin \{f(1), f(2), \ldots, f(k-1)\}$, for $2 \leq k \leq r$. So, using the product rule, $P(n, r) = |\mathsf{Inj}([r], [n])| = n(n-1) \cdots (n-r+1) = \frac{n!}{(n-r)!}$. ∎

Practice **5.2.10.** *1. How many ways are there to make 5 letter words using the ENGLISH alphabet if the letters must be different?*

2. *How many ways are there to arrange the* 5 *letters of the word* $ROYAL$*?*

3. *How many bijections* $f : [12] \to [12]$ *are there if a multiple of* 3 *is mapped to a multiple of* 3*?*

5.2.3 Counting words where letters may repeat

Consider the word $AABAB$. We want to give subscripts $1, 2, 3$ to the A's and subscripts $1, 2$ to the B's so that we create words made with A_1, A_2, A_3, B_1, and B_2. For example, one such word is $A_2A_3B_2A_1B_1$. How many such words can we create? Fill the following table to get all such words. Notice that each of these words become $AABAB$ when we erase the subscripts.

$A_1A_2B_1A_3B_2$	$A_1A_2B_2A_3B_1$
$A_1A_3B_1A_2B_2$	$A_1A_3B_2A_2B_1$
$A_3A_2B_1A_1B_2$	$A_3A_2B_2A_1B_1$

The following is another useful principle. It is a special case of Exercise 3.1.5.13.

Proposition 5.2.11. **[Principle of disjoint pre-images of equal size]** *Let* A, B *be nonempty finite sets and* $f : A \to B$ *be a function satisfying* $|f^{-1}(i)| = k = |f^{-1}(j)|$*, for each* $i, j \in B$*. Then,* $|A| = k|B|$*. In particular, for* $k = 1$ *this principle is also called the principle of bijection.*

Let $n_1, \ldots, n_k \in \mathbb{N}$. Suppose, we are given n_i copies of the symbol A_i, for $i = 1, \ldots, k$. Then, by an **arrangement** of these $n_1 + \cdots + n_k$ symbols, we mean a way of placing them in a row. It is a word made with the symbols $A_1, \ldots, A_k$ containing the symbol A_i exactly n_i times, $i = 1, \ldots, k$. For example, $ABBAA$ is an arrangement of 3 copies of A and 2 copies of B.

Example 5.2.12.

1. How many words of size 5 can be formed using three A's and two B's?

   Ans: Let $A = \{$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 $Er(a)$ to be the word in B obtained by erasing the subscripts. Then, the function $Er : A \to B$ satisfies:

   'for each $b, c \in B, b \neq c$, we have $|Er^{-1}(b)| = |Er^{-1}(c)| = 3!2!$'.

   Thus, by Proposition 5.2.11, $|B| = \frac{|A|}{3!2!} = \frac{5!}{3!2!}$.

2. Determine the number of ways to place 4 couples in a row if each couple sits together.

   Ans: Let X be the set of all arrangements of A, B, C, D. Let Y be the set of all arrangements of A, A, B, B, C, C, D, D in which both the copies of each letter are together. For example $AACCDDBB \in Y$ but $ABBCCDDA \notin Y$. Let Z be the set of all arrangements of A_h, A_w, B_h, B_w, C_h, C_w, D_h, D_w in which A_h, A_w are together, B_h, B_w are together, C_h, C_w are together, and D_h, D_w are together.

   In this setting, we need to find the size of Z. So, define $Er : Z \to Y$ by $Er(z)$ equals the arrangement obtained by erasing the subscripts, namely h and w, that appear in z. Notice that each $y \in Y$ has 2^4 pre-images in Z. Now, define $Mrg : Y \to X$ by $Mrg(y)$ equals the arrangement obtained by merging the two copies of the same letters into one single letter. For example, $Mrg(BBAADDCC) = BADC$. Notice that each x in X has exactly one pre-image in Y. By applying the principle of disjoint pre-images of equal size twice, we see that $|Z| = 2^4|Y| = 2^4|X| = 2^4 4!$, as $|X| = 4!$.

Alternate. Instead of writing it in such a laborious way as the above, let us adopt a more reader friendly way of writing the same. A couple can be thought of as one cohesive group (they are to be seated together). So, the 4 cohesive groups can be arranged in 4! ways. But a couple can sit either as "wife and husband" or "husband and wife". So, the total number of arrangements is $2^4\ 4!$.

Theorem 5.2.13. **[Arrangements]** *Let $n, n_1, n_2, \ldots, n_k \in \mathbb{N}$ and suppose that we have n_i copies of the symbol (object) A_i, for $i = 1, \ldots, k$ and that $n = n_1 + \cdots + n_k$. Then the number of arrangements of these n symbols is*

$$\frac{n!}{n_1! n_2! \cdots n_k!}.$$

The formula remains valid even if we take some of the n_i's to be 0.

Proof. Let S be set of all arrangements of the $n_1 + n_2 + \cdots + n_k$ symbols and let T be the set of all arrangements of the symbols $A_{1,1}, \ldots, A_{1,n_1}, A_{2,1}, \ldots, A_{2,n_2}, \ldots, A_{k,1}, \ldots, A_{k,n_k}$. Define a function $Er : T \to S$ by $Er(t)$ equals the arrangement obtained by erasing the second subscripts that appear in t. Notice that each $s \in S$ has $n_1! n_2! \cdots n_k!$ many pre-images. Hence, by the principle of disjoint pre-images of equal size, we have $|T| = n_1! \cdots n_k! |S|$. As $|T| = (n_1 + n_2 + \cdots + n_k)!$, we obtain the desired result.

Assume that some n_i's are 0 (all cannot be 0 as $n \in \mathbb{N}$). Then our arrangements do not involve the corresponding A_i's. Hence we can use the argument in the previous paragraph and get the number of arrangements. As $0! = 1$, we can insert some $0!$ in the denominator. ∎

We have an immediate special case.

Corollary 5.2.14. *Let $m, n \in \mathbb{N}$. Then the number of arrangements of m copies of A and n copies of B is $\frac{(m+n)!}{m!n!}$.*

5.2.4 Counting subsets

As an immediate application of Corollary 5.2.14, we have the following result which counts the number of subsets of size k of a given set S.

Theorem 5.2.15. *Let $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$. Then the number of subsets of $[n]$ of size k is $\frac{n!}{k!(n-k)!}$.*

Proof. If $k = 0$ or n, then we know that there is only one subset of size k and the formula also gives us the same value. So, let $1 \le k \le n - 1$ and let X be the set of all arrangements of k copies of T's and $n - k$ copies of F's. For an arrangement $x = x_1 x_2 \ldots x_n \in X$, define $f(x_1 \ldots x_n) = \{i \mid x_i = T\}$, *i.e.*, the set of positions where a T appears in x. Then, f is a bijection between X and the set of all k-subsets of $[n]$. Hence, the number of k-subsets of $[n] = |X| = |X| = \frac{n!}{k!(n-k)!}$, by Corollary 5.2.14. ∎

Discussion 5.2.16.

1. For $n \in \mathbb{N}$ and $r \in \{0, 1, \ldots, n\}$, the symbol $C(n, r)$ is used to denote the number of r-subsets of $[n]$. The value of $C(0, 0)$ is taken to be 1. Many texts use the word 'r-combination' for an r-subset.
2. Using Theorem 5.2.15, we see that for $n \in \mathbb{N}_0$ and $r = 0, 1, \ldots, n$, $C(n, r) = \frac{n!}{r!(n-r)!}$. Also it follows from the definition that $C(n, r) = 0$ if $n < r$, and $C(n, r) = 1$ if $n = r$.
3. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}_0$ such that $n = n_1 + \cdots + n_k$. Then by $C(n; n_1, \ldots, n_k)$ we denote the number $\frac{n!}{n_1! n_2! \cdots n_k!}$. By Theorem 5.2.13, it is the number of arrangements of n objects where n_i are of type i, $i = 1, \ldots, k$. By convention, $C(0; 0, \ldots, 0) = 1$.

4. If $n \in \mathbb{N}$ and $n_1, \ldots, n_{k-1} \in \mathbb{N}_0$ with $n_1 + \cdots + n_{k-1} < n$, we also use $C(n; n_1, \ldots, n_{k-1})$ to mean $C(n; n_1, \ldots, n_{k-1}, n - n_1 - \cdots - n_{k-1})$.

5.2.5 Pascal's identity and its combinatorial proof

We aim to supply a combinatorial proof of a very well known identity called the Pascal's identity.

Theorem 5.2.17. **[Pascal]** *Let n and r be non-negative integers. Then*

$$C(n,r) + C(n,r+1) = C(n+1,r+1).$$

Proof. (This is not the combinatorial proof.) If $r > n$, then by definition all the three terms are zero. So, we have the identity. If $r = n$, then the first and the third terms are 1 and the second term is 0. So, again we have the identity. So, let us take $r < n$. Now we can use the formulas for $C(n,r), C(n,r+1)$ and $C(n+1,r+1)$ to verify the identity. ∎

Sometimes, we want to supply a combinatorial proof of an identity, *i.e.*, by associating the terms on the left hand side (LHS) and the right hand side (RHS) with some objects and by showing a one to one correspondence between them. Before we supply a combinatorial proof of Pascal's identify, the reader is advised to go through the following experiment to discover that proof on their own.

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. Can you match the sets in the left with the sets in the right in some natural way?

$$C(5,3)\left\{\begin{array}{l}\{1,2,3\}\\ \\ \{2,3,4\}\\ \{1,2,5\}\\ \\ \\ \{3,4,5\}\end{array}\right. \qquad \Bigg\| \qquad \begin{array}{l}\left.\begin{array}{l}\{1,2,3\}\\ \\ \{2,3,4\}\end{array}\right\} C(4,3)\\ \left.\begin{array}{l}\{1,2\}\\ \\ \\ \{3,4\}\end{array}\right\} C(4,2)\end{array}$$

We now present the combinatorial proof of Theorem 5.2.17.

Proof. If $r > n$, then by definition all the three terms are zero. So we have the identity. If $r = n$, then the first and the third terms are 1 and the second term is 0. So, again we have the identity. So, assume that $r < n$.

Let $S = \{1, 2, \ldots, n, n+1\}$ and A be an $(r+1)$-subset of S. Then, by definition, 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.

Therefore, using the above two cases, 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. ∎

5.2.6 Counting in two ways

Let R and C be two nonempty finite sets and take a function $f : R \times C \to \mathbb{R}$. View the function written as a matrix of real numbers with rows indexed by R and columns indexed by C. Then the total sum of the entries of that matrix can be obtained either 'by first taking the sum of entries in each row and then summing them' or 'by first taking the sum of the entries in each column and then summing them', *i.e.*,

$$\sum_{(x,y)\in R\times C} f(x,y) = \sum_{x\in R}\left(\sum_{y\in C} f(x,y)\right) = \sum_{y\in C}\left(\sum_{x\in R} f(x,y)\right).$$

This is known as 'counting in two ways' and it is a very useful tool to prove some combinatorial identities. Let us see some examples.

Example 5.2.18. 1. [**Newton's Identity**] Let $n \geq r \geq k$ be natural numbers. Then

$$C(n,r)C(r,k) = C(n,k)C(n-k,r-k).$$

In particular, for $k = 1$, the identity becomes $rC(n,r) = nC(n-1,r-1)$. **Ans:** Let us use the method of 'counting in two ways'. So, we take two appropriate sets $R = \{\text{all } r\text{-subsets of } [n]\}$ and $C = \{\text{all } k\text{-subsets of } [n]\}$ and define f on $R \times C$ by $f(A,B) = 1$ if $B \subseteq A$, and $f(A,B) = 0$ if $B \not\subseteq A$.

Then given a set $A \in R$, it has $C(r,k)$ many subsets of A. Thus,

$$\sum_{A\in R}\left(\sum_{B\in C} f(A,B)\right) = \sum_{A\in R} C(r,k) = C(n,r)C(r,k).$$

Similarly, given a set $B \in C$, there are $C(n-k,r-k)$ subsets of $[n]$ that contains B. Hence,

$$\sum_{B\in C}\left(\sum_{A\in R} f(A,B)\right) = \sum_{B\in C} C(n-k,r-k) = C(n,k)C(n-k,r-k).$$

Hence, the identity is established.

Alternate. We now present the same argument in a more reader friendly manner.

Select a team of size r from n students (in $C(n,r)$ ways) and then from that team select k leaders (in $C(r,k)$ ways). So, there are $C(n,r)C(r,k)$ ways of selecting a team and it's leaders from the team itself. Alternately, select the leaders first in $C(n,k)$ ways and out of the rest select another $r-k$ to form the team in $C(n-k,r-k)$ ways. So, using this argument, the number of ways of doing this is $C(n,k)C(n-k,r-k)$.

2. [**Important**] Let $n, r \in \mathbb{N}$, $n \geq r$. Then

$$C(1,r) + C(2,r) + \cdots + C(n,r) = C(n+1,r+1). \tag{5.1}$$

The RHS stands for the class $\mathcal{F}$ of all the subsets of $[n+1]$ of size $r+1$. Let $S \in \mathcal{F}$. Note that S has a maximum element. A moments thought tells us that the maximum element of such a set can vary from $r+1$ to $n+1$. If the maximum of S is $r+1$, then the remaining elements of S have to be chosen in $C(r,r)$ ways. If the maximum of S is $r+2$, then the remaining elements of S has to be chosen in $C(r+1,r)$ ways and so on. If the maximum of S is $n+1$, then the remaining elements of S has to be chosen in $C(n,r)$ ways. Thus, $C(n+1,r+1) = C(r,r) + C(r+1,r) + \cdots + C(n+1,r) = C(1,r) + C(2,r) + \cdots + C(n,r)$. Observe that for $r = 1$, it gives us $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Exercise **5.2.19.** *1. In a school 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 a 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 and selecting a treasurer and a spokesperson among them. 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.*

2. *Prove that $C(pn, pn-n)$ is a multiple of p directly from its expression.*

3. *Determine the number of arrangements of the letters of the word $ABRACADABARAARCADA$.*

4. *Prove the following identities using combinatorial arguments.*

   (a) $C(n,r) = C(n, n-r)$, *for non-negative integers n and r.*

   (b) $C(n,r) = C(r,r)C(n-r,0) + C(r,r-1)C(n-r,1) + \cdots + C(r,0)C(n-r,r)$ *for natural numbers $n \geq r$.*

   (c) $C(n,0)^2 + C(n,1)^2 + \cdots + C(n,n)^2 = C(2n,n)$ *for all $n \in \mathbb{N}$.*

5. *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 $n_1 + n_2 \geq m$.*

---

6. *How many anagrams (rearrangements of letters) of $MISSISSIPPI$ are there so that no two S are adjacent?*

7. *How many rectangles are there in an $n \times n$ square? How many squares are there?*

8. *Supply combinatorial proofs of the following statements.*

   (a) *For each $n \in \mathbb{N}$, prove that $n!$ divides the product of n consecutive natural numbers.*

   (b) *For $m, n \in \mathbb{N}$, the number $(m!)^n$ divides $(mn)!$.*

   (c) *For $n, p \in \mathbb{N}$, the number $C(pn, pn-n)$ is a multiple of p.*

   (d) *Prove combinatorially that $2^n | (n+1) \cdots (2n)$.*

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. *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
```

5.3 Solutions in non-negative integers

There are 3 types of ice-creams available in the market: A, B, C. We want to buy 5 ice-creams in total. In how many ways can we do that? For example, we can buy 5 of type A or we can buy 3 of A and 2 of C. In general, suppose we are buying n_1 of type A, n_2 of type B and n_3 of type C. Then, we must have $n_1 + n_2 + n_3 = 5$. So, we want to know the number of different possible tuples (n_1, n_2, n_3) satisfying certain condition(s).

Let us discuss it in a general setup. 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** $x_1 + \cdots + x_k = n$ **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 $\mathbb{N}_0$.

Theorem 5.3.1. [**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. As there are $C(n + r - 1, r - 1)$ arrangements of n dots and $r - 1$ bars, we see that the number of solutions of $x_1 + \cdots + x_r = n$ in $\mathbb{N}_0$ is $C(n + r - 1, n)$. ∎

Example 5.3.2. Determine the number of words that can be made using all of 3 copies of A and 6 copies of B.

Ans: Note that this number equals the number of arrangements of 3 copies of A and 6 copies of B. Hence, this number is $C(9, 3)$.

Alternate. First put the three A's in row. Now put x_1 B's to the left of the first A, x_2 B's between the first and the second A, x_3 B's between the second and the third A and x_4 B's after the third A. Thus, we need to find number of solutions of $x_1 + x_2 + x_3 + x_4 = 6$ in $\mathbb{N}_0$. By Theorem 5.3.1, the number is $C(6 + 4 - 1, 6) = C(9, 6)$.

Discussion 5.3.3. The question of finding non-negative integers solutions can also be asked in some other styles.

1. In how many ways can we place 6 indistinguishable balls into 4 distinguishable boxes?

   Taking n_i as the number of balls to be put in the i-th box, it is asking us to find number of solutions of $n_1 + n_2 + n_3 + n_4 = 6$ in $\mathbb{N}_0$.

2. A **multiset** is a generalization of a set where elements are allowed to repeat. For example, $\{a, b, a\}$ and $\{a, a, b\}$ mean the same multisets (imagine carrying all of them in a bag). A set is also a multiset. How many multisets of size 6 can be made using the symbols a, b, c, d?

   Taking n_a as the number of a's to be put in the multiset and so on, it is asking us to find solutions of $n_a + n_b + n_c + n_d = 6$ in $\mathbb{N}_0$.

Example 5.3.4. 1. Suppose there are 5 kinds of ice-creams available in our market complex. In how many ways can we buy 15 of them for a party?

   Ans: Suppose we buy x_i ice-creams of the i-th type. Then, the problem reduces to finding the number of solutions of $x_1 + \cdots + x_5 = 15$ in non-negative integers.

2. **[Variables are bounded below by other numbers]** 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: Note that (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, the answer is $C(50,2)$.

3. **[Reducing a related problem]** 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 $x_i - x_{i-1} \geq 3$, $i = 2,3,4,5$? For example, one such choice is $(1,5,8,11,19)$.

   Ans: For each choice of (x_1,x_2,x_3,x_4,x_5), note that

   $$(x_1 - 1) + (x_2 - x_1) + \cdots + (x_5 - x_4) + (20 - x_5) = 19 \quad \textit{i.e.,} \quad d_1 + d_2 + d_3 + d_4 + d_5 + d_6 = 19$$

   where $d_1 \geq 0$, $d_2 \geq 3$, ..., $d_5 \geq 3$ and $d_6 \geq 0$. So, the problem reduces to finding the number of solutions of $n_1 + n_2 + \cdots + n_6 = 7$ in $\mathbb{N}_0$. Hence, the answer is $C(12,5)$.

   Alternate. Take an arrangement of fifteen dots ($\bullet$'s) and five bars ($|$'s) such that between two consecutive bars, there are at least two dots. The position of the bars in each such arrangement gives us one solution. For example,

   $$\bullet\bullet|\bullet\bullet\bullet|\bullet\bullet\bullet|\bullet\bullet|\bullet\bullet\bullet\bullet|\bullet \quad \to \quad (3,7,11,14,19).$$

   Conversely, each solution can be converted into such an arrangement by the following method: let n_1 be the number of dots present to the left of the first bar; n_2 be the number of dots present between the first bar and the second bar and so on. The problem now has been converted to count integer solutions of $n_1+n_2+n_3+n_4+n_5+n_6 = 15$, where $n_1, n_6 \geq 0, n_2, n_3, n_4, n_5 \geq 2$. This is the same as the number of solutions of $n_1+n_2+n_3+n_4+n_5+n_6 = 7$ in $\mathbb{N}_0$.

   Alternate. Notice that $x_1, x_2-3, x_3-6, x_4-9, x_5-12$ is a increasing sequence of numbers from $1.\ldots,8$. For example, $(1,5,8,12,17) \quad \to \quad (1,2,2,3,5)$. And from any increasing sequence of numbers from $1.\ldots,8$ we can get back our original sequence.

   So, the problem reduces to counting the number of increasing sequences of length 5 with digits $1,2,\ldots,8$. But, this is the same as the number of 5-multisets of $[8]$, as each multiset can be sorted to give a unique increasing sequence. Ans: $C(12,5)$.

4. **[Variables are bounded above]** *In this case problems become harder.* 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 the number of solutions in $\mathbb{N}_0$ of $x+y+z=48$ such that $x \leq 17, y \leq 26$ and $z \leq 35$. So, let $A = \{(x,y,z) \in \mathbb{N}_0^3 : x+y+z=48\}$,

   (a) $A_x = \{(x,y,z) \in \mathbb{N}_0^3 : x+y+z=48, x \geq 18\}$,

   (b) $A_y = \{(x,y,z) \in \mathbb{N}_0^3 : x+y+z=48, y \geq 27\}$, and

   (c) $A_z = \{(x,y,z) \in \mathbb{N}_0^3 : x+y+z=48, z \geq 36\}$.

   We know $|A| = C(50,2)$. So, the answer equals $C(50,2) - |A_x \cup A_y \cup A_z|$. The calculation of $|A_x \cup A_y \cup A_z|$ is left to the reader. A more general formula appears in the next chapter.

EXERCISE **5.3.5.** *1. Determine the number of solutions of $x+y+z=7$ with $x,y,z \in \mathbb{N}$?*

2. *Find the number of ways to keep n identical objects in r distinct locations, so that location i gets at least $p_i \geq 0$ elements, $i = 1,2,\cdots,r$.*

3. *Find the number of solutions in non-negative integers of $a+b+c+d+e < 11$.*

4. *How many 4-letter words (with repetition) are there with the letters in alphabetical order?*
5. *Determine the number of increasing sequences of length r using the numbers $1, 2, \ldots, n$.*
6. *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.*
7. *There are 10 types of ice-creams available in the market. We want to buy 3 ice-creams for each of 40 students. For example, we may buy 2 of first type and 1 of second type for a student. In how many ways can this be done?*
8. (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?*

---

9. *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 these two racks?*
10. *How many permutations of $a, b, \ldots, z$ have no 2 vowels together?*
11. *How many rearrangements of 5 copies of a, 5 copies of $b, \ldots,$ 5 copies of z have at least two consonants between any two vowels?*
12. *How many 10-subsets of $\{a, b, \ldots, z\}$ have a pair of consecutive letters?*
13. *How many ways (write an expression) are there to distribute 60 identical balls to 5 persons if Ram and Shyam together get no more than 30 and Mohan gets at least 10?*
14. *In how many ways can we pick 20 letters from 10 A's, 15 B's and 15 C's?*
15. *Evaluate* $\sum\limits_{i_1=1}^{n} \sum\limits_{i_2=1}^{i_1} \sum\limits_{i_3=1}^{i_2} \cdots \sum\limits_{i_k=1}^{i_{k-1}} 1.$

16. *Evaluate* $\sum\limits_{i_1=1}^{9} \sum\limits_{i_2=1}^{i_1} \sum\limits_{i_3=1}^{i_2} \cdots \sum\limits_{i_9=1}^{i_8} i_9^2.$
17. *There are 10 persons to be seated on chairs with numbers 1 to 10. The first person first comes and can seat on any chair. Then for $i = 2, 3, \ldots, 10$, the i-th person enters and takes the seat i if it is available, otherwise any other seat. In how many ways can they be seated?*
18. *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 $1 \le k \le n$ and $\sum\limits_{k \ge 1} S_k(n)$.
19. *Let $n \ge 2$ be a natural number. Supply a bijection between the set of all compositions of n and $\mathcal{P}([n-1])$.*
20. *How many rearrangements of 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?*

   (d) *B and A both precede the first C?*

   (e) *B or A precede the first C?*

5.4 Binomial and multinomial theorems

Discussion 5.4.1. 1. By an **algebraic expansion** of $(x+y+z)^n$ let us 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, z. For example, $x^3 + 3x^2y + 3xy^2 + y^3$ is an algebraic expansion of $(x+y)^3$.

2. By a **word expansion** of $(x+y+z)^n$ we mean an expansion where each term is a word of length n using letters x, y, z. For example, $xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$ is a word expansion of $(x+y)^3$.

3. Algebraic and word expansions for $(x_1 + \cdots + x_r)^n$ are defined similarly.

4. Take the word expansion of $(X+Y+Z)^4$. It contains 3^4 words each of length 4 made with X, Y, Z. Imagine a list the words in the order

$$XXXX, XXXY, XXXZ, XXYX, \ldots, ZZZY, ZZZZ.$$

5. Do you think the word $ZXYZ$ appears in the list? At which position? It is not difficult to see that it appears in the position $1 + (2012)_3$, where $(2012)_3$ is the value computed in base 3. (Prove this by induction!)

6. In fact, each possible word of length 4 that can be made with X, Y, Z, appears somewhere in the word expansion of $(X+Y+Z)^4$.

7. How many words in the list have two Z's, one X and one Y? The answer must be all possible arrangements of Z, Z, X, Y which is $\frac{4!}{2!1!1!}$.

8. Hence, the coefficient of XYZ^2 in the algebraic expansion of $(X+Y+Z)^4$ must be $\frac{4!}{2!1!1!} = C(4; 2, 1, 1)$. We express this by writing

$$\text{CF}\left[XYZ^2, (X+Y+Z)^4\right] = C(4; 2, 1, 1).$$

Theorem 5.4.2. **[Multinomial Theorem]** *Let $n, k \in \mathbb{N}$ and $n_1, \ldots, n_k \in \mathbb{N}_0$ with $n = n_1 + \cdots + n_k$. Then*

$$\text{CF}\left[x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}, (x_1 + \cdots + x_k)^n\right] = C(n; n_1, \cdots, n_k).$$

So

$$(x_1 + \cdots + x_k)^n = \sum_{\substack{n_1, \cdots, n_k \geq 0 \\ n_1 + \cdots + n_k = n}}^{n} C(n; n_1, \cdots, n_k) x_1^{n_1} \cdots x_k^{n_k}.$$

Proof. It is clear that the word expansion of $(x_1 + \cdots + x_k)^n$ contains all possible words of length n made with letters $x_1, \ldots, x_k$. The coefficient of $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ is given by the words of length n that are made with n_1 copies of x_1, n_2 copies of x_2, …, n_k copies of x_k. As we already know, there are $\frac{n!}{n_1! n_2! \cdots n_k!}$ such words. Hence, the first identity follows. The second identity follows from the first one. ∎

Theorem 5.4.3. **[Binomial Theorem]** *Let $n \in \mathbb{N}$ and $0 \leq i \leq n$ be an integer. Then*

$$\text{CF}\left[x^i y^{n-i}, (x+y)^n\right] = C(n, i) \quad \text{or} \quad (x+y)^n = \sum_{k=0}^{n} C(n, k) x^{n-k} y^k.$$

Proof. Follows from Theorem 5.4.2. ∎

Remark 5.4.4. Let $n \in \mathbb{N}$ and $n_1, \ldots, n_k \in \mathbb{Z}$ such that $n = n_1 + \cdots + n_k$. Then, as the term $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ does not appear in the expression of $(x_1 + \cdots + x_k)^n$, we can think that the coefficient $\text{CF}\left[x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}, (x_1 + \cdots + x_k)^n\right] = 0$. Defining $C(n; n_1, \cdots, n_k) = 0$ if any of the n_i's is negative, we now see that the multinomial theorem remains valid even for $n_1, \ldots, n_k \in \mathbb{Z}$. A similar comment is true for the binomial theorem too.

The numbers $C(n, r)$ and $C(n; r_1, \ldots, r_k)$ are thus known as 'binomial coefficients' and 'multinomial coefficients', respectively. An immediate and important corollary to the binomial theorem is the following.

Corollary 5.4.5. *Let $n \in \mathbb{N}$. Then the total number of subsets of $[n]$ is 2^n. (We can also prove this statement using some other arguments. See the exercises.)*

Proof. The number of subsets of size k is $C(n, k)$. Thus the total number of subsets is $C(n, 0) + C(n, 1) + \cdots + C(n, n)$ which is $(1 + 1)^n$ by the binomial theorem. ∎

The example below show how the multinomial coefficients can be seen as an additional tool in our study.

Example 5.4.6. 1. Fix $m, n, k \in \mathbb{N}$. Then show that $C(m + n, k) = \sum\limits_{i=0}^{k} C(m, i)\, C(n, k - i)$.

Ans: First, we give an argument using counting in two ways. We can form a committee of size k from a group consisting of m men and n women in $C(m+n, k)$ ways. On the other hand, such a committee can be formed by taking i many men and $n - i$ many women, where $0 \le i \le k$. In this way our answer is $\sum\limits_{i=0}^{k} C(m, i)\, C(n, k - i)$. Hence, they are the same.

Alternate. We now give an argument using the binomial coefficients. We have $C(m + n, k) = \text{CF}\left[x^k y^{m+n-k}, (x + y)^{m+n}\right] = \text{CF}\left[x^k y^{m+n-k}, (x + y)^m (x + y)^n\right]$

$$= \sum_{i=0}^{k} \text{CF}\left[x^i y^{m-i}, (x + y)^m\right] \text{CF}\left[x^{k-i} y^{n-k+i}, (x + y)^n\right] = \sum_{i=0}^{k} C(m, i) C(n, k - i).$$

2. Let $n > m$ be natural numbers. Prove that $\sum\limits_{k=m}^{n} C(k, m) C(n, k) = C(n, m) 2^{n-m}$.

Ans: Recall that $C(k, m)C(n, k) = C(n, m)C(n - m, k - m)$. Hence,

$$\begin{aligned}\sum_{k=m}^{n} C(k, m) C(n, k) &= \sum_{k=m}^{n} C(n, m) C(n - m, k - m) = C(n, m) \sum_{k=m}^{n} C(n - m, k - m)\\ &= C(n, m) \sum_{s=0}^{n-m} C(n - m, s) = C(n, m) 2^{n-m}.\end{aligned}$$

Alternate. Noticing a combinatorial proof is relatively harder. The RHS stands for (A, B) where $A \subseteq [n]$ of size m and $B \subseteq [n] \setminus A$. For each fixed A, we have 2^{n-m} choices of B, and this is why we have the RHS. On the other hand, we can first select a big set C of size $|C| \ge m$. From this set C, we will take a subset A of size m and we will treat the remaining as B. The LHS expresses the number of ways in which this task can be done.

Alternate. Yet another way to see it is to notice that $C(n, k)C(k, m) = C(n; m, k - m, n - k)$, which is $\text{CF}\left[x^m y^{k-m} z^{n-k}, (x + y + z)^n\right]$. Since, m is fixed (and x's can appear in any m of the n places) this coefficient equals

$$C(n, m) \sum_{k-m=0}^{n-m} \text{CF}\left[y^{k-m} z^{n-k}, (y + z)^{n-m}\right] = C(n, m) 2^{n-m}.$$

3. Determine the number of words of size 5 using letters from 'MATHEMATICIAN' (including multiplicity, *i.e.*, you may use M at most twice).

   Ans: Note that to form such a word, suppose we have selected x_m many M's, x_a many A's, and so on. Then, the problem reduces to finding the number of solutions in non-negative numbers to $x_m + x_a + x_t + x_h + x_e + x_i + x_c + x_n = 5$, with $0 \le x_m, x_t, x_i \le 2$, $0 \le x_a \le 3, 0 \le x_h, x_c, x_n, x_e \le 1$. In that case the number of words that can be formed from them is $C(5; x_m, x_t, x_i, x_a, x_h, x_c, x_n, x_e)$. Hence, the total number of such words is

$$\sum_{\substack{k_1+\cdots+k_8=5 \\ k_1\le 2, k_2\le 3, k_3\le 2, k_4\le 1, k_5\le 1, k_6\le 2, k_7\le 1, k_8\le 1}} C(5; k_1, \cdots, k_8).$$

EXERCISE **5.4.7.** *1. Show that $|\mathcal{P}(\{1,2,\ldots,n\})| = 2^n$ in the following ways.*

   (a) By using 'select a subset is a task with n compulsory parts'.

   (b) By associating a subset with a 0-1 string of length n and evaluating their values in base-2.

   (c) Arguing in the line of 'a subset of $\{1,2,\ldots,n,n+1\}$ either contains $n+1$ or not' and using induction.

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. That is,

$$\sum_{k\ge 0} C(n,2k) = \sum_{k\ge 0} C(n,2k+1) = 2^{n-1}.$$

3. Show that $C(n,\ell) = \sum\limits_{k=0}^{t} C(t,k)\, C(n-t,\ell-k) = \sum\limits_{k=0}^{n} C(t,k)\, C(n-t,\ell-k)$, for any $t, 0 \le t \le n$.

4. Show that $C(n+r+1,r) = \sum\limits_{\ell=0}^{r} C(n+\ell,\ell)$.

5. We already have seen a combinatorial proof of $C(n+1,r+1) = \sum\limits_{\ell=r}^{n} C(\ell,r)$. Supply a different proof by manipulating the binomial coefficients.

---

6. We know that $rC(n,r) = nC(n-1,r-1)$. Use it to evaluate the following sums.

   (a) Evaluate $\sum\limits_{r=0}^{n} rC(n,r)$ for $n \ge 3$.

   (b) Evaluate $\sum\limits_{k=0}^{n} (2k+1)\, C(n,2k+1)$ for $n \ge 3$.

   (c) Evaluate $\sum\limits_{k=0}^{n} (5k+3)\, C(n,2k+1)$ for $n \ge 3$.

   (d) Evaluate $\sum\limits_{k=0}^{n} r^2 C(n,r)$ for $n \ge 3$.

7. For each $i,n \in \mathbb{N}$, define $S_i(n) = \sum\limits_{k=1}^{n} k^i$. Then, we know that $S_1(n) = \dfrac{n(n+1)}{2}, S_2(n) = \dfrac{n(n+1)(2n+1)}{6}$ and $S_3(n) = \left(\dfrac{n(n+1)}{2}\right)^2$. Determine $S_4(n)$. Also, find a recursive method to find closed form expression for $S_i(n)$, for $i \ge 5$.

8. For $n \in \mathbb{N}$, $k_1,\ldots,k_m \in \mathbb{N}$ such that $k_1+\cdots+k_m = n$, show that

$$C(n;k_1,\ldots,k_m) = C(n-1;k_1-1,\ldots,k_m) + \cdots + C(n-1;k_1,\ldots,k_m-1).$$

This is called the **generalized Pascal***'s identity.*

9. *For $n, m \in \mathbb{N}$, evaluate*
$$\sum_{\substack{k_1,\ldots,k_m \in \mathbb{N}_0 \\ k_1+\cdots+k_m=n}} C(n; k_1, \ldots, k_m).$$

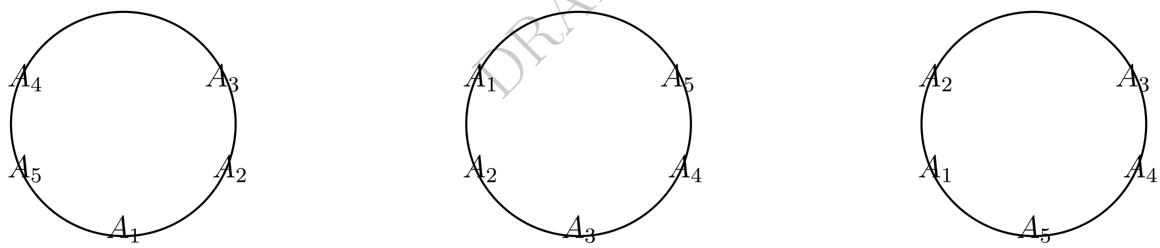
10. *Let $m, n \in \mathbb{N}$. How many terms are there in the (algebraic) expansion of $(x_1 + x_2 + \cdots + x_m)^n$? How many terms involve at least one of each x_i, $i = 1, \ldots, n$? How many terms involve at least two x_1 and at most five x_1?*

11. *Let $n, r \in \mathbb{N}$. By the binomial theorem, we know that $(n+1)^r = \sum\limits_{k=0}^{r} C(r,k)n^k$. Supply a combinatorial proof by using* $\mathsf{Map}([r],[n])$*.*

12. *For $n, m \in \mathbb{N}$ and $r = \lfloor \frac{m}{2} \rfloor$ (greatest integer function) evaluate*
$$\sum_{\substack{k_1,\ldots,k_m \in \mathbb{N}_0 \\ k_1+\cdots+k_m=n}} (-1)^{k_2+k_4+\cdots+k_{2r}} C(n; k_1, \ldots, k_m).$$

5.5 Circular arrangements

Let S be a nonempty finite multiset. By a **circular arrangement** of elements of S, we mean an arrangement of the elements of S on a circle. Two circular arrangements are the same if each element has the same 'clockwise adjacent' element, *i.e.*, one can be obtained as a rotation of the other. By $[x_1, x_2, \ldots, x_n, x_1]$, we shall denote a circular arrangement, keeping the anticlockwise direction in a picture. We use the word **circular permutation** if elements of S are distinct. Thus, exactly two of the following pictures 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 5.1: Circular permutations

Example 5.5.1. Determine the number of circular permutations of $X = \{A_1, A_2, A_3, A_4, A_5\}$.

Ans: 4!. Let $B = \{$circular permutations of $X\}$ and $A = \{$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 5.1 at the gap between A_1 and A_2, 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 $f^{-1}(b) \cap f^{-1}(c) = \varnothing$ (why?[1]). Thus, by the principle of disjoint pre-images of equal size, the number of circular permutations is $5!/5$.

Theorem 5.5.2. [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 $\{1, 2, \ldots, n-1, n\}\}$. Put $B = \{$permutations of $\{1, 2, \ldots, n-$

[1]Think of creating the circular permutation from a given permutation.

$1\}\}$. Define $f : A \to B$ as $f([n, x_1, x_2, \ldots, x_{n-1}, n]) = [x_1, x_2, \ldots, x_{n-1}]$. Define $g : B \to A$ as $g([x_1, x_2, \ldots, x_{n-1}]) = [n, x_1, x_2, \ldots, x_{n-1}, n]$. 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 1.5.5) f is a bijection. ■

Example 5.5.3. 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 5.5.4. 1. Given an arrangement (not a circular 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 the arrangement $[X_2, \ldots, X_n, X_1]$ and by $R_2(X_1, \ldots, X_n)$ we mean the arrangement $[X_3, \ldots, X_n, X_1, X_2]$. 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 $[X_1, \ldots, X_n]$.

Discussion 5.5.5. 1. We have $R_1(ABCABCABC) = [BCABCABCA]$, $R_2(ABCABCABC) = [CABCABCAB]$ and $R_3(ABCABCABC) = [ABCABCABC]$. Thus, the 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 $S = \{A, A, B, B, C, C\}$ with orbit size 2. In fact, if there is an arrangement with orbit size 2 then it's form, by definition, must be $[X_1X_2X_1X_2X_1X_2]$. Thus the element X_1 repeats at least 3 times in S, 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.

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.

Proposition 5.5.6. *The orbit size of an arrangement of an n-multiset is a divisor of n.*

Proof. Suppose, the orbit size of $[X_1, \ldots, X_n]$ is k and $n = kp + r$, for some r, $0 < r < k$. Then,

$$R_k(X_1, \ldots, X_n) = R_{2k}(X_1, \ldots, X_n) = \cdots = R_{kp}(X_1, \ldots, X_n) = R_{k-r}(X_1, \ldots, X_n)$$

as $(p+1)k = pk+k = n-r+k \equiv k-r \pmod{n}$. Thus, $R_{k-r}(X_1, \ldots, X_n) = [X_1, \ldots, X_n]$, contradicting the minimality of k. Hence, $r = 0$. Equivalently, k divides n. ∎

Example 5.5.7. Find the number of circular arrangements of $S = \{A, A, B, B, C, C, D, D, E, E\}$.

Ans: How many arrangements are there of orbit size 1? 0.

How many arrangements are there of orbit size 2? 0.

How many arrangements are there of orbit size 3? 0.

How many arrangements are there of orbit size 4? 0.

How many arrangements are there of orbit size 5? 5!.

How many arrangements are there of orbit size $6, 7, 8, 9$? 0.

How many arrangements are there of orbit size 10? $\frac{10!}{2!2!2!2!2!} - 5!$.

The number of circular arrangements generated by those of orbit size 5 is $5!/5$. The number of circular arrangements generated by those of orbit size 10 is $\frac{10!}{2!2!2!2!2!10} - \frac{5!}{10}$. Thus the total number of circular arrangements is $4! + \frac{10!}{2!2!2!2!2!10} - \frac{5!}{10}$.

Discussion 5.5.8. [Binary operations] We want to provide another way to count the number of circular arrangements. Let $[X_1, \ldots, X_n]$ and $[Y_1, \ldots, Y_n]$ be two arrangements of an n-multiset. Then, in the remainder of this section, we shall consider expressions like $[X_1, \ldots, X_n] + [Y_1, \ldots, Y_n]$. By $[R_i + R_j](X_1, \ldots, X_n)$, we mean the expression $R_i(X_1, \ldots, X_n) + R_j(X_1, \ldots, X_n)$. By $R_i([X_1, \ldots, X_n] + [Y_1, \ldots, Y_n])$ we denote the expression $R_i(X_1, \ldots, X_n) + R_i(Y_1, \ldots, Y_n)$.

Example 5.5.9. Think of all arrangements $P_1, \ldots, P_n$, of two A's, two B's and two C's, where $n = \frac{6!}{2!2!2!}$. 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, R_3 take $[ABCABC]$ to itself; R_1, R_4 will take $[CABCAB]$ to $[ABCABC]$; R_2, R_5 will take $[BCABCA]$ to $[ABCABC]$; and no other arrangement after rotation will give $[ABCABC]$.

Proposition 5.5.10. *Let $P_1, \ldots, P_n$ be all the arrangements of an m-multiset. Then,*

$$[R_0 + \cdots + R_{m-1}](P_1 + \cdots + P_n) = m(P_1 + \cdots + P_n).$$

Proof. In fact, $[R_0 + \cdots + R_{m-1}](P_1 + \cdots + P_n)$ means, take all arrangements and apply all rotations $(R_0, \ldots, R_{m-1})$, and collect all resulting arrangements.

Note that, if we apply R_0 on $(P_1 + \cdots + P_n)$, we get one copy of each arrangement. Similarly, if we apply R_i on $(P_1 + \cdots + P_n)$, we get one copy of each arrangement. So, $[R_0 + \cdots + R_{m-1}](P_1 + \cdots + P_n)$ will contain m copies of each arrangement. ∎

Proposition 5.5.11. *Let P be an arrangement of an m-multiset which has orbit size k. Then the number of rotations R_i, $i = 0, 1, \ldots, m-1$ which* **fix** *P (that is, satisfy $R_i(P) = P$) is $\frac{m}{k}$. Furthermore,*

$$[R_0 + R_1 + \cdots + R_{m-1}](P) = \frac{m}{k} \operatorname{orbit}(P).$$

Proof. As k is the orbit size of P, we already know that k divides m. Put $p = m/k$. Then $R_0, R_k, \ldots, R_{(p-1)k}$ fix P. If there is any other s such that R_s fixes P, then noting that s is not a multiple of k, let $s = kj + r$, where $0 < r < k$. It now follows that $R_r(P) = P$. This is a contradiction to the fact that k is the orbit size of P.

The next assertion follows from the fact that

$$[R_0 + \cdots + R_{k-1}](P) = [R_k + \cdots + R_{2k-1}](P) = \cdots = [R_{(p-1)k} + \cdots + R_{pk-1}](P)$$

is the orbit(P). ■

Discussion 5.5.12. Let P be an arrangement of an m-multiset S which has orbit size k. Recall that each orbit accounts for one circular arrangement of objects in S. Thus $[R_0 + \cdots + R_{m-1}](P)$ accounts for m/k counts of the same circular arrangement.

Now, let $P_1, \ldots, P_n$ be all the arrangements of objects in S. Then,

$$\begin{aligned} \sum_{P_i} (\text{the number of rotations fixing } P_i) \text{ orbit}(P_i) &= \sum_{P_i} [R_0 + \cdots + R_{m-1}](P_i) \\ &= m(P_1 + \cdots + P_n) \\ &= m(\text{all circular arrangements}). \end{aligned}$$

The number of circular arrangements contained in the LHS being the same as that of the RHS, we get that the total number of all circular arrangements is $\frac{1}{m} \sum_{P_i}$ the number of rotations fixing P_i. But, notice that

$$\begin{aligned} \sum_{P_i} \text{the number of rotations fixing } P_i &= \sum_{P_i} |\{R_j | R_j(P_i) = P_i\}| \\ &= |\{(P_i, R_j) | R_j(P_i) = P_i\}| \\ &= \sum_{R_j} |\{P_i | R_j(P_i) = P_i\}| \\ &= \sum_{R_j} \text{the number of } P_i\text{'s fixed by } R_j. \end{aligned}$$

Hence, the total 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 5.5.13. 1. How many circular arrangements of $\{A, A, A, B, B, B, C, C, C\}$ are there?

Ans: First way:

orbit size	no of arrangements	no of circular arrangements
1	0	0
2	0	0
3	$3!$	$\frac{3!}{3} = 2$
$4, 5, 6, 7, 8$	0	0
9	$\frac{9!}{3!3!3!} - 3!$	$\frac{\frac{9!}{3!3!3!} - 3!}{9} = 186$
Total		188

Second way:

Rotations	no of arrangements fixed by it
R_0	$\frac{9!}{3!3!3!}$
R_1	0
R_2	0
R_3	$3!$
R_4, R_5, R_7, R_8	0
R_6	$3!$
Total	$5.6.7.8 + 3! + 3!$

Thus, the number of circular arrangements is

$$\frac{5.6.7.8 + 12}{9} = \frac{(5.2.7.8 + 4)}{3} = \frac{564}{3} = 188.$$

2. Determine the number of circular arrangements of size 5 using the alphabets A, B and C.

   Ans: First way:

orbit size	no of arrangements	no of circular arrangements
1	3	3
$2, 3, 4$	0	0
5	$3^5 - 3$	$\frac{3^5-3}{5} = 48$
Total		51

   Second way:

Rotations	no of arrangements fixed by it
R_0	3^5
R_1	3
R_2	3
R_3	3
R_4	3
Total	$3^5 + 3 + 3 + 3 + 3$

   Hence, the number of circular arrangements is $\frac{3^5+4\cdot 3}{5} = 51$.

   Verify that the answer will be 8 if we have just two alphabets A and B.

Exercise **5.5.14.** *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. *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, in the following cases.*

   (a) *The flowers can have colors 'red' or 'blue'.*

   (b) *The flowers can have the colors 'red', 'blue' or 'green'.*

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, 4 of which are blue and 2 are red.*

4. *Find the number of circular permutations of $\{A, A, B, B, C, C, C, C\}$.*

5. *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 which can have colors,* $R_1, \ldots, R_k$.

---

6. *Persons* $P_1, \ldots, P_{100}$ *are seating on a circle facing the center and talking. With this situation find answers to the following questions.*

   (a) *If* P_i *tells lies, then the person to his right tells truths. What is the minimum possible number of persons telling truths? Give a circular arrangement of* L *and* T *showing that the minimum is attainable. What is the orbit size of this circular arrangement?*

   (b) *What if we change the condition to 'if* P_i *tells lies, then the second person to his right tells truths'? Give a circular arrangement of* L *and* T *showing that the minimum is attainable. What is the orbit size of such a circular arrangement?*

   (c) *What if we change the condition: 'if* P_i *talks lie, then the next two persons to his right talk truth'? Give a circular arrangement of* L *and* T *showing that the minimum is attainable. What is the orbit size of this circular arrangement?*

5.6 Set partitions

Discussion 5.6.1. There are 9 balls with numbers $1, 2, \ldots, 9$ written on them. Imagine that we have to carry them in two identical polythene bags, without having a bag empty. In how many ways, can we do that? Well, we can carry them like

$\{1\}, \{2, 3, 4, 5, 6, 7, 8, 9\}$ or

$\{1, 2, 9\}, \{3, 4, 5, 6, 7, 8\}$ and other ways.

Notice that $\{1, 2, 9\}, \{3, 4, 5, 6, 7, 8\}$ and $\{3, 4, 5, 6, 7, 8\}, \{1, 2, 9\}$ do not give us different ways of carrying as the bags are identical.

Let S be a nonempty set and $k \in \mathbb{N}$. A **partition of S into k subsets** means a collection of k pairwise disjoint nonempty subsets of S whose union is S. For brevity, a partition of S into k subsets is called a **k-partition of S**.

Example 5.6.2. 1. (a) Each of the collections $\big\{\{1, 2\}, \{3\}, \{4, 5, 6\}\big\}, \big\{\{1, 3\}, \{2\}, \{4, 5, 6\}\big\}$ and $\big\{\{1, 2, 3, 4\}, \{5\}, \{6\}\big\}$ is a 3-partition of $[6]$, whereas the collection $\{\{1, 2, 3\}, \{3, 4, 5, 6\}\}$ is not a partition of any set.

2. There are $2^{n-1} - 1$ ways to obtain a 2-partition of $[n]$. To see this, observe that, if $n = 1$, then we cannot have a 2-partition of $[1]$ and the formula also gives the value 0. So let $n \geq 2$. For each non-trivial $A \subseteq [n]$ (that is, $A \neq \varnothing, [n]$), the set $\{A, A^c\}$ is a 2-partition of $[n]$. Since $\{A, A^c\}$ and $\{A^c, A\}$ are regarded as the same 2-partition and since, the total number of non-trivial subsets of $[n]$ equals $2^n - 2$, the required number is $2^{n-1} - 1$.

3. 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.

Discussion 5.6.3. 1. In how many ways can we 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 we remove the brackets, then we get an arrangement of elements of $\{1,2,\ldots,12\}$.

2. How many arrangements do we generate from a partition which has p_i subsets of size n_i, where $n_1 < \cdots < n_k$?

   Ans: $p_1!(n_1!)^{p_1}\cdots p_k!(n_k!)^{p_k} = \prod\limits_{i=1}^{k}[p_i!(n_i!)^{p_i}]$.

Theorem 5.6.4. **[Set partition]** *The number of partitions of $[n]$ consisting of p_i subsets of size n_i, $i = 1,2,\ldots,k$ where $n_1 < \cdots < n_k$, is*

$$\frac{n!}{(n_1!)^{p_1}p_1!\cdots(n_k!)^{p_k}p_k!}.$$

Proof. Let X be the set of all arrangements of elements of $[n]$ and Y be the set partitions of $[n]$ of the given type. Take any $x = x_1\ldots x_n$ be arrangement of elements of $[n]$. Since we know that the sets in the partition have to be in the increasing order of their sizes, this arrangement naturally gives us a way to construct the partition. To do this take the first n_1 letters of this arrangement and make a set. Take the next n_1 letters and make a set. Do this p_1 times. Then take the next n_2 letters and make a set. Continue similarly to finish the job. In fact, once an arrangement x is given, there is only a unique partition of the above type that we will get in this way. Call the resulting partition $f(x)$. Thus we have defined a function $f : X \to Y$.

Note that each partition $y \in Y$ generates $\prod\limits_{i=1}^{k}[p_i!(n_i!)^{p_i}]$ arrangements of elements of $[n]$. This means $|f^{-1}(y)| = \prod\limits_{i=1}^{k}[p_i!(n_i!)^{p_i}]$. Hence, by the principle of disjoint pre-images of equal size, we have $|Y| = \frac{n!}{(n_1!)^{p_1}p_1!\cdots(n_k!)^{p_k}p_k!}$. ∎

Let $n, r \in \mathbb{N}$. Then the number of r-subsets of $[n]$ is called the **Stirling numbers of the second kind** and is denoted by $S(n,r)$. By convention, $S(0,0) = 1$ and $S(n,0) = 0$ for $n \in \mathbb{N}$.

Example 5.6.5. We have $S(5,5) = 1$, as the only way to make a 5-partition of [5] is to consider $\{\{1\},\{2\},\ldots,\{5\}\}$.

We have $S(5,1) = 1$, as the only way to make a 1-partition of [5] is to consider $\{[5]\}$.

We have $S(5,10) = 0$, as there is no way we can make a 10-partition of [5].

We have $S(5,2) = 15$, as the formula is $2^{n-1} - 1$.

We have $S(50,49) = C(50,2)$, as we will have exactly one doubleton set in our partition and rest will be singletons and a subset of size of [50] can be chosen in $C(50,2)$ ways.

Theorem 5.6.6. **[Recurrence for $S(n,r)$]** *Let $n, r \in \mathbb{N}$. Then $S(n+1,r) = S(n,r-1) + rS(n,r)$.*

Proof. If $r = 1$, then the verification is trivial. So let $r > 1$. Take an r-partition F of $[n+1]$. If $\{n+1\}$ is an element of F, then removing that element from F we get an $(r-1)$-partition of $[n]$.

If $\{n+1\}$ is not present in F, then $n+1$ is present in some part with some other elements. Now, if we remove $n+1$ from that part, we get an r-partition of $[n]$. Note that, given any r-partition of $[n]$, by inserting $n+1$ into any of these r parts, we can create r many r-partitions of $[n+1]$. Hence, $S(n+1,r) = S(n,r-1) + rS(n,r)$. ∎

Example 5.6.7. Determine the number of ways of putting n distinct balls into r identical boxes with the restriction that no box is empty.

Ans: Make an r-partition of the set of these balls in $S(n,r)$ ways. One part goes to one box. Since boxes are identical, this can be done in one way. So the answer is $S(n,r)$.

To proceed further, consider the following example.

Example 5.6.8. Let $A = \{a,b,c,d,e\}$ and define an onto function $f : A \to S$ by $f(a) = f(b) = f(c) = 1, f(d) = 2$ and $f(e) = 3$. Then, the collection $\{f^{-1} = \{a,b,c\}, f^{-1}(2) = \{d\}, f^{-1}(3) = \{e\}\}$ gives a 3-partition of A.

Conversely, take a 3-partition of A, say, $\{A_1 = \{a,d\}, A_2 = \{b,e\}, A_3 = \{c\}\}$. Then, this partition gives 3! onto functions f_i from A into $[3]$. Each of them is related to a one-one function $g_i : \{A_1, A_2, A_3\} \to [3]$. We list them below. Notice that $f_i(p) = g_i(A_r)$ if $p \in A_r$.

	A_1	A_2	A_3
g_1	1	2	3
g_2	1	3	2
g_3	2	1	3
g_4	2	3	1
g_5	3	1	2
g_6	3	2	1

$\to$

	a	b	c	d	e
f_1	1	2	3	1	2
f_2	1	3	2	1	3
f_3	2	1	3	2	1
f_4	2	3	1	2	3
f_5	3	1	2	3	1
f_6	3	2	1	3	2

Lemma 5.6.9. *Let $n, k \in \mathbb{N}$. Then the number of onto functions from $[n]$ to $[k]$ is $S(n,k)k!$.*

Proof. Let X be the set of all onto functions from $[n]$ to $[k]$ and Y be the set of all k-partitions of $[n]$.

Observe that, when $f : [n] \to [k]$ is an onto function, then $\{f^{-1}(1), \ldots, f^{-1}(k)\}$ is a unique k-partition of $[n]$. Keeping that in mind, we define $F : X \to Y$ as $F(f) = \{\{f^{-1}(1), \ldots, f^{-1}(k)\}$.

On the other hand, given a k-partition $\alpha = \{S_1, \ldots, S_k\}$ of $[n]$, we can define $k!$ onto functions $f : [n] \to [k]$ by taking a one-one function $\sigma : \{S_1, \ldots, S_k\} \to [k]$ and then defining $f(p) = \sigma(S_i)$ if $p \in S_i$, $i = 1, \ldots, k$. This means $|F^{-1}(\alpha)| = n!$, for each $\alpha \in Y$.

Hence, by the principle of disjoint pre-images of equal size, we have $|X| = k!S(n,k)$. ∎

Lemma 5.6.10. *Let $n, m \in \mathbb{N}$. Then,*

$$n^m = \sum_{k=1}^{n} C(n,k)k!S(m,k). \tag{5.2}$$

Proof. The LHS is the number of all functions $f : [m] \to [n]$.

On the other hand, any function $f : [m] \to [n]$ is an onto function from $[m]$ to $\operatorname{rng} f$, and $\operatorname{rng} f$ can only be a nonempty subset of $[n]$. So, we can first select a subset $A \subseteq [n]$ of size $k \geq 1$ and then consider all onto functions $f : [m] \to A$. This has to be done for each subset A of size k and for each $k = 1, \ldots, n$. Choosing a subset A of size k can be done in $C(n,k)$ many ways and there are $k!S(m,k)$ many onto functions from $[m]$ to A. So the total number of functions becomes the expression in the RHS. ∎

Proposition 5.6.11. *Let $n, k \in \mathbb{N}$. Then* $S(n+1, k+1) = \sum_{i=0}^{n} C(n,i)S(n-i,k) = \sum_{i=0}^{n} C(n,i)S(i,k)$.

Proof. Imagine forming a $(k+1)$-partition of $[n+1]$. The number $n+1$ must belong to some part. Suppose there are i other elements in this part. They can be chosen in $C(n,i)$ ways. The rest of the elements of the set $[n+1]$ must get divided into k parts in $S(n-i,k)$ ways. Since i varies from 0 to n, we have the identity. As $C(n,i) = C(n,n-i)$, we get the second equality. ∎

Remark 5.6.12.

1. Recall that the number of onto functions $f : [n] \to [m]$ is the same as the number of ways to put n distinct objects $1, 2, \ldots, n$ into m distinct boxes $1, 2, \ldots, m$. In fact, this is how, we counted the total number of such functions to be m^n.
2. The number of onto functions $f : [n] \to [m]$ is the same as the number of ways to put n distinct balls into m distinct boxes, so that no box is empty.
3. The numbers $S(r,k)$ can be recursively calculated using Equation (5.2). For example, $S(5,3) = S(4,2) + 3S(4,3) = 2^{4-1} - 1 + 3C(4,2) = 7 + 18 = 25$.

Summary of some work done till now

1. In how many ways can we distribute n distinct books to r students, if there is no restriction at all? All functions : r^n.
2. In how many ways can we distribute n distinct books to r students, if each student gets at most one book? All injections : $C(r,n)n!$.
3. In how many ways can we distribute n distinct books to r students, if each student gets at least one book? All onto functions : $S(n,r)r!$.
4. In how many ways can we carry n distinct books in r identical bags, if there is no restriction at all? All partitions : $\sum_{i=0}^{r} S(n,i)$.
5. In how many ways can we carry n distinct books in r identical bags, if each bag contains at most one book? Partition into singletons : 1.
6. In how many ways can we carry n distinct books in r identical bags, if each bag contains at least one book? All r-partitions : $S(n,r)$.
7. In how many ways can we distribute n identical books to r students, if there is no restriction at all? All non-negative integer solutions : $C(n+r-1, r-1)$.
8. In how many ways can we distribute n identical books to r students, if each student gets at most one book? All n-subset of $[r]$: $C(r,n)$.
9. In how many ways can we distribute n identical books to r students, if each student gets at least one book? All positive integer solutions : $C(n-1, r-1)$.

EXERCISE **5.6.13.**

1. *Determine the number of ways of carrying* 20 *distinct heavy books with* 4 *identical bags if each bag contains* 5 *books?*
2. *Determine the number of ways of distributing* 20 *distinct toys among* 4 *children if each children gets* 5 *toys?*
3. *We know that* $S(n,1) = 1$ *and* $S(n,2) = 2^{n-1} - 1$. *Give a formula for* $S(n,3)$.

4. *For $n \in \mathbb{N}$, let* **Bell**(n) *denote the number of partitions of the set* $[n]$, *i.e.,* $Bell(n) = \sum\limits_{r=0}^{n} S(n,r)$. *It is called the* n^{th} *Bell number. By definition,* $Bell(0) = 1 = Bell(1)$. *Determine* $Bell(n)$, *for* $2 \le n \le 5$. *Prove combinatorially that* $Bell(n+1) = \sum\limits_{k=0}^{n} C(n,k)Bell(k)$.

5. *Suppose* 13 *people get on the lift at level* 0. *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.*

6. *How many functions are there from* $[10]$ *to* $[4]$ *such that each* $i \in [4]$ *has at least two pre-images?*

7. *Let* $n \ge k$ *be natural numbers. Show that* $S(n,k) = \sum 1^{a_1-1}2^{a_2-1}\cdots k^{a_k-1}$, *where the summation is over all solutions of* $a_1 + \cdots + a_k = n$ *in* $\mathbb{N}$, *by showing that the RHS has the same initial values and satisfies the same recurrence relation.*

5.7 Number partitions

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 decreasing order such that $x_1 + \cdots + x_k = n$. By $\pi_n(k)$, we denote the number of partitions of n into exactly k parts and by π_n we denote the number of all partitions of n. Conventionally we take $\pi_0 = 1$. By definition $\pi_n(k) = 0$, whenever $k > n$.

Example 5.7.1. 1. Notice that $(1,1,1,1)$, $(2,2)$, $(2,1,1)$ are some partitions of 4.

2. Notice that $\pi_7(4) = 3$ 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 $\pi_7(3) = 4$.

Discussion 5.7.2. We give here two instances where number partitions occur naturally.

1. Determine the number of ways of carrying n copies of the same book in r identical bags with the restriction that no bag goes empty.

   Ans: As the books are indistinguishable, we need to count the number of books in each bag. As the bags are indistinguishable, arrange them so that the number of books inside the bags are in decreasing order. Also, each bag is nonempty and hence the answer is $\pi_n(r)$.

2. Determine the number of ways of carrying n copies of the same book in r identical bags with with no restriction.

   Ans: As the books are indistinguishable, we need to count the number of books in each bag. As the bags are indistinguishable, arrange them so that the number of books inside the bags are in decreasing order. Also, as empty bags are allowed the resulting sequence (of numbers of books in the bags in increasing order) may have some 0's. Truncating the 0's we obtain a partition of n with at most r parts, that is, $\pi_n(1) + \cdots + \pi_n(r)$.

At times 'a partition of n into k parts' is written in short as 'a k-partition of n'.

Proposition 5.7.3. *Let $n, r \in \mathbb{N}$. Then the number of partitions of n into at most r parts is equal to the number of partitions of $n + r$ into r parts.*

Proof. Given a partition of n into at most r parts, extend it to an r-tuple by adding some 0's at the right end. For example, if $n = 7, r = 4$, we change the partition $(6,1)$ which has at most four parts into $(6,1,0,0)$ which is a four tuple. This can be done uniquely. Next, add 1 to each component of the r-tuple. We get an r-partition of $n+r$. For example, our previous four tuple would now change to $(7,2,1,1)$ which is a partition of 11 into four parts.

Conversely, given an r-partition of $n+r$, subtract 1 from each component. Some of the components might become 0. Truncating them we get a partition of n into at most r parts. ■

Remark 5.7.4. **[Recurrence for $\pi_n(k)$]** Another way of writing the previous result is

$$\pi_n(k) = \pi_{n-k}(0) + \pi_{n-k}(1) + \cdots + \pi_{n-k}(k)$$

and so

$$\pi_n(k) = \pi_{n-1}(k-1) + \pi_{n-k}(k).$$

We can also prove the second one directly using the fact that a k-partition can have the last part 1 or more than 1 and then derive the first one.

Practice **5.7.5.** *Calculate $\pi(n)$ for $n = 1, 2, 3, \ldots, 8$.*

Practice **5.7.6.** *Prove that $\pi_{2r}(r) = \pi_r$ for any $r \in \mathbb{N}$.*

Definition 5.7.7. Let $n, k \in \mathbb{N}$ and $\lambda = (n_1, n_2, \cdots, n_k)$ be a k-partition of n.

1. Then, the **Ferrer's Diagram** of λ is a pictorial representation of the partition created in the following way. The i-th part of the partition is represented by putting n_i equally spaced dots in a row. The first row is on the top. The leftmost dots of each row lies in the same column.
2. The (i,j)**-hook** of the partition consists of the (i,j)-dot along with the dots (of i-th row) to the right of it and the dots (of j-th column) below it. The **hook length** is the number of dots in that particular hook.

Example 5.7.8. Ferrer's diagram for the partitions $\lambda_1 = (5,3,3,2,1,1)$, $\lambda_2 = (6,4,3,1,1)$ and $\lambda_3 = (5,5,4,3,2)$ of 15, 15 and 19 are given below.

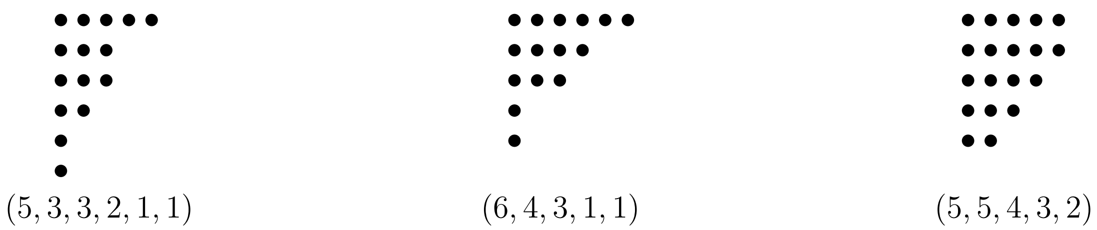


Figure 5.2: Ferrer's diagram of $\lambda_1, \lambda_2, \lambda_3$

Suppose that we have a Ferrer's diagram of some partition λ of n. Observe that the number of dots in the first column of the Ferrer's diagram is greater than or equal to the number of dots in the second column. In general, the number of dots in the i-th column is always greater than or equal to the number of dots in the $(i+1)$-th column. Thus, if we interchange the rows and columns of the Ferrer's diagram (transposing), then the result is another Ferrer's diagram of some partition of n. This new partition is called the **conjugate** of λ and is denoted by λ'. A partition λ of n is called **self conjugate** if $\lambda = \lambda'$.

For instance, if $\lambda = (5,3,3,2,1,1)$ is a partition of 15, then its conjugate is $\lambda' = (6,4,3,1,1)$. The partition $(5,4,3,2,1)$ is a self-conjugate partition of 15.

Remark 5.7.9. Let $\lambda = (n_1, \ldots, n_k)$ be a partition (of some number). One can write the conjugate without drawing the Ferrer's diagram. It's conjugate $\lambda' = (p_1, \ldots, p_{n_1})$ has n_1 components and $p_i =$ the number of components in λ that are at least i. For example, the conjugate of $(5, 3, 1, 1)$ is a partition with 5 components $(p_1, \ldots, p_5)$, where $p_1 =$ the number of components in λ that are at least 1. So $p_1 = 4$. Now, $p_2 =$ the number of components in λ that are at least 2. So $p_2 = 2$. Similarly, $p_3 = 2$, $p_4 = 1$, and $p_5 = 1$. So $\lambda' = (4, 2, 2, 1, 1)$.

Proposition 5.7.10. *Let $n \in \mathbb{N}$. Then the number of self conjugate partitions of n is the same as the number of partitions of n whose parts are distinct odd numbers.*

Proof. Let λ be a self conjugate partition of n with k diagonal dots. For $1 \le i \le k$, define $l_i =$ length of the (i, i)-th hook. Since λ is self-conjugate, each l_i is odd and $(l_1, \ldots, l_k)$ is a strictly decreasing sequence of positive integers with $l_1 + l_2 + \ldots + l_k = n$. Hence, from a self conjugate partition λ of n we have got a partition of n whose parts are distinct and odd.

Conversely, given any partition, say $l = (l_1, \ldots, l_k)$ where parts are distinct and odd, we can get a self conjugate partition by putting l_1 dots in the $(1, 1)$-th hook, l_2 dots in the $(2, 2)$-th hook and so on. Since each l_i is odd, the hook is symmetric and as the hook lengths decrease at least by 2, we see that the corresponding diagram of dots is indeed a Ferrer's diagram. (Try to give a formula for the resulting partition in terms of l_i's.) Hence the result follows. ∎

Proposition 5.7.11. *Let $n \in \mathbb{N}$ and $f(n)$ be the number of partitions of n in which no part is 1. Then $f(n) = \pi_n - \pi_{n-1}$.*

Proof. For $n = 1$, both the sides of the equality are 0. So assume that $n > 1$.

We shall count the complement. Let $\lambda = (n_1, \ldots, n_k)$ be a partition of n with $n_k = 1$. (Since $n > 1$, there are at least two parts.) Then, λ gives rise to 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 number of partitions of n with last part 1 is $\pi_{n-1}(k - 1)$.

Thus, using Remark 5.7.4, the number of partitions of n in which no part is 1 is $\pi_n - \pi_{n-1}$. ∎

EXERCISE **5.7.12.**
1. *Let $n \in \mathbb{N}$. Find an expression for the number of k-partitions of n in which each part is at least 3.*
2. *Let $n, k, m \in \mathbb{N}$. Prove the following.*
   (a) *The number of k-partitions of n with the first (largest) part $m =$ the number of m-partitions of n with the first part k.*
   (b) *The number of k-partitions of n with the first part at most $m =$ the number of partitions of n into at most m parts with the first part k.*
   (c) *The number of partitions of n into at most k parts with the first part at most $m =$ the number of partitions of n into at most m parts with the first part at most k.*

3. *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.*
4. *Recall that a composition of n is an ordered tuple of positive integers whose sum is n. They are also called* **ordered partitions**. *Express the following quantities in terms of Fibonacci numbers ($F_1 = F_2 = 1$).*
   (a) *The number of ordered partitions of n into parts > 1.*
   (b) *The number of ordered partitions of n into parts equal to 1 or 2.*

(c) *The number of ordered partitions of n into odd parts.*

5. *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 partitions of n where no part is divisible by r. Show that $f(n,r) = g(n,r)$.*

5.8 Lattice paths and Catalan numbers

Let $A = (a_1, a_2)$ and $B = (b_1, b_2)$, $a_1 \leq b_1$, $a_2 \leq b_2$, be two points on $\mathbb{Z} \times \mathbb{Z}$. By a **lattice path** from A to B we mean a sequence of points $(A = P_1, \ldots, P_k = B)$ of S such that if $P_i = (x,y)$ then P_{i+1} is either $(x+1, y)$ or $(x, y+1)$, for $1 \leq i \leq k-1$. Thus, at each step we move either one unit right, denoted R, or one unit up, denoted U. For example, from $(2,3)$ if we take the sequence of steps $UURRURRRUR$, then we reach $(8,7)$. This lattice path is shown in the Figure 5.3.

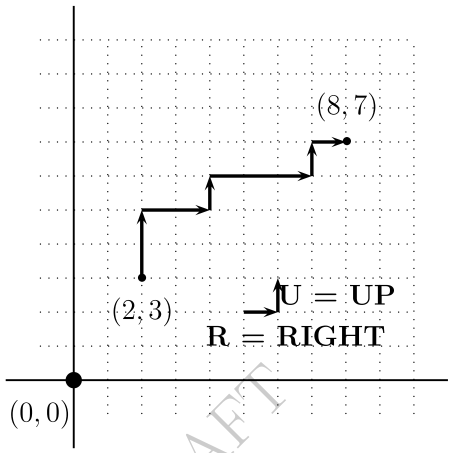


Figure 5.3: A lattice with a lattice path from $(2,3)$ to $(8,7)$

Discussion 5.8.1. How many lattice paths are there from $(0,0)$ to (m,n)?

Ans: As at each step, either the step has to be R or it has to be U. We have to take m many steps of type R in total in order to reach a point with x-coordinate m. Similarly, we have to take n many steps of type U in total in order to reach a point with y-coordinate n. So, any arrangement of m many R's and n many U's will give such a path uniquely. Hence, the answer is $C(m+n, m)$.

Discussion 5.8.2. Use lattice paths to give a combinatorial proof of $\sum\limits_{\ell=0}^{m} C(n+\ell, \ell) = C(n+m+1, m)$.

Ans: Observe that $C(n+m+1, m)$ is the number of lattice paths from $(0,0)$ to $(m, n+1)$. A lattice path from $(0,0)$ to $(m, n+1)$ must touch a point F of the form $(i, n+1)$, $i = 0, 1, \ldots, m$ for the first time. For $i \neq j$, we see that the lattice paths for which $F = (i, n+1)$ are disjoint from the the lattice path for which $F = (j, n+1)$.

Hence, the total number of lattice paths is the sum of the number of lattice paths from $(0,0)$ to $(i, n+1)$. The number of lattice paths for which $F = (i, n+1)$, is nothing but the number of lattice paths from $(0,0)$ to (i,n), which is $C(n+i, i)$. Our proof is complete.

Discussion 5.8.3. 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 $C(2n, n) - C(2n, n-1) = \dfrac{C(2n, n)}{n+1}$.

Discussion 5.8.4. A rectangular grid with m units on x-axis and n units on y-axis is called an **(m, n)-lattice**. By a **standard** (m, n)-lattice, we mean the rectangular grid with opposite corners at $(0, 0)$ and (m, n).

Consider the standard (n, n)-lattice. Recall that a lattice path from $(0, 0)$ to (n, n) can be viewed an arrangement of n many R's and n many U's. An arrangement in which at some position the number of U's is more than that of the R's corresponds to a lattice path which enters the region $y > x$ in that grid.

From the previous discussion, it follows that the number of lattice paths from $(0, 0)$ to (n, n) that do not enter the region above the line $y = x$ is $C(2n, n)/(n + 1)$.

Definition 5.8.5. The n-th **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 $C_0 = 1$.

Example 5.8.6. The different representations of the product $A_1 \cdots A_4$ by using 3 pairs of brackets are $(((A_1A_2)A_3)A_4)$, $((A_1A_2)(A_3A_4))$, $((A_1(A_2A_3))A_4)$, $(A_1((A_2A_3)A_4))$, $(A_1(A_2(A_3A_4)))$. Hence $C_3 = 5$.

Theorem 5.8.7. **[Catalan number]** *Let $n \in \mathbb{N}$. Then $C_n = \frac{C(2n,n)}{n+1}$.*

Proof. Consider a meaningful representation X of the product of $n + 1$ matrices with n pairs of brackets. First we erase, the subscripts, with the understanding that the i-th A from left is A_i.

Claim: After the $(n - k)$-th '(', there are at least $k + 2$ many A's.

Proof of the claim. It is true for $n = 1$, that is when there are only two matrices. Assume it is true for $n = 2, 3, \ldots, p - 1$ Consider a meaningful representation X of the product of $p + 1$ matrices with p pairs of brackets.

Observe that the last (is followed by AA), as the product is meaningful.

Now, treat this (AA) as a single matrix, A. Then our original meaningful representation of the product of $p + 1$ matrices changes into a meaningful representation X^* of p matrices with $p - 1$ pairs of brackets.

Hence, by induction, in X^*, after the $p-k = ((p-1)-(k-1))$-th '(', there are at least $k+1 = k-1+2$ many matrices. This means, in X, after the $(p - k)$-th '(', there are at least $k + 2$ matrices. So the claim is justified.

Drop the right brackets and one A from the right end, to have a sequence of n many '('s and n many A's, where the number of A's used till the $(n - k)$-th '(' is at most $n - (k + 1) = n - k - 1$. So, the number of A's never exceeds the number of '('.

Conversely, given such an arrangement, we can put back the ')'s: first add one more A at the right end; find two consecutive letters from the last '('; put a right bracket after them; treat (AA) as a letter; repeat the process. For example,

$$((A((AAA \to ((A((AAAA \to ((A((AA)AA \to ((A((AA)A)A \to ((A((AA)A))A = ((A((AA)A))A)$$

By previous discussions, the number of such arrangements is $\frac{C(2n,n)}{n+1}$. ∎

Theorem 5.8.8. **[Recurrence relation for C_n]** *Let $n \in \mathbb{N}$. Then* $C_n = \sum\limits_{i=1}^{n} C_{i-1}C_{n-i} = \sum\limits_{i=0}^{n-1} C_iC_{n-1-i}$.

Proof. As C_n is number of ways to multiply $n+1$ pairs of A's with n pairs of brackets, removing the outer pair of brackets, we get two expressions written, one is a meaningful multiplication of k many A's with $k-1$ pairs of brackets and the other is a meaningful multiplication of $n+1-k$ many A's with $n-k$ pairs of brackets, where k can vary from $1, \ldots, n$. These two expressions for a $k = i$ differ from the two expressions for a $k \neq i$. Hence,

$$C_n = \sum_{i=1}^{n} C_{i-1}C_{n-i} = \sum_{i=0}^{n-1} C_iC_{n-1-i}.$$

■

Example 5.8.9. A full binary tree is a rooted binary tree in which every node either has exactly two offsprings or has no offspring, see Figure 5.4. Show that C_n is equal to the number of full binary trees on $2n+1$ vertices.

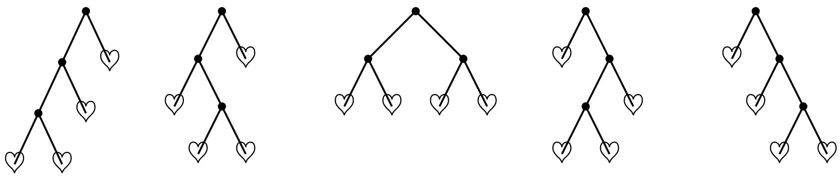


Figure 5.4: Full binary trees on 7 vertices (or 4 leaves)

Let $f(n)$ be the number of full binary trees on $2n+1$ vertices. The idea is to show that $f(n)$ satisfies the same recurrence relation as that of C_n and has the same initial values. We see that $f(0) = 1 = C_0$.

Now take any full binary trees on $2n+1$ vertices and delete the root. We two trees, one on the left, say T_l and one on the right, say T_r. Notice that T_l and T_r are full binary trees and their sizes are $2k+1$ and $2n-2k-1$, respectively, where k can be $0, 1, \ldots, n-1$. And these cases are mutually disjoint, that is, a full binary tree with T_l having k vertices is different from that of one with T_l having different number of vertices. Hence, $f(n) = \sum\limits_{k=0}^{n-1} f(k)f(n-k-1)$. So $f(n) = C_n$.

Remark 5.8.10. The book titled "enumerative combinatorics" by Stanley [13] gives a comprehensive list of places in combinatorics where Catalan numbers appear. The interested reader may have a look at those.

EXERCISE **5.8.11.**

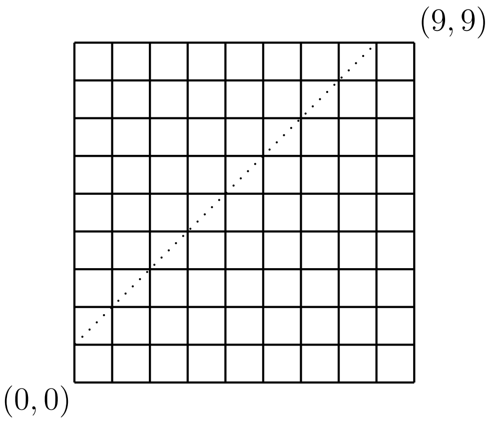
1. *Take $C_0 = 1$. Use the recurrence relation $C_n = \sum\limits_{i=1}^{n} C_{i-1}C_{n-i}$ to show that $C_n = C(2n, n)/(n+1)$.*
2. *Give a bijection between 'the solution set of $x_0 + x_1 + x_2 + \cdots + x_k = n$ in non-negative integers' and 'the number of lattice paths from $(0,0)$ to (n,k)'.*
3. *Use lattice paths to give a combinatorial proof of $\sum\limits_{k=0}^{n} C(n,k) = 2^n$.*
4. *Use lattice paths to give a combinatorial 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).]*

5. *As* $C_n = C(2n, n)/(n+1)$ *is the number of ways of expressing a product of* $n+1$ *many* A*'s using* n *pairs of brackets meaningfully, it is an integer and so* $n+1$ *divides* $C(2n, n)$*. Give an arithmetic proof of this fact.*

6. *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?*

7. *Let* $n \geq 4$ *and 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?*

8. *How many lattice paths are there from* $(0,0)$ *to* $(9,9)$ *which does not cross the dotted line, that is they stay in lower part of the lattice?*



9. *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)?*

10. *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?*

11. *Show that* C_n *also equals the number of integer sequences that satisfy* $1 \leq a_1 \leq a_2 \leq \cdots \leq a_n$ *and* $a_i \leq i$*, for all* $i, 1 \leq i \leq n$*.*

EXERCISE **5.8.12. [Additional exercises]** *:*

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.*

Need to put somewhere

1. For $n \geq 1$, let $a_n = (n-1)n(n+1)$. Write a generating function for a_n and hence evaluate $\sum\limits_{k=1}^{n} (k-1)k(k+1)$.
2. Let $a_n = -3a_{n-1} + 10a_{n+2} + 3 \times 2^n$, for $n \geq 2$ with $a_0 = 0$ and $a_1 = 6$. Use generating function to evaluate a_n.

Chapter 6

Combinatorics - II

6.1 Pigeonhole Principle

The Pigeonhole Principle is an obvious but powerful tool in solving many combinatorial problems. We will prove its mathematical form first.

Theorem 6.1.1. **[Pigeonhole Principle, PHP]** *Let A be a finite set and let $f : A \to \{1, 2, \ldots, n\}$ be a function. Let $p_1, \ldots, p_n \in \mathbb{N}$. If $|A| > p_1 + \cdots + p_n$, then there exists $i \in \{1, 2, \ldots, n\}$ such that $|f^{-1}(i)| > p_i$.*

Proof. On the contrary, suppose that for each $i \in \{1, 2, \ldots, n\}$, $|f^{-1}(i)| \leq p_i$. As A is a disjoint union of the sets $f^{-1}(i)$, we have $|A| = \sum_{i=1}^{n} |f^{-1}(i)| \leq p_1 + \cdots + p_n < |A|$, a contradiction. ∎

The elements of A are thought of as pigeons and the elements of B as pigeon holes; so that the principle is commonly formulated in the following forms, which come in handy in particular problems.

Discussion 6.1.2. **[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 exists $i, 1 \leq i \leq n$ such that the i-th hole contains at least $p_i + 1$ pigeons.

Example 6.1.3.

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 varies 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. 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 $x_i + x_j + x_k \geq 12$.

   Ans: Note that $\frac{\sum\limits_{i=1}^{9} x_i}{9} = \frac{30}{9} = 3 + \frac{3}{9}$. Now use PHP to conclude that there are at least 3 x_i's that are ≥ 4. Hence, the required result follows.

5. Each point of the plane is colored red or blue, then prove that there exist two points of the same color which are at a distance of 1 unit.

   Ans: Take a point, say P. Draw a unit circle with P as the center. If all the points on the circumference have the same color then we are done. Else, the circumference contains a point which has the same color as that of P.

6. 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: Divide the circle into 6 equal sectors by drawing radii so that angle between two consecutive radii is $\pi/3$. By PHP there is a sector containing at least two points. The distance between these two points is at most 1.

7. If $n+1$ integers are selected from $\{1, 2, \ldots, 2n\}$, then there are two, where 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 $y|x$.

8. Given any n integers, $n \geq 1012$ integers, prove that there is a pair that either differ by, or sum to, a multiple of 2021. Is this true if we replace 1012 by 1011?

   Ans: Consider some 1012 integers out of the given ones, say, $n_1, n_2, \ldots, n_{1012}$. Write $S = \{n_1 - n_k, n_1 + n_k : k = 2, \ldots, 1012\}$. Then, $|S| = 2022$ and hence, at least two of them will have the same remainder when divided by 2021. Then, consider their difference.

   The question in the second part has negative answer. For, consider $\{0, 1, 2, \ldots, 1010\}$.

9. Prove that there exist two powers of 3 whose difference is divisible by 2021.

   Ans: Let $S = \{1 = 3^0, 3, 3^2, 3^3, \ldots, 3^{2021}\}$. Then, $|S| = 2022$. As the remainders of any integer when divided by 2021 is $0, 1, 2, \ldots, 2020$, by PHP, there is a pair which has the same remainder. Hence, 2021 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 $3^\ell - 1$. Then $3^\ell - 1 = s \cdot 10^4$ for some positive integer s. That is, $3^\ell = s \cdot 10^4 + 1$ from which the result follows.

11. Suppose that $f(x)$ is a polynomial with integer coefficients. If $f(x) = 5$ for three distinct integers, then for no integer x, $f(x)$ can be equal to 4.

    Ans: Let $f(x) = 5$, for $x \in \{a, b, c\}$. If $f(d) = 4$, for an integer d, then $(d-a)|f(d) - f(a) = -1$. So, $a = d \pm 1$. Similarly $b, c = d \pm 1$. By PHP two of a, b, c are the same, a contradiction.

Alternate. If f is an integer polynomial and $f(m) = 0$ for some integer m, then using the factor/remainder theorem $f(x) = (x - m)g(x)$ for some integer polynomial g. For our problem, we see that $f(x) = (x - a)(x - b)(x - c)g(x) + 5$, where g is an integer polynomial. If $f(n) = 4$, then $(n - a), (n - b), (n - c) | - 1$, so that $(n - a), (n - b), (n - c) \in \{1, -1\}$. By PHP some two of them are the same, a contradiction.

Theorem 6.1.4. *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.*

Does the above statement hold for every collection of mn distinct numbers?

Proof. 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.

The above statement is FALSE. Consider the sequence:

$$n, n - 1, \cdots, 1, 2n, 2n - 1, \ldots, n + 1, 3n, 3n - 1, \cdots, 2n + 1, \cdots, mn, mn - 1, \cdots, mn - n + 1.$$

■

Theorem 6.1.5. *Corresponding to each irrational number a, there exist infinitely many rational numbers $\frac{p}{q}$ such that $|a - \frac{p}{q}| < \frac{1}{q^2}$.*

Proof. It is enough to show that there are infinitely many $(p, q) \in \mathbb{Z}^2$ with $|qa - p| < \frac{1}{q}$. As a is irrational, 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 pair $(p_1, q_1) = (\lfloor ja \rfloor - \lfloor ia \rfloor, j - i)$ satisfies the required property. To generate another pair, 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. ■

Theorem 6.1.6. *Let α be a positive irrational number. Then prove that $S = \{m + n\alpha : m, n \in \mathbb{Z}\}$ is dense in $\mathbb{R}$.*

Proof. Consider any open interval (a, b). By Archimedean property, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < b - a$. Observe that $0 < r_k = k\alpha - \lfloor k\alpha \rfloor < 1$, $k = 1, \ldots, n + 1$. By PHP, some two satisfy

$0 < r_i - r_j < 1/n$. Then $x = r_i - r_j = (i-j)\alpha + \big(\lfloor j\alpha\rfloor - \lfloor i\alpha\rfloor\big) \in S$. Let p be the smallest integer so that $px > a$. If $px \ge b$, then $(a,b) \subseteq \big((p-1)x, px\big)$ and so $b - a \le x < \frac{1}{n}$, which is not possible. So, $px \in (a,b)$ and $px \in S$ as well. Thus, $(a.b) \cap S \ne \emptyset$. ■

EXERCISE **6.1.7.**

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. *Suppose that $f(x)$ is a polynomial with integer coefficients. If*
   (a) *$f(x) = 14$ for three distinct integers, then for no integer x, $f(x)$ can be equal to 15.*
   (b) *$f(x) = 11$ for five distinct integers, then for no integer x, $f(x)$ can be equal to 9.*
3. *There are 7 distinct real numbers. Is it possible to select two of them, say x and y such that $0 < \frac{x-y}{1+xy} < \frac{1}{\sqrt{3}}$?*
4. *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.*
5. *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?*
6. *Choose 5 points at random inside an equilateral triangle of side 2 units. Show that there exist two points that are away from each other by at most 1 unit.*
7. *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.*
8. *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.*
9. *Each point of the plane is colored red or blue, then prove the following.*
   (a) *There is an equilateral triangle all of whose vertices have the same color.*
   (b) *There is a rectangle all of whose vertices have the same color.*
10. *Show that among any 6 integers from $\{1,2,\ldots,10\}$, there exists a pair with odd sum.*
11. *Any 14-subset of $\{1,2,\ldots,46\}$ has four elements a,b,c,d such that $a+b = c+d$.*
12. *Show that if 9 of the 12 chairs in a row are filled, then some 3 consecutive chairs are filled. Will 8 work?*
13. *Show that every n-sequence of integers has a consecutive subsequence with sum divisible by n.*
14. *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 $a+b=c$.*
15. *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.*
16. *Consider a chess board with two of the diagonally opposite corners removed. Is it possible to cover the board with pieces of rectangular dominoes whose size is exactly two board squares?*
17. *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?*
18. *Fifteen squirrels have 104 nuts. Then, some two squirrels have equal number of nuts.*

19. *Let* $\{x_1, x_2, \ldots, x_n\} \subseteq \mathbb{Z}$. *Prove that there exist* $1 \le i \le j \le n$ *such that* $x_i + x_{i+1} + \cdots + x_{j-1} + x_j$ *is a multiple of* 2021, *whenever* $n \ge 2021$.

20. *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.*

21. *Show that there is a non-zero integer multiple of* $\sqrt{2021}$ *whose decimal representation has* 2022 *consecutive zeroes after the first decimal point.*

22. *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.*

23. *Suppose we are given any ten* 4*-subsets of* $\{1, 2, \ldots, 11\}$. *Then, show that some two of them have at least* 2 *elements in common.*

24. *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.*

25. *If* 58 *entries of a* 14×14 *matrix are* 1 *and the remaining entries are* 0, *then prove that there is a* 2×2 *submatrix with all entries* 1.

26. *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* $|f^{-1}(b_i)| \ge a_i$.

27. *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.*

28. *Let* $S \subseteq \{1, 2, \ldots, 100\}$ *be a* 10*-set. Then, some two disjoint subsets of* S *have equal sum.*

29. *Prove that corresponding to each* $n \in \mathbb{N}$, n *odd, there exists an* $\ell \in \mathbb{N}$ *such that* n *divides* $2^{\ell} - 1$.

30. *Does there exist a multiple of* 2021 *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.*

31. *Each natural number has a multiple of the form* $9 \cdots 90 \cdots 0$, *with at least one* 9.

6.2 Principle of Inclusion and Exclusion

We start this section with the following example.

Example 6.2.1. How many natural numbers $n \le 1000$ are not divisible by any of $2, 3$?

Ans: Let $A_2 = \{n \in \mathbb{N} | n \le 1000,\ 2|n\}$ and $A_3 = \{n \in \mathbb{N} | n \le 1000,\ 3|n\}$. 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 6.2.2. **[Principle of Inclusion and Exclusion, PIE]** *Let* $A_1, \cdots, A_n$ *be finite subsets of a set* U. *Then,*

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k+1} \left[\sum_{1 \le i_1 < \cdots < i_k \le n} \left| A_{i_1} \cap \cdots \cap A_{i_k} \right| \right]. \tag{6.1}$$

Or equivalently, the number of elements of U which are in none of $A_1, A_2, \ldots, A_n$ equals

$$\left|U \setminus \bigcup_{i=1}^{n} A_i\right| = |U| - \sum_{k=1}^{n}(-1)^k \left[\sum_{1\le i_1<\cdots<i_k\le n} \left|A_{i_1}\cap\cdots\cap A_{i_k}\right|\right].$$

Proof. Let $x \notin \bigcup_{i=1}^{n} A_i$. Then, we show that inclusion of x in some A_i contributes (increases the value) 1 to both sides of Equation (6.1). 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 (6.1) 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 (6.1) and hence the required result follows. The proof of the equivalent condition is left for the readers. ■

Example 6.2.3. 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 $A_i = \{n \in \mathbb{N} | n \le 10000,\ i|n\}$. Therefore, the required answer is $10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$.

Definition 6.2.4. **[Euler Totient Function]** For a fixed $n \in \mathbb{N}$, the **Euler's totient function** is defined as $\varphi(n) = |\{k \in \mathbb{N} : k \le n, \gcd(k,n) = 1\}|$.

Thus, $\varphi(n)$ is the number of natural numbers less than or equal to n and relatively prime to n. For instance, $\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 3, \varphi(12) = 4$, etc.

Theorem 6.2.5. *Let $p_1, \ldots, p_k$ be the distinct prime divisors of n. 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, $|A_i| = \dfrac{n}{p_i}$, $|A_i \cap A_j| = \dfrac{n}{p_i p_j}$, and so on. By PIE,

$$\begin{aligned}\varphi(n) &= n - |\bigcup_i A_i| = n\Big[1 - \sum_{i=1}^{k}\frac{1}{p_i} + \sum_{1\le i<j\le k}\frac{1}{p_i p_j} - \cdots + (-1)^k \frac{1}{p_1 p_2\cdots p_k}\Big] \\ &= n\big(1 - \frac{1}{p_1}\big)\big(1 - \frac{1}{p_2}\big)\cdots\big(1 - \frac{1}{p_k}\big)\end{aligned}$$

■

Definition 6.2.6. **[Derangement]** A **derangement** of objects in a finite set S is a permutation/arrangement σ on S such that for each x, $\sigma(x) \ne x$. The number of derangements of $\{1,2,\ldots,n\}$ is denoted by D_n with the convention that $D_0 = 1$.

For example, $2,1,4,3$ is a derangement of $1,2,3,4$, but $2,3,1,4$ is not a derangement of $1,2,3,4$.

If a sequence (x_n) converges to some limit ℓ, we say that x_n is approximately ℓ for large values of n, and write $x_n \approx \ell$.

Theorem 6.2.7. *For $n \in \mathbb{N}$, $D_n = n! \sum\limits_{k=0}^{n} \dfrac{(-1)^k}{k!}$. Consequently, $\dfrac{D_n}{n!} \approx \dfrac{1}{e}$.*

Proof. For each $i, 1 \le i \le n$, 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,

$$|\bigcup_i A_i| = n.(n-1)! - C(n,2)(n-2)! + \cdots + (-1)^{n-1}C(n,n)0! = n!\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k!}.$$

So, $D_n = n! - |\bigcup_i A_i| = n!\sum\limits_{k=0}^{n}\frac{(-1)^k}{k!}$. Since $\sum\limits_{k=0}^{\infty}\frac{(-1)^k}{k!} = e^{-1}$, it follows that $\lim\limits_{n\to\infty}\frac{D_n}{n!} = \frac{1}{e}$. ∎

Example 6.2.8. How many square-free integers do not exceed n for a given $n \in \mathbb{N}$?

Answer: Let $P = \{p_1, \cdots, p_s\}$ be the set of primes not exceeding $\sqrt{n}$ and for $1 \le i \le s$, let A_i be the set of integers between 1 and n that are multiples of p_i^2. Then

$$|A_i| = \left\lfloor \frac{n}{p_i^2} \right\rfloor, \quad |A_i \cap A_j| = \left\lfloor \frac{n}{p_i^2 p_j^2} \right\rfloor, \quad \cdots$$

So, the number of square-free integers not greater than n is

$$n - |\bigcup_{i=1}^{s} A_i| = n - \sum_{i=1}^{s}\left\lfloor \frac{n}{p_i^2} \right\rfloor + \sum_{1\le i<j\le s}\left\lfloor \frac{n}{p_i^2 p_j^2} \right\rfloor - \sum_{1\le i<j<k\le s}\left\lfloor \frac{n}{p_i^2 p_j^2 p_k^2} \right\rfloor + \cdots$$

For $n = 100$, we have $P = \{2,3,5,7\}$. So, the number of square-free integers not exceeding 100 is

$$100 - \left\lfloor \frac{100}{4} \right\rfloor - \left\lfloor \frac{100}{9} \right\rfloor - \left\lfloor \frac{100}{25} \right\rfloor - \left\lfloor \frac{100}{49} \right\rfloor + \left\lfloor \frac{100}{36} \right\rfloor + \left\lfloor \frac{100}{100} \right\rfloor = 61.$$

EXERCISE **6.2.9.**

1. *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.*
2. *Let $n \in \mathbb{N}$. Using PIE, show that $S(n,r) = \frac{1}{r!}\sum\limits_{i=0}^{r-1}(-1)^i C(r,i)(r-i)^n$.*
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 over English alphabet that do not contain all the vowels.*
5. *Let $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ Prove that $\varphi(mn) = \varphi(m)\varphi(n)$.*
6. *Determine all natural numbers n satisfying $\varphi(n) = 13$.*
7. *Determine all natural numbers 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. *For each fixed $n \in \mathbb{N}$, use mathematical induction to prove that $\sum\limits_{d|n}\varphi(d) = n$.*
10. *A function $f : \mathbb{N} \to \mathbb{N}$ is said to be* **multiplicative** *if $f(nm) = f(n)f(m)$, whenever $\gcd(n,m) = 1$. 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.*

11. *Show that for* $n \geq 2$, $D_n = \lfloor \frac{n!}{e} + \frac{1}{2} \rfloor$.

12. *Prove combinatorially:* $\sum\limits_{i=0}^{n} C(n,i) D_{n-i} = n!$.

13. *Find the number of non-negative integer solutions of* $a+b+c+d = 27$, *where* $1 \leq a \leq 5$, $2 \leq b \leq 7$, $3 \leq c \leq 9$, $4 \leq d \leq 11$.

14. *Let* x *be a natural number 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?*

15. *In how many ways the digits* $0, 1, \ldots, 9$ *can be arranged so that the digit* i *is never followed immediately by* $i+1$.

16. *Determine the number of strings of length* 15 *that use some or all of the digits* $0, 1, \ldots, 9$, *so that no string contains all the* 10 *digits.*

17. *Determine the number of ways of permuting the* 26 *letters of the English alphabet so that none of the patterns lazy, run, show and pet occurs.*

18. *Let* $S = \{(n_1, n_2, n_3) | n_i \in \mathbb{N}, \sum n_i = 15\}$. *Evaluate* $\sum\limits_{(n_1,n_2,n_3) \in S} \dfrac{15!}{n_1! n_2! n_3!}$.

19. *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?*

6.3 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 6.3.1.

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 $\mathbb{C}$ and is denoted by $\mathbb{Q}[[x]]$. By $\text{CF}[x^n, f]$, we denote 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 $f, g \in \mathbb{Q}[[x]]$ are said to be equal if $\text{CF}[x^n, f] = \text{CF}[x^n, g]$ for all $n \geq 0$.

3. Let $f(x) = \sum\limits_{n \geq 0} a_n x^n$ and $g(x) = \sum\limits_{n \geq 0} b_n x^n$ be elements in $\mathbb{Q}[[x]]$. 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) scalar multiplication is defined by $\text{CF}[x^n, \alpha f] = \alpha \text{CF}[x^n, f]$.

   Thus, with the above operations, the class of formal power series $\mathbb{Q}[[x]]$ over $\mathbb{Q}$, is a vector space which is isomorphic to the space of all sequences.

   (c) One also defines the product (called the **Cauchy product**) 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 6.3.2. 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 $2 \le k \le 6$.

Alternate. In any such word, we need m many A's and n many B's with $m+n=8$, $m \le 6$ and $n \le 6$. 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

$$8!\left[1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\frac{x^5}{5!}+\frac{x^6}{6!}\right]\left[1+y+\frac{y^2}{2!}+\frac{y^3}{3!}+\frac{y^4}{4!}+\frac{y^5}{5!}+\frac{y^6}{6!}\right].$$

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 (rearrangements) are there of the word $MISSISSIPPI$?

Ans: Using basic counting, the answer is $\dfrac{11!}{4!4!2!}$.

Alternate. For another understanding, note that $\dfrac{11!}{4!4!2!} = 11! \times \text{CF}\left[x^{11}, x\dfrac{x^4}{4!}\dfrac{x^4}{4!}\dfrac{x^2}{2!}\right]$. Here the numbers $1 = \text{CF}[x,x]$, $\dfrac{1}{4!} = \text{CF}\left[x^4, \dfrac{x^4}{4!}\right]$, $\dfrac{1}{4!} = \text{CF}\left[x^4, \dfrac{x^4}{4!}\right]$ and $\dfrac{1}{2!} = \text{CF}\left[x^2, \dfrac{x^2}{2!}\right]$ correspond to the number of occurrences of M, I, S and P, respectively. Hence, the readers should note that

$$\begin{aligned}
\frac{11!}{4!4!2!} &= 11!\,\text{CF}\left[x^{11}, (1+x)\big(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}\big)^2\big(1+x+\frac{x^2}{2!}\big)\right], \text{ or} \\
\frac{11!}{4!4!2!} &= 11!\,\text{CF}\left[x^{11}, \big(x+\frac{x^2}{2!}+\cdots\big)\big(\frac{x^4}{4!}+\frac{x^5}{5!}+\cdots\big)^2\big(\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\big)\right]
\end{aligned}$$

3. How many multi-subsets of size 4 of the multiset $\{E,X,A,M,I,N,A,T,I,O,N\}$ are there?

Ans: By direct counting the answer is

$$\begin{aligned}
& C(5,4)+C(5,3)C(3,1)+[C(5,2)C(3,2)+C(5,2)C(3,1)] \\
& +[C(5,1)C(3,3)+C(5,1)C(3,1)C(2,1)]+[C(5,0)C(3,2)+C(5,0)C(3,1)] = 136.
\end{aligned}$$

Alternate. It is as good as asking how many A's are you including and how many E's, etc. Suppose that we are considering A^2EM (means $\{A,A,E,M\}$). But this is a term of degree 4 in

$$(1+A+A^2)(1+E)(1+I+I^2)(1+M)(1+N+N^2)(1+O)(1+T)(1+X).$$

So their number is nothing but

$$\begin{aligned}
& \text{CF}\big[x^4, (1+x)^5(1+x+x^2)^3\big] = \\
& \text{CF}\big[x^4, (1+5x+10x^2+10x^3+5x^4+\cdots)(1+3x+6x^2+7x^3+6x^4+\cdots)\big] = 136.
\end{aligned}$$

4. How many non-negative integer solutions of $u+v+w+t=10$ are there?

   Ans: Note that u can take any value from 0 to 10 which corresponds to $1+x+\cdots+x^{10}$. Hence, 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 6.3.3. [Generating Functions] Let $(b_n) = (b_0, b_1, b_2, \ldots,)$ be a sequence of integers. Then,

1. the **ordinary generating function** (**ogf**) is the formal power series

$$b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots, \text{ and}$$

2. the **exponential generating function** (**egf**) is the formal power series

$$b_0 + b_1 x + b_2 \frac{x^2}{2!} + b_3 \frac{x^3}{3!} + \cdots.$$

If the sequence has finitely many elements then the generating functions have finitely many terms.

Example 6.3.4. 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 $\text{CF}\left[x^r, \dfrac{1}{(1-x^2)(1-x^3)(1-x^5)}\right]$.

Remark 6.3.5. 1. Let $f(x) = \sum\limits_{n\ge 0} a_n \frac{x^n}{n!}, g(x) = \sum\limits_{n\ge 0} b_n \frac{x^n}{n!} \in \mathbb{Q}[[x]]$. Then, in case of egf, their product equals $\sum\limits_{n\ge 0} d_n \frac{x^n}{n!}$, where $d_n = \sum\limits_{k=0}^{n} C(n,k) a_k b_{n-k}$, for $n \ge 0$.

2. Note that $e^{e^x-1} \in \mathbb{Q}[[x]]$ 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

$$\text{CF}\big[x^m, e^{e^x-1}\big] = \text{CF}\left[x^m, \sum_{n\ge 0} \frac{(e^x-1)^n}{n!}\right] = \sum_{n=0}^{m} \text{CF}\left[x^m, \frac{(e^x-1)^n}{n!}\right]. \tag{6.2}$$

   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 $e^{e^x} \notin \mathbb{Q}[[x]]$ as computing $\text{CF}\big[x^m, e^{e^x}\big]$, for all $m \ge 0$, requires infinitely many computations.

3. Recall that if $f(x) = \sum\limits_{n\ge 0} a_n x^n, g(x) = \sum\limits_{n\ge 0} b_n x^n \in \mathbb{Q}[[x]]$ then the composition

$$(f\circ g)(x) = f(g(x)) = \sum_{n\ge 0} a_n (g(x))^n = \sum_{n\ge 0} a_n \Big(\sum_{m\ge 0} b_m x^m\Big)^n$$

   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 $\sum\limits_{k\ge 0} a_k x^k \in \mathbb{Q}[[x]]$ (*i.e.*, with $a_k \in \mathbb{Q}$) and hence e^{x+1} is not a formal power series over $\mathbb{Q}$.

With the algebraic operations as defined in Definition 6.3.1.3, it can be checked that $\mathbb{Q}[[x]]$ 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 $f(x) = \sum\limits_{n\geq 0} a_n x^n$ is said to have a **reciprocal** if there exists another element $g(x) = \sum\limits_{n\geq 0} b_n x^n \in \mathbb{Q}[[x]]$ such that $f(x) \cdot g(x) = 1$. So, the question arises, under what conditions on $\text{CF}[x^n, f]$, can we find $g(x) \in \mathbb{Q}[[x]]$ such that $f(x)g(x) = 1$. The answer to this question is given in the following proposition.

Proposition 6.3.6. *The reciprocal of $f \in \mathbb{Q}[[x]]$ exists if and only if $\text{CF}\big[x^0, f\big] \neq 0$. Further, if $a_n \in \mathbb{Q}$, for all n then $a_n \in \mathbb{Q}$, for all n.*

Proof. Let $g(x) = \sum\limits_{n\geq 0} b_n x^n \in \mathbb{Q}[[x]]$ be the reciprocal of $f(x) = \sum\limits_{n\geq 0} a_n x^n$. 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 $n \geq 1$.

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 $k \leq r$, then using $0 = c_{r+1} = a_{r+1} b_0 + a_r b_1 + \cdots + a_1 b_r + a_0 b_{r+1}$, we get

$$b_{r+1} = -(a_{r+1} b_0 + a_r b_1 + \cdots + a_1 b_r)/a_0.$$

Hence, the required result follows. ■

The next result gives the condition under which the composition $(f \circ g)(x)$ is well defined.

Proposition 6.3.7. *Let $f, g \in \mathbb{Q}[[x]]$. Then, the composition $(f \circ g)(x) \in \mathbb{Q}[[x]]$ 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 $g \in \mathbb{Q}[[x]]$, with $\text{CF}\big[x^0, g(x)\big] = 0$, such that $(f \circ g)(x) = x$. Furthermore, $(g \circ f)(x) \in \mathbb{Q}[[x]]$ and $(g \circ f)(x) = x$.*

Proof. As $(f \circ g)(x) \in \mathbb{Q}[[x]]$, 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, $(f \circ g)(x) \in \mathbb{Q}[[x]]$. 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 6.3.8. **[Basic facts]** *Recall the following statements from Binomial theorem.*

1. $\text{CF}\big[x^n, (1-x)^{-1} = (1 + x + x^2 + \cdots)\big] = 1.$
2. $(a_0 + a_1 x + \cdots)(1 + x + x^2 + \cdots) = a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \cdots.$
3. $\text{CF}\big[x^n, (1-x)^{-r} = (1 + x + x^2 + \cdots)^r\big] = C(n + r - 1, n)$. *Thus,*

$$(1-x)^{-5} = C(4,4) + C(5,4)x + C(6,4)x^2 + \cdots.$$

4. $(1 - x^m)^n = 1 - C(n,1)x^m + C(n,2)x^{2m} - \cdots + (-1)^n x^{nm}.$
5. $(1 + x + x^2 + \cdots + x^{m-1})^n = \left(\dfrac{1-x^m}{1-x}\right)^n = (1-x^m)^n (1 + x + x^2 + \cdots)^n.$

We now define the formal differentiation in $\mathbb{Q}[[x]]$ and give some important results. The proof is left for the reader.

Definition 6.3.9. Let $f(x) = \sum\limits_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]$.

1. **[Formal Differentiation]** Then, the formal differentiation of $f(x)$, denoted $f'(x)$, is defined by

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} + \cdots = \sum_{n\geq 1} na_nx^{n-1}.$$

2. **[Formal Integration]** Then, the formal integration of $f(x)$, denoted $\int f(x)$, is defined by

$$\int f(x)dx = \alpha + a_0x + \frac{a_1}{2}x^2 + \cdots + \frac{a_n}{n+1}x^{n+1} + \cdots = \alpha + \sum_{n\geq 0} \frac{a_n}{n+1}x^{n+1}.$$

Proposition 6.3.10. **[ogf: tricks]** *Let $g(x), h(x)$ be the ogf's for the sequences (a_n), (b_n), respectively. Then, the following are true.*

1. *$Ag(x) + Bh(x)$ is the ogf for $(Aa_n + Bb_n)$.*
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_n), where $M_n = a_n + a_{n-1} + \cdots + a_0$.*
4. *$g(x)h(x)$ is the ogf for (c_n), where $c_n = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_nb_0$.*
5. *$xf'(x)$ is the ogf for $na_n, n = 1, 2, \ldots$.*

Example 6.3.11.

1. Let $a_r = 1$ for all $r \geq 0$. Then, the ogf of the sequence (a_r) equals $1 + x + x^2 + \cdots = (1-x)^{-1} = f(x)$. So, for $r \geq 0$, the ogf for
   (a) $a_r = r$ for all $r \geq 1$ is $xf'(x)$ and
   (b) $a_r = r^2$ for all $r \geq 1$ is $x\big(f'(x) + xf''(x)\big)$.
   (c) Using the above two examples, the ogf of the sequence $a_r = 3r + 5r^2$ for all $r \geq 1$ is $3xf'(x) + 5\big(xf'(x) + x^2f''(x)\big) = 8x(1-x)^{-2} + 10x^2(1-x)^{-3}$.

2. Determine the number of ways to distribute 50 coins among 30 students so that no student gets more than 4 coins equals

$$\begin{aligned}
\text{CF}\big[x^{50}, (1 + x + x^2 + x^3 + x^4)^{30}\big] &= \text{CF}\big[x^{50}, (1-x^5)^{30}(1-x)^{-30}\big] \\
&= \text{CF}\big[x^{50}, (1-x^5)^{30}\left(C(29,29) + C(30,29)x + C(31,29)x^2 + \cdots\right)\big] \\
&= C(79,50) - 30C(74,45) + C(30,2)C(69,40) + \cdots \\
&= \sum_{i=0}^{10} (-1)^i C(30,i)C(79-5i, 29).
\end{aligned}$$

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 5.3.1).

   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 $S := \sum\limits_{k=0}^{\infty} \dfrac{k}{2^k} = \dfrac{1}{2} + \dfrac{2}{2^2} + \dfrac{3}{2^3} + \cdots$.

Ans: Note that

$$\begin{array}{rcl} 2S & = & 1 + \frac{2}{2} + \frac{3}{2^2} + \frac{4}{2^3} + \cdots \\ S & = & 0 + \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots \\ \hline S & = & 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = 2. \end{array}$$

Alternate. Put $f(x) = (1-x)^{-1}$. Then, it has 1 as its radius of convergence and within this radius, the derivative is the same as the power series obtained by term by term differentiation. Thus, $f'(x) = 1 + 2x + 3x^2 + \cdots$ has 1 as its radius of convergence. Hence,

$$S = \frac{1}{2} f'(1/2) = 2.$$

Alternate. Alternately (rearranging terms of an absolutely convergent series) it is

$$\begin{array}{ll} \frac{1}{2} & + \\ \frac{1}{4} + \frac{1}{4} & + \\ \frac{1}{8} + \frac{1}{8} + \frac{1}{8} & + \\ \vdots & \\ \hline 1 + \frac{1}{2} + \cdots = 2. & \end{array}$$

Exercise **6.3.12.** *1. Determine a closed form expression for* $\sum\limits_{n \geq 0} n x^n \in \mathbb{Q}[[x]]$. *Or in other words, write* $\sum\limits_{n \geq 0} n x^n = \dfrac{p(x)}{q(x)}$, *where* $p(x), q(x)$ *are polynomials with integer coefficients.*

2. *Determine the sum of the first* N *positive integers.*

3. *Determine the sum of the squares of the first* N *positive integers.*

4. *Determine a closed form expression for* $\sum\limits_{n \geq 0} \dfrac{n^2 + 5n + 16}{n!}$.

5. *Determine a closed form expression for* $\sum\limits_{k=1}^{N} k^3$.

6. *For* $n, r \in \mathbb{N}$ *determine the number of non-negative solutions to* $x_1 + 2x_2 + \cdots + n x_n = r$ *in the unknowns* x_i*'s.*

7. *Determine* $\sum\limits_{k=0}^{\infty} \frac{1}{2^k} C(n+k-1, k)$.

8. *Find the number of non-negative integer solutions of* $a + b + c + d + e = 27$, *satisfying*

   (a) $3 \leq a \leq 8$,

   (b) $3 \leq a, b, c, d \leq 8$

   (c) c *is a multiple of* 3 *and* e *is a multiple of* 4.

9. *Determine the number of ways in which* 150 *voters can cast their* 150 *votes for* 5 *candidates such that no candidate gets more than* 30 *votes.*

10. *Verify the following table of formal power series.*

Table of Formal Power Series

$e^x = \sum\limits_{k\ge 0} \dfrac{x^k}{k!}$	$(1+x)^n = \sum\limits_{r\ge 0} C(n,k)x^k, n \in \mathbb{N}_0$
$\cos(x) = \sum\limits_{r\ge 0} \dfrac{(-1)^r x^{2r}}{(2r)!}$	$\sin(x) = \sum\limits_{r\ge 0} \dfrac{(-1)^r x^{2r+1}}{(2r+1)!}$
$\cosh(x) = \sum\limits_{r\ge 0} \dfrac{x^{2r}}{(2r)!}$	$\sinh(x) = \sum\limits_{r\ge 0} \dfrac{x^{2r+1}}{(2r+1)!}$
Radius of convergence: $\lvert x\rvert < 1$	
$\log(1-x) = -\sum\limits_{k\ge 1} \dfrac{x^k}{k}$	
$\dfrac{1}{1-x} = \sum\limits_{k\ge 0} x^k$	$\dfrac{1}{(1-x)^n} = \sum\limits_{k\ge 0} C(n+k-1,k)x^k, n \in \mathbb{N}$
$\dfrac{(1+x)^n}{x^r} = \sum\limits_{k\ge -r} C(n,r+k)x^k$	$\dfrac{x^n}{(1-x)^{n+1}} = \sum\limits_{k\ge 0} C(k,n)x^k, n \in \mathbb{N}_0$
Radius of convergence: $\lvert x\rvert < \dfrac{1}{4}$	
$\dfrac{1}{\sqrt{1-4x}} = \sum\limits_{k\ge 0} C(2k,k)x^k$	$\dfrac{1-\sqrt{1-4x}}{2x} = \sum\limits_{k\ge 0} \dfrac{1}{k+1} C(2k,k)x^k$

11. *Find the ogf of the Fibonacci sequence* $(F_n)_{n\ge 0} := (1,1,2,3,\ldots)$*? Hence, show that for* $n \ge 1$, F_n *is the number of ways to write* n *as a sum of* 1*'s and* 2*'s.*

12. *Take a natural number* n*. Find*

$$C(n,0)2^n - C(n-1,1)2^{n-2} + C(n-2,2)2^{n-4} - C(n-3,3)2^{n-6} + \cdots.$$

13. *We know* $(1-x)^{-2} = 1 + 2x + 3x^2 + \cdots$*. Also,*

$$(1-x)^{-2} = (1+x^2-2x)^{-1} = (1-[2x-x^2])^{-1} = 1 + [2x-x^2] + [2x-x^2]^2 + \cdots.$$

So, can you verify this identity, i.e., the coefficient of x^n *in the later expression is actually* $n+1$*?*

6.3.1 Generating Functions and Partitions of n

Recall from Page 95 that a partition of n into k parts is a tuple $(n_1, \cdots, n_k) \in \mathbb{N}^k$ written in non-increasing order, that is, $n_1 \ge n_2 \ge \cdots \ge n_k$, such that $n_1 + n + 2 + \cdots + n_k = n$. Also, recall that π_n is the number of distinct partitions of n. The following result due to Euler gives the generating function of π_n.

Theorem 6.3.13. **[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, $\pi_n = \text{CF}[x^n, \varepsilon(x)]$. ∎

The next result is the same idea as Theorem 6.3.13 and hence the proof is omitted.

Theorem 6.3.14. *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 6.3.15. *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 6.3.14, this number is $\text{CF}\left[x^n, \prod\limits_{i=1}^{r} \frac{1}{1-x^i}\right]$. ■

Theorem 6.3.16. **[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, $n \geq r$. 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 $(\mu_1, \ldots, \mu_k), k \leq r$, 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 6.3.15 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 **6.3.17.**
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 6.3.18. *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.

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.
2. Similar to the first 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 a 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 Exercise 5.4.7.8, 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 6.3.19. 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 $n > 3$.

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 6.3.20. 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,

$$na_n = \text{CF}\left[x^{n-1}, F'\right] = \text{CF}\left[x^{n-1}, F\left[\frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}}\right]\right] = \sum_{k=1}^{n} a_{n-k} b_k,$$

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 **6.3.21.** *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 the corresponding Durfee square. Show that $(1+x)(1+x^3)\cdots = 1+\sum\limits_{k=1}^{\infty}\frac{x^{k^2}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}$.*

3. *Show that the number of partitions of n into distinct terms is the same as the number of partitions of n into odd terms.*

4. *Find the number of r-digit binary numbers that can be formed using an even number of 0s and an even number of 1s.*

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 $\{1, 2, \ldots, n\}$ (convention: $c_0 = 0$), 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 0s.*
   (b) *The sequence has an odd number of 1s and an even number of 0s.*
   (c) *No digit appears exactly twice.*

6.4 Recurrence Relation

Definition 6.4.1. [**Recurrence Relation**] 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 6.4.2. $a_n = 3 + 2a_{n-1}$ 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 6.4.3. [**Difference Equation**] 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 6.4.4. 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 6.4.5. [**Solution of a Recurrence Relation**] A **solution** of a recurrence relation is a function $u(n)$, generally denoted by u_n, satisfying the recurrence relation.

Example 6.4.6. 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 $n \geq 2$ 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 6.4.7. [**LNRC/LHRC**] A recurrence relation is called a **linear nonhomogeneous recurrence relation** with constant coefficients (**LNRC**) of order r if, for a known function f

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + f(n), \text{ where } c_i \in \mathbb{R} \text{ for } 1 \leq i \leq r, c_r \neq 0. \tag{6.3}$$

If $f = 0$, then Equation (6.3) is homogeneous and is called the associated **linear homogeneous recurrence relation** with constant coefficients (**LHRC**).

Theorem 6.4.8. *For $k \in \mathbb{N}$ and $1 \leq i \leq k$, let f_i be known functions. Consider the k number of LNRC*

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + f_i(n) \quad \textit{for } i = 1, \ldots, k, \tag{6.4}$$

with the same set of initial conditions. If $u_i(n)$ is a solution of the i-th recurrence relation, then

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + \sum_{i=1}^{k} \alpha_i f_i(n) \tag{6.5}$$

with the same set of initial conditions has $\sum\limits_{i=1}^{k} \alpha_i u_i(n)$ as it solution.

Proof. The proof is left as an exercise for the reader.

Definition 6.4.9. [**Characteristic Equation**] The equation $x^r - c_1 x^{r-1} - \cdots - c_r = 0$ is called the **characteristic equation** of the LHRC $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$ with $c_r \neq 0$. The roots of the characteristic equation are called the **characteristic roots** of the LHRC.

Observe that if $a_n = x^n$ is a solution of the LHRC $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$ with $c_r \neq 0$, then either $x = 0$ or x is a characteristic root. Further, if $x_1, \ldots, x_r$ are the characteristic roots, then $a_n = x_i^n$ is a solution of the LHRC. It follows that $a_n = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for $\alpha_i \in \mathbb{R}$ is a solution of the given LHRC. We show that the latter form of a solution is a general solution so that a given set of initial conditions may be satisfied.

Theorem 6.4.10. [**General Solution: Distinct Roots**] *If the characteristic roots $x_1, \ldots, x_r$ of an LHRC are distinct, then every solution of the LHRC is a linear combination of $x_1^n, \ldots, x_r^n$. Moreover, the solution is unique if r consecutive initial conditions are given.*

Proof. Let $u(n)$ be any solution of a given LHRC $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$. That is,

$$u(n) = \sum_{j=1}^{r} c_j u(n-j) = c_1 u(n-1) + \cdots + c_r u(n-r).$$

We show that there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ such that $u(n) = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for all $n \in \mathbb{W}$. We first consider a smaller problem, that is, whether the first r values of $u(n)$ can be expressed in this form. The answer will be affirmative provided we can determine the constants $\alpha_1, \ldots, \alpha_r$ so that $u(n) = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for $n = 0, 1, \ldots, r-1$. To explore this, substitute $n = 0, 1, \ldots, r-1$ to obtain the following linear system in the unknowns $\alpha_1, \ldots, \alpha_r$:

$$\begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(r-1) \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_r \\ & \ddots & \\ x_1^{r-1} & \cdots & x_r^{r-1} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix}.$$

Since the above $r \times r$ matrix (commonly known as the Vandermonde matrix) is invertible, there exist $\alpha_1, \ldots, \alpha_r$ such that $u(n) = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for $0 \le n \le r-1$. Hence, we have proved the result for the first r values of $u(n)$. So, let us assume that $u(n) = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for $0 \le n < k$, where $k \ge r$. Notice that for $n = k$, x_i^k is a solution of the given LHRC. So, $x_i^k = \sum\limits_{j=1}^{r} c_j x_i^{k-j}$. Then

$$u(k) = \sum_{j=1}^{r} c_j u(k-j) = \sum_{j=1}^{r} c_j \sum_{i=1}^{r} \alpha_i x_i^{k-j} = \sum_{i=1}^{r} \alpha_i \sum_{j=1}^{r} c_j x_i^{k-j} = \sum_{i=1}^{r} \alpha_i x_i^k.$$

Hence by PMI, $u(n) = \sum\limits_{i=1}^{r} \alpha_i x_i^n$ for all n.

For uniqueness, suppose $u(n)$ and $v(n)$ are solutions of the LHRC satisfying the r initial conditions $u(i) = v(i) = a_i$ for $0 \le i \le r-1$. Write $y(n) = u(n) - v(n)$. Then $y(n)$ satisfies the same LHRC with intial conditions $y(1) = \cdots = y(r) = 0$. By what we have just proved, $y(n) = \sum\limits_{i=1}^{r} \gamma_i x_i^n$ for some constants $\gamma_1, \ldots, \gamma_r$. Treating γ_is as unknowns, and substituting $n = 0, 1, \ldots, r-1$, we arrive at a linear system as above, where u is replaced by y. Since the system matrix there is invertible, it leads to the unique solution $\gamma_1 = \cdots = \gamma_r = 0$. In turn, we obtain $y(n) = 0$ for all n. That is, $u(n) = v(n)$ for all n. ■

Notice that the characteristic roots are, in general, complex numbers, so that the constants in the linear combination can be complex numbers.

Example 6.4.11.

1. Solve $a_n - 4a_{n-2} = 0$ for $n \ge 2$ with $a_0 = 1$ and $a_1 = 1$. **Ans:** The characteristic equation is $x^2 - 4 = 0$. As the characteristic roots $x = \pm 2$ are distinct, the general solution is $a_n = \alpha(-2)^n + \beta\, 2^n$. 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 $n \ge 2$ with $a_0 = 1$ and $a_1 = c$, a constant. **Ans:** The characteristic equation is $x^2 - 3x - 4 = 0$. The characteristic roots are -1 and 4; they are distinct. The general solution is $a_n = \alpha(-1)^n + \beta\, 4^n$. The initial conditions imply $\alpha = \frac{4-c}{5}$ and $\beta = \frac{1+c}{5}$. Thus, the unique general solution is $a_n = \frac{1}{5}\big((4-c)(-1)^n + (1+c)4^n\big)$.

3. Solve the Fibonacci recurrence $a_n = a_{n-1} + a_{n-2}$ with initial conditions $a_0 = 0, a_1 = 1$. **Ans:** The characteristic equation $x^2 - x - 1 = 0$ gives distinct characteristic roots as $\frac{1 \pm \sqrt{5}}{2}$. So, the general solution is $a_n = \alpha\big(\frac{1+\sqrt{5}}{2}\big)^n + \beta\big(\frac{1-\sqrt{5}}{2}\big)^n$. Using the initial conditions, we get $\alpha = 1/\sqrt{5}$, $\beta = -\alpha = -1/\sqrt{5}$. Hence, the required solution is

$$a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]. \tag{6.6}$$

4. Solve the recurrence relation $a_n + a_{n-2} = 0$ with the initial conditions $a_0 = a_1 = 2$. **Ans:** The characteristic equation is $x^2+1 = 0$ with distinct characteristic roots as $\pm i$. The general solution is in the form $a_n = \alpha\, i^n + \beta\,(-i)^n$. Initial conditions imply that $\alpha+\beta = 2$ and $\alpha\, i - \beta\, i = 2$. So, $\alpha = 1 - i$ and $\beta = 1 + i$. Then $a_n = (1-i)i^n + (1+i)(-i)^n$.

5. Consider a triangle with vertices $(a_1, b_1) = (0, 0)$, $(a_2, b_2) = (5, 0)$ and $(a_3, b_3) = (3, 7)$. For $n > 3$, define (a_n, b_n) as the centroid of the triangle formed by (a_{n-1}, b_{n-1}), (a_{n-2}, b_{n-2}) and (a_{n-3}, b_{n-3}). Does the sequence $((a_n, b_n))$ converge? If so, to what limit?

   Ans: Note that the sequence $((a_n, b_n))$ converges if and only if both the sequences (a_n) and (b_n) converge. We will first show that (a_n) converges.

   Let $M_1 = \max\{a_1, a_2, a_3\}$ and $m_1 = \min\{a_1, a_2, a_3\}$. Notice that $m_1 \le a_1, a_2, a_3 \le M_1$. Hence,

$$m_1 \le \frac{a_1+a_2+a_3}{3} \le \frac{2M_1+m_1}{3}, \ i.e., \quad m_1 \le a_4 \le \frac{2M_1+m_1}{3};$$
$$m_1 \le \frac{a_2+a_3+a_4}{3} \le \frac{2M_1+a_4}{3} \le \frac{8M_1+m_1}{9}, \ i.e., \quad m_1 \le a_5 \le \frac{8M_1+m_1}{9}; \qquad \text{and}$$
$$m_1 \le \frac{a_3+a_4+a_5}{3} \le \frac{26M_1+m_1}{27}, \ i.e., \quad m_1 \le a_6 \le \frac{26M_1+m_1}{27}.$$

   As $\frac{2M_1+m_1}{3} \le \frac{8M_1+m_1}{9} \le \frac{26M_1+m_1}{27}$, we see that

$$m_1 \le a_4, a_5, a_6 \le \frac{26M_1+m_1}{27}.$$

   Let $M_2 = \max\{a_4, a_5, a_6\}$ and $m_2 = \min\{a_4, a_5, a_6\}$. Then

$$[m_2, M_2] \subseteq [m_1, M_1] \qquad \text{and} \qquad length([m_2, M_2]) \le \frac{26}{27}\, length([m_1, M_1]).$$

   Similarly, taking $M_n = \max\{a_{3n+1}, a_{3n+2}, a_{3n+3}\}$ and $m_n = \min\{a_{3n+1}, a_{3n+2}, a_{3n+3}\}$, we get a nested sequence of nonempty closed intervals

$$[m_1, M_1] \supseteq [m_2, M_2] \supseteq [m_3, M_3] \supseteq \cdots$$

   with diameters going to zero. By nested interval theorem, $\bigcap\limits_{i=1}^{\infty} [m_i, M_i]$ is a singleton set, say, $\{l\}$. Note that, $[m_{n+1}, M_{n+1}]$ contains all the terms $a_{3n+1}, a_{3n+2}, a_{3n+3}, a_{3n+4}, \ldots$. It now follows that $\lim\limits_{n\to\infty} a_n = l$. Thus, $\lim\limits_{n\to\infty} \frac{a_{n+1}+2a_{n+2}+3a_{n+3}}{6} = l$. But notice that,

$$\frac{a_1+2a_2+3a_3}{6} = \frac{a_2+2a_3+3a_4}{6} = \frac{a_3+2a_4+3a_5}{6} = \cdots.$$

   Thus $l = \frac{a_1+2a_2+3a_3}{6}$. Thus, the limit to the original question is $(19/6, 7/2)$.

* How did we guess the formula? To see that write

$$\begin{array}{rcl} 3a_4 &=& a_1+a_2+a_3 \\ 3a_5 &=& a_2+a_3+a_4 \\ &\vdots& \\ 3a_{n+3} &=& a_n+a_{n+1}+a_{n+2} \\ \hline 3(a_4+a_5+\cdots+a_{n+3}) &=& a_1+2a_2+3(a_3+\cdots+a_n)+2a_{n+1}+a_{n+2} \end{array}$$

Cancelling, we get $a_{n+1}+2a_{n+2}+3a_{n+3} = a_1+2a_2+3a_3$, which is what we required.

Alternate. This method is of interest to us. Note that we have the LHRC

$$a_n = \frac{a_{n-1}+a_{n-2}+a_{n-3}}{3}, \ n > 3.$$

So, the characteristic equation is $3x^3 - x^2 - x - 1 = 0$. Observe that 1 is a root. We now see that $3x^3 - x^2 - x - 1 = (x-1)\boxed{(3x^2+2x+1)}$ and so the other two roots are

$$\alpha := \frac{-2+\sqrt{4-12}}{6} = \frac{-1+\mathrm{i}\sqrt{2}}{3} \quad \text{and} \quad \beta := \frac{-1-\mathrm{i}\sqrt{2}}{3}.$$

Hence, by Theorem 6.4.10, there exist constants $a, b, c \in \mathbb{C}$ such that

$$a_n = a(1)^{n-1} + b(\alpha)^{n-1} + c(\beta)^{n-1}.$$

As $|\alpha| = |\beta| = \frac{1}{\sqrt{3}} < 1$, we see that $a_n \to a$. Using the initial conditions, we get

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \beta \\ 1 & \alpha^2 & \beta^2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

Solving for a gives $a = \frac{a_1+2a_2+3a_3}{6}$.

Theorem 6.4.12. **[General Solution: Multiple Roots]** *Given an LHRC, let t be a characteristic root of multiplicity s. Then $u(n) = t^n \left(\sum\limits_{i=0}^{s-1} \alpha_i n^i\right)$ is a solution (called a* **basic solution***). Moreover, if $t_1, \ldots, t_k$ are the distinct characteristic roots with multiplicities $s_1, \ldots, s_k$, respectively, then every solution is a sum of the k corresponding 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

$$\begin{aligned} G_0 = x^{n-r}F &= x^n - c_1x^{n-1} - \cdots - c_rx^{n-r} \\ G_1 = xG_0' &= nx^n - c_1(n-1)x^{n-1} - \cdots - c_r(n-r)x^{n-r} \\ G_2 = xG_1' &= n^2x^n - c_1(n-1)^2x^{n-1} - \cdots - c_r(n-r)^2x^{n-r} \\ \vdots &= \vdots \\ G_{s-1} = xG_{s-2}' &= n^{s-1}x^n - c_1(n-1)^{s-1}x^{n-1} - \cdots - c_r(n-r)^{s-1}x^{n-r} \end{aligned}$$

Note that each of $G_0, G_1, \ldots, G_{s-1}$ has a zero at t, *i.e.*, for $i = 0, 1, \ldots, s-1$, we have

$$G_i(t) = t^n n^i - c_1t^{n-1}(n-1)^i - \ldots - c_rt^{n-r}(n-r)^i = 0.$$

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

$$0 = \sum_{i=0}^{s-1} \alpha_i G_i(t) = t^nP(n) - c_1t^{n-1}P(n-1) - \cdots - c_rt^{n-r}P(n-r).$$

Hence, by definition $u(n) - c_1u(n-1) - \cdots - c_ru(n-r) = 0$. Therefore, $u(n)$ is a solution of the LHRC.

Now, the second statement follows from Theorem 6.4.10. ■

Example 6.4.13. Suppose that an LHRC has roots $2, 2, 3, 3, 3$. Then, the general solution is given by $2^n(\alpha_1 + n\alpha_2) + 3^n(\beta_1 + n\beta_2 + n^2\beta_3)$.

Consider the LNRC in Equation (6.3). If v_n and w_n are solutions of the LNRC, then $u_n := w_n - v_n$ satisfies the associated LHRC. That is, $w_n = u_n + v_n$ shows that any solution w_n can be expressed as a solution of the associated *LHRC* plus a solution v_n of the LNRC. We summarize this finding in the next theorem.

Theorem 6.4.14. **[LNRC]** *Consider the LNRC in Equation (6.3). Let u_n be a general solution of the associated LHRC. If v_n is a (particular) solution of the LNRC, then $a_n = u_n + v_n$ is a general solution of the LNRC.*

Remark 6.4.15. Theorem 6.4.14 implies that in order to obtain a general solution of an LNRC, we need to solve the associated LHRC for a general solution and also obtain a particular solution of the same LNRC. Unlike an LHRC, no general algorithm is available to obtain a particular solution of an LNRC. In some cases, heuristic methods can be used to obtain a particular solution. 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 LHRC, then $v(n) = ca^n$.
2. If $f(n) = a^n$ and a is a root of LHRC of multiplicity t, then $v(n) = cn^t a^n$.
3. If $f(n) = n^k$ and 1 is not a root of LHRC, then use $v(n) = c_0 + c_1 n + \cdots + c_k n^k$.
4. If $f(n) = n^k$ and 1 is a root of LHRC of multiplicity t, then $v(n) = n^t(c_0 + c_1 n + \cdots + c_k n^k)$.

Example 6.4.16.

1. Solve $a_n = 3a_{n-1} + 2n$ for $n \geq 1$ with $a_0 = 1$.

   Ans: Observe that 3 is the characteristic root of the associated LHRC ($a_n = 3a_{n-1}$). Thus, the general solution of LHRC 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 $a = -3/2$ and $b = -1$. Hence, $a_n = 3^n \alpha - n - 3/2$. Using $a_0 = 1$, check that $\alpha = 5/2$.

2. Solve $a_n = 3a_{n-1} - 2a_{n-2} + 3\,(5)^n$ for $n \geq 3$ with $a_1 = 1, a_2 = 2$.

   Ans: The associated LHRC ($a_n = 3a_{n-1} - 2a_{n-2}$) has the characteristic roots 1 and 2. Thus, the general solution of the LHRC is $u_n = \alpha 1^n + \beta\, 2^n$. Notice that 5 is not a characteristic root. So, $v_n = c\,5^n$ is a particular solution of LNRC. That is, $c\,5^n = 3c\,5^{n-1} - 2c\,5^{n-2} + 3\,(5)^n$. It gives $c = 25/4$. Hence, the general solution of LNRC is in the form $a_n = \alpha + \beta\, 2^n + (25/4)5^n$. One can then determine α and β from the initial conditions.

3. In the previous example, take $f(n) = 3(2^n)$. Trying $c\,(2)^n$ as a particular solution, we have $4c = 6c - 2c + 12$. This is absurd. The reason is that 2 is a characteristic root of the associated LHRC. Now, with the choice of $c\,n(2)^n$ as a particular solution, we get $4nc = 6(n-1)c - 2(n-2)c + 12$. It gives $c = 6$. Hence, the general solution of LNRC is in the form $a_n = \alpha + \beta 2^n + 6n2^n$ from which the constants α and β can be computed using the initial conditions.

6.5 Generating Function from Recurrence Relation

Sometimes we can find a solution to the recurrence relation using the generating function of a_n; see the following example.

Example 6.5.1.

1. Consider solving $a_n = 2a_{n-1} + 1$, $a_0 = 1$.

   Ans: Let $F(x) = a_0 + a_1 x + \cdots$ 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, $F(x) = \dfrac{1}{(1-x)(1-2x)} = \dfrac{2}{1-2x} - \dfrac{1}{1-x}$ so that $a_n = \text{CF}[x^n, F(x)] = 2^{n+1} - 1$.

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 $F(x) = \sum\limits_{n\ge 0} a_n x^n = \sum\limits_{n\ge 1} a_n x^n$. Then using the recurrence relation, we have

   $$F(x) = \sum_{n\ge 0} a_n x^n = x + \sum_{n\ge 2} (a_{n-1} + a_{n-2})\, x^n = x + (x + x^2)F(x).$$

   So, $F(x) = \dfrac{x}{1 - x - x^2}$.

   Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Verify that $(1-\alpha x)(1-\beta x) = 1 - x - x^2$. Then

   $$F(x) = \frac{1}{\sqrt{5}}\Big(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\Big) = \frac{1}{\sqrt{5}}\left(\sum_{n\ge 0}\alpha^n x^n - \sum_{n\ge 0}\beta^n x^n\right).$$

   Therefore, $a_n = \text{CF}[x^n, F(x)] = \dfrac{1}{\sqrt{5}} \sum\limits_{n\ge 0} (\alpha^n - \beta^n)$, which equals Equation (6.6).

The next result follows using a small calculation and hence the proof is left for the reader.

Theorem 6.5.2. **[Obtaining Generating Function from Recurrence Relation]** *Let a_n be the solution of the r-th order LHRC with r initial conditions given by*

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} \quad \textit{with} \quad a_0 = A_0,\ a_1 = A_1,\ a_{r-1} = A_{r-1}. \tag{6.7}$$

Then the generating function of (a_n) is obtained by taking

$$\begin{aligned} F(x) &= A_0 + A_1 x + \cdots + A_{r-1}x^{r-1} + [(c_1 A_{r-1} + \cdots + c_r A_0]x^r + \cdots \\ &= A_0 + A_1 x + \cdots + A_{r-1}x^{r-1} + c_r x^r F + c_{r-1}x^{r-1}(F(x) - A_0) + \cdots + \\ &\qquad c_1 x(F(x) - A_0 - A_1 x - \cdots - A_{r-2}x^{r-2}). \end{aligned}$$

This implies that

$$F(x) = \frac{\sum\limits_{i=0}^{r-1} A_i x^i \ - \ c_1 x \sum\limits_{i=0}^{r-2} A_i x^i \ - \ c_2 x^2 \sum\limits_{i=0}^{r-3} A_i x^i \ - \ \cdots \ - \ c_{r-1}x^{r-1}A_0}{1 \ - \ c_1 x \ - \ \cdots \ - \ c_r x^r}. \tag{6.8}$$

Remark 6.5.3. Then we observe the following about Equation (6.8) in Theorem 6.5.2.

1. Note that the numerator is a polynomial in x of degree at most $r-1$, determined by the initial conditions and the denominator $Q(x)$ is a polynomial of degree r determined by the recurrence relation.

2. Now consider all solutions of the LHRCC $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$ of order r. We already know that they form a vector space of dimension r. Each such solution will give us an ogf as shown above. Since they have the same denominator, if we take linearly independent solutions, we will get linearly independent numerators. It now follows that, if $P(x)$ has degree less than r, then $\dfrac{P(x)}{Q(x)}$ is an ogf for some solution.

3. Note that we can write $1 - c_1 x - \cdots - c_r x^r = (1-\alpha_1 x)^{s_1}\cdots(1-\alpha_k x^k)^{s_k}$, where α_i's are distinct complex numbers and $s_1 + \cdot + s_k = r$. Let $P_1(x)$ have degree less than s_1. Then notice that

   $$\frac{P_1(x)}{(1-\alpha_1 x)^{s_1}} = \frac{P_1(x)(1-\alpha_2 x)^{s_2}\cdots(1-\alpha_k x)^{s_k}}{(1-\alpha_1 x)^{s_1}(1-\alpha_2 x)^{s_2}\cdots(1-\alpha_k x)^{s_k}}$$

is an ogf for some solution. Similarly, $\frac{P_1(x)}{(1-\alpha_1 x)^{s_1}}, \ldots, \frac{P_k(x)}{(1-\alpha_k x)^{s_1}}$ are ogf's of some solutions. Are these solutions linearly independent? Yes. Indeed, if those solutions are linearly dependent, then a linear combination

$$a_1 \frac{P_1(x)}{(1-\alpha_1 x)^{s_1}} + \ldots + a_k \frac{P_k(x)}{(1-\alpha_k x)^{s_1}} = 0.$$

But this is not possible, otherwise, multiplying by $(1-\alpha_1 x)^{s_1}(1-\alpha_2 x)^{s_2} \cdots (1-\alpha_k x)^{s_k}$, we get $a_1 R_1(x) + \cdots + a_k R_k(x)$ is the zero polynomial. As every term except the first one is divisible by $(1-\alpha_1 x)^{s_1}$ and the rhs is also divisible by $(1-\alpha_1 x)^{s_1}$, and that P_1 has degree less than s_1, it follows that $a_1 = 0$. Similarly, all other a_i are 0. Thus we already know that the sequences $(\alpha_1^n), (n\alpha_1^n), \ldots, (n^{s_1-1}\alpha_1^n)$ are linearly independent. Indeed, if there is a combination

$$a_0(\alpha_1^n) + a_1(n\alpha_1^n) + \cdots + a_{s_1-1}(n^{s_1-1}\alpha_1^n) = (0, 0, \cdots),$$

as $\alpha_1 \neq 0$, we would get

$$(a_0 + a_1 n + a_2 n^2 + \cdots + a_{s_1-1} n^{s_1-1}) = (0, 0, \cdots),$$

implying $a_0 = a_1 = \cdots = a_{s_1-1} = 0$.

4. Now suppose that, the sequences

$$(\alpha_1^n), (n\alpha_1^n), \ldots, (n^{s_1-1}\alpha_1^n), \cdots, (\alpha_k^n), (n\alpha_k^n), \ldots, (n^{s_k-1}\alpha_k^n)$$

are linearly dependent. We then have

$$(P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_k(n)\alpha_k^n) = (0, 0, \cdots),$$

for some polynomials $P_i(n)$ with degrees less than s_i, $i = 1, \ldots, k$.

We explain Theorem 6.5.2 by considering the following examples.

Example 6.5.4. 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,

$$\begin{aligned} g(x) - 1 &= \sum_{n\geq 1} C_n x^n = \sum_{n\geq 1} \frac{2(2n-1)}{n+1} C_{n-1} x^n \\ &= \sum_{n=1}^{\infty} \frac{4n+4}{n+1} C_{n-1} x^n + \sum_{n=1}^{\infty} \frac{-6}{n+1} C_{n-1} x^n = 4xg(x) + \frac{-6}{x} \int_0^x t g(t) dt. \end{aligned}$$

So, $[g(x) - 1 - 4xg(x)]x = -6 \int_0^x t g(t) dt$. So, $[g(x) - 1 - 4xg(x)]x = -6 \int_0^x t g(t) dt$. Differentiate with respect to x to get

$$x(1-4x)g' + (1-2x)g = 1.$$

It is a linear ordinary differential equation. Observe that

$$\int \frac{1-2x}{x(1-4x)} dx = \int \left[\frac{1}{x} + \frac{2}{1-4x}\right] dx = \ln\left(\frac{x}{\sqrt{1-4x}}\right).$$

We thus multiply the equation with its integrating factor $\dfrac{x}{\sqrt{1-4x}}$ to obtain

$$g(x)' \frac{x}{\sqrt{1-4x}} + g(x) \frac{1-2x}{(1-4x)^{3/2}} = \frac{1}{(1-4x)^{3/2}} \Leftrightarrow \frac{d}{dx}\left[g(x) \frac{x}{\sqrt{1-4x}}\right] = \frac{1}{(1-4x)^{3/2}}.$$

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 $C_0 = \lim\limits_{x\to 0} g(x) = 1$. Therefore, 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

$$C_n = C_0C_{n-1} + C_1C_{n-2} + \cdots + C_{n-1}C_0. \tag{6.9}$$

Let $g(x)$ be the generating function of C_n; that is, $g(x) = \sum\limits_{n=0}^{\infty} C_n x^n$. Then, for $n \geq 1$,

$$\text{CF}\big[x^{n-1}, g(x)^2\big] = \text{CF}\left[x^{n-1}, \left(\sum_{n=0}^{\infty} C_n x^n\right)^2\right] = \sum_{i=0}^{n-1} C_iC_{n-1-i} = C_n \text{ using Equation (6.9).}$$

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.

   Answer: Let $g(x) = \sum\limits_{n\geq 0} a_n x^n$. Using $C(n+r,r) = C(n+(r+1)-1, n)$, we obtain

$$g(x)^2 = \sum_{n\geq 0}\left(\sum_{k=0}^{n} a_k a_{n-k}\right)x^n = \sum_{n\geq 0} C(n+r,r)x^n = \sum_{n\geq 0} C(n+r,n)x^n = \frac{1}{(1-x)^{r+1}}.$$

   Hence, $a_n = \text{CF}\left[x^n, \frac{1}{(1-x)^{(r+1)/2}}\right]$. For example, when $r = 2$

$$a_n = (-1)^n C(-3/2, n) = \frac{3\cdot 5\cdot 7\cdots(2n+1)}{2^n\ n!} = \frac{(2n+1)!}{2^{2n}n!n!}.$$

3. Determine the sequence $\{f(n,m) : n, m \in \mathbb{W}\}$ which satisfies $f(n,0) = 1$ for all $n \geq 0$, $f(0,m) = 0$ for all $m > 0$, and

$$f(n,m) = f(n-1,m) + f(n-1,m-1) \quad \text{for } n > 0,\ m > 0. \tag{6.10}$$

Answer: For $n > 0$, 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 $n \geq 2$,

$$\begin{aligned} F_n(x) &= \sum_{m\geq 0} f(n,m)x^m = 1 + \sum_{m\geq 1} \left(f(n-1,m) + f(n-1,m-1)\right) x^m \\ &= 1 + \sum_{m\geq 1} f(n-1,m)x^m + \sum_{m\geq 1} f(n-1,m-1)x^m \\ &= F_{n-1}(x) + xF_{n-1}(x) = (1+x)F_{n-1}(x). \end{aligned}$$

By induction it follows that $F_n(x) = (1+x)^n$. 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 $m > 0$, 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 (6.10) 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 $\{S(n,m) : n, m \in \mathbb{W}\}$ which satisfies $S(0,0) = 1$, $S(n,0) = 0$ for $n > 0$, $S(0,m) = 0$ for $m > 0$, and

$$S(n,m) = mS(n-1,m) + S(n-1,m-1), \quad \text{for } n > 0,\ m > 0. \tag{6.11}$$

Answer: For $n > 0$, 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 (6.11) 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, $G_m(y) = \dfrac{y}{1-my}G_{m-1}(y)$. By induction it follows that

$$G_m(y) = \frac{y^m}{(1-y)(1-2y)\cdots(1-my)} = y^m \sum_{k=1}^{m} \frac{\alpha_k}{1-ky}, \tag{6.12}$$

where $\alpha_k = \dfrac{(-1)^{m-k}k^m}{k!\,(m-k)!}$ for $1 \le k \le m$. Then

$$\begin{aligned} S(n,m) &= \mathrm{CF}\left[y^n, y^m \sum_{k=1}^{m} \frac{\alpha_k}{1-ky}\right] = \sum_{k=1}^{m} \mathrm{CF}\left[y^{n-m}, \frac{\alpha_k}{1-ky}\right] \\ &= \sum_{k=1}^{m} \alpha_k k^{n-m} = \sum_{k=1}^{m} \frac{(-1)^{m-k}k^n}{k!\,(m-k)!} \qquad (6.13) \\ &= \frac{1}{m!}\sum_{k=1}^{m}(-1)^{m-k}k^n C(m,k) = \frac{1}{m!}\sum_{k=1}^{m}(-1)^k(m-k)^n C(m,k). \end{aligned}$$

(a) The identity $S(n,m) = \frac{1}{m!}\sum\limits_{k=1}^{m}(-1)^k(m-k)^n C(m,k)$ is known as the **Stirling's Identity**.

(b) As there is no restriction on $n, m \in \mathbb{N}_0$, Equation (6.13) 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. **[Bell Numbers]** Recall that the n-th Bell number $b(n)$ for $n \in \mathbb{N}$, is the number of partitions of $\{1, 2, \ldots, n\}$. By convention we take $b(0) = 1$. For $n \ge 1$,

$$\begin{aligned} b(n) &= \sum_{m=1}^{n} S(n,m) = \sum_{m\ge1} S(n,m) = \sum_{m\ge1}\sum_{k=1}^{m} \frac{(-1)^{m-k}\, k^{n-1}}{(k-1)!\,(m-k)!} \\ &= \sum_{k\ge1} \frac{k^n}{k!} \sum_{m\ge k} \frac{(-1)^{m-k}}{(m-k)!} = \frac{1}{e}\sum_{k\ge1}\frac{k^n}{k!} = \frac{1}{e}\sum_{k\ge0}\frac{k^n}{k!} \qquad (6.14) \end{aligned}$$

as $0^n = 0$ for $n \ge 1$. We see that Equation (6.14) is valid even for $n = 0$. Notice that $b(n)$ has terms of the form $\dfrac{k^n}{k!}$. So, we compute its egf as follows:

$$\begin{aligned} B(x) &= 1 + \sum_{n\ge1} b(n)\frac{x^n}{n!} = 1 + \sum_{n\ge1}\left(\frac{1}{e}\sum_{k\ge1}\frac{k^n}{k!}\right)\frac{x^n}{n!} \\ &= 1 + \frac{1}{e}\sum_{k\ge1}\frac{1}{k!}\sum_{n\ge1}k^n\frac{x^n}{n!} = 1 + \frac{1}{e}\sum_{k\ge1}\frac{1}{k!}\sum_{n\ge1}\frac{(kx)^n}{n!} \\ &= 1 + \frac{1}{e}\sum_{k\ge1}\frac{1}{k!}\left(e^{kx}-1\right) = 1 + \frac{1}{e}\sum_{k\ge1}\left(\frac{(e^x)^k}{k!} - \frac{1}{k!}\right) \\ &= 1 + \frac{1}{e}\left(e^{e^x} - 1 - (e-1)\right) = e^{e^x-1}. \qquad (6.15) \end{aligned}$$

Recall that e^{e^x-1} is a valid formal power series (see Remark 6.3.5). Taking logarithm of Equation (6.15), we get $\log B(x) = e^x - 1$. Hence, $B'(x) = e^x B(x)$, or equivalently

$$B'(x) = \sum_{n\ge1}\frac{b(n)x^{n-1}}{(n-1)!} = e^x\sum_{n\ge0}b(n)\frac{x^n}{n!} = \sum_{m\ge0}\frac{x^m}{m!}\cdot\sum_{n\ge0}b(n)\frac{x^n}{n!}.$$

Thus,

$$\frac{b(n)}{(n-1)!} = \mathrm{CF}\left[x^{n-1}, B'(x)\right] = \mathrm{CF}\left[x^{n-1}, \sum_{m\ge0}\frac{x^m}{m!}\cdot\sum_{n\ge0}b(n)\frac{x^n}{n!}\right] = \sum_{m=0}^{n-1}\frac{1}{(n-1-m)!}\cdot\frac{b(m)}{m!}.$$

Therefore, $b(n) = \sum\limits_{m=0}^{n-1} C(n-1,m)b(m)$ for $n \ge 1$.

Exercise **6.5.5.** 1. *Find the recurrence relation(s) for the number of binary words without having sub-words* 00 *and* 111.

2. *Find the number of subsets (including the empty set) of* $\{1, \ldots, n\}$ *not containing consecutive integers.*

3. *Let* F_n *be the nth Fibonacci number. Prove that if* $n, m \in \mathbb{N}$, *then* F_n *divides* F_{nm}.

4. *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?*

5. (a) *Prove combinatorially that* $D_n = (n-1)(D_{n-1} + D_{n-2})$ *for* $n \geq 2$.

   (b) *Use (a) to show that the egf of* D_n *is* $\dfrac{e^{-x}}{1-x}$.

6. (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?*

7. (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?*

8. *What is the number of integer solutions of* $x + y + z = 10$ *with* $x \geq -1$, $y \geq -2$ *and* $z \geq -3$?

9. *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* $x+y+z = 10$?

10. *How many words of length* 8 *can be formed using the English alphabet, where each letter can appear at most twice? Give answer using generating function.*

11. *Let* $p_1, \ldots, p_n$, $n \geq 2$, *be distinct prime numbers. In how many ways can we partition the set* $\{p_1, \ldots, p_n, p_1^2, \ldots, p_n^2\}$ *into subsets of size two such that no prime is in the same subset containing its square?*

12. *What is the value of* $\sum\limits_{k=0}^{15} (-1)^k C(15,k)(15-k)^5$*?*

13. *Give your answers to the following questions using generating functions:*

    (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 odd entries?*

    (g) *What is the number of partitions of* n *with distinct odd entries?*

    (h) *What is the number of self conjugate partitions of* n*?*

14. *We summarize our findings about partitions in the following table.*

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*	$\pi_n(r) = \mathrm{CF}\left[x^{n-r}, \frac{1}{(1-x)(1-x^2)\cdots(1-x^r)}\right]$
N	*N*	*N*	*Partitions of n of length* $\leq r$	$\sum\limits_{i=1}^{r} \pi_n(i)$

15. *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.*

16. *The characteristic roots of an LHRC are* $2, 2, 2, 3, 3$. *What is the form of the general solution?*

17. *Consider the LNRC* $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + 5^n$. *Give a particular solution.*

18. *Obtain the ogf for* a_n*, where* $a_n = 2a_{n-1} - a_{n-2} + 2^n$, $a_0 = 0$, $a_1 = 1$.

19. *Solve the recurrence relation* $a_n = 2a_{n-1} - a_{n-2} + 2^n + 5$, $a_0 = 0$, $a_1 = 1$.

20. *Find the number of words of size* 12 *made using letters from* $\{A, B, C\}$ *which do not have the sub-word BCA. For instance, BCCABCCABCCA is such a word, but ABCABCCCCCBA is not.*

21. *Find the number of* 8 *letter words made using letters from* $\{A, B, C, D\}$ *in which* 3 *consecutive letters are not allowed to be the same.*

22. *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. What is the the smallest positive integer* n *so that if we distribute* n *balls (without seeing the colors) into these bags, then at least one of the following three conditions is met?*
    Condition 1: *A blue bag contains* 3 *blue balls or* 4 *red balls or* 5 *green balls.*
    Condition 2: *A red bag contains* 3 *blue balls or* 5 *red balls or* 7 *green balls.*
    Condition 3: *A green bag contains* 3 *blue balls or* 6 *red balls or* 9 *green balls.*

23. *Let* $f(x)$ *be a polynomial with integer coefficients. What is the smallest natural number* n *such that if* $f(x) = 2009$ *has* n *distinct integer roots, then* $f(x) = 9002$ *does not have an integer root?*

24. *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*?*

25. *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 *copies. 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 using generating functions.*

26. *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.*

27. *My class has* N *students. 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 using generating functions.*

28. *My class has* N *students. In an examination paper, there are* M *questions. Each student answers all the questions in an order decided by him/her. In how many ways can it happen that some three or more students have followed the same order? Answer using generating function.*

29. *Eleven teachers attended the* Freshers' Party*. 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 using generating function.*

Chapter 7

Introduction to Logic

7.1 Logic of Statements (SL)

We study logic to differentiate between valid and invalid arguments. An **argument** is a set of statements which has two parts: a set of premises and a conclusion. Each premise is a statement which is assumed to hold for the sake of the argument. The conclusion is a statement claimed to hold by the argument. An argument has the structure

Premises: Statement$_1$, ..., Statement$_k$; therefore

Conclusion: Statement$_c$.

The following are instances of arguments:

- Statement$_1$: If today is Monday, then Mr. X gets ₹5.
  Statement$_2$: Today is Monday.
  Statement$_c$: (Therefore,) Mr. X gets ₹5.

- Statement$_1$: If today is Monday, then Mr. X gets ₹5.
  Statement$_2$: Mr. X gets ₹5.
  Statement$_c$: (Therefore,) Today is Monday.

- Statement$_1$: If today is Monday, then Mr. X gets ₹5.
  Statement$_2$: Today is Tuesday.
  Statement$_c$: (Therefore,) Mr. X gets ₹5.

- Statement$_1$: If today is Monday, then Mr. X gets ₹5.
  Statement$_2$: Today is Tuesday.
  Statement$_c$: (Therefore,) Mr. X does not get ₹5.

We understand that the first one is a valid argument, whereas the next three are not. In order to determine whether an argument is valid or not, we need to know the logical form of a statement. A simple statement is an expression which is either false or true but not both. Complex statements are made out of simple ones by using the words ‘not’, ‘and’, ‘or‘, ‘implies’ and ‘if and only if’.

For example, ‘Today is Monday’ is a statement. ‘Today is Tuesday’ is a statement. ‘Today is not Monday’ is a statement. ‘Today is Monday and today is Tuesday’ is also a statement.

Using symbols for simple statements and the words ‘not’, ‘and’, ‘or‘, ‘implies’ and ‘if and only if’ help us in seeing the logical structure of a statement. Normally, we use the symbols $p, q, r, p_1, p_2, \ldots$ to denote simple statements. The quoted words are denoted by $\neg$, $\wedge$, $\vee$, $\to$ and $\leftrightarrow$, respectively. Then the complex statements are made using these symbols along with parentheses by following some specified rules.

We abbreviate the phrase 'Logic of Statements' to 'SL' and present it in the following three sections.

7.2 Formulas and truth values in SL

Definition 7.2.1. Fix a countable set $A = \{p_1, p_2, \ldots\}$ of symbols. Each element of A is called an **atomic formula**. An atomic formula is also called an **atomic variable**. The special symbols $\neg$, $\wedge$, $\vee$, $\rightarrow$ and $\leftrightarrow$ are called **connectives**; their names are 'negation', 'conjunction', 'disjunction', 'implication', and 'biconditional', respectively. The **well formed formulas**, or **formulas**, for short, are generated by using the following rules recursively:

F1: Each atomic formula is a formula.

F2: If x is a formula, then $(\neg x)$ is a formula.

F3: If x and y are formulas, then $(x \wedge y)$, $(x \vee y)$, $(x \rightarrow y)$ and $(x \leftrightarrow y)$ are formulas.

The connective that has been introduced last in the process of generation of the formula is called the **principal connective** in that formula.

The connectives $\vee, \wedge, \rightarrow$, and $\leftrightarrow$ always connect two old formulas 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.* Notice that in every formula, there is a matching pair of parentheses.

Example 7.2.2.

1. The expression $(\neg p_5)$ is a formula.
   Ans: Since $p_5 \in A$, by (F1), it is a formula. By (F2), $(\neg p_5)$ is a formula. The principal connective in the formula is $\neg$.

2. The expression $(\neg(p_3 \wedge (\neg p_4)))$ is a formula.
   Ans: $p_3,\ p_4 \in A$; by (F1), these are formulas. By (F2), $(\neg p_4)$ is a formula. By (F3), $(p_3 \wedge (\neg p_4))$ is a formula. Next, by (F2), $(\neg(p_3 \wedge (\neg p_4)))$ is a formula. The principal connective in the formula is $\neg$.

3. The expression $(p_1 \rightarrow (p_1 \vee p_1))$ is a formula.
   Ans: By (F1), p_1 is a formula. By (F3), $(p_1 \vee p_1)$ is a formula. Once more, by (F3), $(p_1 \rightarrow (p_1 \vee p_1))$ is a formula. The principal connective in the formula is $\rightarrow$.

4. The expression $(p_1 \vee ((\neg(p_1 \rightarrow p_1)) \leftrightarrow (p_3 \wedge p_5)))$ is a formula.
   Ans: By (F1), $p_1,\ p_3$ and p_5 are formulas. By (F3), $(p_1 \rightarrow p_1)$ and $(p_3 \wedge p_5)$ are formulas. By (F2), $(\neg(p_1 \rightarrow p_1))$ is a formula. Next, by two applications of (F3), $(p_1 \vee ((\neg(p_1 \rightarrow p_1)) \leftrightarrow (p_3 \wedge p_5)))$ is a formula. The principal connective in this formula is $\vee$.

5. The expression $\neg p_9$ is not a formula since according to our formation rules, a pair of parentheses should have been used. Of course, with the pair of parentheses, the expression $(\neg p_9)$ is a formula, where the principal connective is $\neg$. Similarly, $(\neg(p_4))$ is not a formula due to extra pair of parentheses, but $(\neg p_4)$ is a formula with the principal connective as $\neg$.

6. The expression $(p_4 \vee p_5$ is not a formula, but $(p_4 \vee p_5)$ is a formula with the principal connective as $\vee$.

7. The expression $(p_6 \vee p_1) \wedge (\neg p_4))$ has one extra right parenthesis. Also, the connective $\wedge$ demands an extra pair of outer parentheses; that is, a left parenthesis is missing. We see that $((p_6 \vee p_1) \wedge (\neg p_4))$ is a formula with the principal connective as $\wedge$.

Convention: For our comfort, we use the symbols $p, q, r, \ldots$ with or without subscripts for atomic formulas in place of $p_1, p_2, \ldots$. Similarly, we ignore the outer parentheses in a formula. By using precedence rules we also cut short some more parentheses. The precedence rules are as follows:

1. $\neg$ has the highest precedence.
2. $\wedge$ and $\vee$ have the next precedence.
3. $\rightarrow$ and $\leftrightarrow$ have the least precedence.

Recall that when we say that $\times$ has more precedence over $+$, the expression $x \times y + z \times w$ means $\big((x \times y) + (z \times w)\big)$. If ambiguity results from using this convention in a context, we expand the abbreviated formulas to formulas and decide the case. We illustrate the convention in the following example.

Example 7.2.3. 1. By abbreviating p_5 as p, we abbreviate $(\neg p_5)$ as $\neg p$.

2. To abbreviate the formula $(\neg(p_3 \wedge (\neg p_4)))$, we write p_3 as p, p_4 as q. Using the precedence rules, our abbreviation is $\neg(p_3 \wedge \neg p_4)$.
3. Writing p_1 as p, we abbreviate $(p_1 \rightarrow (p_1 \vee p_1))$ as $p \rightarrow p \vee p$.
4. Write p_1 as p, p_3 as q, and p_5 as r. Then the formula $(p_1 \vee ((\neg(p_1 \rightarrow p_1)) \leftrightarrow (p_3 \wedge p_5)))$ is abbreviated to $p \vee (\neg(p \rightarrow p) \leftrightarrow q \wedge r))$.

To be careful, we should not abbreviate different atomic formulas to the same symbol in any context. For instance in the last part of the above example, we should not abbreviate both p_1 and p_3 as p.

Assuming familiarity with the process of abbreviation, we regard abbreviated formulas as formulas.

Since statements are supposed to be either true or false, we now discuss how to assign truth values to formulas. Observe that any formula has occurrences of some finite number of atomic variables. Further, if X is any formula, then either $X = p_i$, an atomic variable, or X is in one of the forms: $\neg p$, $p \wedge q$, $p \vee q$, $p \rightarrow q$, or $p \leftrightarrow q$ for formulas p, q, with the principal connective as $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, respectively.

Definition 7.2.4. Let X be a formula. Let B be the set of all formulas generated from the atomic variables occurring in X. A **truth assignment** (appropriate to X) is a function $f : B \rightarrow \{T, F\}$ satisfying the following conditions:

1. For an atomic variable p_i, either $f(p_i) = T$ or $f(p_i) = F$.

   For formulas p and q,

2. $f(\neg p) = F$ if $f(p) = T$, and $f(\neg p) = T$ if $f(p) = F$.
3. $f(p \wedge q) = T$ if $f(p) = f(q) = T$, and $(p \wedge q) = F$ otherwise.
4. $f(p \vee q) = F$ if $f(p) = f(q) = F$, and $f(p \vee q) = T$ otherwise.
5. $f(p \rightarrow q) = F$ if $f(p) = T,\ f(q) = F$, and $f(p \rightarrow q) = T$ otherwise.
6. $f(p \leftrightarrow q) = T$ if $f(p) = f(q)$, and $f(p \leftrightarrow q) = F$ otherwise.

Sometimes we write '$f(p_1, \ldots, p_k)$ is a formula' to mean that 'f is a formula involving the atomic formulas $p_1, \ldots, p_k$'. 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 formulas $p_1, \ldots, p_k$. 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 formulas. 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 formulas. The above definition of assignment of truth values can be depicted in a truth table. It is as follows.

Understanding the connectives in a Truth table:

p	$\neg p$
T	F
F	T

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	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Assignment of truth values to $\neg p,\ p \wedge q,\ p \vee q,\ p \to q,\ p \leftrightarrow q$

For instance, look at the table for $\to$. The second row there tells that when p is assigned T and q is assigned F, $p \to q$ is assigned F. In all other cases, $p \to q$ is assigned T.

Read T as 'true' and F as 'false'. Observe that $\neg$ makes a true statement false and a false statement true. The formula $p \wedge q$ is true if and only if both $p,\ q$ are true; $p \vee q$ is true if and only if at least one of $p,\ q$ is true; $p \leftrightarrow q$ is true when either both $p,\ q$ are true, or when both $p,\ q$ are false. The case that '$p \to q$ is true' closely resembles the sentence 'if p is true, then q is true', though not very obvious. (We illustrate this case in Example 7.2.6 below.) Accordingly, we also read the connectives $\neg,\ \wedge,\ \vee,\ \to$ and $\leftrightarrow$ as *not, and, or, then*[1] and *if and only if*, respectively.

Example 7.2.5. The following is a truth table for the formula $p \vee (q \wedge r)$.

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

Example 7.2.6. Consider the formula $p \to q$, where p and q symbolize the English statements as follows:

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 first three cases as explained below.

1. p is true and q is true. This means 'you attend the class and understand the subject'. Here, $p \to q$ is true.

2. p is false and q is false. This means 'you do not attend the class and do not understand the subject'. In this case, $p \to q$ is true.

3. p is false and q is true. This means 'you do not attend the class but understand the subject'. Here also, $p \to q$ is true.

[1] In many texts, $p \to q$ is read as 'if p then q'. However, it will be easier to read it as 'p then q'.

4. p is true and q is false. This means 'you attend the class and do not understand the subject'. Then $p \to q$ is false.

Thus, a conditional $p \to q$ is true when either p is false or q is true.

Practice **7.2.7.**

1. *Draw a truth table for the formula* $p \wedge \big(\neg p \to (p \vee \neg q)\big)$.
2. *Can both the formulas* $p \to q$ *and* $q \to p$ *be* F *for some assignment on* p *and* q*?*

Depending on the structure of a formula $f(p_1, \ldots, p_n)$ it receives a truth value under an assignment of truth values to the atomic formulas $p_1, \ldots, p_n$. It is quite possible that the formula receives the truth value T under an assignment and it receives the truth value F under another assignment. In this connection we isolate those formulas which receive the same truth value under each assignment.

Definition 7.2.8. A **contradiction** is a formula which takes the truth value F under each assignment. A **tautology** is a formula which takes the truth value T under each assignment. Often we write a contradiction as $\bot$ and a tautology as $\top$.

For example, $p \wedge \neg p$ is a contradiction and $p \vee \neg p$ is a tautology. Once a tautology and a contradiction are given new tautologies and contradictions can be obtained by using the following theorem.

Theorem 7.2.9. *Let A be a formula having at least one occurrence of an atomic variable p. Let B be any formula. Denote by $A[p/B]$ the formula obtained by replacing each occurrence of p by B in A.*

1. *If A is a contradiction, then $A[p/B]$ is a contradiction.*
2. *If A is a tautology, then $A[p/B]$ is a tautology.*

Proof. Let A be a contradiction. For ease in notation, write $A = A(p; p_1, \ldots, p_n)$, where other than p, the atomic variables occurring in A are $p_1, \ldots, p_n$. Similarly, write $A[p/B] = A(B; p_1, \ldots, p_n)$. Let f be any truth assignment that assigns truth values to $p, p_1, \ldots, p_n$ and also to all atomic variables occurring in B.

If f assigns T to B, then the value of $A[p/B]$ is the same as that of $A(T; p_1, \ldots, p_n)$, which is F since A is a contradiction.

If f assigns F to B, then the value of $A[p/B]$ is the same as that of $A(F; p_1, \ldots, p_n)$, which is F since A is a contradiction.

Hence, $A[p/B]$ takes the value F under the assignment f. Since f is an arbitrary assignment, we conclude that $A[p/B]$ is a contradiction. This proves the first statement.

Statement 2 is proved similarly. ∎

For example, $((p \to q) \wedge (q \leftrightarrow r)) \wedge \neg((p \to q) \wedge (q \leftrightarrow r))$ is a contradiction, since it is obtained from $p \wedge \neg p$ by replacing p with $((p \to q) \wedge (q \leftrightarrow r))$. Similarly, $((p \to q) \wedge (q \leftrightarrow r)) \vee \neg((p \to q) \wedge (q \leftrightarrow r))$ is a tautology since it is obtained from $p \vee \neg p$ by replacing p with $((p \to q) \wedge (q \leftrightarrow r))$.

7.3 Equivalence and Normal forms in SL

In an algebraic identity such as $(x + y)^2 = x^2 + 2xy + y^2$, when we replace the variables x, y with some numbers we see that both the sides give the same value. Such expressions help us in simplifying algebraic expressions. Analogously, we introduce the notion of equivalence which will help us in simplifying formulas.

Definition 7.3.1. Two formula A and B are called **equivalent** if under any truth assignment, both receive the same truth value. When A and B are equivalent, we write $A \equiv B$.

Thus, equivalent formulas are evaluated the same in each row of their truth table. Notice that the set of atomic variables occurring in both the formulas may not be same; so a truth table is to be constructed taking care of all the atomic variables involved.

Example 7.3.2.

1. Is $p \to q \equiv \neg q \to \neg p$?
   Ans: We construct a truth table as follows.

p	q	$p \to q$	$\neg q \to \neg p$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

   Since in each row of the truth table, the truth values of the two formulas match, they are equivalent.

2. Is $p \equiv p \wedge (q \vee (\neg q))$?
   Ans: The truth table is constructed below.

p	q	$p \wedge (q \vee (\neg q))$
T	T	T
T	F	T
F	T	F
F	F	F

   Since in each row of the truth table the values of p and that of $p \wedge (q \vee (\neg q))$ match, they are equivalent.

PRACTICE **7.3.3.** *Is $p \vee \neg p \equiv q \vee \neg q$?*

When many atomic variables are involved, it may be time consuming to construct a truth table. In such a case, equivalence may be shown by using one of the following methods:

1. $A \equiv B$ if and only if whenever A is true, B is true, and whenever B is true, A is also true.
2. $A \equiv B$ if and only if whenever B is false, A is false, and whenever B is false, A is also false.

Example 7.3.4. Show that $p \to q \equiv \neg q \to \neg p$.
Ans: $p \to q$ is false if and only if p is true and q is false
if and only if $\neg p$ is false and $\neg q$ is true
if and only if $\neg q \to \neg p$ is false.
Hence $p \to q \equiv \neg q \to \neg p$.

Proposition 7.3.5. **[Laws]** *Let p, q, r be formulas. Then the following equivalences hold:*

1. **[Commutativity]** $p \vee q \equiv q \vee p, \quad p \wedge q \equiv q \wedge p$

2. **[Associativity]** $p \vee (q \vee r) \equiv (p \vee q) \vee r, \quad p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

3. **[Distributivity]** $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r), \quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

4. **[De Morgan]** $\neg(p \vee q) \equiv \neg p \wedge \neg q, \quad \neg(p \wedge q) \equiv \neg p \vee \neg q$
5. **[Idempotence]** $p \vee p \equiv p, \quad p \wedge p \equiv p$
6. **[Constants]** $\bot \vee p \equiv p, \quad \bot \wedge p \equiv \bot, \quad \top \vee p \equiv \top, \quad \top \wedge p \equiv p, \quad p \vee \neg p \equiv \top, \quad p \wedge \neg p \equiv \bot,$
   where $\bot$ denotes contradiction and $\top$ denotes tautology.
7. **[Double Negation]** $\neg(\neg p) \equiv p$
8. **[Absorption]** $p \vee (p \wedge q) \equiv p, \quad p \wedge (p \vee q) \equiv p$
9. **[Implication]** $p \to q \equiv \neg p \vee q, \quad \neg(p \to q) \equiv p \wedge \neg q$
10. **[Contraposition]** $p \to q \equiv \neg q \to \neg p, \quad p \to \neg q \equiv q \to \neg p$
11. **[Biconditional]** $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q), \quad p \leftrightarrow q \equiv (\neg p \vee q) \wedge (p \vee \neg q),$
    $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

Proof. Construct the truth tables and verify. ∎

Remark 7.3.6. The statement $q \to p$ is called the **converse** of the statement $p \to q$. In general, a statement is not equivalent to its converse. Reason: The assignment f that assigns T to p and F to q, assigns F to $p \to q$ but assigns T to $q \to p$. Also, the assignment g that assigns T to q and F to p assigns F to $q \to p$ while it assigns T to $p \to q$. Compare this with the Rule of Contraposition. The **contrapositive** of a statement $p \to q$ is $\neg q \to \neg p$. The rule says that a statement is equivalent to its contrapositive.

The above laws help us in proving equivalence of some formulas, in addition to the method of truth tables and helps us in analyzing when the formulas are true or false.

Example 7.3.7. We use the laws to show the following:

1. $p \to (q \to r) \equiv (p \wedge q) \to r.$
2. $\neg(p \leftrightarrow q) \equiv \neg p \leftrightarrow q.$
3. $p \to q \equiv p \leftrightarrow p \wedge q.$

Ans:

(1)
$$\begin{aligned} p \to (q \to r) &\equiv \neg p \vee (\neg q \vee r) && \text{as } p \to p \equiv (\neg p) \vee q \\ &\equiv (\neg p \vee \neg q) \vee r && \text{Associativity} \\ &\equiv \neg(p \wedge q) \vee r && \text{De Morgan} \\ &\equiv (p \wedge q) \to r && \text{as } p \to p \equiv (\neg p) \vee q \end{aligned}$$

(2)
$$\begin{aligned} \neg(p \leftrightarrow q) &\equiv \neg\big((p \wedge q) \vee (\neg p \wedge \neg q)\big) && \text{Biconditional} \\ &\equiv \neg(p \wedge q) \wedge \neg(\neg p \wedge \neg q) && \text{De Morgan} \\ &\equiv (\neg p \vee \neg q) \wedge (p \vee q) && \text{De Morgan, Double negation} \\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge q) \vee (\neg q \wedge p) \vee (\neg q \wedge q) && \text{Distributivity} \\ &\equiv (\neg p \wedge q) \vee (\neg q \wedge p) && \text{Constants} \\ &\equiv (\neg p \wedge q) \vee (\neg\neg p \wedge \neg q) && \text{Double negation} \\ &\equiv \neg p \leftrightarrow q && \text{Biconditional} \end{aligned}$$

(3)
$$\begin{aligned} p \leftrightarrow p \wedge q &\equiv \big(\neg p \vee (p \wedge q)\big) \wedge \big(p \vee \neg(p \wedge q)\big) && \text{Biconditional} \\ &\equiv \big(\neg p \vee (p \wedge q)\big) \wedge (p \vee (\neg p \vee \neg q)) && \text{De Morgan} \\ &\equiv (\neg p \vee p) \wedge (\neg p \vee q) \wedge (p \vee (\neg p \vee \neg q)) && \text{Distributivity} \\ &\equiv \neg p \vee q && \text{Constants} \\ &\equiv p \to q && \text{Implication} \end{aligned}$$

PRACTICE **7.3.8.**

1. *Does the absorption law imply* $p \vee (p \wedge (\neg q)) \equiv p$ *and* $p \wedge (p \vee (\neg q)) \equiv p$*?*
2. *Write a statement equivalent to* $(p \to q) \to \big(p \to (q \to \neg r)\big)$ *where* $\to$ *and* $\leftrightarrow$ *do not occur. Simplify so that the number of occurrences of connectives is minimum.*

Any formula has a truth table. On the other hand, if a truth table is given, can we construct a formula corresponding to it? For example, can we have a formula involving the atomic variables p, q, r such that the formula receives the truth value T under the assignment T, F, T to p, q, r, respectively? We see that the formula $p \wedge \neg q \wedge r$ does the job.

Definition 7.3.9. A **truth function** of n variables is any function from $\{T, F\}^n \to \{T, F\}$. A truth function is **expressed by** a formula if the formula has the same truth table as that of the truth function.

If ϕ is a truth function of n variables $p_1, \ldots, p_n$, then a truth table can be constructed to depict it. Such a truth table will have n columns and 2^n rows, each row showing the different assignments of truth values to the variables. The $(n+1)$-th column is filled with T or F corresponding to each row. For example, the truth function $\phi : \{T, F\}^2 \to \{T, F\}$ given by

$$\phi(T, T) = T, \ \phi(T, F) = F, \ \phi(F, T) = T, \ \phi(F, F) = F$$

is depicted by the truth table

p	q	ϕ
T	T	T
T	F	F
F	T	T
F	F	F

Notice that there are 2^{2^n} number of truth functions involving n number of variables. Obviously, any formula is a truth function. The question is whether any truth function can be expressed by a formula.

Experiment: Consider the variables p, q, r in that order.
A formula which takes value T only on the assignment TTT is $p \wedge q \wedge r$. Verify.
A formula which takes value T only on the assignment TTF is $p \wedge q \wedge \neg r$. Verify.
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, *i.e.*, whose truth table is the following:

p	q	r	A
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

Theorem 7.3.10. *Each truth function of n variables is expressed by a formula involving n variables.*

Proof. Let ϕ be a truth function of n variables. Let $p_1, \ldots, p_n$ be n number of atomic variables. If $\mathsf{rng}\,\phi = \{F\}$, then $A \equiv \bot$. Thus, take $A = p_1 \wedge \neg p_1 \wedge p_2 \wedge \cdots \wedge p_n$. Otherwise, collect all those assignments f such that $\phi(f) = T$. Suppose this set is $\{f_1, \ldots, f_m\}$. Corresponding to each f_i, define the formula $B_i = r_1 \wedge r_2 \wedge \cdots \wedge r_n$, where for $1 \leq j \leq n$,

$$r_j = \begin{cases} p_j & \text{if } f(p_j) = T \\ \neg p_j & \text{if } f(p_j) = F. \end{cases}$$

Notice that the formula B_i takes the value T only on the assignment f_i. Thus, $A = B_1 \vee B_2 \vee \cdots \vee B_m$ is the required formula. ∎

Example 7.3.11. Construct a formula that expresses the truth function ϕ given by

p	q	ϕ
T	T	T
T	F	T
F	T	F
F	F	F

Ans: The truth function ϕ is true only for the truth assignments f_1 and f_2, where $f_1(p) = f_1(q) = T$ and $f_2(p) = T, f_2(q) = F$. The corresponding formulas are $B_1 = p \wedge q$ and $B_2 = p \wedge \neg q$. So the formula that expresses ϕ is $(p \wedge q) \vee (p \wedge \neg q)$.

As the proof of Theorem 7.3.10 shows, each truth function can be expressed by a formula which has a special form. In particular, every formula can be equivalently expressed by a formula in such a special form. We define such a special form, along with another related special form.

Definition 7.3.12. An atomic formula and the negation of an atomic formula are together called **literals**. We say that a formula A is in **disjunctive normal form** (in short, DNF) if it is a disjunction of conjunctions of literals. We say that a formula A is in **conjunctive normal form** (in short, CNF) if it is a conjunction of disjunctions of literals. Both DNF and CNF are called **normal forms**.

Example 7.3.13. The formulas $(p \wedge \neg q) \vee \neg r$ and $(p \wedge \neg q) \vee (q \wedge \neg r) \vee (r \wedge s)$ are in DNF; $(p \vee \neg q) \wedge r$ and $(p \vee q) \wedge (q \vee \neg r) \wedge (r \vee s)$ are in CNF; while $p,\ p \vee q,\ \neg p \wedge q$ are in both CNF and DNF.

PRACTICE **7.3.14.** *Write 5 formulas in CNF involving p, q, r.*

Theorem 7.3.15. *Any formula is equivalent to a formula in DNF, and also to a formula in CNF.*

Proof. Since each formula is a truth function, the first assertion follows from Theorem 7.3.10. The second assertion can be proved similarly. Alternatively, if A is a formula, get a DNF for $\neg A$; then negate the DNF and use the distributivity laws to get an equivalent CNF. ∎

PRACTICE **7.3.16.** *Write all the truth functions on two variables and write formulas for them.*

A CNF and/or DNF representation of a formula can be computed by using equivalences. First, we eliminate the connectives $\rightarrow$ and $\leftrightarrow$ by using the laws of Implication and Biconditional, *i.e.*, by using the equivalences $x \rightarrow y \equiv \neg x \vee y$ and $x \leftrightarrow y \equiv (\neg x \vee y) \wedge (x \vee \neg y)$. Next, we use the law of De Morgan and Double negation, that is, $\neg(x \vee y) \equiv (\neg x \wedge \neg y)$, $\neg(x \wedge y) \equiv (\neg x \vee \neg y)$ and $\neg\neg x \equiv x$ so that the earlier obtained formula is equivalent to the one, in which each occurrence of the connective $\neg$ precedes atomic variables. Finally, we use the laws of distributivity to obtain an equivalent formula, which is in CNF and/or DNF. The formula so obtained can also be simplified using the laws of Absorption. The following examples illustrate this method.

Example 7.3.17. Find a formula in DNF and also one in CNF equivalent to

$$((p \to q) \wedge (q \to r)) \vee ((p \wedge q) \to r).$$

We apply various laws in bringing the formula to its DNF and CNF as follows. Complete this by mentioning the laws at each step.

$$\begin{aligned} &((p \to q) \wedge (q \to r)) \vee ((p \wedge q) \to r) \\ &\equiv ((\neg p \vee q) \wedge (\neg q \vee r)) \vee (\neg(p \wedge q) \vee r) \\ &\equiv ((\neg p \vee q) \wedge (\neg q \vee r)) \vee (\neg p \vee \neg q \vee r) \end{aligned}$$

Ans: Using Distributivity on $(\neg p \vee q) \wedge (\neg q \vee r)$, we get the DNF as

$$(\neg p \wedge \neg q) \vee (\neg p \wedge r) \vee (q \wedge \neg q) \vee (q \wedge r) \vee (\neg p \vee \neg q \vee r).$$

Using Distributivity on the whole formula, we get the CNF as

$$(\neg p \vee q \vee \neg p \vee \neg q \vee r) \wedge (\neg q \vee r \vee \neg p \vee \neg q \vee r).$$

Notice that the CNF can be simplified using Absorption laws. The simplified formula equivalent to the original formula is $\neg p \vee \neg q \vee r$, which is in both DNF and CNF.

EXERCISE **7.3.18.**

1. *Use induction on the number of connectives to show that any formula is equivalent to a formula in DNF and a formula in CNF.*

2. *A set of connectives is called* **adequate** *if every other connective can be expressed in terms of the given ones. For instance, DNF and CNF conversion show that $\{\neg, \wedge, \vee\}$ is an adequate set. Determine which are adequate:*
   (a) $\{\neg, \wedge\}$ (b) $\{\neg, \vee\}$ (c) $\{\neg, \to\}$ (d) $\{\wedge, \vee\}$ (e) $\{\neg, \leftrightarrow\}$ (f) $\{\to, \vee, \wedge\}$.

3. *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 the same under b. Thus, the value of $f \leftrightarrow g$ is T under b. As b is an arbitrary assignment, we see that $f \leftrightarrow g$ is a tautology.*

   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 tautology. Assume that $f \not\equiv g$. Then, there is an assignment b under which f and g take different truth values.

   So, suppose that f takes T and g takes F under b. Then $f \to g$ 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. ∎

4. *The* **dual** *P^* of a formula P involving the connectives $\vee, \wedge, \neg$ is obtained by interchanging $\vee$ with $\wedge$. For instance, the dual of $\neg(p \vee q) \wedge r$ is $\neg(p \wedge q) \vee r$. Prove the following:*

(a) *Let $A(p_1, \ldots, p_k)$ be a formula involving the atomic variables $p_1, \ldots, p_k$ and 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 for $1 \le i \le k$, then $A(\neg p_1, \ldots, \neg p_k) \equiv \neg A^*(p_1, \ldots, p_k)$.*

(b) *Let A, B be formulas that use only the connectives $\vee, \wedge$ and $\neg$. If $A \equiv B$, then $A^* \equiv B^*$.*

7.4 Inferences in SL

We now turn our attention towards the main goal of logic: when is a given argument valid? An argument has the form: "$S_1, \ldots, S_n$. Therefore, Q.". Here, $S_1, \ldots, S_n$ and Q are sentences in some natural language. To translate such an argument to SL involves translating the sentences to formulas in SL. Suppose $S_1, \ldots, S_n, Q$ are translated to the formulas $P_1, \ldots, P_n, C$, respectively. Our goal is to determine whether C is true under the assumption that each of $P_1, \ldots, P_n$ is true. The translated entity corresponding to the argument is denoted by

$$P_1, \ldots, P_n \overset{?}{\Rightarrow} C$$

and is called an *inference*. We use the terminology that $P_1, \ldots, P_n$ are premises and C is the conclusion of this inference. Once the truth of C is determined from the assumption that $P_1, \ldots, P_n$ are true, we would like to write

$$\text{the inference } \; P_1, \ldots, P_n \overset{?}{\Rightarrow} C \; \text{ is valid.}$$

This last assertion is written as

$$P_1, \ldots, P_n \Rightarrow C.$$

We formally define the notions involved.

Definition 7.4.1. An **inference** is an expression of the form $\{P_1, \ldots, P_n\} \overset{?}{\Rightarrow} C$, where $P_1, \ldots, P_n$ and C are formulas. We also write the inference as $P_1, \ldots, P_n \overset{?}{\Rightarrow} C$. The formulas $P_1, \ldots, P_n$ are called the **premises** or **hypotheses**, and C is called the **conclusion** of the inference. We say that the inference is **valid** if $(P_1 \wedge \cdots \wedge P_n) \to C$ is a tautology; in this case, we write $\{P_1, \ldots, P_n\} \Rightarrow C$, and also $P_1, \ldots, P_n \Rightarrow C$. We read the symbol $\Rightarrow$ as 'implies'. When the inference is valid, we also say that C is a **logical conclusion** of the premises $P_1, \ldots, P_n$.

Example 7.4.2.

1. Is the following argument valid?

   If $x = 4$, then discrete math is bad. Discrete math is bad. Therefore, $x = 4$.

   Ans: Denote '$x = 4$' by p and 'discrete mathematics is bad' by q. The argument is translated to SL as the inference $\{p \to q,\ q\} \overset{?}{\Rightarrow} p$. The question is whether the inference is valid or not, *i.e.*, whether $\{p \to q,\ q\} \Rightarrow p$. We need to determine whether $(p \to q) \wedge q \to p$ is a tautology or not.

   Consider the assignment f with $f(p) = F$ and $f(q) = T$. In this assignment, $p \to q$ is T; $(p \to q) \wedge q$ is T; consequently, $(p \to q) \wedge q \to p$ is F. Hence, the argument is invalid.

2. Is the following argument valid?

   If discrete math is bad, then $x = 4$. Discrete math is bad. Therefore, $x = 4$.

Ans: Denote '$x = 4$' by p and 'discrete mathematics is bad' by q. The argument is translated into the inference $\{q \to p,\ q\} \overset{?}{\Rightarrow} p$. To determine whether it is valid, we need to find whether $(q \to p) \wedge q \to p$ is a tautology.

For this, suppose there is an assignment for which $(q \to p) \wedge q \to p$ takes the value F. Then for that assignment, p must be F and $(q \to p) \wedge q$ must be T. As $(q \to p) \wedge q$ is T, q must be T and $q \to p$ must be T. Thus, we need to have, p is F, q is T, and $q \to p$ is T. This is impossible.

Hence, there is no assignment for which $(q \to p) \wedge q \to p$ is F. Hence, it is a tautology. So p logically follows from $q \to p$ and q. That is, $\{q \to p,\ q\} \Rightarrow p$. The argument is valid.

Remark 7.4.3. Let A, B be formulas. $A \Rightarrow B$ means that $A \to B$ is a tautology. Similarly, $B \Rightarrow A$ means $B \to A$ is a tautology. Hence "$A \Rightarrow B$ and $B \Rightarrow A$" is same as "$A \leftrightarrow B$ is a tautology", which is again same as $A \equiv B$. Thus, sometimes $A \equiv B$ is also written as $A \Leftrightarrow B$.

While proving an inference to be correct, we only show that the falsity of the conclusion does not go along with the truth of the premises, *i.e.*, the premises and the negation of the conclusion cannot be true simultaneously. And, if the conclusion of an inference is in the form $p \to q$, we often ignore the cases when p is false. This is so because when p is false, $p \to q$ is true, and in this case, we need not use any premise towards a correct inference. These two proof methods are encapsulated in the following result.

Theorem 7.4.4. *Let $A_1, \ldots, A_n$ and X, Y be formulas.*

1. [**Rule of Contradiction**] $A_1, \ldots, A_n \Rightarrow X$ *if and only if* $A_1 \wedge \cdots \wedge A_n \wedge \neg X$ *is a contradiction.*
2. [**Rule of Deduction**] $A_1, \ldots, A_n \Rightarrow X \to Y$ *if and only if* $A_1, \ldots, A_n, X \Rightarrow Y$.

Proof. (1) Suppose $A_1, \ldots, A_n \Rightarrow X$. Let f be a truth assignment. Then f assigns T to $A_1 \wedge \cdots \wedge A_n \to X$. If f assigns any one of $A_1, \ldots, A_n$ to F, then it assigns F to $A_1 \wedge \cdots \wedge A_n \wedge \neg X$. Otherwise, f assigns T to each of $A_1, \ldots, A_n$. Since f assigns T to $A_1 \wedge \cdots \wedge A_n \to X$, f assigns T to X. In this case, f assigns F to $A_1 \wedge \cdots \wedge A_n \wedge \neg X$. Hence, each assignment f assigns F to $A_1 \wedge \cdots \wedge A_n \wedge \neg X$. Thus, $A_1 \wedge \cdots \wedge A_n \wedge \neg X$ is a contradiction.

Conversely, suppose $A_1 \wedge \cdots \wedge A_n \wedge \neg X$ is a contradiction. Let f be an assignment. If f assigns F to any of $A_1, \ldots, A_n$, then f assigns T to $A_1, \ldots, A_n \to X$. Otherwise, suppose f assigns T to all of $A_1, \ldots, A_n$. Since $A_1 \wedge \cdots \wedge A_n \wedge \neg X$ is a contradiction, f assigns F to $\neg X$. That is, f assigns T to X. Hence, f assigns T to $A_1, \ldots, A_n \to X$. That is, each assignment f assigns T to $A_1, \ldots, A_n \to X$. Therefore, $A_1, \ldots, A_n \Rightarrow X$.

(2) We use (1) repeatedly and the equivalence $\neg(X \to Y) \equiv X \wedge \neg Y$ to obtain the following:
$A_1, \ldots, A_n \Rightarrow X \to Y$
if and only if $A_1 \wedge \cdots \wedge A_n \wedge \neg(X \to Y)$ is a contradiction
if and only if $A_1 \wedge \cdots \wedge A_n \wedge X \wedge \neg Y$ is a contradiction
if and only if $A_1 \wedge \cdots \wedge A_n \wedge X \Rightarrow Y$. ∎

Example 7.4.5. [**MP, MT, HS, AI, OI**]

1. Show that $p,\ p \to q \Rightarrow q$.

   Ans: Suppose p and $p \to q$ are T (under an assignment). Suppose q is F (under the same assignment). As $p \to q$ is T, p must be F. This is a contradiction.

   Alternate. By the rule of Deduction, $(p,\ p \to q) \Rightarrow q \equiv (p \to q, p) \Rightarrow q$ if and only if $p \to q \Rightarrow p \to q$ if and only if $(p \to q) \to (p \to q)$ is a tautology; and this is true.

   This inference is called **Modus Ponens**, often abbreviated to **MP**.

2. Show that $\neg q,\ p \to q \Rightarrow \neg p$.

   Ans: Suppose $\neg q$ and $p \to q$ are T. If $\neg p$ is F, then p is T. Now that $p \to q$ is T, we see that q is T. This is a contradiction.

   Alternate. By the rule of Deduction, $\neg q,\ p \to q \Rightarrow \neg p$ if and only if $(p \to q) \to (\neg q \to \neg p)$ is a tautology; and this follows from Contraposition.

   This inference is called **Modus Tolens**, often abbreviated to **MT**.

3. Show that $p \to q,\ q \to r \Rightarrow p \to r$.

   Ans: Suppose $p \to r$ is F. Then p is T and r is F. As r is F and $q \to r$ is T, q must be F. As q is F and $p \to q$ is T, p is F, a contradiction.

   Alternate. Using the rule of Deduction, we need to show that $p \to q, q \to r, p \Rightarrow r$. Using Modus Ponens $p, p \to q \Rightarrow q$, we have $(p \to q, q \to r, p) \equiv (q, q \to r)$ which in turn implies r (again using Modus Ponens).

   This inference is called **Hypothetical Syllogism** abbreviated to **HS**.

4. Show that $p \to q,\ p \to r \Rightarrow p \to q \wedge r$.

   Ans: Suppose p is T. Since $p \to q$ is T, q is T. Since $p \to r$ is T, r is T. Then $q \wedge r$ is T. Hence $p \to q \wedge r$ is T.

   This inference is called **And Introduction**, abbreviated to **AI**.

5. Show that $p \to r,\ q \to r \Rightarrow p \vee q \to r$.

   Ans: Suppose $p \vee q \to r$ is F. Then $p \vee q$ is T and r is F. Since r is F and the premise $p \to r$ is T, we have p is F. Similarly, the premise $q \to r$ gives q is F. Now, the three statements p is F, q is F and $p \vee q$ is T lead to a contradiction.

   This inference is called **Or Introduction**, abbreviated to **OI**.

As you see, correctness of an inference may be proved in three ways. Consider an inference

$$A_1, \ldots, A_n \overset{?}{\Rightarrow} C.$$

We find out the atomic formulas involved in all the formulas A_i and C. Then we construct a truth table having columns devoted to all A_is and also C. Next, we mark all those rows, where all A_is are T. In all these rows, check whether C is also T. If yes, then the inference is correct, else, the inference is incorrect. This method of proof is called **Proof by Truth Table**.

Instead of constructing a truth table, one analyzes all possibilities of assigning truth values to the atomic formulas so that the premises are true, and then shows that in all these cases, the conclusion is also true. This method also comes under the method of truth table.

In another variation of the truth table method, we consider all possibilities of assigning truth values to the atomic variables so that the conclusion is false. In each of these cases, we show that at least one premise becomes false. This method is sometimes referred to as the *indirect truth table method.*

Thus, the truth table method has three varieties of proofs: one - construction of truth table, two - analyzing the cases when premises are true, and three - analyzing the cases when the conclusion is false. We see that when the conclusion is in the form $p \to q$, it is advantageous to use the third variation.

Alternatively, we may use the laws and the already known valid inferences such as Modus Ponens, Modus Tolens, Hypothetical Syllogism, And Introduction, and Or Introduction to construct a proof of the required inference. In this method, a **proof** is defined as a finite sequence of formulas, where each formula is either a premise (some A_i), or a tautology, or is derived from earlier formulas using some law or already known valid inferences. The last formula in such a sequence must be the conclusion C. Such a proof is called a **Direct Proof**. If the conclusion C is in the form $p \to q$, then we may use p as a new premise, and construct a proof with conclusion q. In symbols,

$$A_1, \ldots, A_n \Rightarrow p \to q \text{ if and only if } A_1, \ldots, A_n, p \Rightarrow q$$

This follows from the rule of Deduction; see Theorem 7.4.4.

As the third alternative, we construct a proof using the rule of Contradiction. Such a proof is called an **Indirect proof**. In such a proof, one uses $\neg C$ as a new premise, and then derives a contradiction. Schematically,

$$A_1, \ldots, A_n \Rightarrow C \text{ if and only if } A_1, \ldots, A_n, \neg C \Rightarrow \perp$$

This method is justified by the rule of Contradiction as shown in Theorem 7.4.4. While constructing the proof, when we find that some formula X has appeared in a line, and also $\neg X$ has appeared in some line, then it would mean that the same set of premises imply X as well as $\neg X$. This is a contradiction. Thus we mention these two lines as our justification and write $\perp$ on the last line.

In practice, we use the rule of Deduction and the rule of Contradiction to bring the given inference to another form and proceed towards constructing a proof of the new inference. We explain these methods of proof in the following example.

Example 7.4.6. Determine validity of the following 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.

Ans: Let us symbolize the simple statements as follows:

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.

We need to determine the validity of the inference

$$q \wedge a \to m, f \to q, \neg p \to a \overset{?}{\Rightarrow} \neg m \to \neg f \vee p.$$

Proof by Truth table: In this case, we have five atomic formulas; the truth table will consist of 2^5 rows. After construction, we will find that there are more than twenty cases, where the premises are true. In all theses cases, we will find that the conclusion is also true.

However, this is time consuming. Even analyzing the truth values so that the premises are true is no less time consuming. We will rather use the indirect truth table method.

Suppose the conclusion $\neg m \to (\neg f \vee p)$ is F and each of the premises $q \wedge a \to m, f \to q$ and $\neg p \to a$ is T.

Now, $\neg m \to (\neg f \vee p)$ is F means $\neg f \vee p$ is F and $\neg m$ is T. Hence, the atomic variables m, f and p take values F, T and F, respectively. Since $f \to q$ is T and f is T, q must be T. Similarly, $\neg p \to a$

is T gives a is T. Then $(q \wedge a) \to m$ is T and both q and a are T give m is T. This contradicts $\neg m$ taking the value T.

Therefore, the inference is valid; that is, $q \wedge a \to m, f \to q, \neg p \to a \Rightarrow \neg m \to \neg f \vee p$; and hence the argument is valid.

Direct Proof: First, we plan how to go about: from $f \to q$ and $\neg p \to a$, we get $f \wedge \neg p \to q \wedge a$. Then $q \wedge a \to m$ gives $f \wedge \neg p \to m$. Its contrapositive is $\neg m \to \neg f \vee p$. This plan is rewritten as a proof below, where we mention the justification on the right side, which may be a tautology, a premise, a law, or a known rule (valid inference) that uses previous lines.

1.	$f \wedge \neg p \to f$	$(p \wedge q \Rightarrow p)$
2.	$f \wedge \neg p \to \neg p$	$(p \wedge q \Rightarrow q)$
3.	$f \to q$	(Premise)
4.	$f \wedge \neg p \to q$	$(1, 3, \mathrm{HS})$
5.	$\neg p \to a$	(Premise)
6.	$f \wedge \neg p \to a$	$(2, 5, \mathrm{HS})$
7.	$f \wedge \neg p \to (q \wedge a)$	$(4, 6, \mathrm{AI})$
8.	$q \wedge a \to m$	(Premise)
9.	$f \wedge \neg p \to m$	$(7, 8, \mathrm{HS})$
10.	$\neg m \to \neg(f \wedge \neg p)$	(Contraposition)
11.	$\neg m \to \neg f \vee \neg\neg p$	(De Morgan)
12.	$\neg m \to \neg f \vee p$	(Double negation)

Indirect Proof: Using the rule of Deduction and Contradiction, we have

$q \wedge a \to m,\ f \to q,\ \neg p \to a \Rightarrow \neg m \to \neg f \vee p$

if and only if $q \wedge a \to m,\ f \to q,\ \neg p \to a,\ \neg m \Rightarrow \neg f \vee p$

if and only if $q \wedge a \to m,\ f \to q,\ \neg p \to a,\ \neg m,\ \neg(\neg f \vee p) \Rightarrow \perp$.

We then proceed to construct a proof of the last assertion.

1.	$\neg(\neg f \vee p)$	(premise)
2.	$f \wedge \neg p$	(De Morgan, Double negation)
3.	f	$(p \wedge q \Rightarrow p)$
4.	$\neg p$	$(p \wedge q \Rightarrow q)$
5.	$f \to q$	(Premise)
6.	q	$(3, 5, \mathrm{MP})$
7.	$\neg p \to a$	(Premise)
8.	a	$(4, 7, \mathrm{MP})$
9.	$q \wedge a$	$(6, 8, \mathrm{AI})$
10.	$q \wedge a \to m$	(Premise)
11.	m	$(9, 10, \mathrm{MP})$
12.	$\neg m$	(Premise)
13.	$\perp$	$(11, 12)$

Exercise **7.4.7.**

1. *List all the nonequivalent formulas involving atomic variables p and q which take truth value T on exactly half of the assignments.*

2. *Let A and B be two formulas involving the atomic variables $p_1, \ldots, p_k$. Prove that $A \equiv B$ if and only if '$A \leftrightarrow B$ is a tautology'.*

3. *Prove* $(p \to q \vee r) \equiv (p \wedge \neg q \to r)$ *in three different ways: truth table method, simplification, by proving both* $p \to q \vee r \Rightarrow p \wedge \neg q \to r$ *and* $p \wedge \neg q \to r \Rightarrow p \to q \vee r$.

4. *Determine which of the following are logically equivalent:*
   (a) $q \to s$
   (b) $(p \to r \vee s) \wedge (q \wedge r \to s)$
   (c) $(s \to q \vee r) \wedge (q \wedge s \to r)$
   (d) $\big(p \vee r \vee (s \to p)\big) \wedge \big(p \to (s \to r)\big)$
   (e) $\big(p \vee s \vee (q \to p)\big) \wedge \big(p \to (q \to s)\big)$.

5. *Let* A *be a formula that involves the connectives* $\wedge$, $\vee$, $\to$, *and atomic variables* $p_1, \cdots, p_k$. *Show that the truth value of* A *is* T *under the assignment* $f(p_1) = \cdots = f(p_k) = T$.

6. *Verify the following assertions by analyzing truth table, and also by constructing a proof:*
   (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) $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
   (k) $p \wedge q,\ p \vee q \Rightarrow p \to q$
   (l) $p_0 \to p_1,\ p_1 \to p_2,\ \ldots,\ p_9 \to p_{10} \Rightarrow \neg p_0 \vee p_5$.
   (m) $\neg p \vee q \to r,\ s \vee \neg q,\ \neg t,\ p \to t,\ \neg p \wedge r \to \neg s \Rightarrow \neg q$.
   (n) $p \to q,\ r \vee s,\ \neg s \to \neg t,\ \neg q \vee s,\ \neg s,\ \neg p \wedge r \to u,\ w \vee t \Rightarrow u \wedge w$.

7. [**Monotonicity**] *Let* $S_1 \subseteq S_2$ *be finite sets of formulas and let* A *be a formula. Show that if* $S_1 \Rightarrow A$, *then* $S_2 \Rightarrow A$. *(We have used this result without mention.)*

8. *Determine which of the following arguments is/are correct:*
   (a) *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. (Assume that a subject is either bad or good.)*
   (b) *Three persons X, Y and Z are making statements. We know that if X is wrong, then Y is right; if Y is wrong, then Z is right; and if Z is wrong, then X is right. Does it follow that at least two of them are always right?*
   (c) *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 a lot of small irritating disturbances to the instructor. The lecture proceeds and the students are comfortable. Therefore, the instructor faces disturbances.*

9. *The normal forms can be used for inferences. The clue lies in seeing when a normal form is a tautology or a contradiction. Let* $A = C_1 \vee \cdots \vee C_m$ *be a formula in DNF and let* $B = D_1 \wedge \cdots \wedge D_n$ *be a formula in CNF, where* C_i*s are conjunctions of literals and* D_j*s are disjunctions of literals. Prove the following:*
   (a) *A is a tautology if and only if each C_i has an occurrence of p and also $\neg p$ for some atomic variable p. Such a p may vary from C_i to C_i.*
   (b) *B is a contradiction if and only if each D_i has an occurrence of p and also $\neg p$ for some atomic variable p. Such a p may vary from D_j to D_j.*
   Ans: *Similar to the first part.*

10. *Let A and B be two formulas having the truth tables given below. How many nonequivalent formulas C involving the atomic formulas p, q, r are there such that $\{A, B\} \Rightarrow C$?*

p	q	r	A
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	B
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

11. *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.*

12. *Assume that $F \leq T$. Let ϕ and ψ be two truth functions on the variables $p_1, \ldots, p_9$. Suppose that for each assignment f, we have $\phi(f) \leq \psi(f)$. Does this imply that $\phi \to \psi$ is a tautology?*

13. *Consider the set S of all nonequivalent formulas written using two atomic variables p and q. For $A, B \in S$, define $A \leq B$ if $A \Rightarrow B$. Prove that this is a partial order on S. Draw its Hasse diagram.*

7.5 Predicate logic (PL)

How do we symbolize the argument 'x runs faster than y, y runs faster than z, hence x runs faster than z'? It is clear that, it is not $\{p, q\} \Rightarrow r$, as it is an invalid argument, whereas the given argument is valid. Notice that we are making this statement on a set, where the elements are comparable as to who runs faster than whom. In other words, we require something called a predicate $faster(x, y)$ which takes truth values T or F depending on the inputs as elements from such a set.

Definition 7.5.1. A **k-place predicate** $P(x_1, \ldots, x_k)$ is a sentence involving the variables $x_1, \ldots, x_k$ to which a truth value can be assigned under each assignment of values to $x_1, \ldots, x_k$ from a nonempty set, called a **universe of discourses** (*UD*).

Example 7.5.2.

1. Let $P(x)$ mean '$x > 0$'. Then $P(x)$ is a 1-place predicate. On the *UD*: $[-1, 1]$, *i.e.*, when an element $a \in [-1, 1]$ is selected corresponding to x, the resulting statement $P(a)$ is either T or F.
2. Let $P(x, y)$ mean '$x^2 + y^2 = 1$'. Then $P(x, y)$ is a 2-place predicate. On the *UD*: $\mathbb{R}$, when two elements $a, b \in \mathbb{R}$ are selected corresponding to x, y, the resulting statement $P(a, b)$ is either T or F.

3. Let $P(x, y, z)$ mean 'x and y are children of z'. Then $P(x, y)$ is a 3-place predicate. On the UD: the set of all human beings, when three human beings a, b, c are selected corresponding to x, y, z, the resulting statement $P(a, b, c)$ is either T or F.

Definition 7.5.3. The **well formed formulas**, called **formulas** for short, of Predicate logic (**PL**) are generated by using the following rules recursively:

1. Any predicate is a formula, called an **atomic formula**.
2. If A, B are formulas, then $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ and $(A \leftrightarrow B)$ are formulas.
3. If A is a formula and x is a variable, then $(\forall x\, A)$ and $(\exists x\, A)$ are formulas.

The symbols $\forall$ and $\exists$ are called **quantifiers**, where $\forall$ is the *universal quantifier* and $\exists$ is the *existential quantifier*. Read $\forall$ as 'for each' and $\exists$ as 'there exists'.

For example, $(\neg(\exists x\, P(x, y, z)))$, $(\forall y\, (\neg(\exists x\, P(x, y, z))))$, $\big(\forall z\, \big(\neg((\exists z\, R(z)) \to R(z))\big)\big)$ are formulas.

Remark 7.5.4. We use the same term *formula* to mean a formula in SL, and one in PL. Notice that PL is an extension of SL; so there should not be any confusion in the use of this term.

Definition 7.5.5. Let P be a formula.

1. In $(\forall x\, P)$ or $(\exists x\, P)$ the formula P is called the **scope** of the quantifier (extent to which that quantification applies).
2. (a) If no quantifier occurs in P, then any occurrence of x in $(\forall x\, P)$ is said to be **bound by** the quantifier $\forall$, and any occurrence of x in $(\exists x\, P)$ is said to be *bound by* the quantifier $\exists$.

   (b) If some quantifiers occur in P, then any occurrence of x in $(\forall x\, P)$ which is not already bound by any quantifier occurring in P, is said to be *bound by* this occurrence of $\forall$. A similar statement holds for the quantifier $\exists$.
3. An occurrence of a variable in a formula is called a **free occurrence** if that occurrence of the variable is not bound by any quantifier. A variable in a formula is called a **free variable** if it has at least one free occurrence in the formula.

Example 7.5.6. Let $P(x, y, z)$ and $R(z)$ be predicates.

1. In $(\exists x\, P(x, y, z))$, the occurrence of y and z are free and both the occurrences of x are bound.
2. In $(\forall y\, (\exists x\, P(x, y, z)))$, all occurrences of x and y are bound and the occurrence of z is free.
3. In $\big(\forall z\big((\exists z R(z)) \to R(z)\big)\big)$, the middle two z's are bound by $\exists$ and the first and the last occurrences of z are bound by $\forall$.[1]

Convention: Once the formation of formulas, scope, bound and free occurrences of variables are understood, we will put forth the precedence rules so that formulas can be written in an abbreviated form. The precedence rules are the following:

1. Outer parentheses are ignored.
2. $\neg$, $\forall$ and $\exists$ have the highest precedence.
3. $\wedge$ and $\vee$ have the next precedence.
4. $\to$ and $\leftrightarrow$ have the least precedence.

[1] Normally, we do not repeat the variable symbols used in the quantifiers. We will see that this formula is equivalent to $\big(\forall z\big((\exists y R(y)) \to R(z)\big)\big)$.

For example, using the precedence rules, the formulas

$$(\neg(\exists x\, P(x,y,z))),\ (\forall y\, (\neg(\exists x\, P(x,y,z)))),\ \big(\forall z\big(\neg((\exists z R(z)) \to R(z))\big)\big),\ \big(\forall z\big((\exists y R(y)) \to R(z)\big)\big)$$

are respectively abbreviated to

$$\neg\exists x\, P(x,y,z),\ \forall y\,\neg\exists x\, P(x,y,z),\ \forall z\neg(\exists z R(z) \to R(z)),\ \forall z(\exists y R(y) \to R(z)).$$

We will use the abbreviated formulas with the understanding that in case an ambiguity arises, we would resort back to the original form.

Definition 7.5.7. 1. Let A be a formula. An **interpretation** for A means fixing a nonempty set UD (called the **universe of discourse**), assigning values to the free variables in A, and giving meanings of the predicates in A. Schematically,

$$\text{An interpretation for } A: \begin{cases} \text{fix } UD\text{, assumed to be nonempty,} \\ \text{assign values to the free variables ocurring in } A, \\ \text{give meanings to the predicates occurring in } A. \end{cases}$$

If x is a variable, its value must be an element of UD; and if $P(x_1, \ldots, x_n)$ has n arguments, then its meaning must be an n-ary relation on UD.

2. Let I be an interpretation for a formula $\forall x P$. Then we say '$\forall x P$ is T under I' if for each $a \in UD$, the value of $P|_{x=a}$ is T. Here, $P|_{x=a}$ means the expression obtained from P by replacing each free occurrence of x with a.

   Similarly, we say '$\exists x P$ is T under I' if for some $a \in UD$, the value of $P|_{x=a}$ is T.

3. If P is a formula, then it will have a truth value T or F under each interpretation. (So you can imagine a formula as a huge truth table.)

4. At times, the meaning of a formula under an interpretation, is also called an interpretation.

Remark 7.5.8. Formally, an interpretation I gives meaning to a predicate $P(x_1, \ldots, x_n)$ by assigning it to an n-ary relation, say, P' on the UD. So, $P|_{x_1=a_1,\ldots,x_n=a_n}$ means $(a_1, \ldots, a_n) \in P'$. For ease in notation, we continue with the informal assertion "$P|_{x=a}$ means the expression obtained from P by replacing each free occurrence of x with a", which is applied recursively.

Example 7.5.9. Consider the formula $\forall x\, P(x,y)$.

1. Take $\mathbb{N}$ as UD. Let $P(x,y)$ mean '$x > y$'. Let us assign 1 to the free variable y. Then the formula is interpreted as 'each natural number is greater than 1', which has truth value F.

2. Take $\mathbb{N}$ as UD. Let $P(x,y)$ mean '$x + y$ is an integer', and assign y to 2. Then the formula is interpreted as 'when we add 2 to each natural number we get an integer'; it has truth value T.

Example 7.5.10. Let UD be the set of all human beings. Consider the 2-place predicate $R(x,y)$: 'x runs faster than y'. Then

1. $\forall x\, \forall y\, R(x,y)$ means 'each human being runs faster than every human being'.

2. $\forall x\, \exists y\, R(x,y)$ means 'for each human being there is a human being who runs slower'.

3. $\exists x\, \exists y\, R(x,y)$ means 'there is a human being who runs faster than some human being'.

4. $\exists x\, \forall y\, R(x,y)$ means 'there is a human being who runs faster than every human being '.

Remark 7.5.11. [**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 7.5.12.

1. Translate: Each person in this class room is either a BTech student or an MSc student.

   Ans: Does the statement guarantee that there is a person in the room? No. All it says, 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 formula is $\forall x \left(P(x) \to B(x) \vee M(x)\right)$.

2. Translate: There is a student in this class room who speaks Hindi or English.

   Ans: 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 formula is $\exists x \left(S(x) \wedge (H(x) \vee E(x))\right)$.

   Note that $\exists x \left(S(x) \to H(x) \vee E(x)\right)$ is not the correct translation. Why?[1]

Notice that if a formula in PL has no free variables, then its translation into English will result in a statement. Similarly, when English statements are translated into PL-formulas, they will result in formulas having no free variables.

Example 7.5.13. Using the vocabulary $Q(x)$: x is a rational number, $R(x)$: x is a real number, and $L(x)$: x is less than 2, the following formulas are translated into English sentences, as shown:

1. $\forall x\big(Q(x) \to R(x)\big)$: Every rational number is a real number.
2. $\exists x\big(\neg Q(x) \wedge R(x)\big)$: There is a real number which is not rational.
3. $\forall x\big(Q(x) \wedge L(x) \to R(x) \wedge L(x)\big)$: Every rational number less than 2 is a real number less than 2.
4. $\forall x\big(Q(x) \wedge L(x)\big) \to \forall x\big(R(x) \wedge L(x)\big)$: If each rational number is less than 2, then each real number is less than 2.

EXERCISE **7.5.14.** *Translate the following sentences into PL:*

1. *If there is a man on Mars, he is a genius.*
2. *For each student in IITG there is a student in IITG with more CPI.*
3. *Every natural number is either the square of a natural number or its square root is irrational.*
4. *For every real number x there is a real number y such that $x + y = 0$.*

   In the rest of the exercises, fill in the blank with a PL-formula so that the definition will be complete.

5. *A subset $S \subseteq \mathbb{R}^n$ is called compact, if —. Use the predicates $O(x, A)$: x is an open cover of A; $S(x, y)$: x is a subset of y; and $C(x, A)$: x is a finite cover of A.*
6. *A function $f : \mathbb{R} \to \mathbb{R}$ is called continuous at a point a, if —. Use UD $= \mathbb{R}$ and the predicates $P(x)$: x is positive; and $Q(x, y, z)$: $|x - y| < z$.*
7. *A function $f : \mathbb{R} \to \mathbb{R}$ is called continuous if —. Use UD $= \mathbb{R}$ and the predicates $P(x)$: x is positive; and $Q(x, y, z)$: $|x - y| < z$.*
8. *A function $f : \mathbb{R} \to \mathbb{R}$ is called uniformly continuous if —. Use UD $= \mathbb{R}$ and the predicates $P(x)$: x is positive; and $Q(x, y, z)$: $|x - y| < z$.*
9. *A function $f : S \to T$ is called a bijection if —. Use predicates $B(x, A)$: x is an element of A; and $E(x, y)$: x is equal to y.*

[1]Remember, $\exists x\,(P(x) \to Q(x))$ never asserts $P(x)$. But $\exists x\,(P(x) \wedge Q(x))$ asserts both $P(x)$ and $Q(x)$.

7.6 Equivalences and Validity in PL

In parallel with SL, we isolate those formulas which receive the truth value T under every interpretation; and use this notion to define equivalence of two given formulas.

Definition 7.6.1. A formula is called **valid** if every interpretation evaluates it to T. A formula, which receives the truth value F under each interpretation is called **unsatisfiable**. Two formulas A and B are called **equivalent**, written $A \equiv B$, if $A \leftrightarrow B$ is valid.

Notice that formulas A and B are equivalent if and only if under each interpretation, A and B have the same truth value.

In first line of the next example what is unary relation? One assigns x to a or a to x at different places in different paragraphs

Example 7.6.2. Let $R(x)$ be a predicate.

1. $R(x) \to R(x)$ is valid.

   Reason: To see this, suppose I is an interpretation that fixes $R(x)$ to a unary relation, say, R' on some UD; and that assigns x to some element, say, $a \in UD$. Notice that $R' \subseteq UD$. Now, I assigns T to $R(x)$ if and only if $a \in R'$. The formula $R(x) \to R(x)$ is interpreted as the sentence: if $a \in R'$, then $a \in R'$. This sentence is true in any UD. Since I is an arbitrary interpretation, we conclude that $R(x) \to R(x)$ is valid.

2. $R(x) \wedge \neg R(x)$ is unsatisfiable.

   Reason: Consider an interpretation I with any UD. Suppose I assigns x to $b \in UD$; and interprets $R(x)$ as the unary relation $R' \subseteq UD$. The formula $R(x) \wedge \neg R(x)$ is interpreted as the statement: $b \in R'$ and $b \notin R'$. This is false. Since I is an arbitrary interpretation, $R(x) \wedge \neg R(x)$ is unsatisfiable.

3. Are the formulas $\forall x\, R(x)$ and $\forall z\, R(z)$ equivalent?

   Reason: Let I be an interpretation. Under I, suppose that the formula $\forall x\, R(x)$ is T. It means that for each $a \in UD$, the value of $P(a)$ is T. Then $\forall z\, R(z)$ is T under I. The argument is similar if $\forall x\, R(x)$ is F under I. Since I is an arbitrary interpretation, the two formulas are equivalent.

   Similarly, $\exists x\, R(x) \equiv \exists y\, R(y)$.

4. Consider the formulas $\forall z\, \big(\exists z\, R(z) \to R(z)\big)$ and $\forall y\, \big(\exists z\, R(z) \to R(y)\big)$. Let I be an interpretation. Assume that $\forall\, z\big(\exists z\, R(z) \to R(z)\big)$ is T under I. This means $\big(\exists z\, R(z) \to R(z)\big)|_{z=a}$ is T for each $a \in UD$. This means $\big(\exists z\, R(z) \to R(a)\big)$ is T for each $a \in UD$. But this also means that $\forall y\, \big(\exists z\, R(z) \to R(y)\big)$ is T under I.

   Similarly, if $\forall z\, \big(\exists z\, R(z) \to R(z)\big)$ is F under I, then $\forall y\, \big(\exists z\, R(z) \to R(y)\big)$ is F under I. As I is arbitrary, $\forall z\, \big(\exists z\, R(z) \to R(z)\big) \equiv \forall y\, \big(\exists z\, R(z) \to R(y)\big)$.

Proposition 7.6.3. *Let P and Q be formulas. The following are true:*

1. *All tautologies of SL are valid in PL.*
2. *If P is valid and x is any variable, then both $\forall x\, P$ and $\exists x\, P$ are valid.*
3. $\neg(\forall x\, P) \equiv \exists x\, \neg P$, $\neg(\exists x\, P) \equiv \forall x\, \neg P$.
4. $\forall x\, \forall y\, P \equiv \forall y\, \forall x\, P$, $\exists x\, \exists y\, P \equiv \exists y\, \exists x\, P$.
5. $\forall x\, (P \wedge Q) \equiv \forall x\, P \wedge \forall x\, Q$, $\exists x\, (P \vee Q) \equiv \exists x\, P \vee \exists x\, Q$.

Proof. (1) In a tautology of SL, replace all atomic formulas by predicates of PL (chosen respectively). For instance, in the tautology $p \to (q \to p)$, replacing p by $P(x, y)$ and q by $R(x, y, z)$, we get the formula $P(x, y) \to (R(x, y, z) \to P(x, y))$. The assertion says that the resulting formula of PL is valid. Observe that the connectives are interpreted the same way in PL as in SL. Therefore, the assertion holds.

(2) Let P be a valid formula and let x be any variable. Let I be an interpretation. Let $a \in UD$. Since P is valid, $P|_{x=a}$ is T. This holds for each element a of UD. So, both the statements

"There exists $a \in UD$, $P|_{x=a}$ is T." and "For each $a \in UD$, $P|_{x=a}$ is T."

hold. (Recall that $UD \neq \varnothing$.) Therefore, under I, both $\exists x\, P$ and $\forall x\, P$ are T. Since I is an arbitrary interpretation, both $\exists x\, P$ and $\forall x\, P$ are valid.

(3) Assume that under some interpretation I, the formula $\neg(\forall x\, P)$ is T. So, $\forall x\, P$ is F under I. That is, for some $a \in UD$, $P|_{x=a}$ is F under I. Thus, $\neg(P|_{x=a})$ is T under I. Hence, $\exists x \neg P$ is T under I.

Conversely, suppose that $\exists x\, \neg P$ is T under an interpretation I. Then there is an $a \in UD$ such that $(\neg P)|_{x=a}$ is T under I. This means, $P|_{x=a}$ is F under I. Hence, $\forall x P$ is F under I. That is, $\neg(\forall x P)$ is T under I. This proves the first assertion.

For the second assertion, we use the first assertion as follows:

$$\neg(\exists x\, P) \equiv \neg(\exists x\, \neg\neg P) \equiv \neg\neg(\forall x\, \neg P) \equiv \forall x\, \neg P.$$

(4) Consider the formulas $\exists x\, \exists y\, P$ and $\exists y\, \exists x P$. Let I be an interpretation. Suppose $\exists x\, \exists y\, P$ is T under I. Then for some $a \in UD$, we have $(\exists y\, P)|_{x=a}$ is T under I. Then again, for some $b \in UD$, we have $P|_{x=a,y=b}$ is T under I. Since $P|_{x=a,y=b} = P|_{y=b,x=a}$, we see that $(\exists x\, P)|_{y=b}$ is T under I. This means $\exists y\, \exists x\, P$ is T under I. A similar argument shows that if $\exists y\, \exists x\, P$ is T under I, then $\exists x\, \exists y\, P$ is also T under I. This proves the second assertion.

For the first assertion, we use the second as follows:

$$\forall x\, \forall y\, P \equiv \neg\neg(\forall x\, \forall y\, P) \equiv \neg(\exists x\, \exists y\, \neg P) \equiv \neg(\exists y\, \exists x\, \neg P) \equiv \forall y\, \forall x \neg\neg P \equiv \forall y\, \forall x\, P.$$

(5) Let I be an interpretation under which $\forall x\, (P \wedge Q)$ is T. Then for each element $a \in UD$, $(P \wedge Q)|_{x=a}$ is T. However, $(P \wedge Q)|_{x=a} = \big(P|_{x=a}\big) \wedge \big(Q|_{x=a}\big)$. Thus, both $\big(P|_{x=a}\big)$ and $\big(Q|_{x=a}\big)$ are T under I. Now, for each element $a \in UD$, $\big(P|_{x=a}\big)$ is T under I implies that $\forall x\, P$ is T under I. Similarly, for each element $a \in UD$, $\big(Q|_{x=a}\big)$ is T under I implies that $\forall x\, Q$ is T under I. Therefore, $\forall x\, P \wedge \forall x\, Q$ is T under I.

Conversely, suppose $\forall x\, P \wedge \forall x\, Q$ is T under I. Then both $\forall x\, P$ and $\forall x\, Q$ are T under I. Then for each element $a \in UD$, $P|_{x=a}$ is T, and for each element $b \in UD$, $Q|_{x=b}$ is T. Let $c \in UD$. It follows that under I, $P|_{x=c}$ is T and $Q|_{x=c}$ is T. That is, for each $c \in UD$, $(P \wedge Q)|_{x=c}$ is T under I. Hence $\forall x\, (P \wedge Q)$ is T under I.

We conclude that under I, the formula $\forall x\, (P \wedge Q) \leftrightarrow (\forall x\, P) \wedge (\forall x\, Q)$ is T. Since I is an arbitrary interpretation, this biconditional is valid, so that $\forall x\, (P \wedge Q) \equiv \forall x\, P \wedge \forall x\, Q$.

The second assertion is obtained from the first as in the following:

$$\begin{aligned} \exists x\, (P \vee Q) &\equiv \neg\neg\exists x\, (P \vee Q) \equiv \neg\forall x\, \neg(p \vee Q) \equiv \neg\forall x\, (\neg P \wedge \neg Q) \equiv \neg\big((\forall x\, \neg P) \wedge (\forall x\, \neg Q)\big) \\ &\equiv \neg\big(\neg(\exists x\, P) \wedge \neg(\exists x\, Q)\big) \equiv \neg\neg\big((\exists x\, P) \vee (\exists x\, Q)\big) \equiv \exists x\, P \vee \exists x\, Q. \end{aligned}$$ ■

The first part in Proposition 7.6.3 says that all the rules of the logic of Statements also hold in Predicate logic. For instance, the $p \vee \neg p$ being a tautology, it follows that $\forall x\, P \vee \neg\forall x, P$ is valid. Again, $\neg\forall x\, P \equiv \exists x\, \neg P$. Hence $\forall x\, P \vee \exists x\, \neg P$ is valid. You may similarly obtain many more valid formulas in PL, and formulate many equivalences accordingly.

In the following example, we show that different quantifiers do not commute, $\forall$ does not distribute over $\vee$, and $\exists$ does not distribute over $\wedge$.

Example 7.6.4.

1. $\exists x\, \forall y\, P \not\equiv \forall y\, \exists x\, P$.
   Reason: Consider P as the predicate $Q(x, y)$ in the $UD = \mathbb{N}$. Interpret $Q(x, y)$ as '$x > y$'. Then $\exists x\, \forall y\, P$ is the formula $\exists x\, \forall y Q(x, y)$. It means 'There is a natural number larger than all natural numbers'. Clearly, this is false. The formula $\forall y\, \exists x\, P$ is $\forall y\, \exists x\, Q(x, y)$. It means 'for each natural number there is a larger natural number', which is true.

2. $\forall x\, (P \vee Q) \not\equiv \forall x\, P \vee \forall x\, Q$.
   Reason: Consider P as the predicate $O(x)$ and Q as the predicate $E(x)$ in the $UD = \mathbb{N}$. Interpret $O(x)$ as 'x is odd', and $E(x)$ as 'x is even'. Then $\forall x\, (P \vee Q)$ is the formula $\forall x\, (O(x) \vee E(x))$. It means each natural number is either odd or even. This is true. Now, $\forall x\, P \vee \forall x\, Q$ is the formula $\forall x\, O(x) \vee \forall x\, E(x)$. It means Either all natural numbers are odd, or all natural numbers are even. Clearly, this is false.

3. $\exists x\, (P \wedge Q) \not\equiv \exists x\, P \wedge \exists x\, Q$.
   Reason: Consider the predicates and their interpretations as in (2). The formula $\exists x\, (P \wedge Q)$ is interpreted as 'there is a natural number which is both odd and even'. This is false. Where as the formula $\exists x\, P \wedge \exists x\, Q$ is interpreted as the true sentence 'there exists a natural number which is odd, and also there exists a natural number which is even'.

Example 7.6.5. Is $\forall x\, \big(R(x) \to \exists y\, R(y) \wedge P(x, y)\big) \equiv \forall x\, \exists y\, \big(R(x) \to R(y) \wedge P(x, y)\big)$?

Ans: First, let us check the validity of $X \to Y$, where

$$X = \forall x\, \big(R(x) \to \exists y\, R(y) \wedge P(x, y)\big), \quad Y = \forall x\, \exists y\, \big(R(x) \to R(y) \wedge P(x, y)\big).$$

Suppose that $X \to Y$ is invalid. So there is an interpretation I under which X is T and Y is F. As Y is F, we see that for some $a \in UD$,

$\exists y \big(R(a) \to R(y) \wedge P(a, y)\big)$ is F.

That is, for each $y \in UD$, $R(a) \to \big(R(y) \wedge P(a, y)\big)$ is F.

That is, $R(a)$ is T and for each y, $R(y) \wedge P(a, y)$ is F.

That is, $R(a)$ is T and $\exists y\, (R(y) \wedge P(a, y))$ is F.

That is, $R(a) \to \exists y\, (R(y) \wedge P(a, y))$ is F.

This leads to a contradiction since $X = \forall x\, \big(R(x) \to \exists y\, R(y) \wedge P(x, y)\big)$ is T.

Similarly, one shows that $Y \to X$ is valid.

Alternate. Write $A = R(x) \to \exists y\, R(y) \wedge P(x, y)$ and $B = \exists y\, \big(R(x) \to R(y) \wedge P(x, y)\big)$. Consider an element $a \in UD$. If $R(a)$ is F, Then both X and Y are T. So, suppose $R(a)$ is T. Notice that $R(a) \to \exists y\, (R(y) \wedge P(a, y))$ and $\exists y\, \big(R(a) \to (R(y) \wedge P(a, y)\big)$ have the same truth value. Thus, $A \equiv B$. It follows that $\forall x A \equiv \forall x B$, that is, $X \equiv Y$.

Exercise **7.6.6.**

1. *Show that* $\forall x\, \big(R(x) \to \exists y\, (R(y) \wedge P(x, y))\big)$ *is not valid.*

2. *Show that* $\forall x\, \big(P(x) \to Q(x)\big) \to \exists x\, \big(\neg P(x) \to \neg Q(x)\big)$ *is not valid.*

3. *Let* P *and* Q *be formulas. Determine whether* $\forall x(P \to Q) \equiv \forall x P \to \forall x Q$.

7.7 Inferences in PL

As in SL, we translate arguments to inferences in PL. The validity of inferences are defined in an analogous manner.

Definition 7.7.1. An **inference** is an expression of the form $\{P_1, \ldots, P_n\} \stackrel{?}{\Rightarrow} C$, where the formulas $P_1, \ldots, P_n$ are called **premises** or **hypotheses**, and the formula C is called the **conclusion** of the inference. We say that the inference is **valid**, and write $\{P_1, \ldots, P_n\} \Rightarrow C$, if $(P_1 \wedge \cdots \wedge P_n) \to C$ is valid. In such a case, we also say that C is a **logical conclusion** of the premises $P_1, \ldots, P_n$.

We abbreviate $\{P_1, \ldots, P_n\} \stackrel{?}{\Rightarrow} C$ to $P_1, \ldots, P_n \stackrel{?}{\Rightarrow} C$ and $\{P_1, \ldots, P_n\} \Rightarrow C$ to $P_1, \ldots, P_n \Rightarrow C$; and read the symbol $\Rightarrow$ as 'implies'.

It follows that $X \equiv Y$ if and only if both $X \Rightarrow Y$ and $Y \Rightarrow X$ hold.

Since PL is an extension of SL, we will use all the laws and rules including the Rules of Contradiction and Deduction. Moreover, to prove that $P_1, \ldots, P_n \Rightarrow C$, all that we have to do is assume that all premises $P_1, \ldots, P_n$ are T under an arbitrary interpretation I and show that under the same I, C must be T. Alternatively, using the rule of Contradiction, $P_1, \ldots, P_n \Rightarrow C$ can be proved by assuming that an interpretation I makes the conclusion C false, and then showing that I makes at least one of the premises $P_1, \ldots, P_n$ false.

We have seen in Example 7.6.4 that some of the equivalences do not hold. In fact, we have shown that one part of the equivalences fail. Namely,

$$\forall y\, \exists x\, P \not\Rightarrow \exists x\, \forall y\, P, \quad \forall x\, (P \vee Q) \not\Rightarrow \forall x\, P \vee \forall x\, Q, \quad \exists x\, P \wedge \exists x\, Q \not\Rightarrow \exists x\, (P \wedge Q).$$

We show that their converse implications hold.

Proposition 7.7.2. *Let P and Q be formulas. Then the following assertions hold:*

1. $\exists x\, \forall y\, P \Rightarrow \forall y\, \exists x\, P$.
2. $\forall x\, P \vee \forall x\, Q \Rightarrow \forall x\, (P \vee Q)$.
3. $\exists x\, (P \wedge Q) \Rightarrow \exists x\, P \wedge \exists x\, Q$.

Proof. (1) Let I be an interpretation under which $\exists x\, \forall y\, P$ is T. and $\forall y\, \exists x\, P$ is F. Then there is an element $a \in UD$ such that $(\forall y\, P)|_{x=a}$ is T. Then for each $b \in UD$, $P|_{x=a,y=b}$ is T. It implies that for each $b \in UD$, $(\exists y\, P)|_{x=a}$ is T. Hence $\forall y\, \exists x\, P$ is T. Since I is an arbitrary interpretation, we conclude that $\exists x\, \forall y\, P \Rightarrow \forall y\, \exists x\, P$.

(2) Let I be an interpretation under which $\forall x\, P \vee \forall x\, Q$ is T. If $\forall x\, P$ is T, then for each $a \in UD$, $P|_{x=a}$ is T. However, $P|_{x=a}$ is T implies that $P|_{x=a} \vee Q|_{x=a}$ is T; and $P|_{x=a} \vee Q|_{x=a} = (P \vee Q)|_{x=a}$. Thus, for each $a \in UD$, $(P \vee Q)|_{x=a}$ is T. So, under I ,$\forall x\, (P \vee Q)$ is T. Similarly, it follows that if $\forall x\, Q$ is T under I, then $\forall x\, (P \vee Q)$ is also T. In any case, $\forall x\, (P \vee Q)$ is T under I. Since I is an arbitrary interpretation, $\forall x\, P \vee \forall x\, Q \Rightarrow \forall x\, (P \vee Q)$.

(3) We know $\neg(\exists x\, P \wedge \exists x\, Q) \equiv \forall x\, \neg P \vee \neg \forall x\, \neg Q$. By (2), $\forall x\, \neg P \vee \neg \forall x\, \neg Q \Rightarrow \forall x\, (\neg P \vee \neg Q)$. Now, $\forall x\, (\neg P \vee \neg Q) \equiv \forall x\, \neg(P \wedge Q) \equiv \neg \exists x\, (P \wedge Q)$. Hence, $\neg(\exists x\, P \wedge \exists x\, Q) \Rightarrow \neg \exists x\, (P \wedge Q)$. This is same as $\exists x\, (P \wedge Q) \Rightarrow \exists x\, P \wedge \exists x\, Q$. ■

Example 7.7.3. Any student who appears in the exam and gets a score below 30, gets F grade. A student x_0 has not written the exam. Therefore x_0 should get F grade. Do you agree?

Ans: 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[1] $\forall x\big(S(x) \wedge E(x) \wedge B(x) \to F(x)\big), S(x_0) \wedge \neg E(x_0) \Rightarrow F(x_0)$.

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, the premises mean 'every positive integer is a natural number' and '$\sqrt{2}$ is a positive real number which is not rational'. Both of them are true. Whereas the conclusion means '$\sqrt{2}$ is a natural number', which is false. So the argument is incorrect.

Example 7.7.4. Translate the following argument into PL and then check whether it is correct:

> All scientists are human beings. Therefore, all children of scientists are children of human beings.

Ans: Let $S(x)$ mean 'x is a scientist', $H(x)$ mean 'x is a human being', and $C(x, y)$ mean 'x is a child of y'. Then our hypothesis is $\forall x\,(S(x) \to H(x))$. A few possible translation of the conclusion are the following:

1. $\forall x\,(\exists y\,(S(y) \wedge C(x, y)) \to \exists z\,(H(z) \wedge C(x, z)))$. It means 'for each x, if x has a scientist father then x has a human father'. This is a correct translation.
2. $\forall x\,(\forall y\,(S(y) \wedge C(x, y)) \to \forall z\,(H(z) \wedge C(x, z)))$. 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'. This is a wrong translation.
3. $\forall x\,(S(x) \to \forall y\,(C(y, x) \to \exists z\,(H(z) \wedge C(y, z))))$. This means 'for each x, if x is a scientist, then each child of x has a human father'. This is also a correct translation.
4. $\forall x\,\forall y\,(S(x) \wedge C(y, x)) \to \forall x\,\forall y\,(H(x) \wedge C(x, y))$. This means 'if each x is a scientist and each y is a child of x (y can be equal to x), then each x is a human being and each y is a child of x'. This is a wrong translation.

So, let us check whether $\forall x\,(S(x) \to H(x)) \Rightarrow \forall x\,(\exists y\,(S(y) \wedge C(x, y)) \to \exists z\,(H(z) \wedge C(x, z)))$.

Let I be an interpretation under which $\forall x\,(S(x) \to H(x))$ is T. Let b be any element of UD. Suppose that $\exists y\,(S(y) \wedge C(b, y))$ is T under I. Then there is an element $a \in UD$ such that $S(a) \wedge C(b, a)$ is T. Since $\forall x\,(S(x) \to H(x))$ is T, we see that $S(a) \to H(a)$ is T. It follows that $H(a) \wedge C(b, a)$ is T. Hence under I, $\exists z\,(H(z) \wedge C(b, z))$ is T.

Using the Rule of Deduction, we conclude that under I, the formula $\exists y\,(S(y) \wedge C(b, y)) \to \exists z\,(H(z) \wedge C(b, z))$ is T. Since this holds for any arbitrary element $b \in UD$, we conclude that under I, $\forall x\,\big(\exists y\,(S(y) \wedge C(x, y)) \to \exists z\,(H(z) \wedge C(x, z))\big)$ is T. Since I is an arbitrary interpretation, this proves that the conclusion logically follows from the premise.

Example 7.7.5. Let P be a formula and let R be a formula that does not have any occurrence of x. Show that

$$\forall x\,(R \vee P) \equiv R \vee \forall x\,P, \quad \forall x\,(R \to P) \equiv R \to \forall x\,P,$$

$$\exists x\,(R \wedge P) \equiv R \wedge \exists x\,P, \quad \exists x\,(R \to P) \equiv R \to \exists x\,P.$$

$$\forall x\,P \to R \equiv \exists x\,(P \to R), \quad \exists x\,P \to R \equiv \forall x\,(P \to R).$$

Ans: We already know that $\forall x\,R \vee \forall x\,P \Rightarrow \forall x\,(R \vee P)$. Since R does not have any occurrence of x, $R \equiv \forall x\,R$. Hence $R \vee \forall x\,P \Rightarrow \forall x\,(R \vee P)$. For the converse, let I be an interpretation under which $\forall x\,(R \vee P)$ is T. Then for each element $a \in UD$, $(R \vee P)|_{x=a}$ is T. Since R does not have any occurrence of x, $(R \vee P)|_{x=a} = R \vee P|_{x=a}$. So, under I, either R is T or for each $a \in UD$, $P|_{x=a}$ is T.

[1] Actually x_0 here is not a variable; it is a constant. Constants are interpreted as elements of UD just like variables, but their occurrence in a formula is never categorized into bound or free.

That is, under I, $R \vee \forall x\, P$ is T. Since I is an arbitrary interpretation, $\forall x\,(R \vee P) \Rightarrow R \vee \forall x\, P$. We conclude that $\forall x\,(R \vee P) \equiv R \vee \forall x\, P$.

Others follow from the above by using the equivalences $A \to B \equiv \neg A \vee B$, $\neg\forall x\, A \equiv \exists x \neg A$, $\neg\exists x\, A \equiv \forall x\, \neg A$, $\neg\neg A \equiv A$, $\neg(A \vee B) \equiv \neg A \wedge \neg B$ and $\neg(A \wedge B) \equiv \neg A \vee \neg B$.

Remark 7.7.6.

1. If S is a given set and P is a formula, sometimes we use $\forall(x \in S)P$ and $\exists(x \in S)P$. These are nothing but $\forall x(E(x) \to P)$ and $\exists x(E(x) \wedge P)$, respectively, where, $E(x)$ means $x \in S$.
2. At times, while dealing with real numbers or very familiar sets, we use certain predicate symbols in an informal way. For example, we may write $x \in S$ instead of using something like $E(x, S)$; or we may use $x > 0$ instead of using something like $P(x)$.

   For example, in the set $\mathbb{R}$, the meaning of

   $$\exists(\epsilon > 0)\big(\forall(\delta > 0)(0 < |x - a| < \delta \to |f(x) - \ell| < \epsilon)\big)$$

   is: “the set $\{|f(x) - \ell| : x \in \mathbb{R},\ 0 < |x - a|\}$ has an upper bound ϵ”.

Logic is used primarily to define and argue about mathematical systems. The predicate logic developed so far is not enough to do that, in general. We need to extend it further by including the equality predicate, constants, and function symbols. The equality predicate is a predicate like any other but it is to be interpreted as the equality or identity relation on any *UD*. For instance, Peano’s axioms formulated to define the natural number system uses the constant symbol 1, the function symbol S and the equality predicate $=$. Such an extension of PL is called the *first order logic*, which we do not deal with here. However, the logical structure to tackle mathematical theories is provided by PL.

In some of the exercises that follow you may use constants and the equality predicate freely if required for translation into the formal language of PL. Revisit Example 7.7.3, where we have used a constant symbol x_0.

Exercise **7.7.7.**

1. *Let $f : \mathbb{R} \to \mathbb{R}$ be a function and let $a, \ell \in \mathbb{R}$. Write a formal definition of $\lim\limits_{x \to a} f(x) \neq \ell$.*
2. *In the following, fill in the blank with a PL-formula so that the definition will be complete:*
   - (a) *A subset $S \subseteq \mathbb{R}^n$ is called connected if —.*
   - (b) *A set S is called a group if —.*
   - (c) *A subset $S \subseteq \mathbb{R}^n$ is called a subspace if —.*
   - (d) *A function $f : \mathbb{R}^n \to \mathbb{R}^k$ is called a linear transformation if —.*
   - (e) *A function $f : (S, \circ) \to (T, +)$ is called a group isomorphism if —.*
   - (f) *A function $f : \mathbb{V} \to \mathbb{W}$ is called a vector space isomorphism if —.*
3. *Translate and check for validity of the following arguments.*
   - (a) *The decimal representation of a rational number either terminates or recurs, whereas that of an irrational number neither terminates nor recurs. The square root of a natural number either has a decimal representation which terminates or has a non-terminating decimal representation and also a non-recurring decimal representation. The square root of all natural numbers which are squares have decimal representations that terminate. 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.*

(c) *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.*

Use predicates $S(x)$*:* x *is a student ,* $B(x)$*:* x *write the exam using blue ink,* $Bl(x)$*:* x *write the exam using black ink,* $R(x)$*:* x *writes roll number,* $I(x)$*:* x *has ID card,* $F(x)$*:* x *gets F grade.*

(d) *Check whether the following argument is correct:*

Every mango is either an apple or an orange. Every pineapple is a mango. No apples are pineapples. Every object is either an apple or a pineapple or a mango or an orange. Therefore, if an apple is a pineapple, then it is an orange.

Use predicates $M(x)$*:* x *is a mango,* $A(x)$*:* x *is an apple,* $P(x)$*:* x *is a pineapple,* $O(x)$*:* x *is an orange.*

Chapter 8

Partially Ordered Sets, Lattices and Boolean Algebra

8.1 Partial Orders

A relation can also be used to define an order on a set. For example, the words in a dictionary are arranged according to a lexicographic ordering. So, ordering the objects according to a particular rule brings a certain structure to the area of study. In the set of natural numbers, the relation "less than or equal to" enables us to conclude whether a number precedes or succeeds another number. Similarly, the relation $\subseteq$ also brings an ordering to the set of sets. In this section, we study the concept of "order".

The reader is already aware of what reflexive, symmetric and transitive relations are. We now introduce a fourth relation called an "antisymmetric" relation.

Definition 8.1.1. The relation f defined on a nonempty set X is called an anti-symmetric relation if and only if, $\forall\, x, y \in X$, the property $(x, y) \in f$ and $(y, x) \in f$ implies that $x = y$.

It is possible to interpret an anti-symmetric relation using the arrow diagrams of relations. In this context, a relation is called anti-symmetric if, whenever there is an arrow going from one element to an element different from it, there does not exist an arrow going back from the second element to the first.

Example 8.1.2. 1. Example 1.3.6.1 is an anti-symmetric relation.

2. Let $R_1 = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \text{ divides } y\}$ and $R_2 = \{(x, y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \mid x \text{ divides } y\}$.
   (a) Show that R_1 is an anti-symmetric relation on the set of positive integers.
   (b) Show that R_2 is not an anti-symmetric relation on the set of integers by giving a counter example.

There are two relations which play a prominent role in mathematics. One of them is the equivalence relation, which we have already seen is a relation which is reflexive, symmetric and transitive. We now introduce the other relation called a partial order.

Definition 8.1.3. A relation f on a nonempty set X is called a **partial order** if f is reflexive, transitive and anti-symmetric. Here (X, f) is a *partially ordered set* and is colloquially referred to as a *poset*.

The relation *less than or equal to* on the set of real numbers and the relation *subset* on the set of sets are two fundamental partial orders. These can be thought of as models for the general partial order. It is common practice to use the symbol $\preceq$ to denote a partial order. Further, if $(X, \preceq)$ is a poset and $x \preceq y$, then we read this as x is less than or equal to y.

Definition 8.1.4. Let $(X, \preceq)$ be a poset. It there exist elements x and y in X, such that either $(x, y) \in \preceq$ or $(y, x) \in \preceq$ holds, then x and y are said to be **comparable**. In neither (x, y) nor (y, x) belongs to $\preceq$, then x and y are said to be **incomparable**.

Example 8.1.5.

1. Let $X = \{1, 2, 3, 4, 5\}$.
   (a) The identity relation **Id** on X is reflexive, transitive and anti-symmetric and is therefore a partial order. However, no two elements of X are comparable.
   (b) The relation $\mathbf{Id} \cup \{(1, 2)\}$ is also a partial order on X. Here 1 and 2 are comparable.
   (c) The relation $\preceq = \mathbf{Id} \cup \{(1, 2), (2, 1)\}$ is both reflexive and transitive, but not anti-symmetric. Observe that $(1, 2)$, $(2, 1) \in \preceq$ and $1 \neq 2$.
   (d) The relation $\mathbf{Id} \cup \{(1, 2), (3, 4)\}$ is a partial order on X. Here, 1 and 2 are comparable and so are 3 and 4.
2. Let $X = \mathbb{N}$. The relation $\preceq = \{(a, b) : a \text{ divides } b\}$ is a partial order on X.
3. Let X be a nonempty collection of sets. Here, $\preceq = \{(A, B) : A, B \in X, A \subseteq B\}$ is a partial order on X.
4. On $\mathbb{R}$ the set $\preceq = \{(a, b) : a \leq b\}$ is a partial order. It is called the *usual partial order* on $\mathbb{R}$.

PRACTICE **8.1.6.** *Construct a partial order on the set* $\{1, 2, 3, 4, 5\}$

1. *of maximum cardinality and*
2. *of minimum cardinality.*

In Example 8.1.5(4) any two elements are comparable, whereas in Example 8.1.5(1a), no two elements are comparable.

Definition 8.1.7. Let $(X, \preceq)$ be a poset.

1. If any two elements in the poset $(X, \preceq)$ are comparable, then $\preceq$ is called a **linear order** and $(X, \preceq)$ is called a **linearly ordered set**. Often a linear order is also referred to as a total order or a complete order.
2. A subset, C of X, is called a **chain** if and only if $\preceq$ induces a linear order on C. If C is a finite set, then the **length** of C is equal to the number of elements if C. If C is not a finite set, then the length of C is said to be infinite.
3. A subset, A of X, is called an **antichain** if and only if no two elements of A are comparable. The length of an antichain is defined in precisely the same manner as that of the chain.
4. The maximum of the lengths of the chains of X is called the **height** of X and the maximum of the lengths of the antichains of X is called the **width** of X.

Let X be a nonempty set and let f be a relation on X. Then, recall from Definition 1.6.1 that f is *reflexive* if $(x, x) \in f$ for all $x \in X$; f is transitive if $(x, y) \in f$ and $(y, z) \in f$ imply $(x, z) \in f$ for all $x, y, z \in X$; and f is *anti-symmetric* if $(x, y) \in f$ and $x \neq y$ implies $(y, x) \notin f$, *i.e.*, for all distinct elements x, y of X both (x, y) and (y, x) cannot be in f. Relations which are simultaneously reflexive, transitive and anti-symmetric play an important role in mathematics; and we give a name to such relations.

Definition 8.1.8. Let X be a nonempty set. A relation f on X is called a **partial order** if f is reflexive, transitive and anti-symmetric. Let f be a partial order on X and let $a, b \in X$. Then, a and b are said to be **comparable** (with respect to the partial order f) if either $(a, b) \in f$ or $(b, a) \in f$.

When a partial order satisfies some other desirable properties, they are given different names. We fix some of these in the following definition.

Definition 8.1.9. Let X be a nonempty set.

1. The pair (X, f) is called a **partially ordered set** (in short, **poset**) if f is a partial order on X.
2. A partial order f on X is called a **linear order** if either $(x, y) \in f$ or $(y, x) \in f$ for all $x, y \in X$, *i.e.*, when any two elements of X are comparable. A linear order is also called a **total order**, or a **complete order**.
3. The poset (X, f) is said to be a **linearly ordered set** if f is a linear order on X.
4. A linearly ordered subset of a poset is called a **chain** in the poset. The maximum size of a chain in a poset is called the **height** of a poset.
5. Let (X, f) be a poset and let $A \subseteq X$. A is called an **anti-chain** in the poset if no two elements of A are comparable. The maximum size of an anti-chain in a poset is called the **width** of the poset.

You may imagine the elements of a linearly ordered set as points on a line. The height of a poset is the maximum of the cardinalities of all chains in the poset. The width of a poset is the maximum of the cardinalities of all anti-chains in the poset.

Example 8.1.10.

1. The poset in Example 8.1.5.1a has height 1 (size of the chain $\{1\}$) and width 5 (size of the anti-chain $\{1, 2, 3, 4, 5\}$).
2. The poset in Example 8.1.5.1b has height 2 (respective chain is $\{1, 2\}$) and width 4 (respective anti-chains are $\{2, 3, 4, 5\}$ and $\{1, 3, 4, 5\}$).
3. The poset in Example 8.1.5.1d has height 2 (respective chains are $\{1, 2\}$ and $\{3, 4\}$) and width 3 (a respective anti-chain is $\{1, 3, 5\}$). Find other anti-chains.
4. The usual order (usual $\leq$) in $\mathbb{N}$ is a linear/complete/total order. The same holds for the usual order in $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.
5. If (X, f) is a finite linearly ordered set then the singleton subsets of X are the only anti-chains. In this case, the height of X is the number of elements in X and the width of X is 1.
6. The set $\mathbb{N}$ with the partial order f defined by "$(a, b) \in f$ if a divides b" is not linearly ordered. However, the set $\{1, 2, 4, 8, 16\}$ is a chain. This is just a linearly ordered subset of the poset. There are larger chains, for example, $\{2^k : k = 0, 1, 2, \ldots\}$. The set of all primes is an anti-chain here. The poset $(\mathbb{N}, f)$ has infinite height and infinite width.
7. The poset $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \subseteq)$ is not linearly ordered. However, $\{\varnothing, \{1, 2\}, \{1, 2, 3, 4, 5\}\}$ is a chain in it. Also, $\{\varnothing, \{2\}, \{2, 3\}, \{2, 3, 4\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$ is a chain. The height of this poset is 6. What is its width?

Convention: It is common to use $\leq$ in infix notation for a partial order. That is, if f is a partial order on a nonempty set X we write $x \leq y$ to mean that $(x, y) \in f$. Accordingly, the poset (X, f) is written as $(X, \leq)$. Also, instead of writing '(X, f) is a poset' we will often write 'X is a poset with the partial order f'. Following custom, by $x \geq y$ we mean $y \leq x$; by $x < y$ we mean that $x \leq y$ and $x \neq y$; by $x > y$ we mean $y < x$. Also, we read $x \leq y$ as x is less than or equal to y; $x < y$ as x is less than y; $x \geq y$ as x is greater than or equal to y; and $x > y$ as x is larger than y.

Practice **8.1.11.** *Let $n \in \mathbb{N}$. Define $P_n = \{k \in \mathbb{N} : k \text{ divides } n\}$. Define a relation $\leq_n$ on P_n by $\leq_n = \{(a, b) : a \text{ divides } b\}$. 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 linearly ordered set.*

In any finite set of symbols, we can fix a linear order by arbitrarily declaring which symbol comes next to which other symbol. Further, the same linear order can be extended to the set of all words formed using those symbols, such as that followed in a dictionary.

Definition 8.1.12. Let $(\Sigma, \leq)$ be a finite linearly ordered set (like the English alphabet with $a < b < c < \cdots < z$) and let Σ^* be the collection of all words formed using the elements of Σ. For $a = a_1 a_2 \cdots a_n$, $b = b_1 b_2 \cdots b_m \in \Sigma^*$ for $m, n \in \mathbb{N}$, 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 $i = 1, 2, \ldots, n = \min\{m, n\}$.

Then $(\Sigma^*, \leq)$ is a linearly ordered set. This ordering is called the **lexicographic** or **dictionary** ordering. Sometimes Σ is called the *alphabet* and the linearly ordered set Σ^* is called the *dictionary.*

Practice **8.1.13.** *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 D_1 and D_2 equinumerous?*

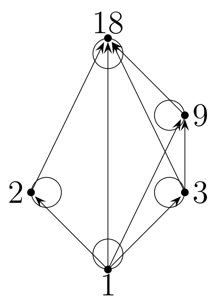
Discussion 8.1.14. [**Directed Graph Representation of a Finite Poset**] Often we represent a finite poset $(X, \leq)$ by a picture. The process is described below.

(a) Put a dot (called a node) for each element of X and label it with that element.

(b) If $a \leq b$, draw a directed line (an arrow) from the node labeled a to the node labeled b.

(c) Put a loop at the node labeled a for each $a \in X$.

1. A directed graph representation of the poset $(A, \leq)$ with $A = \{1, 2, 3, 9, 18\}$ and $\leq$ as the 'divides' relation ($a \leq b$ if $a|b$) is given below.



An abbreviated diagrammatic representation of a finite poset is defined below.

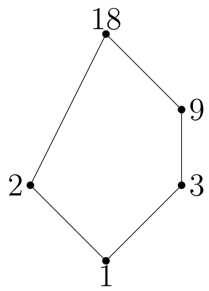
Definition 8.1.15. The **Hasse diagram** of a finite poset $(X, \leq)$ is a picture drawn in the following way:

1. Each element of X is represented by a point and is labeled with the element.
2. If $a \leq b$ then the point labeled a must appear at a lower height than the point labeled 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.

We will see later that for each finite poset a Hasse diagram exists; see Discussion 8.1.23.

Example 8.1.16. Hasse diagram for the poset $(A, \leq)$ with $A = \{1, 2, 3, 9, 18\}$ and $\leq$ as the 'divides' relation is given below.



PRACTICE **8.1.17.** *Draw the Hasse diagram for*

1. $\{1, 2, 3\} \times \{1, 2, 3, 4\}$ *under lexicographic order.*
2. $\{1, 2, 3, 6, 9, 18\}$ *(all positive divisors of* 18*) with the relation as 'divides'.*
3. $\{2, 3, 4, 5, 6, 7, 8\}$ *with the 'divides' relation.*

Proposition 8.1.18. *Let X and Y be nonempty sets. Let $\mathcal{F}$ be a nonempty family of partial functions from X to Y. Suppose $(\mathcal{F}, \subseteq)$ is a linearly ordered set. Let $h = \bigcup\limits_{f \in \mathcal{F}} f$. Then the following are true:*

1. *h is a partial function from X to Y.*
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.

1. Suppose that h is not a partial function. We have $x \in \mathsf{dom}\, h$ and $(x, y), (x, z) \in h,\ y \neq z$. Then there are $f, g \in \mathcal{F}$, such that $(x, y) \in f$ and $(x, z) \in g$. As $\mathcal{F}$ is linearly ordered, either $f \subseteq g$ or $g \subseteq f$. If $f \subseteq g$, then $(x, y) \in g$ and $(x, z) \in g$. Then, g is not a partial function, a contradiction. Similarly, $g \subseteq f$ leads to 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, *i.e.*, $x \in \mathsf{dom}\, f$ for a partial function f. Hence, $x \in \bigcup\limits_{f \in \mathcal{F}} \mathsf{dom}\, f$. ■

PRACTICE **8.1.19.** *Prove the other parts of Proposition 8.1.18.*

We fix some more terminology for posets related to extreme elements.

Definition 8.1.20. Let $(X, \leq)$ be a poset and let $A \subseteq X$.

1. We say that an element $x \in X$ is an **upper bound** of A if for each $z \in A,\ z \leq x$; or equivalently, when each element of A is less than or equal to x. An element $y \in X$ is called a **lower bound** of A if for each $z \in A,\ y \leq z$; or equivalently, when y is less than or equal to each element of A.
2. An element $x \in A$ is called the **maximum** of A, if x is an upper bound of A. Thus, maximum of A is an upper bound of A which is contained in A. Such an element is unique provided it exists. In this case, we denote $x = \max\{z : z \in A\}$. Similarly, **minimum** of A is an element $y \in A$ which is a lower bound of A. If minimum of A exists, then it is unique; and we write $y = \min\{z : z \in A\}$.

3. An element $x \in X$ is called the **least upper bound (lub)** of A in X if x is an upper bound of A and for each upper bound y of A, we have $x \leq y$; *i.e.*, when x is the minimum (least) element of the set of all upper bounds of A. Similarly, the **greatest lower bound (glb)** of A is a lower bound of A which is greater than or equal to all upper bounds of A; it is the maximum (largest) of the set of all lower bounds of A.

4. An element $x \in A$ is a **maximal** element of A if $x \leq z$ for some $z \in A$ implies $x = z$; or equivalently, when no element in A is larger than x. An element $y \in A$ is called a **minimal** element of A if $z \leq y$ for some $z \in A$ implies $y = z$; or equivalently, when no element in A is less than y.

Example 8.1.21. Consider the two posets $X = \{a, b, c\}$ and $Y = \{a, b, c, d\}$ described by the following Hasse diagrams:

Figure 8.1: Posets X and Y

1. Let $A = X$. 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. The following table illustrates the definitions by taking different subsets A of X, and also considering the same A as a subset of Y.

	$A = \{b, c\} \subseteq X$	$A = \{a, c\} \subseteq X$	$A = \{b, c\} \subseteq Y$
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	a	a	a
Lower bound(s) of A in Y	a	a	a
Upper bound(s) of A in X	does not exist	c	d
Upper bound(s) of A in Y	does not exist	c	d
Maximum element of A	does not exist	c	does not exist
Minimum element of A	does not exist	a	does not exist
lub of A in X	does not exist	c	d
lub of A in Y	does not exist	c	d
glb of A in X	a	a	a
glb of A in Y	a	a	a

Practice **8.1.22.**

1. *Apply induction to show that a finite poset has a maximal element and a minimal element.*
2. *Let $(X, \leq)$ be a poset and let Y be a nonempty subset of X. For $a, b \in Y$, define $a \leq_Y b$ if $a \leq b$. Show that $\leq_Y$ is a partial order on Y. This is called the* **induced partial order** *on Y.*

Discussion 8.1.23. **[Hasse diagram exists]** Let $(X, \leq)$ be a finite poset. Let $x_1, \ldots, x_k$ be the minimal elements of X. (See Practice 8.1.22.1.) Draw k points on the same horizontal line and label them $x_1, \ldots, x_k$. Now consider $Y = X \setminus \{x_1, \ldots, x_k\}$ with the induced partial order $\leq_Y$. By induction, the picture of $(Y, \leq_Y)$ 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 $x_i \leq y_j$ in X. This is the Hasse diagram for the poset $(X, \leq)$.

Remark 8.1.24. **[Bounds of the Empty Set]** Let $(X, \leq)$ be a poset. Then each $x \in X$ is an upper bound for $\varnothing$ as well as a lower bound for $\varnothing$. So, an lub for $\varnothing$ may or may not exist. For example, if $X = \{1, 2, 3\}$ and $\leq$ is the usual order, then $\mathsf{lub}\, \varnothing = 1$. Whereas, if $X = \mathbb{Z}$ and $\leq$ is the usual order, then an lub for $\varnothing$ does not exist. Similar statements hold for glb.

Another important class of partial orders is introduced next.

Definition 8.1.25. A linear order $\leq$ on a nonempty set X is said to be a **well order** if each nonempty subset of X has minimum. We call $(X, \leq)$ a well ordered set to mean that $\leq$ is a well order on X.

Often we use the phrase 'X is a well ordered set with the ordering as $\leq$' to mean '$(X, \leq)$ is a well ordered set'.

Recall that in a linearly ordered set X, if a minimum of a subset exists, it is an element of the subset and it is unique. Thus to say that every subset (of X) has minimum is same as saying every subset has its minimum, which is unique and is an element of that subset. Further, if each subset of X has a minimal element, then such a minimal element is the minimum of the subset. Thus a linearly ordered set is well ordered if and only if every nonempty subset has a minimal element.

Example 8.1.26.
1. The set $\mathbb{Z}$ with the usual order is not well ordered, as $\{-1, -2, \ldots, \}$ has no minimum.
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 order is well ordered.
4. The set $\mathbb{R}$ with the usual order (usual $\leq$) is not well ordered as the set $(0, 1)$ has no minimum.

What to write before this theorem? Also, it will be better to include the following theorem: "Every finite poset can be embedded in a totally ordered set".

Theorem 8.1.27. **[Principle of Transfinite Induction]** *Let $(W, \leq)$ be a well ordered set. Let $A \subseteq W$ satisfying "suppose for each $x \in W$, the condition $\{y \in W : y < x\} \subseteq A$ implies $x \in A$". Then $A = W$.*

Proof. Suppose $A \neq W$. Then $A^c = W \setminus A \neq \varnothing$. As W is well ordered, let s be the minimum of A^c in W. Notice that $s \in A^c$, and hence any element of W that is less than s is in A.

Consider the set $W_s := \{y \in W : y < s\}$. If $z \in W_s$, then $z < s$. So, by definition of A^c, $z \in A$. Hence, $W_s \subseteq A$. Then, by the given condition, $s \in A$. This is a contradiction. ∎

For any element a in a well ordered set $(W, \leq)$, the subset $W_a := \{x \in W : x < a\}$ is called the **initial segment of** a. In the well ordered set $\mathbb{N}$, the intiial segment of any natural number n is the set $\{1, \ldots, n-1\}$. The principle of transfinite induction says that if the condition that an initial segment of an element, say x_0, is contained in a subset, say A, implies that the element is in the subset ($x_0 \in A$), then the subset (A) cannot leave out any element of the well ordered set. We leave it as an exercise to supply a formal proof that this principle is same as the principle of mathematical induction in $\mathbb{N}$.

EXERCISE **8.1.28.**

1. *Determine the maximal elements, minimal elements, lower bounds, upper bounds, maximum, minimum, lub and glb of A in the following posets (X, f).*
   (a) *Take $X = \mathbb{Z}$ with the usual order (usual $\leq$) and $A = \mathbb{Z}$.*
   (b) *Take $X = \mathbb{N}$, $f = \{(i,i) : i \in \mathbb{N}\}$ and $A = \{4, 5, 6, 7\}$.*
2. *Does there exist a poset with exactly 5 maximal chains of sizes 2, 3, 4, 5, 6, and 2 maximal elements? If yes, draw the Hasse diagram. If no, give reasons.*
3. *Consider the poset $X = \{1, 2, 3, 6, 9, 18\}$ with 'divides' relation.*
   (a) *Draw the Hasse diagram of the poset.*
   (b) *What is its height? What is its width.*
   (c) *Let $A = \{2, 3, 6\} \subseteq X$. What are the maximal elements, minimal elements, maximum, minimum, lower bounds, upper bounds, glb and lub of A?*
4. *Construct the Hasse diagram for the '$\subseteq$' relation on $\mathcal{P}(\{a, b, c\})$.*
5. *Consider the poset $X = \{(1,1), (1,2), (1,3), \ldots\} \cup \{(2,1)(3,1), (4,1), \ldots\}$ with the partial order*

$$f = \bigcup_{\substack{m,n \in \mathbb{N} \\ m \leq n}} \{((1,m), (1,n))\} \bigcup \bigcup_{\substack{m,n \in \mathbb{N} \\ m \leq n}} \{((m,1), (n,1))\}.$$

   (a) *Does X have any minimal element(s)?*
   (b) *Does every subset of X have a lower bound?*
   (c) *Is X linearly ordered?*
   (d) *Is it true that every nonempty subset of X has a minimal element?*
   (e) *Is it true that every nonempty subset of X has a minimum?*
   (f) *What type of nonempty subsets of X always have a minimum?*
6. **[Tarski]** *A set X is finite if and only if every nonempty family of subsets of X has a minimal element in the poset $(\mathcal{P}(X), \subseteq)$.*
7. *Prove or disprove each of the following assertions:*
   (a) *There are at least 5 functions $f : \mathbb{R} \to \mathbb{R}$ which are partial orders.*
   (b) *Take $\mathbb{N}$ with the usual order. Then the dictionary order on $\mathbb{N}^2$ is a well order.*
   (c) *Take $\mathbb{N}$ with the usual order and $\mathbb{N}^2$ with the dictionary order. Then any nonempty subset of $\mathbb{N}^2$ which is bounded above has an lub.*
   (d) *There exists a partial order on $\mathbb{N}$ for which each nonempty subset has at least one but finitely many upper bounds, and also at least one but finitely many lower bounds?*
   (e) *There exists a partial order on $\mathbb{N}$ for which there are infinitely many maximal elements but has no minimal element.*
   (f) *Every countable linearly ordered set is well ordered with respect to the same ordering.*

(g) *Every countable chain which is bounded below, in a poset, is well ordered with respect to the same ordering.*

(h) *The set* $\mathbb{Q}$ *can be well ordered.*

(i) *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. Are there more than* 500 *ways to do that?*

(j) *An infinite poset in which each nonempty finite set has a minimum, must be linearly ordered.*

(k) *A finite poset in which each nonempty finite set has a minimum, must be well ordered.*

(l) *An infinite poset in which each nonempty finite set has a minimum, must be well ordered.*

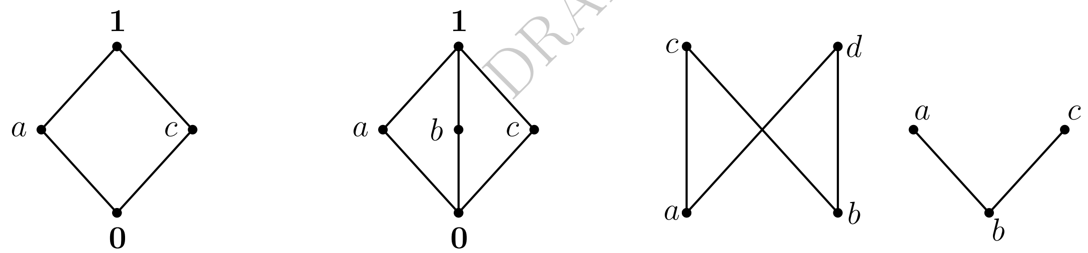
(m) *Every total order corresponds to an equivalence relation.*

8. *Show that the principle of transfinite induction is same as the principle of mathematical induction in the well ordered set* $(\mathbb{N}, \leq)$.

8.2 Lattices

In a poset, it is not necessary that two elements x, y should have a common upper bound. For instance, consider the poset $\{1, 2, \ldots, 6\}$ with "$a \leq b$ if and only if a divides b". The elements 5 and 3 have no common upper bound.

Similarly, in a poset, if a pair $\{x, y\}$ has at least one upper bound, it is not necessary that the set $\{x, y\}$ has an lub. For example, look at the poset described by the third Hasse diagram in Figure 8.2. The set $\{a, b\}$ has c and d as upper bounds, but there is no lub of $\{a, b\}$.



A distributive lattice A non-distributive lattice Both are non-lattices

Figure 8.2: Hasse diagrams

Definition 8.2.1.

1. A poset $(L, \leq)$ is called a **lattice** if each pair $x, y \in L$ has an lub and also a glb. An lub of x, y is also written as $x \vee y$ (read as 'x or y' / 'join of x and y') and a glb of x, y as $x \wedge y$ (read as 'x and y' / 'meet of x and y'). Do you want to write join and meet here or in Boolean Algebras? I added it. They appear in the next section.

2. A lattice is called a **distributive lattice** if for all pairs of elements x, y the following conditions, called *distributive laws*, are satisfied:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Example 8.2.2.

1. Consider the poset $L = \{0, 1\}$, where $0 < 1$. So, L is a linearly ordered set. In this case, $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$. Hence, L is a distributive lattice.

2. The set $\mathbb{N}$ with the usual order is a distributive lattice, where $\vee = \max$ and $\wedge = \min$. We consider two cases to verify that $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. The second distributive law is left as an exercise to the reader.

   (a) *Case 1:* $a \geq \min\{b, c\}$. Then, either $a \geq b$ or $a \geq c$, say $a \geq b$. So, $\max\{a, b\} = a$ and $\max\{a, c\} \geq a$. Thus,

   $$\begin{aligned} a \vee (b \wedge c) &= \max\{a, \min\{b, c\}\} \\ &= a = \min\big\{\max\{a, b\}, \max\{a, c\}\big\} = (a \vee b) \wedge (a \vee c). \end{aligned}$$

   (b) *Case 2:* $a < \min\{b, c\}$. Then, $a < b$ and $a < c$. So, $\max\{a, b\} = b$ and $\max\{a, c\} = c$. Thus,

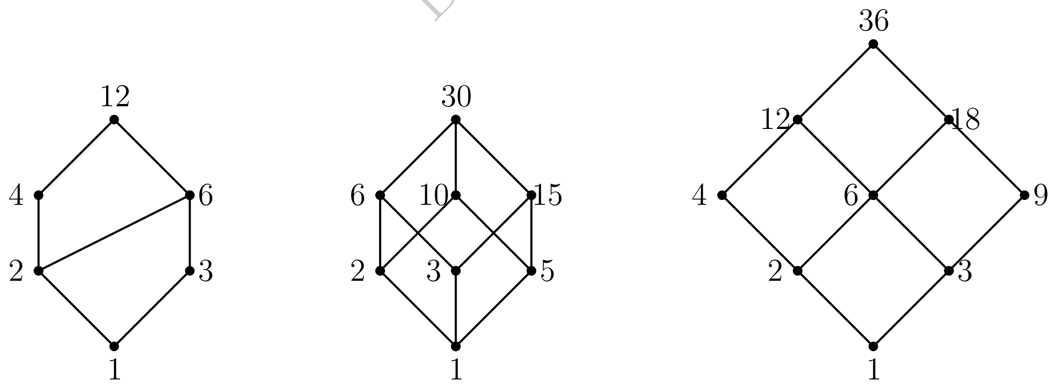
   $$\begin{aligned} a \vee (b \wedge c) &= \max\{a, \min\{b, c\}\} \\ &= \min\{b, c\} = \min\big\{\max\{a, b\}, \max\{a, c\}\big\} = (a \vee b) \wedge (a \vee c). \end{aligned}$$

3. The poset described by the first diagram in Figure 8.2 is a distributive lattice. (Verify.)

4. The poset described by the second diagram in Figure 8.2 is a lattice but not a distributive lattice. (Verify by computing $a \vee (b \wedge c)$ and $(a \vee b) \wedge (a \vee c)$ separately.)

5. Let $S = \{a, b, c\}$. Consider the poset $\mathcal{P}(S)$ with the partial order as $\subseteq$. Then $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. Verify that $\mathcal{P}(S)$ is a distributive lattice.

6. Fix a positive integer n and let $D(n)$ denote the set of all divisors of n. For elements $x, y \in D(n)$, define $x \leq y$ if x divides y. Then $(D(n), \leq)$ is a distributive lattice, where $\vee = \mathsf{lcm}$ and $\wedge = \gcd$. For $n = 12, 30$ and 36, the corresponding lattices are shown below.



   To check the first distributive law, let $a, b, c \in D(n)$, p a prime, and let $k \in \mathbb{N}$. Further, let $p^k \mid \mathsf{lcm}\{a, \gcd\{b, c\}\}$. Then, either $p^k \mid a$ or $p^k \mid b, c$. In that case, $p^k \mid \mathsf{lcm}\{a, b\}$ and $p^k \mid \mathsf{lcm}\{a, c\}$. So, $p^k \mid \gcd\{\mathsf{lcm}\{a, b\}, \mathsf{lcm}\{a, c\}\}$.

   Now, let us assume that $p^k \mid \gcd\{\mathsf{lcm}\{a, b\}, \mathsf{lcm}\{a, c\}\}$. Then, $p^k \mid \mathsf{lcm}\{a, b\}$ and $p^k \mid \mathsf{lcm}\{a, c\}$. Then, either $p^k \mid a$ or ($p^k \mid b$ and $p^k \mid c$). So, $p^k \mid \mathsf{lcm}\{a, \gcd\{b, c\}\}$.

   Thus, any power of a prime divides $a \vee (b \wedge c)$ if and only if it divides $(a \vee b) \wedge (a \vee c)$. Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Similarly, the second distributive law can be verified.

PRACTICE **8.2.3.**

1. *Fix a prime p and a positive integer n. Draw the Hasse diagram of $D(p^n)$. Does this correspond to a linearly ordered set? Give reasons for your answer.*

2. *Let n be a positive integer. Prove that $D(n)$ is a linearly ordered set if and only if $n = p^m$ for some prime p and a positive integer m.*

3. *Is every linearly ordered set a distributive lattice?*

We now prove the basic results on $\wedge$ and $\vee$.

Proposition 8.2.4. [**Laws**] *In a lattice $(L, \leq)$, the following are true:*

1. [**Idempotence**] : $a \vee a = a, \quad a \wedge a = a$
2. [**Commutativity**] : $a \vee b = b \vee a, \quad a \wedge b = b \wedge a$
3. [**Associativity**] : $a \vee (b \vee c) = (a \vee b) \vee c, \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$
4. $a \leq b \Leftrightarrow a \vee b = b$. *Similarly,* $a \leq b \Leftrightarrow a \wedge b = a$
5. [**Absorption**] : $a \vee (a \wedge b) = a = a \wedge (a \vee b)$
6. [**Isotonicity**] : $b \leq c \Rightarrow a \vee b \leq a \vee c, \quad b \leq c \Rightarrow a \wedge b \leq a \wedge c$
7. $a \leq b,\ c \leq d \Rightarrow a \vee c \leq b \vee d, \quad a \leq b,\ c \leq d \Rightarrow a \wedge c \leq b \wedge d$
8. [**Distributive Inequality**] : $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c), \quad a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$
9. [**Modularity**] : $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$

Proof. We prove only the first parts of all assertions; the second parts can be proved similarly.

(1) $a \vee a$ is an upper bound of $\{a, a\}$. Hence $a \vee a \geq a$. On the other hand, a is an upper bound of $\{a, a\}$. So, $a \vee a$ being the least of all upper bounds of $\{a, a\}$, is less than or equal to a. Hence $a \vee a = a$.

(2) $a \leq b \vee a,\ b \leq b \vee a$. So, $b \vee a$ is an upper bound of a, b. Since $a \vee b$ is the least of all upper bounds of a, b, we have $a \vee b \leq b \vee a$. Exchanging a and b, we get $b \vee a \leq a \vee b$. Hence $a \vee b = b \vee a$.

(3) Let $d = a \vee (b \vee c)$. Then, $d \geq a,\ d \geq b \vee c$ so that $d \geq a$, $d \geq b$ and $d \geq c$. So, $d \geq a \vee b$ and $d \geq c$. That is, $d \geq (a \vee b) \vee c$. Similarly, $e = (a \vee b) \vee c$ implies $e \geq a \vee (b \vee c)$. Thus, the first part of the result follows.

(4) Let $a \leq b$. As b is an upper bound of $\{a, b\}$, and $a \vee b$ is the least of all upper bounds of $\{a, b\}$, we have $a \vee b \leq b$. 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 $a \leq a \vee b = b$. Therefore, $a \leq b \Leftrightarrow a \vee b = b$.

(5) By definition $a \wedge b \leq a$. So, $a \vee (a \wedge b) \leq a \vee a = a$ using (1). Also, by definition $a \vee (a \wedge b) \geq a$. Hence, $a \vee (a \wedge b) = a$.

(6) 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 of $\{a, b\}$. Thus, $a \vee c \geq \mathsf{lub}\{a, b\} = a \vee b$.

(7) Using (6), we have $a \vee c \leq b \vee c \leq b \vee d$. Again, using (6), we get $a \wedge c \leq b \wedge c \leq b \wedge d$.

(8) 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 $c \leq a \vee c$, by (7), we get $b \wedge c \leq (a \vee b) \wedge (a \vee c)$. So, by definition $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

(9) Let $a \leq c$. Then, $a \vee c = c$ and hence by (8), 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 $a \leq a \vee (b \wedge c) \leq (a \vee b) \wedge c \leq c$. Thus the required result follows. ∎

PRACTICE **8.2.5.** *Show that in a lattice one distributive law implies the other.*

From two given lattices, a new lattice can be created by taking the product.

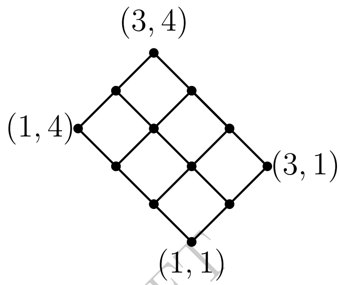
Before defining Direct Product of lattices, do we need to show that if $a = (a_1, a_2) \leq (b_1, b_2) = b$ whenever $a_1 \leq_1 b_1$ and $a_2 \leq_2 b_2$ then $a \vee b = (a_1 \vee_1 b_1, a_2 \vee_2 b_2)$ and $a \wedge b = (a_1 \wedge_1 b_1, a_2 \wedge_2 b_2)$.

Definition 8.2.6. Let $(L_1, \leq_1)$ and $(L_2, \leq_2)$ be lattices. 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 $a_2 \leq_2 b_2$, *i.e.*, if b dominates a entry-wise. This is called the **lattice order** on $L_1 \times L_2$. 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 lattices $(L_1, \leq_1)$ and $(L_2, \leq_2)$.

Example 8.2.7.

1. Consider $L = \{0, 1\}$ with the usual order $(0 \leq 1)$. 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 $a_i \leq b_i$ for each i. This is the n-fold direct product of L with itself. 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 the usual orders. Hasse diagram of the direct product $\{1, 2, 3\} \times \{1, 2, 3, 4\}$ is given below.



Practice 8.2.8. *Consider $\mathbb{N}$ with the usual order. The lattice order defined on $\mathbb{N}^2$ is different from the lexicographic order on $\mathbb{N}^2$. Draw pictures for all $(a, b) \leq (5, 6)$ in both the orders to verify this.*

Proposition 8.2.9. *The direct product of two distributive lattices is a distributive lattice.*

Proof. Let (a_1, b_1), (a_2, b_2), (a_3, b_3) be elements in the direct product of two distributive lattices. Then

$$\begin{aligned}
[(a_1, b_1) \vee (a_2, b_2)] \wedge (a_3, b_3) &= (a_1 \vee a_2, b_1 \vee b_2) \wedge (a_3, b_3) \\
&= \big((a_1 \vee a_2) \wedge a_3, (b_1 \vee b_2) \wedge b_3\big) \\
&= \big((a_1 \wedge a_3) \vee (a_2 \wedge a_3),\ (b_1 \wedge b_3) \vee (b_2 \wedge b_3)\big) \\
&= \big((a_1 \wedge a_3), (b_1 \wedge b_3)\big) \vee \big((a_2 \wedge a_3), (b_2 \wedge b_3)\big) \\
&= \big((a_1, b_1) \wedge (a_3, b_3)\big) \vee \big((a_2, b_2) \wedge (a_3, b_3)\big)
\end{aligned}$$

This verifies one of the distributive laws. Similarly, the other one can be verified, or use Practice 8.2.5. ■

As in all algebraic structures, there is a notion of lattice homomorphism and also lattice isomorphism. Informally, a homomorphism is a function from one lattice to the other which preserves the two operations of $\vee$ and $\wedge$; and an isomorphism is a bijective homomorphism.

Definition 8.2.10. Let $(L_1, \leq_1)$ and $(L_2, \leq_2)$ be 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**. Further, if f is a bijection, then it is called a **lattice isomorphism**.

Example 8.2.11.

1. Let D be the set of all words formed using the letters $a, b, \ldots, z$ and let $S \subseteq D$ consist of all words of length at most six. With the dictionary order, where $a \le b \le \cdots \le z$, both D and S are lattices. Define $f : D \to S$ as $f(d) = d$ if d has length at most six, otherwise $f(d)$ is obtained from d by keeping its first six letters intact and chopping off the rest. Then, f is a homomorphism. It is not an isomorphism as $f(\text{isomor}) = f(\text{isomorphism})$.

2. Consider the lattice $\mathbb{N}$ with the usual order. Let $S = \{0, 1, 2\}$ with the 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

$$f(m \vee n) = f(m) = 0, \quad f(m) \vee f(n) = 0 \vee 1 = 1.$$

   Thus $f(m \vee n) \ne f(m) \vee f(n)$. So, 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 $f^{-1}(1) = \mathbb{N} \setminus \{1, 2, \ldots, k\}$ for some $k \in \mathbb{N}$.

   (c) $f^{-1}(0) = \{1, 2, \ldots, k\}$, $f^{-1}(1) = \{k+1, k+2, \ldots, k+r\}$ and $f^{-1}(2) = \mathbb{N} \setminus \{1, 2, \ldots, k+r\}$ for some $k, r \in \mathbb{N}$.

In a lattice there may or may not exist an element which is greater than or equal to every other element. If such an element exists, which is greater than or equal to every other element, then it is called a *largest element.* In fact, a largest element is unique. For, suppose in a lattice $(L, \le)$ there exist elements a, b such that for all $x \in L$, we have $x \le a$ and $x \le b$. Then, in particular, $a \le b$ and $b \le a$ so that $a = b$. Thus, a lattice can have only one largest element. Similarly, a lattice can have only one smallest element.

Definition 8.2.12. Let $(L, \le)$ be a lattice. It is called a **bounded lattice** if there exist elements $\alpha, \beta \in L$ such that for each $x \in L$, we have $x \le \alpha$ and $\beta \le x$. Such an element α is called the **largest element** of L, and is denoted by $\mathbf{1}$. The element $\beta \in L$ satisfying $\beta \le x$ for all $x \in L$ is called the **smallest element** of L, and is denoted by $\mathbf{0}$.

Notice that if a lattice is bounded, then $\mathbf{1}$ is the lub of the lattice and $\mathbf{0}$ is the glb of the lattice.

Definition 8.2.13. A lattice $(L, \le)$ is said to be **complete** if each nonempty subset of L has lub and glb in L. For $A \subseteq L$, we write lub of A as $\vee A$, and glb of A, as $\wedge A$.

It follows that each complete lattice is a bounded lattice.

Example 8.2.14.

1. Verify that the lattices in Figure 8.3 are complete.

2. The set $[0, 5]$ with the usual order is a lattice which is both bounded and complete. So, is the set $[0, 1) \cup [2, 3]$.

3. The set $(0, 5]$ with the usual order is a lattice which is neither bounded nor complete.

4. The set $[0, 1) \cup (2, 3]$ with the usual order is a lattice which is bounded but not complete.

5. Every finite lattice is complete, and hence, bounded. (Use induction.)

6. The set $\mathbb{R}$ with the usual order is a lattice. It is not a complete lattice. Observe that the completeness property of $\mathbb{R}$, *i.e.*, "for every bounded nonempty subset a glb and an lub exist" is different from the completeness in the *lattice sense*.

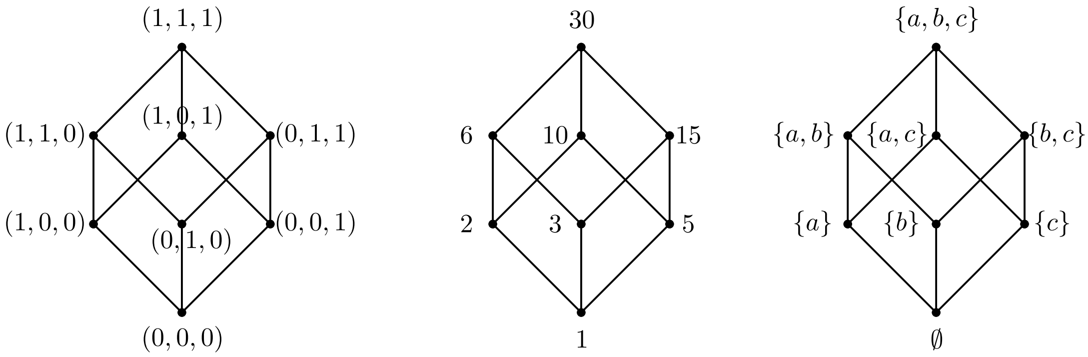


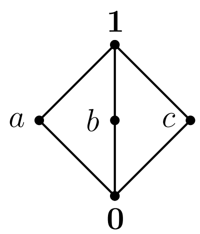
Figure 8.3: Complete lattices

Definition 8.2.15. Let $(L, \leq)$ be a bounded lattice. We say that $(L, \leq)$ is a **complemented** lattice if for each $x \in L$, there exists $y \in L$ such that $x \vee y = \mathbf{1}$ and $x \wedge y = \mathbf{0}$. Such an element y corresponding to the element x is called a **complement** of x, and is denoted by $\neg x$.

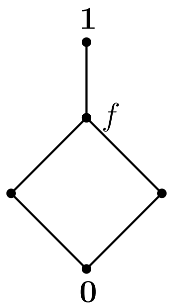
Example 8.2.16.

1. The interval $[0, 1]$ with the usual ordering is a distributive lattice but is not complemented. In fact, if $x \in (0, 1)$, then it does not have a complement.

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

Why the first 8 rows in the table given below? They already appear in Proposition 8.2.4. If you want to write then it will be nice to just mention it as a separate table. In the proof, the first eight are already proved earlier.

Theorem 8.2.17. **[The Comparison Table]** *Let $(L, \leq)$ be a lattice and let $a, b, c \in L$. 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*
$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$	*Any lattice*
[**Absorption**] $a \wedge (a \vee b) = a = a \vee (a \wedge b)$	*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**] $\{a \vee c = b \vee c,\ a \vee \neg c = b \vee \neg c\} \Rightarrow a = b$ $\{a \wedge c = b \wedge c,\ a \wedge \neg c = b \wedge \neg c\} \Rightarrow a = b$	*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; others are left as exercises. Cancellation property:

$$
\begin{aligned}
b &= b \vee \mathbf{0} = b \vee (c \wedge \neg c) = (b \vee c) \wedge (b \vee \neg c) = (a \vee c) \wedge (a \vee \neg c) = a \vee (c \wedge \neg c) = a \vee \mathbf{0} = a. \\
b &= b \wedge \mathbf{1} = b \wedge (c \vee \neg c) = (b \wedge c) \vee (b \wedge \neg c) = (a \wedge c) \vee (a \wedge \neg c) = a \wedge (c \vee \neg c) = a \wedge \mathbf{1} = a.
\end{aligned}
$$

De-Morgan's property:

$$
\begin{aligned}
(a \vee b) \vee (\neg a \wedge \neg b) &= (a \vee b \vee \neg a) \wedge (a \vee b \vee \neg b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}. \\
(a \vee b) \wedge (\neg a \wedge \neg b) &= (a \wedge \neg a \wedge \neg b) \vee (b \wedge \neg a \wedge \neg b) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}. \\
(a \wedge b) \vee (\neg a \vee \neg b) &= (a \vee \neg a \vee \neg b) \wedge (b \vee \neg a \vee \neg b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}. \\
(a \wedge b) \wedge (\neg a \vee \neg b) &= (a \wedge b \wedge \neg a) \vee (a \wedge b \wedge \neg b) = \mathbf{0} \wedge \mathbf{0} = \mathbf{0}.
\end{aligned}
$$

Using Definition 8.2.15 on the first two equalities, we get $\neg(a \vee b) = \neg a \wedge \neg b$; and using it again on the last two equalities, we obtain $\neg(a \wedge b) = (\neg a \vee \neg b)$.

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 $a \vee \neg b = (a \vee b) \vee \neg b = \mathbf{1}$. Similarly, the second part is proved. ∎

Exercise **8.2.18.**

1. *Prove that every linearly ordered set is a distributive lattice.*
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 a Hasse diagram representing it.*

4. *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?*
5. *Show that* $\{0, 1, 2, \ldots\}$ *is a complete lattice under divisibility relation (What do you mean by the next sentence "allow* $(0, 0)$ *in the relation"). Characterize those sets* A *for which* $\vee A = 0$.
6. *Is the lattice* $\{1, 2\} \times \{1, 2\} \times \{1, 2\} \times \{1, 2\}$ *isomorphic to* $\{1, 2, 3, 4\} \times \{1, 2, 3, 4\}$*?*
7. *Prove or disprove: If* L *is a lattice which is not complete, then there exists a one-one function from* $\mathbb{N}$ *to* L.
8. *Draw the Hasse diagram of a finite complemented lattice which is not distributive.*
9. *Fix* $n \in \mathbb{N}$. *Let* $p_1, p_2, \ldots, p_n$ *be* n *distinct primes. Prove that the lattice* $D(N)$*, (See Example 8.2.2.6) 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* $n = 3$ *with* $p_1 = 2,\ p_2 = 3,\ p_3 = 5$ *is shown in Figure 8.3.*
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.*

8.3 Boolean Algebras

In a distributive complemented lattice (see Theorem 8.2.17) the binary operations $\vee$, $\wedge$, and the unary operation $\neg$ satisfy certain properties. Taking cue from these properties, we define an algebraic structure and later show that the algebraic structure is capable of capturing the seemingly more general notion of a distributive complemented lattice.

Definition 8.3.1. A **Boolean algebra** is a nonempty set S which is closed under the binary operations $\vee$ (called **join**), $\wedge$ (called **meet**), and the unary operation $\neg$ (called **inverse** or **complement**) satisfying the following properties for all $x, y, z \in S$:

1. [**Commutativity**] : $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$.
2. [**Distributivity**] : $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
3. [**Identity elements**] : There exist elements $\mathbf{0},\ \mathbf{1} \in S$ such that $x \vee \mathbf{0} = x$ and $x \wedge \mathbf{1} = x$.
4. [**Inverse**] : $x \vee \neg x = \mathbf{1}$ and $x \wedge \neg x = \mathbf{0}$.

When required, we write the Boolean algebra S as $(S, \vee, \wedge, \neg)$ showing the operations explicitly.

Notice that the fourth property in the definition above uses the two special elements $\mathbf{0}$ and $\mathbf{1}$, whose existence has been asserted in the third property. This is meaningful when these two elements are uniquely determined by the third property. We show that it is indeed the case.

Proposition 8.3.2. *Let* S *be a Boolean algebra. Then the following statements are true:*

1. *Elements* $\mathbf{0}$ *and* $\mathbf{1}$ *are unique.*
2. *Corresponding to each* $s \in S$, $\neg s$ *is the unique element in* S *that satisfies the property:* $s \vee \neg s = \mathbf{1}$ *and* $s \wedge \neg s = \mathbf{0}$.
3. *For each* $s \in S$, $\neg\neg s = s$.

Proof. (1) Let $\mathbf{0}_1,\ \mathbf{0}_2 \in S$ be such that for each $x \in S$, $x \vee \mathbf{0}_1 = x$ and $x \vee \mathbf{0}_2 = x$. Then, in particular, $\mathbf{0}_2 \vee \mathbf{0}_1 = \mathbf{0}_2$ and $\mathbf{0}_1 \vee \mathbf{0}_2 = \mathbf{0}_1$. By Commutativity, $\mathbf{0}_2 \vee \mathbf{0}_1 = \mathbf{0}_1 \vee \mathbf{0}_2$. So, $\mathbf{0}_2 = \mathbf{0}_1$. That is, $\mathbf{0}$ is the unique element satisfying the property that for each $x \in S$, $\mathbf{0} \vee x = x$. A similar argument shows that $\mathbf{1}$ is the unique element that satisfies the property that for each $x \in S$, $x \wedge \mathbf{1} = x$.

(2) Let $s \in S$. By definition, $\neg s$ satisfies the required properties. For the converse, suppose $t, r \in S$ are 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, due to commutativity. ■

Example 8.3.3.

1. Let S be a nonempty set. Then $\mathcal{P}(S)$ is a Boolean algebra with $\vee = \cup$, $\wedge = \cap$, $\neg A = A^c$, $\mathbf{0} = \varnothing$ and $\mathbf{1} = S$. This is called the **power set Boolean algebra**. So, we have Boolean algebras of finite size as well as of uncountable size.
2. Take $D(30) = \{n \in \mathbb{N} : n \,|\, 30\}$ with $a \vee b = \mathsf{lcm}(a, b)$, $a \wedge b = \gcd(a, b)$ and $\neg a = \frac{30}{a}$. It is a Boolean algebra with $\mathbf{0} = 1$ and $\mathbf{1} = 30$.
3. Let $B = \{T, F\}$, where $\vee, \wedge$ and $\neg$ are the usual connectives. It is a Boolean algebra with $\mathbf{0} = F$ and $\mathbf{1} = T$.
4. Let B be the set of all truth functions involving the variables $p_1, \ldots, p_n$, with usual operations $\vee, \wedge$ and $\neg$. Then B is a Boolean algebra with $\mathbf{0} = \bot$ and $\mathbf{1} = \top$. This is called the **free Boolean algebra** on the generators $p_1, \ldots, p_n$. (See Chapter 7.)
5. The set of all formulas (of finite length) involving variables $p_1, p_2, \ldots$ is a Boolean algebra with usual operations. This is also called the *free Boolean algebra* on the generators $p_1, p_2, \ldots$. Here also $\mathbf{0} = \bot$ and $\mathbf{1} = \top$. So, we have a Boolean algebra of denumerable size.

Remark 8.3.4. The rules of Boolean algebra treat $(\vee, \mathbf{0})$ and $(\wedge, \mathbf{1})$ equally. Notice that the second parts in the defining conditions of Definition 8.3.1 can be obtained from the corresponding first parts by replacing $\vee$ with $\wedge$, $\wedge$ with $\vee$, $\mathbf{0}$ with $\mathbf{1}$, and $\mathbf{1}$ with $\mathbf{0}$ simultaneously. Thus, any statement that one can derive from these assumptions has a dual version which is derivable from the same assumptions. This is called the **principle of duality**.

Why are we proving the theorem? Except "constants" don't the other follow from what has already been done?

Theorem 8.3.5. **[Laws]** *Let S be a Boolean algebra. Then the following laws hold for all $s, t \in S$:*

1. **[Constants]** : $\neg \mathbf{0} = \mathbf{1}$, $\quad \neg \mathbf{1} = \mathbf{0}$, $\quad s \vee \mathbf{1} = \mathbf{1}$, $\quad s \wedge \mathbf{1} = s$, $\quad s \vee \mathbf{0} = s$, $\quad s \wedge \mathbf{0} = \mathbf{0}$.
2. **[Idempotence]** : $s \vee s = s$, $\quad s \wedge s = s$.
3. **[Absorption]** : $s \vee (s \wedge t) = s$, $\quad s \wedge (s \vee t) = s$.
4. **[Cancellation]** : $s \vee t = r \vee t,\ s \vee \neg t = r \vee \neg t \Rightarrow s = r$.
5. **[Cancellation]** : $s \wedge t = r \wedge t,\ s \wedge \neg t = r \wedge \neg t \Rightarrow s = r$.
6. **[Associativity]** : $(s \vee t) \vee r = s \vee (t \vee r)$, $\quad (s \wedge t) \wedge r = s \wedge (t \wedge r)$.

Proof. We give the proof of the first part of each item and that of its dual is left for the reader.

(1) $\mathbf{1} = \mathbf{0} \vee (\neg \mathbf{0}) = \neg \mathbf{0}$.

$s \vee \mathbf{1} = (s \vee \mathbf{1}) \wedge \mathbf{1} = (s \vee \mathbf{1}) \wedge (s \vee \neg s) = s \vee (\mathbf{1} \wedge \neg s) = s \vee \neg s = \mathbf{1}$.
$s \vee \mathbf{0} = s \vee (s \wedge \neg s) = (s \vee s) \wedge (s \vee \neg s) = s \wedge \mathbf{1} = s$.

(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) $s \vee (s \wedge t) = (s \wedge \mathbf{1}) \vee (s \wedge t) = s \wedge (\mathbf{1} \vee t) = s \wedge \mathbf{1} = s$.

(4) Suppose that $s \vee t = r \vee t$ and $s \vee \neg t = r \vee \neg t$. Then
$s = s \vee \mathbf{0} = s \vee (t \wedge \neg t) = (s \vee t) \wedge (s \vee \neg t) = (r \vee t) \wedge (r \vee \neg t) = r \vee (t \wedge \neg t) = r \vee \mathbf{0} = r$.

(5) This is the dual of (4) and left as an exercise.

(6) Using distributivity and absorption, we have

$$\begin{aligned}
&\big(s \vee (t \vee r)\big) \wedge \neg s = (s \wedge \neg s) \vee \big((t \vee r) \wedge \neg s\big) = \mathbf{0} \vee \big((t \vee r) \wedge \neg s\big) \\
&= \big((t \vee r) \wedge \neg s\big) = (t \wedge \neg s) \vee (r \wedge \neg s). \\
&\big((s \vee t) \vee r\big) \wedge \neg s = \big((s \vee t) \wedge \neg s\big) \vee (r \wedge \neg s) = \big((s \wedge \neg s) \vee (t \wedge \neg s)\big) \vee (r \wedge \neg s) \\
&= \big((\mathbf{0} \vee (t \wedge \neg s)\big) \vee (r \wedge \neg s) = (t \wedge \neg s) \vee (r \wedge \neg s).
\end{aligned}$$

Hence, $\big(s \vee (t \vee r)\big) \wedge \neg s = \big((s \vee t) \vee r\big) \wedge \neg s$.
Also, $\big((s \vee t) \vee r\big) \wedge s = \big((s \vee t) \wedge s\big) \vee (r \wedge s) = s \vee (r \wedge s) = s = \big(s \vee (t \vee r)\big) \wedge s$.
Now, apply Cancellation law to obtain the required result. ■

Isomorphisms between two similar algebraic structures help us in understanding an unfamiliar entity through a familiar one. Boolean algebras are no exceptions.

Definition 8.3.6. Let $(B_1, \vee_1, \wedge_1, \neg_1)$ and $(B_2, \vee_2, \wedge_2, \neg_2)$ 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 $\neg$. In such a case,

$$f(\mathbf{0}_1) = \mathbf{0}_2,\ f(\mathbf{1}_1) = \mathbf{1}_2,\ f(a \vee_1 b) = f(a) \vee_2 f(b),\ f(a \wedge_1 b) = f(a) \wedge_2 f(b),\ f(\neg_1 a) = \neg_2 f(a).$$

A **Boolean isomorphism** is a Boolean homomorphism which is a bijection.

Unless we expect an ambiguity in reading and interpreting the symbols, we will not write the subscripts with the operations explicitly as is done in Definition 8.3.6.

Example 8.3.7. Recall the notation $[n] = \{1, 2, \ldots, n\}$. The function $f : \mathcal{P}([4]) \to \mathcal{P}([3])$ defined by $f(S) = S \setminus \{4\}$ is a Boolean homomorphism. We check two of the properties and leave others as exercises.

$$f(A \vee B) = f(A \cup B) = (A \cup B) \setminus \{4\} = (A \setminus \{4\}) \cup (B \setminus \{4\}) = f(A) \vee f(B).$$
$$f(\mathbf{1}) = f([4]) = [4] \setminus \{4\} = [3] = \mathbf{1}.$$

Exercise **8.3.8.** 1. *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 $f(\mathbf{0}_1) = \mathbf{0}_2$, $f(\mathbf{1}_1) = \mathbf{1}_2$, $f(a \vee_1 b) = f(a) \vee_2 f(b)$ and $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$. Then, prove that f also satisfies the fifth condition, namely $f(\neg_1 a) = \neg_2 f(a)$.*

2. *Let B be a Boolean algebra. If $a, b \in B$ with $a \wedge b \neq a$ then $a \wedge \neg b \neq \mathbf{0}$.*

3. *Let B be a Boolean algebra. Then prove the following:*
   (a) *If B has three distinct atoms p, q and r, then $p \vee q \neq p \vee q \vee r$.*
   (b) *Let $b \in B$. If p, q and r are the only atoms less than or equal to b, then $b = p \vee q \vee r$.*

4. *Prove or disprove: Let $f : B_1 \to B_2$ be a Boolean homomorphism and let $a \in B_1$ be an atom. Then $f(a)$ is an atom of B_2.*

5. *What is the number of Boolean homomorphisms from $\mathcal{P}([4])$ to $\mathcal{P}([3])$?*

6. *How many Boolean homomorphisms from $\mathcal{P}([4])$ onto $\mathcal{P}([3])$ exist?*

7. *See Example 8.3.3.2. How many atoms does $D(30030)$ have? How many elements does it have?*

We will show that finite Boolean algebras are simply the power set Boolean algebras, up to isomorphism. Towards this, looking a Boolean algebra as a lattice will be of help.

Let $(L, \leq)$ be a distributive complemented lattice. Then, L has two binary operations $\vee$ and $\wedge$ and the unary operation $\neg x$. It can be verified that $(L, \vee, \wedge, \neg)$ is a Boolean algebra. Conversely, let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. Is it possible to define a partial order $\leq$ on L so that $(B, \leq)$ will be a distributive complemented lattice, and then in this lattice, the resulting operations of $\vee$, $\wedge$ and $\neg$ will be the same operations we have started with?

Theorem 8.3.9. *Let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. Define the relation $\leq$ on B by*

$$a \leq b \text{ if and only if } a \wedge b = a \quad \text{for all } a, b \in B.$$

Then $(B, \leq)$ is a distributive complemented lattice in which $\mathsf{lub}\{a, b\} = a \vee b$ and $\mathsf{glb}\{a, b\} = a \wedge b$ for all $a, b \in B$.

Proof. We first verify that $(B, \leq)$ is a partial order.
Reflexive: $s \leq s$ if and only if $s \wedge s = s$, which is true.
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 $s \wedge t = s$ and $t \wedge r = t$. Using associativity, $s \wedge r = (s \wedge t) \wedge r = s \wedge (t \wedge r) = s \wedge t = s$; consequently, $s \leq r$.

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 $\{a, b\}$. Analogous arguments show that $a \wedge b = \mathsf{glb}\{a, b\}$.

Since for all $a, b \in B$, $a \vee b$ and $a \wedge b$ are in B, we see that $\mathsf{lub}\{a, b\}$ and $\mathsf{glb}\{a, b\}$ exist. Thus $(B, \leq)$ is a lattice.

Further, if $a \in B$, then $\neg a \in B$. This provides the complement of a in the lattice $(B, \leq)$. Further, both the distributive properties are already satisfied in B. Hence $(B, \leq)$ is a distributive complemented lattice. ∎

In view of Theorem 8.3.9, we give the following definition.

Definition 8.3.10. Let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. The relation $\leq$ on B given by

$$a \leq b \text{ if and only if } a \wedge b = a \quad \text{for all } a, b \in B$$

is called the **induced partial order**. A minimal element of B with respect to the partial order $\leq$, which is different from $\mathbf{0}$ is called an **atom** in B.

It follows from Theorem 8.3.9 that a Boolean algebra can be defined as a distributive complemented lattice. In this development, one then proves the defining properties and the laws of a Boolean algebra.

Example 8.3.11.

1. In the power set Boolean algebra, singleton sets are the only atoms.

2. In Example 8.3.3.2, atoms of $D(30)$ are $2, 3$ and 5.

3. The $\{F, T\}$ Boolean algebra has only one atom, namely T.

Practice **8.3.12.**

1. *What are 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?*

The following two results are intuitively obvious.

Proposition 8.3.13. *Each finite Boolean algebra has at least one atom.*

Proof. Let B be a finite Boolean algebra. Assume that no element of B is an atom. Now, $\mathbf{0} < \mathbf{1}$ and $\mathbf{1}$ is not an atom. Then there exists $b_1 \in B$ such that $0 < b_1 < \mathbf{1}$. Since b_1 is not an atom, there exists $b_2 \in B$ such that $0 < b_2 < b_1 < \mathbf{1}$. By induction it follows that we have a sequence of elements (b_i) such that $0 < \cdots < b_i < b_{i-1} < \cdots < b_1 < \mathbf{1}$. As B is finite, there exist $k > j$ such that $b_k = b_j$. We then have $b_k < b_{k-1} < \cdots < b_j = b_k$. This is impossible. Hence B has at least one atom. ∎

Proposition 8.3.14. *Let p and q be atoms in a Boolean algebra B. If $p \neq q$, then $p \wedge q = \mathbf{0}$.*

Proof. Suppose that $p \wedge q \neq \mathbf{0}$. We know that $p \wedge q \leq p$. If $p \wedge q \neq p$, then $p \wedge q < p$. But this is not possible since p is an atom. So, $p \wedge q = p$. Similarly, $q \wedge p = q$. By commutativity, $p = p \wedge q = q \wedge p = q$. ∎

Theorem 8.3.15. **[Representation]** *Let B be a finite Boolean algebra. Then there exists a set X such that B is isomorphic to $\mathcal{P}(X)$.*

Proof. Let X be the set of all atoms of B. By Proposition 8.3.13, $X \neq \varnothing$. Define $f : B \to \mathcal{P}(X)$ by $f(b) = \{x \in B : x \text{ is an atom and } x \leq b\}$ for $b \in B$. We show that f is the required Boolean isomorphism.

Injection: Suppose $b_1 \neq b_2$. Then, either $b_1 \not\leq b_2$ or $b_2 \not\leq b_1$. Without loss of generality, let $b_1 \not\leq b_2$. 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 $b_1 \wedge \neg b_2 \neq \mathbf{0}$ (see Exercise 8.3.8.2). So, there exists an atom $x \leq (b_1 \wedge \neg b_2)$ and hence $x = x \wedge b_1 \wedge \neg b_2$. Then

$$x \wedge b_1 = (x \wedge b_1 \wedge \neg b_2) \wedge b_1 = x \wedge b_1 \wedge \neg b_2 = x.$$

Thus, $x \leq b_1$. Similarly, $x \leq \neg b_2$. As $x \neq \mathbf{0}$, we cannot have $x \leq b_2$ (for, $x \leq \neg b_2$ and $x \leq b_2$ imply $x \leq b_2 \wedge \neg b_2 = \mathbf{0}$). Thus there is an atom in $f(b_1)$ which is not in $f(b_2)$. Therefore, $f(b_1) \neq f(b_2)$.
Surjection: Let $A = \{x_1, \ldots, x_k\} \subseteq X$. Write $a = x_1 \vee \cdots \vee x_k$ (if $A = \varnothing$, take $a = \mathbf{0}$). Clearly, $A \subseteq f(a)$. We show that $A = f(a)$. So, let $y \in f(a)$. Then y is an atom in B and

$$y = y \wedge a = y \wedge (x_1 \vee \cdots \vee x_k) = (y \wedge x_1) \vee \cdots \vee (y \wedge x_k).$$

Since $y \neq \mathbf{0}$, by Proposition 8.3.14, $y \wedge x_i \neq \mathbf{0}$ for some $i \in \{1, 2, \ldots, k\}$. As x_i and y are atoms, we have $y = y \wedge x_i = x_i$ and hence $y \in A$. That is, $f(a) \subseteq A$ so that $f(a) = A$. Thus, f is a surjection.
Preserving $\mathbf{0}, \mathbf{1}$: Clearly $f(\mathbf{0}) = \varnothing$ and $f(\mathbf{1}) = X$.
Preserving $\vee, \wedge$: By definition,

$$\begin{aligned} x \in f(b_1 \wedge b_2) \quad &\Leftrightarrow \quad x \leq b_1 \wedge b_2 \;\Leftrightarrow\; x \leq b_1 \text{ and } x \leq b_2 \\ &\Leftrightarrow \quad x \in f(b_1) \text{ and } x \in f(b_2) \;\Leftrightarrow\; x \in f(b_1) \cap f(b_2). \end{aligned}$$

For the other one, let $x \in f(b_1 \vee b_2)$. Then, $x = x \wedge (b_1 \vee b_2) = (x \wedge b_1) \vee (x \wedge b_2)$. So, $x \wedge b_1 \neq \mathbf{0}$ or $x \wedge b_2 \neq \mathbf{0}$. Without loss of generality, suppose $x \wedge b_1 \neq \mathbf{0}$. 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, $x \le b_1$ and hence $x \le b_1 \vee b_2$ which in turn implies that $x \in f(b_1 \vee b_2)$. Therefore, $x \in f(b_1 \vee b_2) \Leftrightarrow x \in f(b_1) \cup f(b_2)$.
Preserving $\neg$: Let $x \in B$. Then $f(x) \cup f(\neg x) = f(x \vee \neg x) = f(\mathbf{1}) = X$ and $f(x) \cap f(\neg x) = f(x \wedge \neg x) = f(\mathbf{0}) = \varnothing$. Thus $f(\neg x) = \big(f(x)\big)^c$. ∎

As immediate consequences of the representation theorem, we obtain the following results. The readers should provide a proof.

Corollary 8.3.16. *Let B be a finite Boolean algebra.*

1. *If B has exactly k atoms then B is isomorphic to $\mathcal{P}(\{1, 2, \ldots, k\})$. Hence, B has exactly 2^k elements.*
2. *Fix $b \in B$. If $p_1, \ldots, p_n$ are the only atoms less than or equal to b, then $b = p_1 \vee \cdots \vee p_n$.*

EXERCISE **8.3.17.**

1. *Supply a Boolean homomorphism f from $\mathcal{P}([4])$ to $\mathcal{P}([3])$ such that $\mathsf{rng}\, f$ has 4 elements.*
2. *Prove or disprove: The number of Boolean homomorphisms from $\mathcal{P}([4])$ to $\mathcal{P}([3])$ is less than the number of lattice homomorphisms from $\mathcal{P}([4])$ to $\mathcal{P}([3])$.*
3. *Show that a lattice homomorphism on a Boolean algebra which preserves $\mathbf{0}$ and $\mathbf{1}$ is a Boolean homomorphism.*
4. *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?*
5. *We know that a finite Boolean algebra must have at least one atom. Is 'finite' necessary?*
6. *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.*
7. *Show that the set of subsets of $\mathbb{N}$ which are either finite or have a finite complement is a denumerable Boolean algebra. Find the atoms. Is it isomorphic to the free Boolean algebra with generators $p_1, p_2, \cdots$?*
8. *Let B be a Boolean algebra and let $x_i \in B$ for $i = 1, 2, \ldots$. 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?*
9. *Show that a Boolean algebra with at least 3 atoms has at least 2^3 elements.*
10. *Prove or disprove: If B_1 and B_2 are finite Boolean algebras each of size $k > 100$, then they must be isomorphic and there must be more than k isomorphisms between them.*
11. *Let $\mathcal{F}(\mathbb{N}) = \{X \subseteq \mathbb{N} : X$ is finite or X^c is finite$\}$. Similarly, define $\mathcal{F}(\mathbb{R})$. Show that both $\mathcal{F}(\mathbb{N})$ and $\mathcal{F}(\mathbb{R})$ are Boolean algebras, where $\vee = \cup$, $\wedge = \cap$ and $\neg(Y) = Y^c$. What is $\le$ here?*
12. *Give examples of two denumerable non-isomorphic Boolean algebras.*
13. *Give examples of two uncountable non-isomorphic Boolean algebras.*

8.4 Axiom of choice and its equivalents

As mentioned earlier, unrestricted use of apparently natural constructions led to paradoxes in the informal theory of sets. This brought forth many axiomatizations of Set theory. Mathematicians working in various branches, specifically those who worked on the foundations of mathematics, raised some concerns regarding one particular axiom, called the *Axiom of Choice.* A priori, it is inconceivable that this *seemingly obvious* statement should generate so much controversy. The controversy and debate generated by the axiom of choice among mathematicians might be put in parallel to the much discussed *Euclid's parallel postulate.* Though Axiom of choice looked very innocent, some of its consequences were counter-intuitive. More than a century had passed before it was formulated. It had been used in many branches of mathematics with much success in proving very important results.

There are different versions of the axiom of choice and some more equivalent statements, popularly accepted as Lemmas or Principles named after their originators. We will give an overview of the topic in this section and discuss its usefulness. The reader may refer to [7] and [11] for details.

We know that the Cartesian product of two nonempty sets is nonempty. Using induction, we can show that the product of a finite number of nonempty sets is nonempty. Is it true that the product of an infinite number of nonempty sets is nonempty? Axiom of choice posits that it is indeed true.

Axiom 8.4.1. [**Axiom of Choice (AC)**] *The product of a nonempty family of nonempty sets is nonempty.*

Recall that if $\{A_\alpha\}_{\alpha\in I}$ is a nonempty family of nonempty sets with the index set I, then the union of all sets in this family is denoted by $\underset{\alpha\in I}{\cup} A_\alpha$. Similarly, the product of this family consists of all functions f from I to $\underset{\alpha\in I}{\cup} A_\alpha$, where $f(\alpha)\in A_\alpha$ for each $\alpha\in I$. Thus AC asserts that at least one such function exists. Notice that any arbitrary family of sets $\mathcal{C}$ can be written as an indexed family by taking the index set as $\mathcal{C}$ itself; for, $\mathcal{C}=\{A_\alpha\}_{\alpha\in\mathcal{C}}$ with $A_\alpha=\alpha$. The union of such a family of sets is thus $\underset{Y\in\mathcal{C}}{\cup} Y$; which is also written as $\cup\mathcal{C}$. Hence a reformulation of AC is as follows:

AC: Given any nonempty family $\mathcal{C}$ of nonempty sets, there exists a function $f:\mathcal{C}\to\underset{Y\in\mathcal{C}}{\cup} Y$, called **the choice function**, such that $f(X)\in X$ for each X in $\mathcal{C}$.

Another formulation of AC is given in the following axiom. It so closely resembles AC that it goes by the acronym AC1.

Axiom 8.4.2. [**Axiom of Choice** 1 **(AC1)**] *Given any nonempty family $\mathcal{C}$ of nonempty disjoint sets, there exists a set B such that for each set X in $\mathcal{C}$, $X\cap B$ is a singleton set.*

Intuitively, one arrives at the set B in AC1 by choosing an element from each set in the given family.

Theorem 8.4.3. *AC1 is equivalent to AC.*

Proof. Assume that AC1 is true. Let $\{B_\alpha:\alpha\in I\}$ be a nonempty family of nonempty sets. For each $\alpha\in I$, write $C_\alpha=\{(x,\alpha):x\in B_\alpha\}$. In a way C_α is a copy of B_α, the only difference being C_α consists of ordered pairs (x,α) instead of the element x in B_α. Consider the family of sets $\mathcal{C}=\{C_\alpha:\alpha\in I\}$. Notice that if $\alpha\neq\beta$, then $C_\alpha\cap C_\beta=\varnothing$. Thus $\mathcal{C}$ is a nonempty family of disjoint nonempty sets. By AC1, there exists a set A such that $A\cap C_\alpha$ is a singleton set. Write $A\cap C_\alpha=\{(x_\alpha,\alpha)\}$, where $x_\alpha\in B_\alpha$. Define the function $f:\{B_\alpha:\alpha\in I\}\to\underset{\alpha\in I}{\cup} B_\alpha$ by $f(B_\alpha)=x_\alpha$. Clearly, f is well defined and $f(B_\alpha)\in B_\alpha$ for each $\alpha\in I$. Therefore, AC is true. The proof of "AC implies AC1" is left as an exercise. ∎

There are many general statements equivalent to Axiom of Choice. We will state only some of them and discuss their applications. For one of the equivalents of AC, we require a new notion that we introduce now.

Definition 8.4.4. A family of sets $\mathcal{C}$ is called a **family of finite character** if for any set A,

$$A \in \mathcal{C} \text{ if and only if each finite subset of } A \text{ is in } \mathcal{C}.$$

Example 8.4.5.

1. The empty family is a family of finite character.
2. The power set of any set is a family of finite character.
3. $\{\varnothing, \{1\}, \{2\}\}$ is a family of finite character.
4. Let V be a nontrivial vector space. As we know, a subset A of V is linearly independent if and only if all finite subsets of A are linearly independent. Therefore, the family of linearly independent subsets of V is a family of finite character.

Proposition 8.4.6. *Let A and B be two nonempty sets. Show that $\mathcal{P}(A) \cup \mathcal{P}(B)$ is a family of finite character.*

Proof. Let $\mathcal{C} = \mathcal{P}(A) \cup \mathcal{P}(B)$ and let $X \in \mathcal{C}$. Suppose $X \in \mathcal{P}(A)$. Then $X \subseteq A$. If Y is a finite subset of X, then $Y \subseteq A$. Then $Y \in \mathcal{P}(A)$. Similarly, if $X \in \mathcal{P}(B)$, then all finite subsets of X are in $\mathcal{P}(B)$. Thus, all finite subsets of X are in $\mathcal{P}(A) \cup \mathcal{P}(B)$.

Conversely, suppose X is a set such that all finite subsets of X are in $\mathcal{P}(A) \cup \mathcal{P}(B)$. We need to show that X is in $\mathcal{P}(A) \cup \mathcal{P}(B)$.

Assume the contrary, that $X \nsubseteq A$ and $X \nsubseteq B$. Then there exist elements $x \in X \setminus A$ and $y \in X \setminus B$. Now, $\{x, y\}$ is a finite subset of X; and hence $\{x, y\} \in \mathcal{P}(A) \cup \mathcal{P}(B)$. But $\{x, y\}$ is neither in $\mathcal{P}(A)$ nor in $\mathcal{P}(B)$, a contradiction. ■

PRACTICE **8.4.7.** *Let $\{A_\alpha\}_{\alpha \in I}$ be a nonempty family of nonempty sets. Show that $\bigcup_{\alpha \in I} P(A_\alpha)$ need not be a family of finite character.*

The following theorem lists some of the widely used equivalents of the axiom of choice. You will find some of them intuitively appealing while others are not. Nonetheless each of them follows from the other.

Theorem 8.4.8. *The following are equivalent to the axiom of choice:*

1. [**Tukey's lemma**] *Every nonempty family of finite character has a maximal element.*
2. [**Hausdorff's maximality principle**] *Every nonempty poset contains a maximal chain.*
3. [**Zorn's lemma**] *In a nonempty poset, if every chain has an upper bound, then the poset has a maximal element.*
4. [**Zermelo's well ordering principle**] *Every set can be well ordered.*

Proof. (AC $\Rightarrow$ Tukey's lemma) As usual, in a family of sets, we consider the partial order as $\subseteq$. Assume that the axiom of choice (AC) is true but Taukey's lemma is false. Let $\mathcal{F}$ be a nonempty family of finite character without any maximal element. So, each set A in the family $\mathcal{F}$ has a proper superset in $\mathcal{F}$. For each $A \in \mathcal{F}$, define $\mathcal{S}_A$ as the family of proper supersets of A that are in $\mathcal{F}$. Thus for each set A in the family $\mathcal{F}$, the family $\mathcal{S}_A$ is nonempty. Now, the collection of families $\mathcal{S}_A$, that is, $\{\mathcal{S}_A\}_{A \in \mathcal{F}}$ is a collection of families indexed by the family $\mathcal{F}$. The product of this indexed family is the set of all functions from $\mathcal{F}$ to $\bigcup_{A \in \mathcal{F}} \mathcal{S}_A$. Since each $\mathcal{S}_A$ is nonempty, AC implies that there exists such a function f. Consequently, for each $A \in \mathcal{F}$, $f(A) \in \mathcal{S}_A$, that is, $f(A)$ is a proper superset of A.

For convenience, call a sub-family $\mathcal{E}$ of $\mathcal{F}$ an *f-inductive family* if the following conditions hold:

$$\text{(i) } \varnothing \in \mathcal{E}, \quad \text{(ii) if } A \in \mathcal{E}, \text{ then } f(A) \in \mathcal{E}, \quad \text{(iii) if } \mathcal{B} \text{ is a chain in } \mathcal{E}, \text{ then } \cup\mathcal{B} \in \mathcal{E}.$$

Notice that $\mathcal{F}$ itself is f-inductive. Let $\mathcal{H}$ be the intersection of all f-inductive sub-families of $\mathcal{F}$. It is easy to see that $\mathcal{H}$ is f-inductive. We show that $\mathcal{H}$ is a chain.

In order to do that define the following family of sets

$$\mathcal{L} = \{A \in \mathcal{F} : \text{ if } B \in \mathcal{H} \text{ and } B \text{ is a proper subset of } A, \text{ then } f(B) \subseteq A\}.$$

Since $\mathcal{F}$ has no maximal element, $\mathcal{L}$ is a nonempty family. Fix any $L \in \mathcal{L}$.

Claim 1: For any $H \in \mathcal{H}$, we have either $H \subseteq L$ or $f(L) \subseteq H$.

To see this, consider the sub-family $\mathcal{C}$ of $\mathcal{H}$ defined by

$$\mathcal{C} = \{H \in \mathcal{H} \mid H \subseteq L \text{ or } f(L) \subseteq H\}.$$

We first show that $\mathcal{C}$ is an f-inductive set.

Clearly, $\varnothing$ is in $\mathcal{C}$. Observe that for any set A in $\mathcal{C}$, the following are true:

1. If A is a proper subset of L, then $f(A) \subseteq L$, as $L \in \mathcal{L}$. So $f(A) \in \mathcal{C}$.
2. If $A = L$, then $f(A) = f(L) \Rightarrow f(L) \subseteq f(A) \Rightarrow f(A) \in \mathcal{C}$.
3. If $f(L) \subseteq A$, then $f(L) \subseteq A \subseteq f(A)$. So $f(A) \in \mathcal{C}$.
4. If $\mathcal{B}$ is a chain in $\mathcal{C}$, then $\cup \mathcal{B} \in \mathcal{C}$.

   Reason: If each element of $\mathcal{B}$ is subset of L, then $\cup\mathcal{B} \subseteq L$ and so it is in $\mathcal{C}$. If some element B of $\mathcal{B}$ is not a subset of L, then $f(L) \subseteq B$ and so $f(L) \subseteq \cup\mathcal{B}$; thus $\cup\mathcal{B} \in \mathcal{C}$.

Thus $\mathcal{C}$ is an f-inductive set. Since $\mathcal{H}$ is the intersection of all f-inductive families, $\mathcal{H} \subseteq \mathcal{C}$. Also, by the very definition of $\mathcal{C}$, we have $\mathcal{C} \subseteq \mathcal{H}$. Therefore, $\mathcal{C} = \mathcal{H}$. Again, the definition of $\mathcal{C}$ implies that if $H \in \mathcal{H}$, then either $H \subseteq L$ or $f(L) \subseteq H$.

Claim 2: $\mathcal{L} = \mathcal{H}$.

We first show that $\mathcal{L}$ is an f-inductive family.

Clearly, $\varnothing$ is in $\mathcal{L}$. Let $L \in \mathcal{L}$. Does it follow that $f(L) \in \mathcal{L}$? To answer this, let B be a proper subset of $f(L)$. If $B \not\subseteq L$, then since $L \in \mathcal{L}$, $f(L) \subseteq B$, which is not possible. Hence $B \subseteq L$. Now, if $B = L$, then $f(B) = f(L)$. Otherwise, B is a proper subset of L. Since $L \in \mathcal{L}$, $f(B) \subseteq L \subseteq f(L)$. In any case, $f(B) \subseteq f(L)$. Hence $f(L) \in \mathcal{L}$.

Let $\mathcal{B}$ be a chain in $\mathcal{L}$. Is it true that $\cup\mathcal{B} \in \mathcal{L}$? Well, let H be a proper subset of $\cup\mathcal{B}$. We show that $f(H) \subseteq \cup\mathcal{B}$. For this, let $B \in \mathcal{B}$. If H is a proper subset of B, then since $B \in \mathcal{B} \subseteq \mathcal{L}$, we have $f(H) \subseteq B \subseteq \cup\mathcal{B}$. If $H = B$, then since B is a proper subset of $\cup\mathcal{B}$, $\cup\mathcal{B} \in \mathcal{H}$ and $B \in \mathcal{L}$, we have $f(H) = f(B) \subseteq \cup\mathcal{B}$. Otherwise, for each $B \in \mathcal{B}$, we have $H \not\subseteq B$. As $B \in \mathcal{L}$, $f(B) \subseteq H$. So, $B \subseteq H$, for each B and then $\cup\mathcal{B} \subseteq H$. But this is not possible as H is a proper subset of $\cup\mathcal{B}$. Therefore, $\cup\mathcal{B} \in \mathcal{L}$.

Hence, $\mathcal{L}$ is an f-inductive family. Since $\mathcal{H}$ is the intersection of all f-inductive families, $\mathcal{H} \subseteq \mathcal{L}$. Also, by the very definition of $\mathcal{L}$, we have $\mathcal{L} \subseteq \mathcal{H}$. Therefore, $\mathcal{L} = \mathcal{H}$.

Form Claim 1, we conclude that for each pair of sets H_1, H_2 in $\mathcal{H}$, we have either $H_2 \subseteq H_1$ or $f(H_1) \subseteq H_2 \Rightarrow H_1 \subseteq H_2$. So $\mathcal{H}$ is a chain. Using Claim 2, we see that $\mathcal{H}$ is a chain in $\mathcal{F}$ satisfying

$$\text{(a) } \varnothing \in \mathcal{H}, \qquad \text{(b) if } A \in \mathcal{H}, \text{ then } f(A) \in \mathcal{H}, \qquad \text{(c) } \bigcup_{A \in \mathcal{H}} A \in \mathcal{H}.$$

Now, starting with $\varnothing$ we see that $\varnothing \in \mathcal{H}$ and $f(\varnothing) \in \mathcal{H}$, and then $f^2(\varnothing) \in \mathcal{H}$, etc. Using induction, we have $f^n(\varnothing) \in \mathcal{H}$ for each $n \in \mathbb{N}$. It then follows that

$$\bigcup_{n \in \mathbb{N}} f^n(\varnothing) \text{ is a proper subset of } f\Big(\bigcup_{n \in \mathbb{N}} f^n(\varnothing)\Big) \subseteq \bigcup_{n \in \mathbb{N}} f^n(\varnothing).$$

This is a contradiction.

(Tukey's lemma $\Rightarrow$ Hausdorff's maximality principle) Assume that Tukey's lemma is true. Let X be a nonempty poset. Denote by $\mathcal{C}$, the family of all chains in X. Let Y be a set such that all its finite subsets are in $\mathcal{C}$. Then for any $x, z \in Y$, we have $\{x, z\} \in \mathcal{C}$; so, x and z are comparable. Thus, Y is a chain and so Y is a set in $\mathcal{C}$. Hence the family $\mathcal{C}$ is a family of finite character. Therefore, by Tukey's lemma, X has a maximal chain.

(Hausdorff's maximality principle $\Rightarrow$ Zorn's lemma) Assume that Hausdorff's maximality principle is true. Let $(X, \leq)$ be a nonempty poset in which every chain has an upper bound. Due to Hausdorff's maximality principle, $(X, \leq)$ has a maximal chain C. Let a be an upper bound of C. Suppose a is not a maximal element of $(X, \leq)$. Then there exists $b \in X$ such that $a < b$. Then $C \cup \{b\}$ becomes a larger chain than C, contradicting the assumption that C is a maximal chain in $(X, \leq)$. Hence a is a maximal element of $(X, \leq)$. We have shown that if every chain in $(X, \leq)$ has an upper bound in $(X, \leq)$, then $(X, \leq)$ has a maximal element. This proves Zorn's lemma.

(Zorn's lemma $\Rightarrow$ Zermelo's well ordering principle) Assume that Zorn's lemma is true. Let X be a nonempty set. Consider the family of all well ordered subsets of X, with their respective well orders:

$$\mathcal{F} = \{(A, \leq_A) : A \subseteq X \text{ and } \leq_A \text{ is a well order on } A\}.$$

Notice that $\mathcal{F}$ is a set of ordered pairs, where the first element is a subset of X and the second element is a well order on that subset. For $(B, \leq_B), (C, \leq_C)$ in $\mathcal{F}$, define $(B, \leq_B) \leq (C, \leq_C)$ if

$$B \subseteq C, \quad \leq_B \subseteq \leq_C, \quad \text{if } b \in B \text{ and } c \in C \setminus B, \text{ then } (b, c) \in \leq_B .$$

We leave it as an exercise to show that $\leq$ is a partial order on $\mathcal{F}$. We wish to see that the poset $(\mathcal{F}, \leq)$ satisfies the hypotheses of Zorn's lemma.

Let $\mathcal{C}$ be a nonempty chain in $(\mathcal{F}, \leq)$. We propose that $(W, \leq_W)$ is an upper bound of $\mathcal{C}$, where

$$W = \cup\{A : (A, \leq_A) \in \mathcal{C}\}, \quad \leq_W = \cup\{\leq_A : (A, \leq_A) \in \mathcal{C}\}.$$

Notice that the proposal goes through provided $(W, \leq_W) \in \mathcal{F}$. We leave it as an exercise to show that $\leq_W$ is a linear order on W. We need to show that if P is a nonempty subset of W, then there exists $p_0 \in P$ such that $p_0 \leq_W p$ for each $p \in P$.

So, let P be a nonempty subset of W. Given $p \in P$, there exists $(D, \leq_D)$ such that $p \in D$. Consider the set $S_p := \{x \in P : x \leq_D P\}$. It has a minimum, say p_0 as $\leq_D$ is a well order on D. We claim that p_0 is the minimum of P with respect to $\leq_W$. For, suppose that there exists $p_1 \in W$ such that $p_1 \leq_W p_0$, $p_0 \neq p_1$. Clearly, $p_1 \notin D$, otherwise p_0 cannot be the minimum of S_p. So, let $p_1 \in E$ for some pair $(E, \leq_E) \in \mathcal{C}$. As $(D, \leq_D)$ and $(E, \leq_E)$ are in the chain $\mathcal{C}$, either $D \subseteq E$ or $E \subseteq D$. But $p_1 \in E$ and $p_1 \notin D$; so, $E \nsubseteq D$. Hence, D is a proper subset of E. That is, there exists $b \in E$ such that $D = \{x \in E : x \leq_E b, \ x \neq b\}$. It follows that $p_0 \leq_E b$, $p_0 \neq b$ and $b \leq_E p_1$. This contradicts $p_1 \leq_W p_0$ as $\leq_W = \leq_B$ on E.

Hence our proposal goes through, that is, $\mathcal{C}$ has an upper bound, namely, $(W, \leq_W)$. By Zorn's lemma, $\mathcal{F}$ has a maximal element. Call such a maximal element $(Y, \leq_Y)$. Notice that $(Y, \leq_Y)$ is a well ordered set. Now, if Y is a proper subset of X, then we have an element $x \in X \setminus Y$. We can then extend $\leq_Y$ to a well order on $Y \cup \{x\}$. This will contradict the maximality of $(Y, \leq_Y)$. Hence, $Y = X$. We rename $\leq_Y$ as $\leq_X$ and conclude that $(X, \leq_X)$ is a well ordered set.

(Zermelo's Well ordering principle $\Rightarrow$ AC). Assume that Zermelo's well ordering principle is true. Let $\{X_\alpha\}_{\alpha \in L}$ be a nonempty family of nonempty sets. Write $X = \underset{\alpha \in L}{\cup} X_\alpha$. By Zermelo's well ordering principle, we have a well order, say, $\leq$ on X. Hence, each set X_α being a nonempty subset of X, has a minimum m_α. Define f on L by $f(\alpha) = m_\alpha$ for each $\alpha \in L$. Then $f \in \prod\limits_{\alpha \in L} X_\alpha$. ■

Example 8.4.9. Without using AC, show that $\mathbb{Z}$ and $\mathbb{Q}$ can be well ordered.

Ans: For $x, y \in \mathbb{Z}$, $x \neq y$, define $x < y$ if either $|x| < |y|$ or $|x| = |y|$ with x negative. In this partial order, the elements of $\mathbb{Z}$ may be listed as $0, -1, 1, -2, 2, -3, 3, \ldots$. Clearly, $(\mathbb{Z}, \leq)$ is a well ordered set.

For $\mathbb{Q}$, recall that the set of positive rational numbers, $\mathbb{Q}_+$, is denumerable. So, let $r_1, r_2, \ldots$ be an enumeration of $\mathbb{Q}_+$. Then enumerate $\mathbb{Q}$ by $0, -r_1, r_1, -r_2, r_2, \ldots$. This provides a well order on $\mathbb{Q}$.

More directly, since $\mathbb{Z}$ is denumerable, any enumeration of it gives a well order on it; same for $\mathbb{Q}$.

However, we do not know yet how to construct a well order on $\mathbb{R}$. It is one of the reasons why many mathematicians do not accept AC as one of the axioms of Set theory.

We now discuss some applications of the axiom of choice. Due to Theorem 8.4.8, we are free to use any of its equivalents when need arises. Further, since every set can be well ordered (assuming AC), the Principle of transfinite induction (See Theorem 8.1.27.) can be used in any set with the help of the well order.

Corollary 8.4.10. [Injection-Surjection] *Let A and B be nonempty sets. Then there exists a one-one function from A to B if and only if there exists an onto function from B to A.*

Proof. Let $f : A \to B$ be a one-one function. Then $f^{-1} : \mathsf{rng}\, f \to A$ is one-one and onto. Now, fix an element $a \in A$. Define the function $g : B \to A$ by

$$g(x) = \begin{cases} f^{-1}(x) & \text{if } x \in \mathsf{rng}\, f \\ a & \text{if } x \in B \setminus \mathsf{rng}\, f. \end{cases}$$

Then g is a an onto function.

Conversely, let $g : B \to A$ be an onto function. For any $x \in A$, $g^{-1}(x)$ is a nonempty subset of B. Consider the family $\mathcal{C} = \{g^{-1}(\alpha) : \alpha \in A\}$. Now, $\mathcal{C}$ is a nonempty family of nonempty sets. Further, $\bigcup\limits_{\alpha \in A} g^{-1}(\alpha) = B$. By the axiom of choice, there exists a function $f : A \to B$, where for each $\alpha \in A$, $f(\alpha) \in g^{-1}(\alpha)$. Since g is a function, $g^{-1}(\alpha) \cap g^{-1}(\beta) = \varnothing$ for $\alpha \neq \beta$. So, f is one-one. ■

The *Cardinal numbers* are symbols that we associate with sets such that equinumerous sets get the same symbol. We denote the cardinal number of a set A by $|A|$. If A is a finite set, then $|A|$ is the number of elements in A, which is some natural number m.

Generalizing the observation that "$|[m]| = |[n]|$ if and only if $m = n$" and "$|[m]| \leq |[n]|$ if and only if $m \leq n$" we introduce the following definition to compare cardinal numbers.

Definition 8.4.11. Let A and B be sets. By $|A|$ we mean the **cardinality** of A. By a **cardinal number**, we mean the cardinality of some set. Comparison of cardinality of sets and some related notation are defined as follows:

1. $|A| \leq |B|$ if there exists a one-one function from A to B.
2. $|A| \geq |B|$ if $|B| \leq |A|$.
3. $|A| = |B|$ if there is a bijection $f : A \to B$.
4. $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$.
5. $|\varnothing| = 0, \quad |[n]| = n, \quad |\mathbb{N}| = \aleph_0$.

6. If $x = |A|$, then by 2^x we mean $|\mathcal{P}(A)|$.
7. If $|B| = \aleph_k$, then we write $|\mathcal{P}(B)| = \aleph_{k+1} = 2^{\aleph_k}$.

Observe that, due to AC, $|A| \geq |B|$ if and only if there exists an onto function $f : A \to B$. Further, Cantor-Schröder-Bernstein (CSB) theorem implies that $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$. why this paragraph as we have mentioned it in item 3 above

Example 8.4.12.

1. If α, β, γ are cardinal numbers such that $\alpha \leq \beta$ and $\beta \leq \gamma$, then $\alpha \leq \gamma$.

   Ans: It says, if there exist a one-one function f from A to B and a one-one function g from B to C, then there is a one-one function from A to C. This is true, as $g \circ f$ is such a function.

2. If α is any cardinal number, then $\alpha < 2^\alpha$.

   Ans: If A is any set, then Cantor's theorem says that there is no onto function from A to $\mathcal{P}(A)$. That is, $|A| \neq |\mathcal{P}(A)|$. However, the function $f : A \to \mathcal{P}(A)$ given by $f(a) = \{a\}$ is a one-one function. That is, $|A| \leq |\mathcal{P}(A)|$. Hence, the result follows.

3. The cardinal numbers we know till now are

   $$0, 1, 2, 3, \ldots, \aleph_0 = |\mathbb{N}|, \aleph_1 = 2^{\aleph_0} = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|, \aleph_2 = 2^{\aleph_1} = 2^{2^{\aleph_0}} = |\mathcal{P}(\mathcal{P}(\mathbb{N}))| = |\mathcal{P}(\mathbb{R})|, \ldots.$$

4. The cardinal numbers $\aleph_0, \aleph_1, \aleph_2, \ldots$ are infinite cardinal numbers. In general, $|A|$ for any infinite set A, is called an *infinite cardinal.*

5. The *generalized continuum hypothesis* by Cantor asserts that there is no cardinal number between an infinite cardinal number α and 2^α.

Again, generalizing on the operations on natural numbers, we obtain the following definition for adding and multiplying cardinal numbers.

Definition 8.4.13. Let A and B be sets. Write $\alpha = |A|$ and $\beta = |B|$. Then, the **addition** and **multiplication** of cardinal numbers are defined as follows:

1. If $A \cap B = \varnothing$, then $\alpha + \beta := |A \cup B|$.
2. $\alpha\beta := |A \times B|$.

We abbreviate $\alpha\alpha\cdots$ (m times) to α^m.

Notice that we have a restriction in defining addition. But that is not a problem as the following example shows.

Example 8.4.14. Let A and B be sets. Show the following:

1. There exists an object x which is not an element of A.
2. There exist sets C and D such that $|C| = |A|$, $|B| = |D|$ and $C \cap D \neq \varnothing$.

Ans: (1) Since $|A| < |\mathcal{P}(A)|$, $A \neq \mathcal{P}(A)$. Hence there exists $x \in \mathcal{P}(A)$ which is not an element of A.

(2) Using (1), let x be an object which is not in $A \cup B$, and let y be an object which is not in $A \cup B \cup \{x\}$. Write $C = A \times \{x\}$ and $D = B \times \{y\}$. Then C and D satisfy all the requirements.

We will simply write $C = A \times \{0\}$ and $D = B \times \{1\}$ instead of using the objects x and y.

Example 8.4.15. Let A and B be nonempty sets. Then either $|A| \le |B|$ or $|B| \le |A|$.

Proof. Let $\mathcal{F}$ be the family of all one-one functions f with $\mathsf{dom}\, f \subseteq A$ and $\mathsf{rng}\, f \subseteq B$. Since A and B are nonempty sets, $\mathcal{F}$ is nonempty. Consider the poset $(\mathcal{F}, \subseteq)$. By Hausdorff's maximality principle, we have a maximal chain C. Write $g = \underset{f\in C}{\cup} f$.

It is easy to see that g is one-one, $\mathsf{dom}\, g = \underset{f\in C}{\cup} \mathsf{dom}\, f$ and $\mathsf{rng}\, g = \underset{f\in C}{\cup} \mathsf{rng}\, f$.

If $\mathsf{dom}\, g$ is a proper subset of A and $\mathsf{rng}\, g$ is a proper subset of B, then take $x \in A \setminus \mathsf{dom}\, g$ and $y \in B \setminus \mathsf{rng}\, g$. Then $h = g \cup \{(x, y)\}$ is a one-one function in $\mathcal{F}$ and $h \notin C$. Thus $C \cup \{h\}$ is a larger chain, a contradiction to the maximality of C.

So either $\mathsf{dom}\, g = A$, in which case $|A| \le |B|$; or $\mathsf{rng}\, g = B$, in which case $|B| \le |A|$.

Example 8.4.16. If α is an infinite cardinal number, then $\alpha + \alpha = \alpha$.

Proof. Let A, B be infinite sets with $\alpha = |A| = |B|$. In view of Example 8.4.14, assume that $\alpha = |A \times \{0\}| = |A \times \{1\}|$, where $A \times \{0\}$ and $A \times \{1\}$ are disjoint sets.

Let $\mathcal{F}$ be the set of all one-one functions with domain as a subset of A and range as $\mathsf{dom}\, f \times \{0, 1\}$. Then $(\mathcal{F}, \subseteq)$ is a nonempty poset. By Hausdorff's maximality principle we have a maximal chain $\mathcal{C}$. Write $g = \underset{f\in \mathcal{C}}{\cup} f$. We see that $\mathsf{dom}\, g = \underset{f\in \mathcal{C}}{\cup} \mathsf{dom}\, f$. Now, if $y \in \mathsf{rng}\, g$, then $\mathsf{rng}\, g = \underset{f\in \mathcal{C}}{\cup} \mathsf{rng}\, f$ implies $y \in \mathsf{rng}\, f$ for some f. However, $\mathsf{rng}\, f = \mathsf{dom}\, f \times \{0, 1\}$. So, there exists $x \in \mathsf{dom}\, f$ such that $y = (x, 0)$ or $(x, 1)$. Since $x \in \mathsf{dom}\, g$, we have $y \in \mathsf{dom}\, g \times \{0, 1\}$. Conversely, for any $x \in \mathsf{dom}\, g$, we have $x \in \mathsf{dom}\, f$ for some f and hence $(x, 0), (x, 1) \in \mathsf{rng}\, f \subseteq \mathsf{rng}\, g$. Therefore, $\mathsf{rng}\, g = \mathsf{dom}\, g \times \{0, 1\}$.

Further, g is an onto function from $\mathsf{dom}\, g$ to $\mathsf{rng}\, g$. We want to show that g is also one-one. On the contrary, suppose that we have $a, b \in \mathsf{dom}\, g$ and $c \in \mathsf{rng}\, g$ such that $a \ne b$ and $(a, c), (b, c) \in g$. As $g = \underset{f\in \mathcal{C}}{\cup} f$, there exists $h \in \mathcal{C}$ such that $(a, c) \in f$ and $(b, c) \in h$. Notice that h is one-one. Since $\mathcal{C}$ is a chain, either $f \subseteq h$ or $h \subseteq f$. If $f \subseteq h$, then $(a, c), (b, c) \in h$, a contradiction to the fact that h is one-one. Similarly, $h \subseteq f$ contradicts the fact that f is one-one. Thus, we conclude that g is one-one; and hence it is a bijection from $\mathsf{dom}\, g$ to $\mathsf{rng}\, g = \mathsf{dom}\, g \times \{0, 1\}$.

Is the set $A \setminus \mathsf{dom}\, g$ finite or infinite? Suppose $A \setminus \mathsf{dom}\, g$ is infinite. Then $A \setminus \mathsf{dom}\, g$ contains a denumerable set, say D. There exists a bijection $\phi : D \to D \times \{0, 1\}$. Then the function $\psi = g \cup \phi$ is a bijection. As

$$\psi : \mathsf{dom}\, g \cup D \to (\mathsf{dom}\, g \times \{0, 1\}) \cup (D \times \{0, 1\}) = (\mathsf{dom}\, g \cup D) \times \{0, 1\}$$

is a bijection, we see that $\psi \in \mathcal{F}$. Further, g is a proper subset of ψ; so that $\psi \notin \mathcal{C}$. Hence, $\mathcal{C} \cup \{\psi\}$ is a larger chain than $\mathcal{C}$, a contradiction.

Hence, $A \setminus \mathsf{dom}\, g$ is finite. Write $A \setminus \mathsf{dom}\, g = \{x_1, \ldots, x_n\}$. By the train-seat argument, we find a bijection from $A \setminus \{x_1, \ldots, x_n\}$ to A. That is, $|A \setminus \{x_1, \ldots, x_n\}| = |A| = \alpha$. So, $|\mathsf{dom}\, g| = \alpha$, and g is a bijection from $\mathsf{dom}\, g$ to $\mathsf{dom}\, g \times \{0, 1\}$. Therefore, $\alpha = \alpha + \alpha$.

A more general result is proved in the following example.

Example 8.4.17. If α is an infinite cardinal number, then $\alpha^2 = \alpha$.

A proof along the lines of the previous example can be constructed for $\alpha^2 = \alpha$; however, we give another using Zorn's lemma.

Proof. Let A be an infinite set with $|A| = \alpha$. So, A has a denumerable subset N. Clearly, there is a bijection $f : N \to N^2$. $(N^2 = N \times N.)$ Define the set

$$X = \{(M, g) : N \subseteq M \subseteq A \text{ and } g : M \to M^2 \text{ is a bijection}\}.$$

Define the partial order $\le$ on X by

$$(M, g) \le (K, h) \Leftrightarrow (M \subseteq K \text{ and } g \text{ is a restriction of } h \text{ to } M).$$

It is easy to see that in the poset $(X, \leq)$, every chain has an upper bound. By Zorn's lemma, $(X, \leq)$ has a maximal element, say, (B, ϕ).

Consider the set $C = A \setminus B$; and write $\beta = |B|$, $\gamma = |C|$. Notice that the definition of X implies that $\beta^2 = \beta$. Suppose $\beta \leq \gamma$. Then there exists $D \subseteq C$ such that $|D| = \beta$. Write $E = (B \cup D)^2 \setminus B^2$ and $\epsilon = |E|$. Then

$$\beta = |D| \leq |D^2| \leq \epsilon^2 = 3\beta^2 = 3\beta \leq \beta^2 = \beta.$$

Hence $\epsilon = \beta$. Thus, there exists a bijection $\psi : D \to E$. Define the function $\xi : (B \cup D) \to (B \cup D)^2$ by

$$\xi(x) = \begin{cases} \phi(x) & \text{if } x \in B \\ \psi(x) & \text{if } x \in D. \end{cases}$$

Clearly, ξ is a bijection that extends ϕ. This contradicts the maximality of (B, ϕ). Hence $\gamma \leq \beta$. Then

$$\alpha \leq \alpha^2 = \beta^2 + \beta\gamma + \gamma\beta + \gamma^2 \leq 4\beta^2 = 4\beta \leq \beta^2 = \beta \leq \alpha.$$

Therefore, $\alpha^2 = \alpha$.

PRACTICE **8.4.18.** *Let α, β, γ be cardinal numbers with $\beta \leq \gamma$. Show that $\alpha + \beta \leq \alpha + \gamma$ and $\alpha\beta \leq \alpha\gamma$.*

Example 8.4.19. Every partial order on a nonempty set can be extended to a linear order.

Proof. Let (X, f) be a nonempty poset. We show that there exists a linear order g on X such that $f \subseteq g$. Towards this, let $\mathcal{F}$ be the family of all partial orders h on X such that $f \subseteq h$. Since $f \in \mathcal{F}$, the poset $(\mathcal{F}, \subseteq)$ is nonempty. By Hausdorff's maximality principle, it has a maximal chain, say C. Write $g = \underset{h \in C}{\cup} f$.

It is easy to verify that g is a partial order. Suppose that g is not a linear order on X. Then there exists distinct $x, y \in X$ such that $(x, y) \notin g$ and $(y, x) \notin g$.

Define $L_x = \{z : (z, x) \in g\}$ and $M_y = \{z : (y, z) \in g\}$. If $z \in L_x \cap M_y$, then $(y, x) \in g$ by transitivity. Hence $L_x \cap M_y = \varnothing$. Note that $x \in L_x$ and $y \in M_y$. Write $g_1 = g \cup (L_x \times M_y)$. We show that g_1 a partial order.

Reflexivity: Trivial.

Antisymmetry: Let $(a, b), (b, a) \in g_1$. Both of $(a, b), (b, a)$ cannot be in $L_x \times M_y$, as $L_x \cap M_y = \varnothing$. Suppose one of them is in $L_x \times M_y$ and the other is in g. Without loss of generality, assume that $(a, b) \in L_x \times M_y$ and $(b, a) \in g$. This means $(a, x) \in g$, $(y, b) \in g$, and $(b, a) \in g$. But then $(y, x) \in g$, a contradiction. Therefore, both of $(a, b), (b, a)$ are in g, and hence $a = b$.

Transitivity: Let $(a, b), (b, c) \in g_1$. Clearly, both of them are not in g_1. If both of them are in g, we have nothing to prove. So let $(a, b) \in L_x \times M_y$ and $(b, c) \in g$. This means $(a, x) \in g$, $(y, b) \in g$ and $(b, c) \in g$. From the last two, $c \in M_y$. So $(a, c) \in L_x \times M_y \subseteq g_1$.

Notice that $g_1 \notin C$. Then $C \cup \{g_1\}$ is a larger chain than C, a contradiction.

Example 8.4.20. Let H be an Abelian subgroup of a non-Abelian group G. Show that there is a maximal Abelian subgroup J of G such that $H \subseteq J$.

Ans: Let $\mathcal{F}$ be the set of all Abelian subgroups of G which contain H. Notice that $H \in \mathcal{F}$. By Hausdorff's maximality principle there is a maximal chain $\mathcal{C}$ in $\mathcal{F}$. Observe that $H \in \mathcal{C}$, otherwise we could extend C. Write $J = \underset{A \in \mathcal{C}}{\cup} A$. It is easy to check that J is an Abelian subgroup of G. If J_0 is any Abelian subgroup that contains J properly, then $J_0 \notin \mathcal{C}$ and $J_0 \in \mathcal{F}$. Thus $\mathcal{C} \cup \{J_0\}$ is a larger chain than $\mathcal{C}$, which contradicts the maximality of $\mathcal{C}$.

Example 8.4.21. Show that every vector space has a Hamel basis.

Ans: Recall that a Hamel basis of a vector space is a maximal linearly independent subset of the vector space. Of course, the trivial vector space $\{0\}$ has the only Hamel basis as $\varnothing$.

Let $\mathbb{V}$ be a vector space. Recall that the family $\mathcal{F}$ of linearly independent subsets of $\mathbb{V}$ is a family of finite character. By Tukey's lemma, the family $\mathcal{F}$, ordered as usual by the subset relation, has a maximal element. Such a maximal element is a Hamel basis for $\mathbb{V}$.

Example 8.4.22. Let $(L, \leq)$ be a nonempty linearly ordered set. Prove that there exists $W \subseteq L$ such that $\leq$ well orders W, and for each $x \in L$, there exists $y \in W$ such that $x \leq y$. (For example, for $L = \mathbb{R}$, we can take $W = \mathbb{N}$.)

Proof. Take an element $\ell \in L$. The singleton set $\{\ell\}$ is well ordered by $\leq$. Let $\mathcal{F}$ be the family of subsets of L satisfying the condition: "each set in L is well ordered by $\leq$ with ℓ as its minimum". Notice that $\{\ell\} \in \mathcal{F}$.

On $\mathcal{F}$ we define a partial order g by $(A, B) \in g$ if and only if $A \subseteq B$ and elements of $B \setminus A$ are upper bounds of A.

Then $(\mathcal{F}, g)$ is a nonempty poset. By Hausdorff's maximality principle we have a maximal chain in $\mathcal{F}$, say $\mathcal{C}$. Clearly, this chain starts with $\{\ell\}$. Write $W = \bigcup\limits_{A \in \mathcal{C}} A$. Then it is clear that $W \subseteq L$.

To show that W is well ordered, let $B \subseteq W$ be a nonempty set. Let $b \in B$. Then there is a set $C_b \in \mathcal{C}$ such that $b \in C_b$. Recall that C_b is well ordered. Consider the initial segment $I(b) = \{x \in C_b : x < b\}$. Then $(I(b) \cup \{b\}) \cap B$ is a nonempty subset of C_b; hence it has a minimum, say, w in $(I(b) \cup \{b\}) \cap B$.

We claim that w is the minimum of B. Suppose, on the contrary that there exists $y \in B$ such that $y < w$. As $w \leq b$, we see that $y < b$. If $y \in C_b$, then $y \in I(b)$, and hence $y \in (I(b) \cup \{b\}) \cap B$, which implies that $w \leq y$. So $y \notin C_b$. In that case, y can only belong to a set in $\mathcal{C}$ that comes after C_b (which is a proper superset of C_b). But then y is an upper bound of C_b, contradicting $y < b$.

Thus W is well ordered. Now, suppose there exists $p \in L$ which is a strict upper bound of W. Then $W_0 := W \cup \{p\}$ is well ordered and $\mathcal{C} \cup \{W_0\}$ is a larger chain than $\mathcal{C}$, contradicting the maximality of C. That is, no element in L is strictly larger than every element of W. In other words, for each $x \in L$, there exists $y \in W$ such that $x \leq y$.

Exercise **8.4.23.**

1. *Let A and B be two nonempty sets. Show that there is a set C such that $C \cap A = \varnothing$ and $|C| = |B|$.*
2. *Let X be the set of all infinite sequences formed using $0, 1$ and let Y be the set of all infinite sequences formed using $0, 1, 2$. Which one is larger, $|X|$ or $|Y|$?*
3. *Let α, β be infinite cardinal numbers with $\alpha \leq \beta$. Then $\alpha + \beta = \beta$ and $\alpha\beta = \beta$.*
4. *Show that $\mathbb{R}$ is not a finite dimensional vector space over $\mathbb{Q}$.*
5. *Let X be a vector space. Let A and S be nonempty subsets of X, where A is linearly independent, $A \subseteq S$ and span$(S) = X$. Show that there exists a Hamel basis B such that $A \subseteq B \subseteq S$.*
6. *Let A be a nonwmpty set and let $\mathbb{F}$ be a field. Write $\mathbb{F}^A := \{f : f$ 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.*

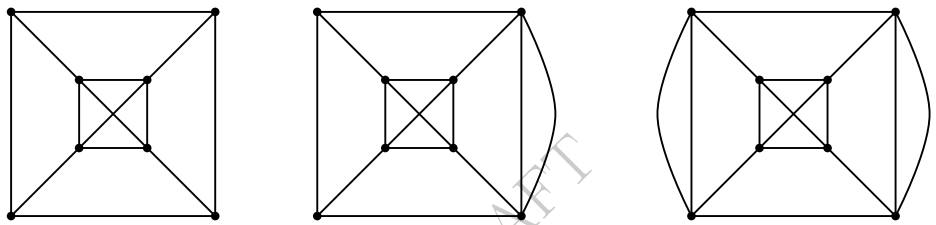
Chapter 9

Graphs - I

9.1 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 9.1.1. A **pseudograph** G is a pair (V, E) where V is a nonempty set and E is a multiset of 2-elements sets 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 9.1.2. $G = \Big(\{1,2,3,4\},\ \big\{\{1,1\},\{1,2\},\{2,2\},\{3,4\},\{3,4\}\big\}\Big)$ is a pseudograph.

Discussion 9.1.3. 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 9.1.4. A picture for the pseudograph in Example 9.1.2 is given in Figure 9.1.

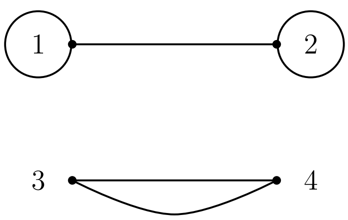


Figure 9.1: A pseudograph

Definition 9.1.5. Let $G = (V, E)$ be a graph. Then the following definitions and notations are in order.

1. we sometimes use $V(G)$ in place of V for the vertex set and $E(G)$ in place of E for the edge set.
2. The number $|V(G)|$ is called the **order** of the graph G, and is denoted by $|G|$. By $\|G\|$, we denote the number of edges of G. A graph with n vertices and m edges is called an (n, m) **graph**.
3. 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'.
4. If uv is an edge in G, then we say that the vertices u and v are **adjacent** in G, and also that u is a **neighbor** of v. We write $u \sim v$ to denote that u is adjacent to v.
5. 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.
6. Two edges e_1 and e_2 are called **adjacent** if they have a common end vertex.
7. A graph is said to be **non-trivial** if it has at least one edge; else it is called a **trivial** graph.
8. A **multigraph** is a pseudograph without loops. A multigraph is a **simple graph** if no edge appears twice.
9. In this book, we consider only simple graphs with finite vertex sets. Thus, by a **graph**, we will mean a simple graph with a finite vertex set, unless stated otherwise.
10. 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** of G, denoted $\alpha(G)$.

Discussion 9.1.6. 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 9.1.7. Consider the graph G in Figure 9.2. The vertex 12 is an isolated vertex whereas the vertex 10 is a pendant 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.

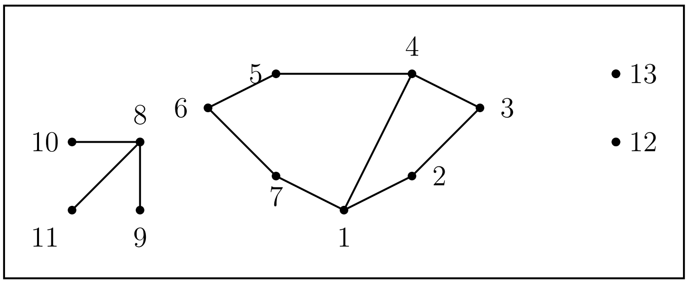


Figure 9.2: A graph G.

Definition 9.1.8. Let $G = (V, E)$ be a graph on n vertices, say $V = \{1, \ldots, n\}$. 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 $E = \{\{i, i+1\} : 1 \le i \le n-1\}$.
3. **Cycle graph**, denoted C_n, if $E = \{\{i, i+1\} : 1 \le i \le n-1\} \cup \{n, 1\}$.
4. **Bipartite graph** if $V = V_1 \cup V_2$ such that $|V_1|, |V_2| \ge 1$, $V_1 \cap V_2 = \varnothing$ 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 $E = \{\{i, j\} : 1 \le i \le r, 1 \le j \le s\}$.

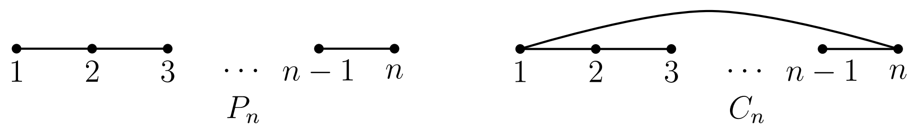


Figure 9.3: P_n and C_n.

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.

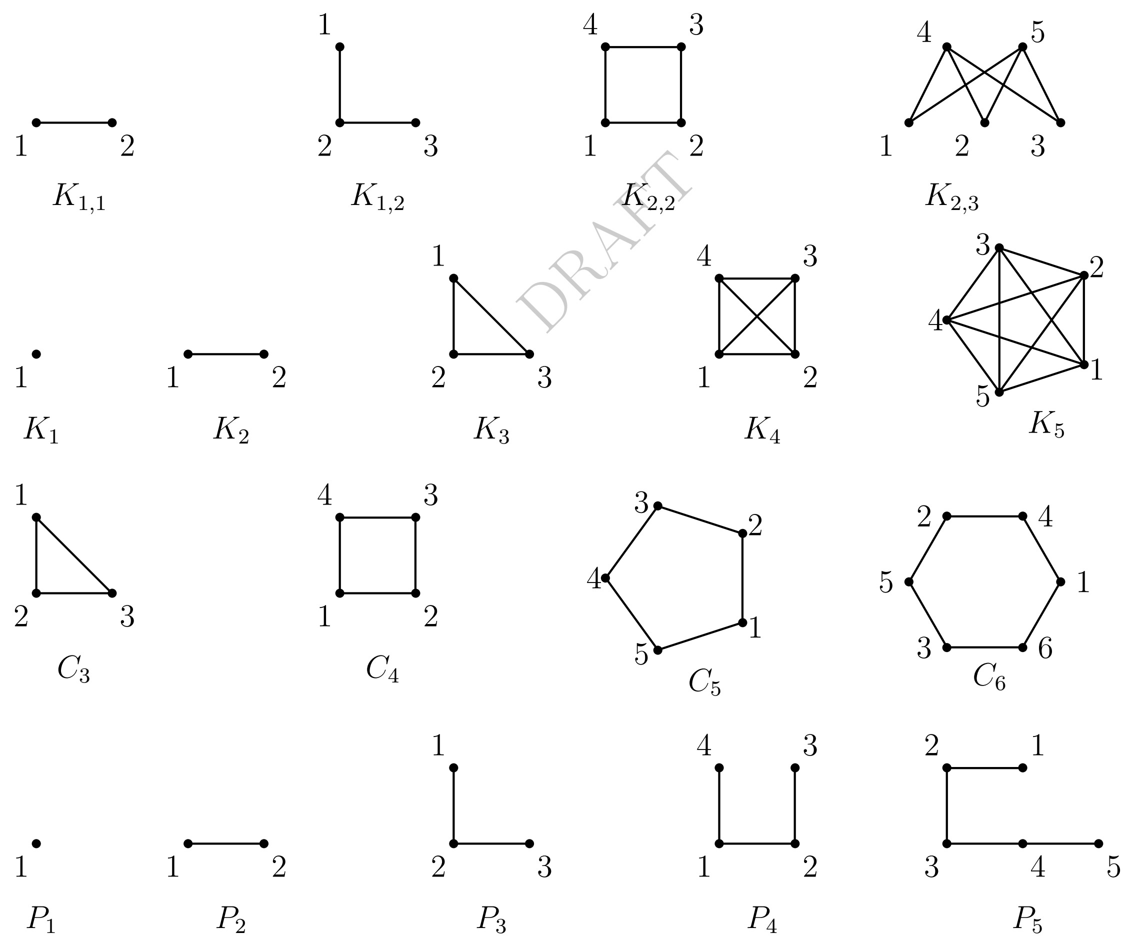


Figure 9.4: Some well known family of graphs

QUIZ **9.1.9.** *What is the maximum number of edges possible in a simple graph of order n?*

Lemma 9.1.10. **[Hand shaking lemma]** *In any graph (simple) 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 $\sum_{v\in V} d(v)$. Hence, $\sum_{v\in V} d(v) = 2|E|$. Note that

$$2|E| = \sum_{v\in V} d(v) = \sum_{v:d(v) \text{ is odd}} d(v) + \sum_{v:d(v) \text{ is even}} d(v)$$

Since $\sum_{v:d(v) \text{ is even}} d(v)$ is even, the above implies that $\sum_{v:d(v) \text{ is even}} d(v)$ must be even as well. Therefore, the number of vertices of odd degree is even. ∎

QUIZ **9.1.11.** *In a party of 27 persons, prove that someone must have an even number of friends assuming that friendship is mutual.*

Example 9.1.12. The graph in Figure 9.5 is called the **Petersen graph**. We shall use it as an example in many places.

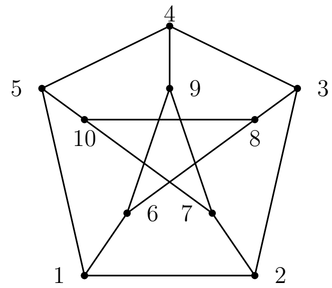


Figure 9.5: Petersen graphs

Proposition 9.1.13. *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. First, suppose G has exactly one isolated vertex. Then, the remaining $n-1$ vertices have degrees between 1 and $n-2$ and hence by PHP, the result follows. Otherwise, G has no isolated vertex. Then G has n vertices whose degrees lie between 1 and $n-1$. Again by PHP, we get the required result. ∎

EXERCISE **9.1.14.**

1. *Let $G = (V, E)$ 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 $G = (V, E)$ be a graph having exactly two vertices, say u and v, of odd degree. Then, prove that there is a path in G connecting u and v.*

Definition 9.1.15. Let $G = (V, E)$ be a graph. Then,

1. the **minimum degree** of a vertex in G is denoted by $\delta(G)$ and the **maximum degree** of a vertex in G is denoted by $\Delta(G)$.
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 9.1.16.

1. The cycle graph C_n is 2-regular whereas the complete graph K_n is $(n-1)$-regular.
2. The Petersen graph and the complete graph K_4 are cubic.
3. The graph P_4 is not regular.
4. Consider the graph G in Figure 9.2. We have $\delta(G) = 0$ and $\Delta(G) = 3$.

QUIZ **9.1.17.** *Can we have a cubic graph on 5 vertices?*

Definition 9.1.18. Let $G = (V(G), E(G))$ be a graph.

1. Then a graph H is a called a **subgraph** of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.
2. Then a subgraph H of G is called a **spanning subgraph** if $V(G) = V(H)$.
3. Then a k-regular spanning subgraph is called a **k-factor** of G.
4. If $U \subseteq V(G)$, then the **induced subgraph** of G on U is denoted by $\langle U \rangle = (U, E)$, where the edge set $E = \{\{u, v\} \in E(G) : u, v \in U\}$.

Example 9.1.19. 1. Consider the graph G in Figure 9.2.

(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 as $\{9, 10\} \notin E(G)$.

(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 as $\{8, 9\} \in E(G)$ but not in $E(H_2)$.

(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 **9.1.20.** *Consider K_8 on the vertex set $\{1, 2, \ldots, 8\}$. How many 1-factors does it have?*

Definition 9.1.21. Let $G = (V(G), E(G))$ be a graph.

1. If $v \in V(G)$ then the graph $G - v$, called the **vertex deleted subgraph**, is obtained from G by deleting v and all the edges that are incident with v.
2. If $e \in E(G)$, then the graph $G - e = (V, E(G) \setminus \{e\})$ is called the **edge deleted subgraph**.
3. 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**.
4. The **complement** $\overline{G}$ of a graph G is defined as $(V(G), E)$, where $E = \{uv : u \neq v, uv \notin E(G)\}$.

Example 9.1.22. 1. Consider the graph G in Figure 9.2. 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 $H_2 - 8 = \langle\{6, 7, 9, 10, 12\}\rangle$.

2. See Figure 9.6 for two examples of complement graphs.

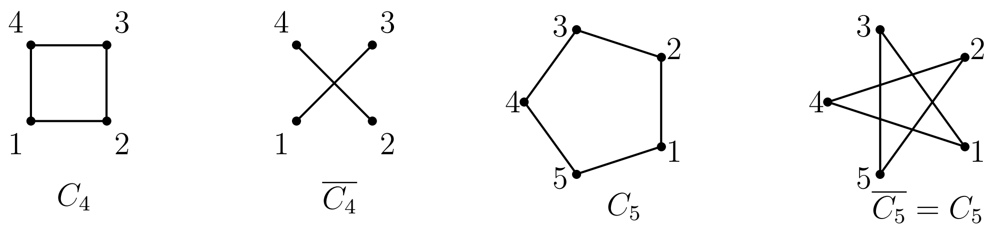


Figure 9.6: Complement graphs

3. The complement of K_3 contains 3 isolated points/vertices.
4. For any graph G, $\|G\| + \|\overline{G}\| = \binom{|G|}{2}$.
5. 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 **9.1.23.** 1. *Characterize graphs G such that $\Delta(G)+\Delta(\overline{G})=n-1$.*

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 9.1.24. Let $G=(V(G),E(G))$ and $H=(V(H),E(H))$ be two graphs.

1. Then their **intersection**, denoted $G\cap H$, is defined as $(V(G)\cap V(H),E(G)\cap E(H))$.
2. Then their **union**, denoted $G\cup H$, is defined as $(V(G)\cup V(H),E(G)\cup E(H))$.
3. Then their **disjoint union** is the union while treating the vertex sets as disjoint sets.
4. If $V(G)\cap V(H)=\varnothing$, then their **join**, denoted $G+H$ has $V(G)\cup V(H)$ as the vertex set and $E(G)\cup E(H)\cup\{uv : u\in V(G),\, v\in V(H)\}$ as the edge set.
5. Then their **Cartesian product**, denoted $G\times H$, has $V(G)\times V(H)$ as the vertex set and the edge set consists of all elements $\{(u,v),(u',v')\}$, where either $u=u'$ and $\{v,v'\}\in E(H)$, or $v=v'$ and $\{u,u'\}\in E(G)$.

Example 9.1.25. Two graphs G and H with their intersection $G\cap H$, their union $G\cup H$ and their disjoint union as G_1 are shown in Figure 9.7. Further, the join of K_2+K_3 and $\overline{K_2}+\overline{K_2}$ are also given. Note that $K_2+K_3=K_5$ and $\overline{K}_2+\overline{K}_2=C_4$.

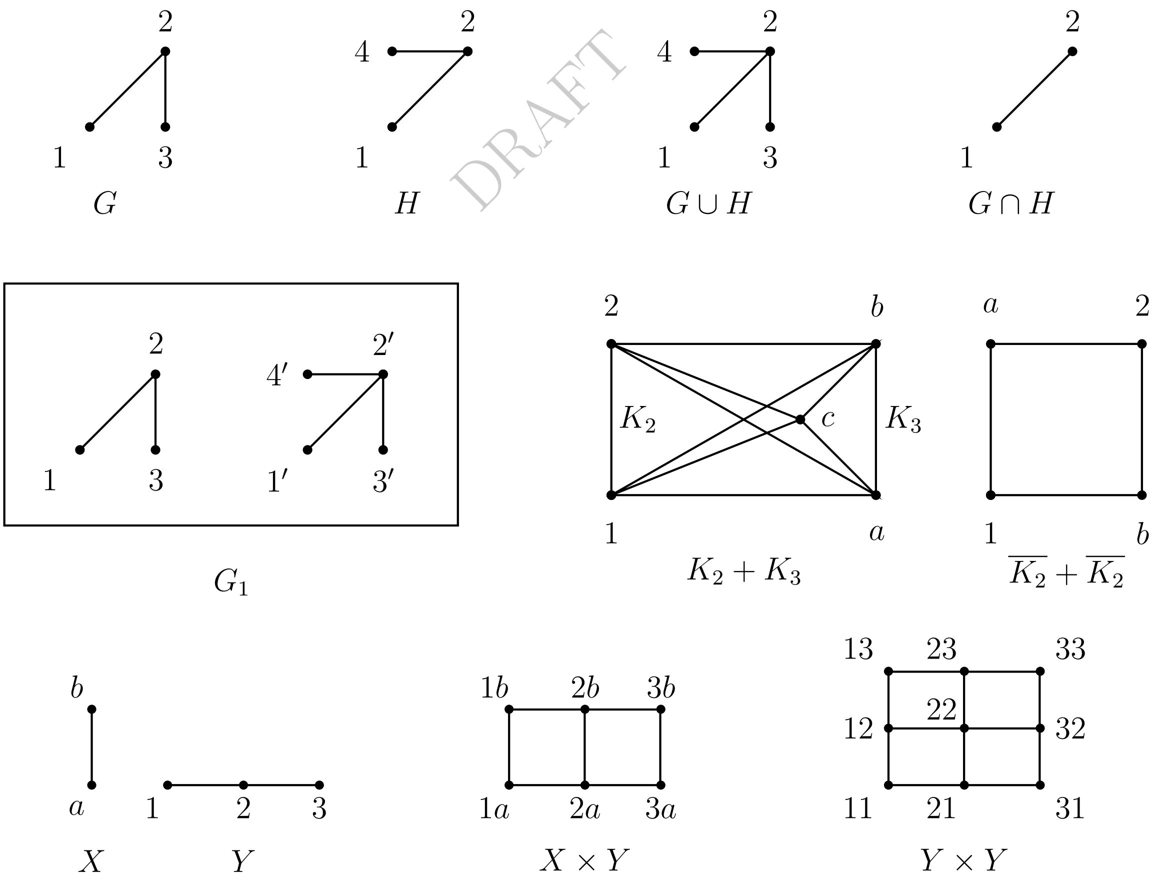


Figure 9.7: Examples of graph constructions (see Definition 9.1.24)

Quiz **9.1.26.** 1. *What is the complement of the disjoint union of $\overline{G}$ and $\overline{H}$?*

2. *Is $K_{m,n}=\overline{K}_m+\overline{K}_n$?*

9.2 Connectedness

Definition 9.2.1. Let $G = (V, E)$ be a graph and let $u, v \in V$.

1. A *u*-*v* **walk** in G is a finite sequence of vertices $[u = v_1, v_2, \cdots, v_{k-1}, v_k = v]$ such that $v_i v_{i+1} \in E$, for all $i = 1, \cdots, k-1$.
2. The **length** of a walk is the number of edges on it.
3. A walk is called a **trail** if edges on the walk are not repeated.
4. A u-v walk is a called a **path** if the vertices involved are all distinct, except that u and v can be the same.
5. If P is a 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**.
6. A walk (trail, path) is called **closed** if $u = v$.
7. The **length** of a path is the number of edges on it. A path can have length 0.
8. 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 cut-vertex).

Example 9.2.2. 1. Take $G = K_5$ with vertex set $\{1, 2, 3, 4, 5\}$.

(a) Then $[1, 2, 3, 2, 1, 2, 5, 4, 3]$ is an 8 walk in G and $[1, 2, 2, 1]$ is not a walk.

(b) The walk $[1, 2, 3, 4, 5, 2, 4, 1]$ is a closed trail.

(c) The walk $[1, 2, 3, 5, 4, 1]$ is a closed path, *i.e.*, it is a 5-cycle.

(d) The maximum length of a cycle in G is 5 and the minimum length of a cycle in G is 3.

(e) The number of 3-cycles in G is $\binom{5}{3} = 10$.

(f) Verify that the number of 4-cycles in G is not $\binom{5}{4}$. Can it be $3 \times \binom{5}{4}$?

2. Let G be the Petersen graph. Then, G has a 9-cycle, namely, $[6, 8, 10, 5, 4, 3, 2, 7, 9, 6]$. But, G has no 10-cycles. We shall see this when we discuss the Hamiltonian graphs.

Proposition 9.2.3. *Let u and v be distinct vertices in a graph G. Let $W = [u = u_1, \ldots, u_k = v]$ be a walk. Then W contains a 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 a u-v walk but of shorter length. Thus, using induction on the length of the walk, the desired result follows. ∎

Definition 9.2.4. Let $G = (V, E)$ be a graph.

1. The **distance** $d(u, v)$ between two vertices $u, v \in V, u \neq v$ is the shortest length of a u-v path in G. If no such path exists, the distance is taken to be ∞.
2. The greatest distance between any two vertices in a graph G is called the **diameter** of G, and is denoted by $\mathsf{diam}(G)$.
3. Let $dist_v = \max\limits_{u \in V} d(v, u)$. The **radius** is the $\min\limits_{v \in V} dist_v$ and the **center** is the set of all vertices v for which $dist_v$ is the radius.
4. 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 9.2.5. The Petersen graph has diameter 2, radius 2 and each vertex is in the center. Further, its girth is 5.

Exercise **9.2.6.** *1. Determine the diameter, radius, center and girth of the following graphs: P_n, C_n, K_n and $K_{n,m}$.*

2. Let G be a graph. Then, show that the distance function $d(u,v)$ is a metric on $V(G)$. That is, it satisfies

(a) $d(u,v) \geq 0$ for all $u, v \in V(G)$ and $d(u,v) = 0$ if and only if $u = v$,

(b) $d(u,v) = d(v,u)$ for all $u, v \in V(G)$ and

(c) $d(u,v) \leq d(u,w) + d(w,u)$ for all $u, v, w \in V(G)$.

Proposition 9.2.7. *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. Choose $i \geq 2$ such that v_i is adjacent to v_k. Then, $[v_i, v_{i+1}, \ldots, v_k, v_i]$ is a cycle. ■

Proposition 9.2.8. *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 v_1v_2. There must be an alive edge v_2v_3; otherwise, v_2 is incident to just one alive edge and some dead edges so that v_2 has received more signal than it has sent. Similarly, get 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 $E(H) \neq \varnothing$, 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 9.2.7, H has a cycle. ■

Proposition 9.2.9. *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 9.2.8, 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 9.2.10. Let $C = [v_1, \ldots, v_k = v_1]$ be a cycle in a graph G. An edge v_iv_j in G is called a **chord** of C if it is not an edge of C. G is called **chordal** if each cycle of length at least 4 has a chord. G is **acyclic** if it has no cycles.

For example, complete graphs are chordal, so are the acyclic graphs. The Petersen graph is not chordal.

Quiz **9.2.11.** *1. How many acyclic graphs are there on the vertex set $\{1, 2, 3\}$?*

2. How many chordal graphs are there on the vertex set $\{1, 2, 3, 4\}$?

Definition 9.2.12. 1. A graph G is said to be a **maximal** graph with respect to a property P if G has property P and no proper supergraph of G has the property P. The term **minimal** graph is defined similarly.

> Notice!
>
> The class of all graphs with that property is the poset here. So, the maximality and the minimality are defined naturally.

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 a 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 9.2.13. Consider the graph G shown in Figure 9.2.

1. Some cliques in G are $\langle\{8, 10\}\rangle$, $\langle\{2\}\rangle$. The first is a maximal clique. 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 **9.2.14.** *What is $\omega(G)$ for the Petersen graph?*

Proposition 9.2.15. *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. So, let i be the smallest positive integer such that v_i is adjacent to v_k. Then

$$\delta(G) \leq d(v_k) \leq |\{v_i, v_{i+1}, \cdots, v_{k-1}\}|.$$

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 9.2.16. The **edge density**, denoted $\varepsilon(G)$, is defined to be the number $\frac{|E(G)|}{|V(G)|}$.

QUIZ **9.2.17.** *1. When does the deletion of a vertex reduces its edge density?*

2. Is $\frac{\delta(G)}{2}$ a lower bound for $\varepsilon(G)$?

3. Suppose that $\varepsilon(G) \geq \delta(G)$. Should we have a vertex $v \in V(G)$ with $\varepsilon(G) \geq d(v)$?

Proposition 9.2.18. *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 $H = G$. Otherwise, there exists $v \in V(G)$ with $\varepsilon(G) \geq d(v)$. Put $G_1 = G - v$. Then, using $\varepsilon(G) \geq d(v)$, we have $\varepsilon(G_1) = \frac{\|G_1\|}{n-1} = \varepsilon(G) + \frac{\varepsilon(G) - d(v)}{n-1} \geq \varepsilon(G)$.

If $\varepsilon(G_1) < \delta(G_1)$, then $H = G_1$. Otherwise, there exists $u \in V(G_1)$ with $\varepsilon(G_1) \geq d(u)$. Put $G_2 = G_1 - u$. Again, we 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 increasing." 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. ∎

9.3 Isomorphism in graphs

Definition 9.3.1. 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 9.3.2. Consider the graphs in Figure 9.8. We observe the following:

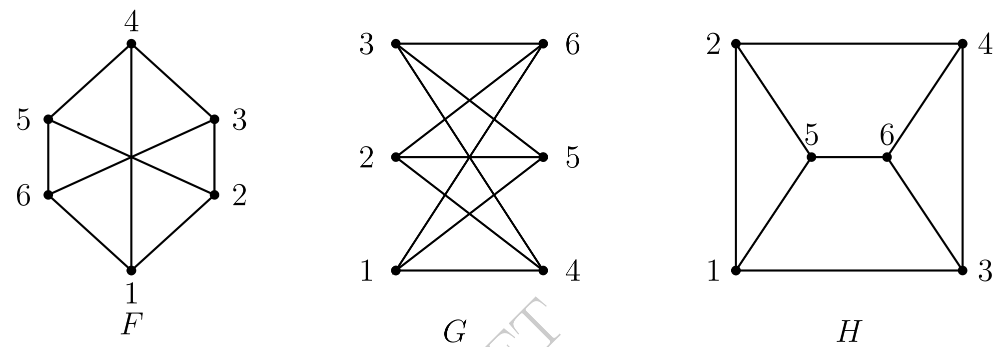


Figure 9.8: $F \cong G$ but $F \ncong H$

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 have a 3-cycle.
2. 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. So, $F \cong G$.

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 9.3.3. **[Isomorphism]** Let F and G be isomorphic under $f : V(F) \to V(G)$. 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 **9.3.4.** *Take the graphs F and G of Figure 9.8. 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 9.3.3. List $V(F')$ and $E(F')$. List $V(G)$ and $E(G)$. Notice that they are the same.*

Definition 9.3.5. A graph G is called **self-complementary** if $G \cong \overline{G}$.

Example 9.3.6. Let G be a self-complementary graph on n vertices. Then $\|G\| = n(n-1)/4$ as $\|G\| = \|\overline{G}\|$ and there are $\binom{n}{2}$ edges in the complete graph. Thus, either $n = 4k$ or $n = 4k+1$. Now, verify the following:

1. The path $P_4 = [0, 1, 2, 3]$ is self complimentary. An isomorphism from P_4 to $\overline{P}_4$ 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 C_5 to $\overline{C}_5$ is described by $f(i) = 2i \pmod 5$.

Exercise **9.3.7.** *1. Construct a self-complementary graph of order* $4k$.

2. Construct a self-complementary graph of order $4k+1$.

Definition 9.3.8. A **graph invariant** is a function which assigns the same value (output) to isomorphic graphs.

Observe that some of the graph invariants are: $|G|$, $\|G\|$, $\Delta(G)$, $\delta(G)$, $\omega(G)$, $\alpha(G)$, $\varepsilon(G)$, and the multiset $\{d(v) : v \in V(G)\}$.

Exercise **9.3.9.** *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 9.3.10. *Let G and H be graphs and let $f : G \to H$ be an isomorphism. For any $v \in V(G)$, $G - v \cong H - f(v)$.*

Proof. Consider the bijection $g : V(G-v) \to V(H - f(v))$ described by $g = f_{V(G-v)}$. ■

Definition 9.3.11. An isomorphism of G to G is called an **automorphism**.

Example 9.3.12.
1. The identity map, denoted $\mathbf{e}$ 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 9.3.13. *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 with $\mathbf{e}$ as the identity element.*

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 9.3.14. Determine $\Gamma(C_5)$.

Ans: Consider $C_5 = [1, \ldots, 5, 1]$. Note that $\sigma = (2, 3, 4, 5, 1)$ is an automorphism. Hence, $\{\mathbf{e}, \sigma, \sigma^2, \ldots, \sigma^4\} \subseteq \Gamma(C_5)$ as $\sigma^5 = \mathbf{e}$.

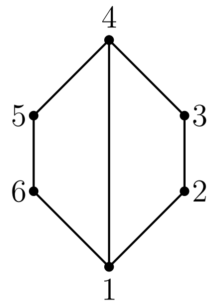
Now, let μ be an automorphism with $\mu(1) = i$. Put $\tau = \sigma^{6-i}\mu$. Then, τ is an automorphism with $\tau(1) = 1$. If $\tau(2) = 2$, then the adjacency structure implies that $\tau(j) = j$ for $j = 3, 4, 5$. In this case, $\sigma^{6-i}\mu = \mathbf{e}$; consequently, $\mu = \sigma^{i-6} = \sigma^{i-1}$.

If $\tau(2) \neq 2$, then $\tau(2) = 5$ as 1 is adjacent only to the vertices 2 and 5. In this case, verify that $\tau(3) = 4$ and hence $\tau = (2, 5)(3, 4)$ 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.

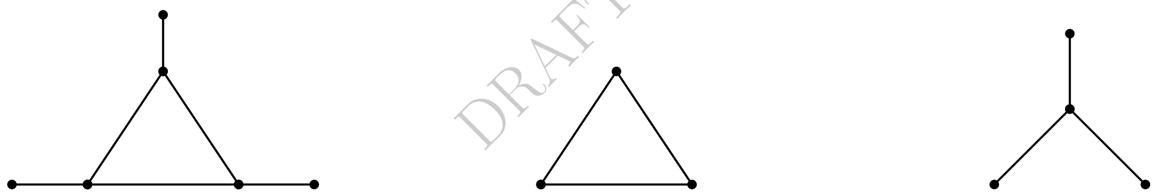
Example 9.3.15. Notice that $\Gamma(C_5)$ has a subgroup $\Gamma_1 = \{\mathbf{e}, \sigma, \sigma^2, \sigma^3, \sigma^4\}$, with $\sigma^5 = \mathbf{e}$, of order 5. Let G be a subgraph of C_5 obtained by deleting some (zero allowed) edges. If $\|G\| = 5$, then $|\Gamma(G)| = 10$. If $\|G\| = 0$, then $|\Gamma(G)| = |S_5| = 5!$. 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 **9.3.16.**

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 $\Gamma(H)$.*
4. *List the automorphisms of the following graph.*



5. *Determine the automorphism groups of the following graph. Are the three groups isomorphic?*



9.4 Trees

Definition 9.4.1. 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.

Theorem 9.4.2. *Let G be a connected graph with $|G| \geq 2$ and let $v \in V(G)$.*

1. *If $d(v) = 1$, then $G - v$ is connected, so that v is never a cut-vertex.*
2. *If $G - v$ is connected, then either $d(v) = 1$ or v is on a cycle.*

Proof. 1. Let $u, w \in V(G - v)$, $u \neq w$. As G is connected, there is a 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.

2. Assume that $G - v$ is connected. If $d_G(v) = 1$, then there is nothing to prove. 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 **9.4.3.** *Let G be a graph and v be a vertex on a cycle. Can $G - v$ be disconnected?*

Definition 9.4.4. 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 9.4.5. *Let G be connected and let $e = uv$ 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 $w \in V(G)$. Since G is connected, there is a path, say P, from w to u. Moreover, either P contains v as its internal vertex or P does not 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. ■

Theorem 9.4.6. *Let G be a graph and let e be an edge. Then, e is a cut-edge if and only if e is not on a cycle.*

Proof. Suppose that $e = uv$ is a cut-edge of G. Let F be the component of G that contains e. Then, by Proposition 9.4.5, $F - e$ 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 $e = uv$. Then $[v = v_1, \ldots, v_k = u]$ is a u-v path in $F - e$. Hence, $F - e$ is still connected. A contradiction. Thus, e cannot be on any cycle.

Conversely, let $e = uv$ 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 a 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. ■

EXERCISE **9.4.7.** *Let G be a graph on $n > 2$ vertices. If $\|G\| > \binom{n-1}{2}$, is G necessarily connected? Give an 'if and only if' condition for the connectedness of a graph with exactly $\binom{n-1}{2}$ edges.*

Definition 9.4.8. A connected acyclic graph is called a **tree**. A **forest** is a graph whose components are trees.

Thus, any acyclic graph is a forest and any component of it is a tree.

Proposition 9.4.9. *A tree on n vertices has $n - 1$ edges.*

Proof. We apply strong induction on n. 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 $\|T\| = \|T_1\| + \|T_2\| + 1 = n_1 - 1 + n_2 - 1 + 1 = n_1 + n_2 - 1 = n - 1$. ■

Corollary 9.4.10. *A tree with at least two vertices has at least two pendant vertices.*

Proof. Let T be any tree on $n \geq 2$ vertices. Then $\sum\limits_{v\in V(T)} d(v) = 2\|E(T)\| = 2(n - 1) = 2n - 2$. By PHP, T has at least two vertices of degree 1. ■

Theorem 9.4.11. *Let G be a graph with n vertices. Then the following are equivalent:*

1. *G is a tree.*

2. *G is a maximal acyclic graph.*
3. *G is a minimal connected graph.*
4. *G is acyclic and it has $n-1$ edges.*
5. *G is connected and it has $n-1$ edges.*
6. *Between any two distinct vertices of G there exists a unique path.*

Proof. (1)$\Leftrightarrow$(2). Let G be a tree. On the contrary, suppose that G is not maximal acyclic. Then there exist $u, v \in V(G)$ such that $G + uv$ is acyclic. If in G, there exists a u-v path, then $G + uv$ would have a cycle containing the edge uv. So, in G, there is no u-v path. It contradicts the assumption that G is a tree and hence connected.

Conversely, suppose that G is maximal acyclic. If G is not a tree, then G has at least two components. Let u and v be two vertices from different components, so that there exists no u-v path in G. Thus $G + uv$ has no cycle. This contradicts the assumption that G is maximal acyclic.

(1)$\Leftrightarrow$(3). Let G be a tree. Then G is connected. Let $e = uv$ be an edge of G. By (2), e is the only u-v path. Then $G - e$ is disconnected. Hence G is minimal connected.

Conversely, suppose G is minimal connected. If G is not a tree, then there is a cycle in G. Let u, v be two adjacent vertices on such a cycle. Now, $G - uv$ is still connected. It contradicts the assumption that G is minimal connected.

(1)$\Leftrightarrow$(4). Let G be a tree. Then G is acyclic, and By Proposition 9.4.9, G has $n-1$ edges.

Conversely, let G by acyclic and G has $n-1$ edges. If possible, let G be disconnected. Then G has components $G_1, \ldots, G_k, k \geq 2$. As G is acyclic, each G_i is a tree on, say $n_i \geq 1$ vertices, with $\sum\limits_{i=1}^{k} n_i = n$. As $k \geq 2$, we have $\|G\| = \sum\limits_{i=1}^{k}(n_i - 1) = n - k < n - 1 = \|G\|$, a contradiction.

(1)$\Leftrightarrow$(5). Let G be a tree. Then G is connected, and By Proposition 9.4.9, G has $n-1$ edges.

Conversely, assume that G is connected and G has $n-1$ edges. On the contrary, suppose that G is not a tree. Then G has a cycle. Select an edge e from the cycle. Notice 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 9.4.9, $\|H\| = n - 1$. But, in the above argument, we have deleted at least one edge and hence, $\|G\| \geq n$. This gives a contradiction to $\|G\| = n - 1$.

(1)$\Leftrightarrow$(6). Let G be a tree. Since G is connected, between any two distinct vertices of G there exists a path. If there exist more than one path between $u, v \in V(G)$, then by Proposition 9.2.8 any two of these u-v paths will contain a cycle. This is not possible as G is acyclic. Hence the uniqueness of such a path.

Conversely, let (6) hold. Then G is clearly connected. Further, if G has a cycle, then that cycle would provide two paths between any two vertices on the cycle. Hence G is acyclic, *i.e.*, G is a tree. ∎

Proposition 9.4.12. *The center of a tree is either a singleton or has 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.

On the contrary, 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 $\|P(x,w)\| < \|P(x,u)\| \le k$. Thus in either case, 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 **9.4.13.** *Draw a tree on 8 vertices. Label $V(T)$ as $1,\ldots,8$ so that each vertex $i \ge 2$ is adjacent to exactly one element of $\{1,2,\ldots,i-1\}$.*

Proposition 9.4.14. *Let T be a tree on n vertices. Let G be a graph with $\delta(G) \ge n-1$. Then G has a subgraph H with $H \cong T$.*

Proof. We prove the result by induction on n. 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 $\delta(G) \ge n-1$.

Due to Corollary 9.4.10, 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, $\delta(G) \ge n-1 > n-2$. 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 $\delta(G) \ge n-1$, 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. ■

Definition 9.4.15. 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 9.4.16. For example, Consider the tree T in Figure 9.9.

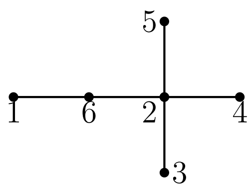


Figure 9.9: A tree T on 6 vertices

Then, the above process proceeds as follows.

Exercise **9.4.17.** *In the above process, prove that $u_j = i$, for some j, if and only if $d(i) \ge 2$.*

Example 9.4.18. Can I get back the original tree T from the Prüfer code $2,2,2,6$?

Answer: 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.

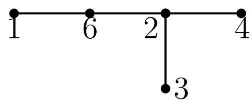
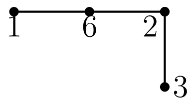
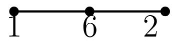
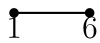
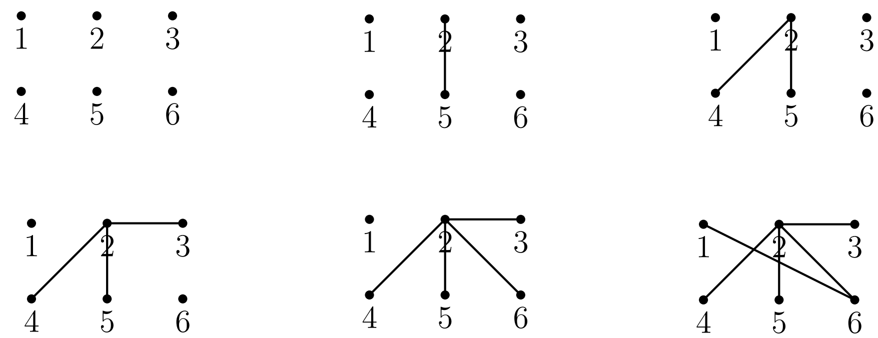
Step	**Pendant $\mathbf{v_i}$**	**Neighbor $\mathbf{u_i}$**	$\mathbf{P_T = X(1), X(2), \ldots}$	$\mathbf{T_i = T - v_i}$
1	5	2	2	
2	4	2	2,2	
3	3	2	2,2,2	
4	2	6	2,2,2,6	

Figure 9.10: A tree T on 6 vertices

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 9.4.19. *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, at 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 the 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 **9.4.20.** *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 9.4.21. *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 $|T| < n$. 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 9.4.22. *Let S be a set of $n \geq 3$ integers and let 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 $P_{T'} = X'$.

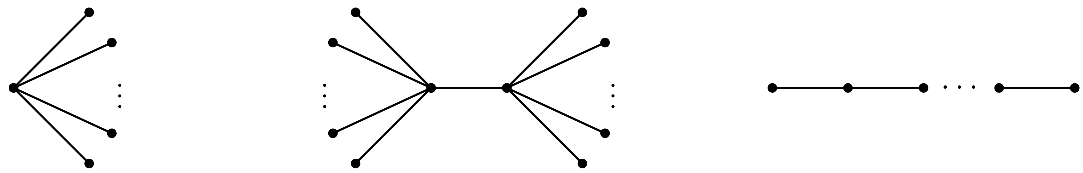
Let T be the tree obtained by adding a new pendant v at the vertex $X(1)$ of T'. In T', the vertices $X(i)$, for $i \geq 2$, were not available as pendants and now in T the vertex $X(1)$ is also not available as a pendant (here some $X(i)$'s may be the same). Let $R' = \{x \in S' \,:\, x \notin X'\}$ 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 9.4.23. [**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 by $f(T) = P_T$, the Prüfer code, is a one-one and onto mapping. As $|G| = n^{n-2}$, the required result follows. ∎

Exercise **9.4.24.**

1. *Find out all non-isomorphic trees of order* 6 *or less.*
2. *Count with diameter: how many non-isomorphic trees are there of order* 7*?*
3. *Show that every automorphism of a tree fixes a vertex or an edge.*
4. *Give a class of trees T with $|\Gamma(T)| = 6$.*
5. *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 $uv \in E(T)$ such that $\sigma(u) = v$?*
6. *Let T be a tree with center $\{u\}$ and radius r. Let v satisfy $d(u, v) = r$. Show that $d(v) = 1$.*
7. *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'.*
8. *Let T be a tree with center $\{u\}$ and $\sigma \in \Gamma(T)$. Show that $\sigma(u) = u$.*
9. *Is it possible to have a tree such that $|\Gamma(T)| = 7$?*
10. *Construct a tree T on vertices $S = \{1, 2, 3, 6, 7, 8, 9\}$ for which $P_T = 6, 3, 7, 1, 2$.*
11. *Draw the tree on the vertex set $\{1, 2, \ldots, 12\}$ whose Prüfer code is* 9954449795.
12. *Practice with examples: get the Prüfer code from a tree; get the tree from a given code and a vertex set.*



13. *How many trees of the following forms are there on the vertex set* $\{1, 2, \ldots, 100\}$*?*
14. *Show that any tree has at least* $\Delta(T)$ *leaves (pendant edges).*
15. *Let* T *be a tree and* T_1, T_2, T_3 *be subtrees of* T *such that* $T_1 \cap T_3 \neq \varnothing$, $T_2 \cap T_3 \neq \varnothing$ *and* $T_1 \cap T_2 \cap T_3 = \varnothing$. *Show that* $T_1 \cap T_2 = \varnothing$.
16. *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*?*
17. *A connected graph* G *is said to be* **unicyclic** *if* G *has exactly one cycle as its subgraph. Prove that if* G *is connected and* $|G| = \|G\|$, *then* G *is a unicyclic graph.*

9.5 Eulerian graphs

Definition 9.5.1. 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 of Königsberg (the present day Kaliningrad) is divided into 4 land masses by the river Pregolya. These land masses are joined by 7 bridges (see Figure 9.11). 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 9.11 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".

Theorem 9.5.2. **[Euler,** 1736] *A connected graph is Eulerian if and only if each vertex in the graph is of even degree.*

Proof. Let G be a connected graph. Suppose G has an Eulerian tour, say $W = [v_0, v_1, \ldots, v_k, v_0]$. Observe that whenever we arrive at a vertex $v \neq v_0$ 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 appears r times in the tour. Also, if v_0 appears r times in the tour then $d(v_0) = 2(r-1)$. Hence, $d(v)$ is always even.

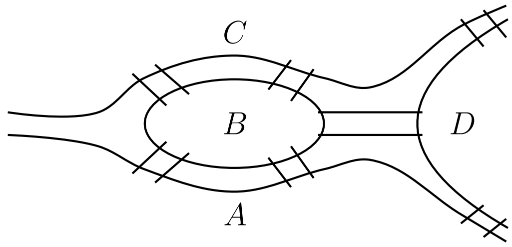


Figure 9.11: Königsberg bridge problem

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 tour compared to W, a contradiction. Thus, there is no edge lying outside W and hence W is an Eulerian tour. ∎

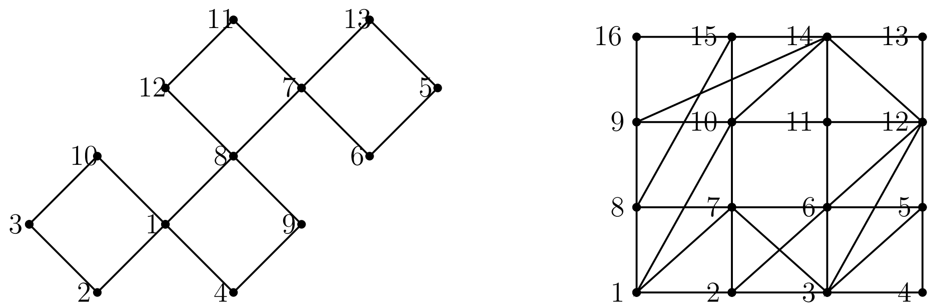
Proposition 9.5.3. *Let G be a connected graph with exactly two vertices of odd degree. Then, there is an Eulerian walk starting at one of those vertices and ending at the other.*

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 9.5.2, 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 **9.5.4.** *Let G be an Eulerian graph and let 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 **9.5.5.** *Find Eulerian tours for the following graphs.*



Theorem 9.5.6. **[Finding Eulerian tour]** *The previous algorithm correctly gives an Eulerian tour provided 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 non-trivial 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, $C - uv + v_0 v$ is a connected graph with each vertex of even degree. So, by Theorem 9.5.2, the graph $C - uv + v_0 v$ 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 9.5.2, 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 **9.5.7.** *1. Apply the algorithm to graphs of Exercise 9.5.5. Also, create connected graphs, where each vertex is of even degree, and apply the above algorithm.*

2. *Give a necessary and sufficient condition on m and n so that $K_{m,n}$ is Eulerian.*

3. *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?

4. *Prove: A connected graph G is Eulerian if and only if the $E(G)$ can be partitioned into cycles.*

9.6 Hamiltonian graphs

Definition 9.6.1. let G be a graph. 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 9.6.2. 1. For each positive integer $n \geq 3$, the cycle C_n is Hamiltonian.

2. The graphs corresponding to all platonic solids are Hamiltonian.

3. The Petersen graph is a non-Hamiltonian Graph (the proof appears below).

Proposition 9.6.3. *The Petersen graph is not Hamiltonian.*

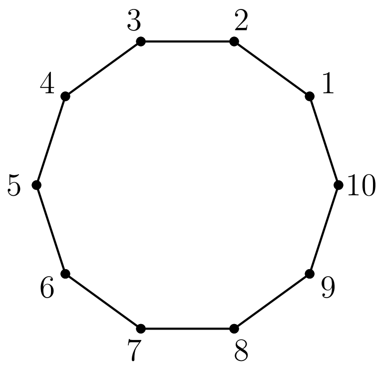


Figure 9.12: A Hamiltonian graph

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 9.6.4. *Let G be a Hamiltonian graph. Then, for $S \subseteq V(G)$ with $S \neq \varnothing$, 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 9.6.5. [**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. We first show that G is connected. If possible, let 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 $v \in V(G)$. Therefore, G is connected.

Now, let $P = [v_1, v_2, \cdots, v_k]$ be a longest path in G. Since P is a 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 a path of longest length, a contradiction. Thus, the required result follows. ∎

A slight relaxation on the sufficient condition of a graph to be Hamiltonian is provided by the following result. We expect the reader to prove it.

Theorem 9.6.6. [**Ore,** 1960] *Let G be a graph on $n \geq 3$ vertices such that $d(u) + d(v) \geq n$ for every pair of non-adjacent vertices u and v. Then G is Hamiltonian.*

Lemma 9.6.7. *Let u and v be two non-adjacent vertices of a graph G such that $d(u) + d(v) \geq |G|$. Then G is Hamiltonian if and only if $G + uv$ is Hamiltonian.*

Proof. If G is Hamiltonian, then so is $G+uv$. Conversely, suppose that $G+uv$ is Hamiltonian. If $G+uv$ has a Hamiltonian cycle not using uv, then G is Hamiltonian. Otherwise, let $[u = v_1, \ldots v_n = v, u]$ be a Hamiltonian cycle in $G + uv$. Then, the path $[v_1, \ldots, v_n]$ is available in G. Now proceeding as in the proof of Dirac's theorem, as $d(v_1) + d(v_n) \geq n$, we see that there must exist an i such that $v_1 \sim v_i$ and $v_n \sim v_{i-1}$. Then the cycle $[v_1, v_i, v_{i+1}, \ldots, v_n, v_{i-1}, v_{i-2}, \ldots, v_1]$ is a Hamiltonian cycle in G. ■

Discussion 9.6.8. [**Closure**] Let G be a graph on n vertices, $n \geq 2$. Suppose we perform the following operation(s) on G.

Step 1: If G has two nonadjacent vertices $u \neq v$ such that $d(u) + d(v) \geq n$, then add the edge (u, v) in G and treating the resulting graph as G, repeat Step 1, until the graph has no nonadjacent vertices $u \neq v$ satisfying $d(u) + d(v) \geq n$.

Step 2: If G has no nonadjacent vertices $u \neq v$ such that $d(u) + d(v) \geq n$, then stop.

For example, let G be the trivial graph on 10 vertices (G has no edge). Then, the application of the above operation stops with the trivial graph itself. Whereas, if G is the graph obtained from K_{10} by deleting the edges $\{1, 2\}$ and $\{3, 4\}$, then applying the above operation gives K_{10} as the result.

Notice that in the above example, one might have added the edge $\{1, 2\}$ first and then the edge $\{3, 4\}$ whereas some one else might have added $\{3, 4\}$ first and then $\{1, 2\}$. However, they both get the same end result. We prove this for any graph G. Before that, note that, if G is any graph on n vertices, then the above operation can add at most a finitely many edges as the end result has to be a subgraph of K_n.

Proposition 9.6.9. *Let G be a graph on n vertices. Suppose the application of the operations described in Discussion 9.6.8 to G by following two different sequences of edge additions gives K and F as the end results. Then $K = F$.*

Proof. Let K and F be obtained by sequentially adding edges

$$(e\text{-list}) \qquad e_1 = u_1v_1, \ldots, e_k = u_kv_k \qquad \text{and} \qquad (f\text{-list}) \qquad f_1 = x_1y_1, \ldots, f_r = x_ry_r,$$

respectively, to G in that order.

Assume that $K \neq F$. Then, without loss of generality, suppose an edge has been added in the e-list which doesn't appear in the f-list. Let e_i be the first such edge in the e-list which does not appear in the f-list. Put $H = G + e_1 + \cdots + e_{i-1}$. As $e_1, \ldots, e_{i-1}$ are in the f-list, we see that H is a subgraph of F.

Furthermore, taking $e_i = \{u, v\}$, as e_i was the next to be added in the e-list, it follows that $d_H(u) + d_H(v) \geq n$. But as H is a subgraph of F, we see that $d_F(u) + d_F(v) \geq n$ too.

This means that F is not the end result, because in an end result there are no nonadjacent vertices $u \neq v$ with sum of degrees at least n. This is a contradiction. ■

Let G be a graph. The graph obtained as the end result of applying the operation described in Discussion 9.6.8, is called the **closure of** G, denoted $C(G)$. (It is obtained by repeatedly choosing pairs of non-adjacent vertices u, v such that $d(u) + d(v) \geq |G|$ and adding edges between them until no such pair of vertices exist.) Proposition 9.6.9 tells us that for any graph G, $C(G)$ is unique.

Corollary 9.6.10. *Let G be a graph. Then G is Hamiltonian if and only if $C(G)$ is Hamiltonian. In particular, if $C(G)$ is Hamiltonian, then G is Hamiltonian.*

Proof. Follows from Lemma 9.6.7. ■

QUIZ **9.6.11.** *Let G be a graph on $n \geq 3$ vertices. If G has a cut-vertex, then prove that $C(G) \neq K_n$.*

Theorem 9.6.12. *Let $d_1 \le \cdots \le d_n$ be the vertex degrees of G which satisfy the property*

$$R : \text{If } d_k \le k \text{ then } d_{n-k} \ge n-k \text{ for each } k < n/2.$$

Then 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 $d_H(u) + d_H(v) \le n-1$. 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 $d_H(v) \ge d_H(u) = k$ (say). As $d_H(u) + d_H(v) \le n-1$, we get $k < n/2$.

Now, let $S_v = \{x \in V(H) : x \ne v, xv \notin E(H)\}$ and $S_u = \{w \in V(H) : w \ne u, wu \notin E(H)\}$. 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 ($S_u \cup \{u\}$) 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 **9.6.13.** *Let $d_1 \le \cdots \le d_n$ be the vertex degrees of G which satisfy the property R (see Theorem 9.6.12). Then show that $C(G)$ also has property R.*

Definition 9.6.14. 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 9.6.15. 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 $\Delta(G)$.

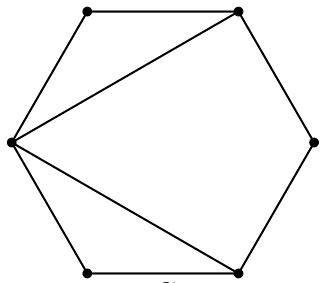
Exercise **9.6.16.**
1. *Let G be a connected Eulerian graph. Show that the line graph of G is Hamiltonian. Is the converse true?*
2. *What can you say about the clique number of a line graph?*

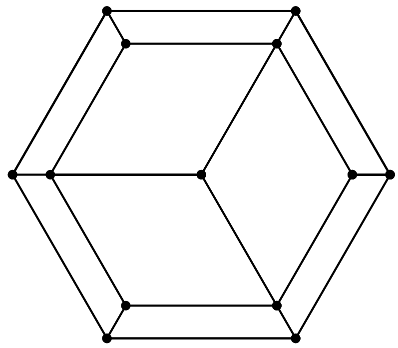
Theorem 9.6.17. *A connected graph G is isomorphic to its line graph if and only if $G = C_n$ for some $n \ge 3$.*

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 **9.6.18.**
1. *Consider the graphs shown below.*
   (a) *Determine the closure of G.*





(b) Show that H is not Hamiltonian.

2. *Give a necessary and sufficient condition on $m, n \in \mathbf{N}$ so that $K_{m,n}$ is Hamiltonian.*
3. *Show that any graph with at least 3 vertices and atleast $\binom{n-1}{2} + 2$ edges is Hamiltonian.*
4. *Show that for any $n \geq 3$ there is a graph H with $\|G\| = \binom{n-1}{2} + 1$ that is not Hamiltonian. But, prove that all such graphs H admit a Hamiltonian path (a path containing all vertices of H).*

9.7 Bipartite graphs

Definition 9.7.1. A graph is said to be 2-**colorable** if its vertices can be colored with two colors in a way that adjacent vertices get different colors.

Example 9.7.2. Prove the following results.

1. Every tree is 2-colorable.
2. Every cycle of even length is 2-colorable.
3. The complete bipartite graphs, namely $K_{m,n}$, are 2-colorable
4. Petersen graph is not 2-colorable but 3-colorable.

Lemma 9.7.3. *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 9.7.4. *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. (1)⇒(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.

(2)⇒(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.

(2)⇒(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.

(3)⇒(2). Suppose that G does not have an odd cycle. Pick any vertex v. Define

$$\begin{aligned} V_1 &= \{w : \text{ there is a walk of even length from } v \text{ to } w\} \\ V_2 &= \{w : \text{ there is a walk of odd length from } v \text{ to } w\}. \end{aligned}$$

Clearly, $v \in V_1$. Also, G does not have an odd cycle implies that $V_1 \cap V_2 = \varnothing$ (use Lemma 9.7.3). As G is connected each w is either in V_1 or in V_2.

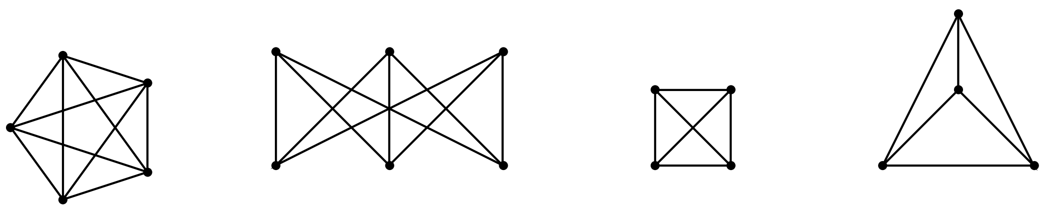
Let $x \in V_1$. Then, there is an even path $P(v, x)$ from v to x. If $xy \in E(G)$, then we have a v-y walk of odd length. Deleting all cycles from this walk, we have an odd v-y path. Thus, $y \in V_2$. Similarly, if $x \in V_2$ and $xy \in E$, then $y \in V_1$. Thus, G is bipartite with parts V_1, V_2. ∎

Exercise **9.7.5.**

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 the statements in Example 9.7.2.*
4. *Let G and H be two bipartite graphs. Prove that $G \times H$ is also a bipartite graph.*

9.8 Planar graphs

Definition 9.8.1. A graph is said to be **embedded** on a surface S when it is drawn on S so that no two edges intersect. A **plane graph** is a graph drawn on the plane where no two edges intersect. A graph is said to be **planar** if it can be embedded on the plane.



K_5-Non-planar $K_{3,3}$-Non-planar K_4 K_4 - Planar embedding

Figure 9.13: Planar and non-planar graphs

Example 9.8.2.

1. A tree is embeddable on a plane..
2. Any cycle C_n, $n \geq 3$ is planar.
3. The planar embedding of K_4 is given in Figure 9.13.
4. Draw a planar embedding of $K_{2,3}$.
5. Draw a planar embedding of the edges of a 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 9.8.3. 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 9.14).

Example 9.8.4. Consider the following planar embedding of the graphs X_1 and X_2.

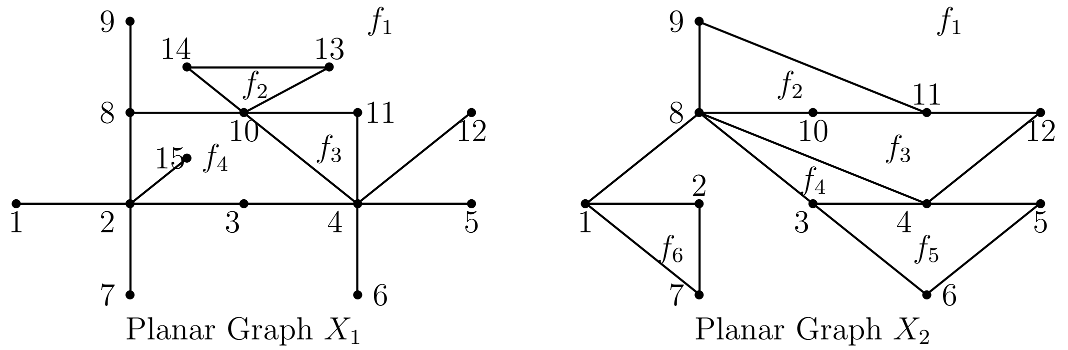


Figure 9.14: Planar graphs with labeled faces to understand the Euler's theorem

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.
3. Any planar embedding of a tree has only one face, the exterior face.
4. Any planar embedding of a cycle has two faces.

From the table, we observe that each edge of X_1 appears in two faces. This is easily seen for the faces that do not 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. Notice 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 stated next.

Theorem 9.8.5. [**Euler Formula**] *Let G be a connected plane graph with f number of faces. Then*

$$|G| - \|G\| + f = 2. \tag{9.1}$$

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 $|G| - \|G\| + f = n - (n-1) + 1 = 2$.

Assume that Equation (9.1) is true for all plane connected graphs having $2 \leq f < n$. Let G be a connected planar graph with $f = n$. Choose an edge that is not a cut-edge, say e. Then, $G - e$ is still a connected graph. Notice that the edge e is incident with two separate faces. So, its removal will combine the two faces, and hence $G - e$ has only $n - 1$ faces. Thus, using the induction hypothesis

$$|G| - \|G\| + f = |G - e| - (\|G - e\| + 1) + n = |G - e| - \|G - e\| + (n - 1) = 2.$$

Hence the required result follows. ■

Lemma 9.8.6. *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 $2\|G\| \geq 4f \Leftrightarrow \|G\| \geq 2f$.*

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 9.8.7. *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 (9.1), $f = 7$. But, by Lemma 9.8.6, 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 9.8.6, one has $18 = 2\|G\| \geq 4f = 20$, a contradiction. ■

Definition 9.8.8. 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, the paths P_n and P_m are homeomorphic for all $m, n \in \mathbf{N}$. Similarly, all the cyclic graphs are homeomorphic to the cycle C_3. (We are considering only simple graphs. In general, one can say that all cyclic graphs are homeomorphic to the graph $G = (V, E)$, where $V = \{v\}$ and $E = \{\{v, v\}\}$. It is a graph having exactly one vertex and a loop). Also, note that if two graphs are isomorphic then they are also homeomorphic. Figure 9.15 gives examples of homeomorphic graphs that are different from a path or a cycle.

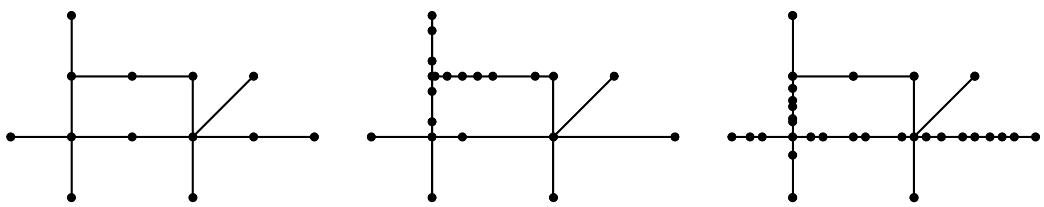


Figure 9.15: Homeomorphic graphs

The following result characterizes planar graphs via homeomorphisms, which we do not prove.

Theorem 9.8.9. [**Kuratowski,** 1930] *A graph is planar if and only if it has no subgraph homeomorphic to K_5 or $K_{3,3}$.*

We have the following observations that directly follow from Kuratowski's theorem.

Remark 9.8.10. 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 9.8.11. Let G be a graph. Define a relation on the edges of G by $e_1 \simeq e_2$ 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.

The following result, which we do not prove, characterizes planar graphs via blocks.

Proposition 9.8.12. *A graph G is planar if and only if each of its blocks are planar.*

Definition 9.8.13. A graph is called **maximal planar** if it is planar and addition of any more edges results in a non-planar graph.

Notice that a maximal planar graph is necessarily connected.

Proposition 9.8.14. *If G is a maximal planar graph with at least 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 **9.8.15.**

1. *Prove/disprove: A two colorable graph is necessarily planar.*
2. *Suppose that G is a plane graph such that each face is a 4-cycle. What is the number of edges in G?*
3. *Show that the Petersen graph has a subgraph homeomorphic to $K_{3,3}$.*
4. *Show that a plane graph with at least 3 vertices can have at most $2|G| - 5$ bounded faces.*
5. *Let G be a plane graph with f faces and k components. Prove that $|G| - \|G\| + f = k + 1$ (use induction).*
6. *If G is a plane graph without 3-cycles, then show that $\delta(G) \leq 3$.*
7. *Is it necessary that a plane graph G should contain a vertex of degree less than 5?*
8. *Show that any plane graph with at least 4 vertices has a vertex of degree at most five.*
9. *Show that any plane graph with at least 4 vertices has at least four vertices of degree at most 5.*
10. *Produce a planar embedding of the graph G given in Figure 9.16.*

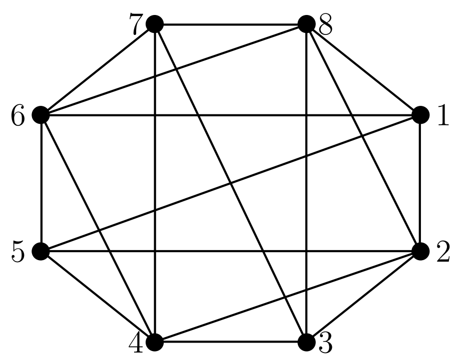


Figure 9.16: A graph on 8 vertices

9.9 Vertex coloring

Definition 9.9.1. 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 **9.9.2.** *Every connected bipartite graph on* ≥ 2 *vertices has chromatic number* 2.

Theorem 9.9.3. *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, labeled $1, 2, \ldots, n+1$. 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. ■

In this connection we state the following result without proof.

Theorem 9.9.4. [**Brooks,** 1941] *If* G *is a graph which is neither complete nor an odd cycle, then* $\chi(G) \leq \Delta(G)$.

Theorem 9.9.5. [**5-Color Theorem**] *Every Planar graph is* 5*-colorable.*

Proof. Let G be a minimal planar graph on n vertices and m edges, such that G is not 5-colorable. Then, $n \geq 6$, and by Proposition 9.8.14, $m \leq 3n - 6$. So, $n\,\delta(G) \leq 2m \leq 6n - 12$ and hence, $\delta(G) \leq 2m/n \leq 5$. Let v be a vertex such that $d(v) \leq 5$. 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. ■

Chapter 10

Graphs - II

10.1 Connectivity

Proposition 10.1.1. *Let G be a connected graph on the 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 cases $G - k$ is connected. Now, use the induction hypothesis to get the required result. ∎

Definition 10.1.2. 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 10.1.3.

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.

Recall that a graph is said to be a non-trivial graph if it has at least one edge.

Definition 10.1.4. 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** of a non-trivial graph G, denoted by $\kappa(G)$, is the largest k such that G is k-connected. Convention: $\kappa(K_1) = 0$.

Example 10.1.5.

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 10.1 is 2-connected but not 3-connected. Thus, $\kappa(G) = 2$.

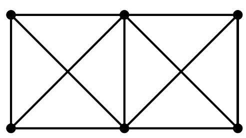


Figure 10.1: graph with vertex connectivity 2

5. The Petersen graph is 3-connected.

Definition 10.1.6. A graph G is called **ℓ-edge connected** if $|G| > 1$ and $G - F$ is connected for every $F \subseteq E(G)$ with $|F| < \ell$. 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 10.1.7.
1. Note that $\lambda(P_n) = 1, \lambda(C_n) = 2$ and $\lambda(K_n) = n - 1$ for $n > 1$.
2. Let T be a tree on $n \geq 2$ vertices. Then, $\lambda(T) = 1$.
3. For the graph G in Figure 10.1, $\lambda(G) = 3$.
4. For the Petersen graph G, $\lambda(G) = 3$.

EXERCISE **10.1.8.** *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 10.1.9. **[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 a 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 **10.1.10.** *Give a lower bound on the number of edges of a graph G on n vertices with vertex connectivity $\kappa(G) = k$.*

In this connection, we state the following result without proof.

Theorem 10.1.11. **[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 $\delta(G) = c$.*

Theorem 10.1.12. **[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

$$\begin{aligned} n &= |G| \geq \Delta(G) \geq 4k \geq 2k - 1, && (10.1)\\ m &= \|G\| \geq \frac{1}{2}(\text{average degree } \times n) \geq 2kn \geq (2k-3)(n-k+1)+1. && (10.2)\end{aligned}$$

We use induction to show that if G satisfies Equations (10.1) and (10.2), 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 $\frac{n(n-1)}{2}$ many edges and hence $G = K_n$. Thus $K_{k+1} \subseteq K_n = G$.

Assume $n \geq 2k$ and Equations (10.1) and (10.2) hold for graphs having less than n vertices. If v is a vertex with $d(v) \leq 2k - 3$, then $G - v$ is a graph on $n - 1$ vertices and

$$\|G\| \geq (2k-3)(n-k+1) + 1 - (2k-3) = (2k-3)((n-1)-k+1)+1.$$

Hence, by the induction hypothesis $G - v$ has a k-connected subgraph.

So, let $d(v) \geq 2k-2$, for each vertex v. If G is k-connected then we have nothing to prove. Assume, on the contrary, that G is not k-connected. Then $G = G_1 \cup G_2$ with $|G_1 \cap G_2| < k$, $|G_1| < n$ and $|G_2| < n$. Thus each of $G_1 - V(G_2)$ and $G_2 - V(G_1)$ has at least one vertex, and there is no edge between those vertices 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,

$$|G_1| + |G_2| = |G_1 \cup G_2| + |G_1 \cap G_2| \leq n + (k-1) = n + k - 1. \tag{10.3}$$

If G_1 or G_2 satisfies Equation (10.2), using induction hypothesis, the result follows. Otherwise, $\|G_i\| \leq (2k-3)(|G_i| - k + 1)$, for $i = 1, 2$. Using Equation (10.3), we obtain

$$m = \|G\| \leq \|G_1\| + \|G_2\| \leq (2k-3)(|G_1| + |G_2| - 2k + 2) \leq (2k-3)(n-k+1),$$

a contradiction to Equation (10.2); and hence the required result follows. ■

The following characterization of k-connected graphs is often helpful.

Theorem 10.1.13. [**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.*

10.2 Matching in graphs

Definition 10.2.1. 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 10.2.2. 1. In Figure 10.2, $M_1 = \{u_1u_2\}$ is a matching. If e is any edge, then $M_2 = \{e\}$ is a matching. 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 maximum matching (why?). Can you give another maximum matching?

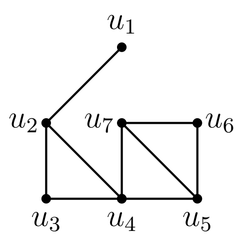


Figure 10.2: A graph

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 and u_7.
4. Any graph with a perfect matching must have even order as each edge saturates two vertices. So, the graph in Figure 10.2 cannot have a perfect matching.

Definition 10.2.3. 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 10.2.4. Consider the graph in Figure 10.2.

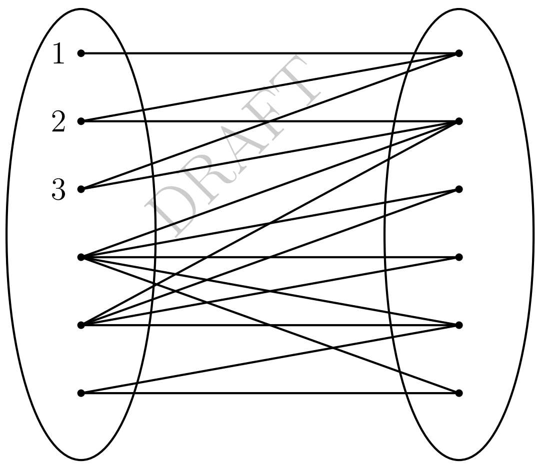
1. The path $[u_1, u_2]$ is M_1-alternating. The only path of length 2 which is M_1-alternating is $[u_1, u_2, u_3]$. Why is the path $[u_1, u_2, u_4]$ not M_1-alternating of length 2?
2. The path $[u_1, u_2, u_4, u_7]$ is not M_3-alternating. But, $[u_2, u_3, u_4, u_7]$ is M_3-alternating.
3. The path $P = [u_1, u_2, u_3, u_4, u_7, u_6]$ 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 10.2.5. **[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 **10.2.6.** *How do we find a maximum matching in a graph G.*

Example 10.2.7. 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.

Theorem 10.2.8. **[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 $|N(S)| \geq |S|$ for each $S \subseteq X$.*

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 $S \subseteq X$. If possible, let 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 $N(\{x, x_1\})$. As $|N(\{x, x_1\})| \geq |\{x, x_1\}|$ and M^* does not saturate x, $N(\{x, x_1\})$ 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 10.2.9. *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 partitions of $V(G)$. 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 10.2.10. Let G be a graph. Then a subset S of $V(G)$ 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 **10.2.11.** *1. Can there be a graph in which the size of a minimum covering is $|G|$?*

2. Show that for any graph G the size of a minimum covering is $n - \alpha(G)$.

3. Characterize G in terms of its girth if the size of a minimum covering is $|G| - 2$.

Proposition 10.2.12. *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 $|M^*| > |M|$. 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 **10.2.13.** *Let $G = K_n$, $n \geq 3$. Then, determine*

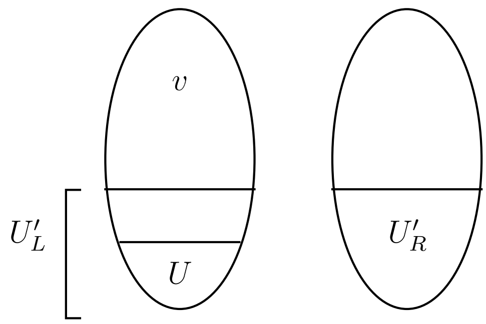
1. the cardinality of a maximum matching?

2. the cardinality of a minimum covering?

Is the converse of Proposition 10.2.12 necessarily true? Can you guess the class of graphs for which the converse of Proposition 10.2.12 is true?

Theorem 10.2.14. **[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 (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 on 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 $u \in U$ 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 $w \in R \setminus U'_R$, 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 10.2.12. ■

Alternate. 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 by M. 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 10.2.12, we get $|K| = |M|$. Furthermore, by Proposition 10.2.12, we also see that K is a minimum covering. ■

Exercise **10.2.15.** 1. *How many perfect matchings are there in a labeled K_{2n}?*

2. *Characterize G if the size of a minimum covering is $|G| - 1$.*

10.3 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 as follows:

Any graph with at least 6 vertices has either K_3 or $\overline{K}_3$ as its subgraph.

Definition 10.3.1. 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 its subgraph.

Example 10.3.2. As C_5 does not have K_3 or $\overline{K}_3$ as its 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 [6] for a table).

Proposition 10.3.3. *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 $d(a) \leq 4$. 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 non-adjacent 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 **10.3.4.** 1. *Can you draw a graph on 8 vertices*

(a) *which does not have $K_3, \overline{K}_4$ in it?*

(b) *which does not have $K_4, \overline{K}_3$ in it?*

2. *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 10.3.5. **[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 $\overline{K}_n$). ∎

EXERCISE **10.3.6.** *Is it true that in any group of 7 persons there are 3 mutual friends or 4 mutual strangers?*

10.4 Degree sequence

Definition 10.4.1. 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 increasing sequence $d = (d_1, \ldots, d_n)$ of non-negative integers is **graphic** if there is a graph whose degree sequence is d.

Example 10.4.2. Show that $(1, 1, 3, 3)$ is not graphic.

Ans: Let the vertices be $\{u, v, w, x\}$. If $d(u) = d(v) = 3$, then $u \sim v, w, x$ and $v \sim u, w, x$. Thus, $d(w) \geq 2$ and $d(x) \geq 2$.

Theorem 10.4.3. *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 $\sum d_i = 2n - 2$.* *Consider $n \geq 5$. Then you can decompose the path on n vertices as union of K_2 and C_{n-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 10.4.4. **[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 $d_{i_1} \le d_{i_2} \le \cdots \le d_{i_k}$. If $d_{i_1} \ge d_v$ 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

$$\sum_{v \in N_{G'}(n)} d_v \ge \sum_{u \in N_G(n)} d_u. \tag{10.4}$$

As, $v_0 \not\sim n$, the vertex v_0 has a neighbor $v \ne i_1$ with $v \not\sim i_1$ as $d_{i_1} < d_{v_0}$. Now, consider the graph $G' = G - \{v_0, v\} + \{n, v_0\} + \{i_1, v\} - \{i_1, n\}$. Then, G' also has d as its degree sequence with $N_{G'}(n) = \{v_0, i_2, \ldots, i_k\}$. Thus, (10.4) 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 **10.4.5.**

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.*
2. *For each of the degree sequences given below, draw the graph; or else, argue why it is not graphic.*
   (a) $(2,2,3,4,4,5)$
   (b) $(1,2,2,3,3,4)$
   (c) $(2,2,3,3,3,3,3,3,4,4)$
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?*

10.5 Representing graphs with matrices

Definition 10.5.1. Let $G = (V, E)$ be a simple (undirected) graph on vertices $1, \ldots, n$. Then the $n \times n$ matrix, called the **adjacency matrix** $A(G)$ of G (or simply A), is defined by

$$A(G) = [a_{ij}], \quad a_{ij} = \begin{cases} 1 & \text{if } \{i,j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Let H be the graph obtained by relabeling the vertices of G. Then $A(H) = S^{-1}A(G)S$, 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 ignore possible labeling of the vertices of G.

Example 10.5.2. 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 **10.5.3.**

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 $A(G) = P^t A(H) P$ for some permutation matrix P.*

Theorem 10.5.4. *The (i,j)th entry of $B = A(G)^k$ is the number of i-j walks of length k in G.*

Proof. Write $A(G) = [a_{ij}]$ and $B = [b_{ij}]$. Then $B = A(G)^k$ implies that

$$b_{ij} = \sum_{i_1,\ldots,i_{k-1}} a_{ii_1} a_{i_1 i_2} \cdots a_{i_{k-1} i_k}.$$

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 10.5.5. *Let G be a graph of order n. Then, G is connected if and only if all entries of $\big[I + A(G)\big]^{n-1}$ are positive.*

Proof. Write $B = I + A$. 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 $n-1$. Therefore, G is connected. ■

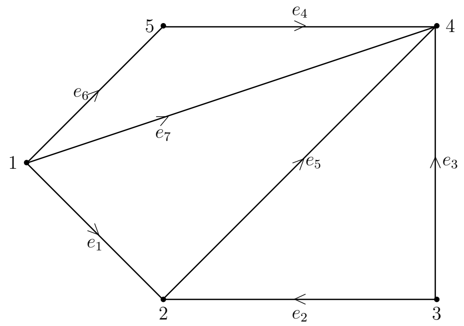
Exercise **10.5.6.** *Let G be a graph with adjacency matrix A. Prove the following:*

1. *The eigenvalues of A are all real.*
2. *The eigenvectors of A can be chosen to form an orthonormal basis of $\mathbb{R}^n$.*
3. *Each rational eigenvalue of A is an integer.*
4. *If $G = K_n$, then $A = J - I$, where J is the matrix with each entry 1.*
5. *If $G = K_n$, then the eigenvalues of A are $n-1$ with multiplicity 1, and -1 with multiplicity $n-1$.*
6. *Let $\overline{G}$ be the complement graph of G. Then, $A(\overline{G}) = J - I - A$.*
7. *If G is k-regular then the following are true:*
   (a) *k is an eigenvalue of A.*
   (b) *$n-k-1$ is an eigenvalue of $\overline{G}$.*
   (c) *If $\lambda \neq k$ is an eigenvalue of A, then $-1-\lambda$ is an eigenvalue of $A(\overline{G})$.*
8. *If G is bipartite then there exists a permutation matrix P such that $B = P^t A P = \begin{bmatrix} \mathbf{0} & B_1 \\ B_1^t & \mathbf{0} \end{bmatrix}$. Further, prove that λ is an eigenvalue of A if and only if $-\lambda$ is an eigenvalue of A.*

Definition 10.5.7. 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)th entry is given 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 10.5.8. Consider the graph given below.



It has $V(G) = \{1, 2, 3, 4, 5\}$ and $E(G) = \{e_1, e_2, \ldots, e_7\}$. Its incidence matrix is

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 \end{bmatrix}.$$

Exercise **10.5.9.** *Let G be a graph on n vertices and m edges. Prove the following:*

1. $Q^tQ = diag(d_1, d_2, \ldots, d_n) - A$, *where* $diag(d_1, d_2, \ldots, d_n)$ *is the diagonal matrix with* d_i*s as the degrees of* n *vertices.*
2. $QQ^t = 2I - A(L(G))$, *where* $A(L(G))$ *is the adjacency matrix of the line graph* $L(G)$ *of* G.
3. *If* $\mathbf{e}$ *is the vector with each component as* 1, *then* $Q^t\mathbf{e} = \mathbf{0}$.
4. *If* G *is connected, then* $rank(Q) = n - 1$.
5. *Any square submatrix of* Q *is unimodular; that is, the determinant of any square submatrix of* Q *is either* -1 *or* 0 *or* 1.

Chapter 11

Polya Theory*

In Section 5.5, we have already studied ideas and problems related with circular permutations. In this chapter, we would like to generalize the ideas in that section to a more general setting. This will help us to get answers to the following type of questions:

1. How many different necklace configurations are possible if we use 6 beads of 3 different colors? Or for that matter what if we use n beads of m different colors?
2. How many different necklace configurations are possible if we use 12 beads among which 3 are *red*, 5 are *blue* and 4 are *green*? And a generalization of this problem?

Observe that if we want to look at different color configurations of a necklace formed using 6 beads, we need to understand the symmetries, not just the circular rotations, of a hexagon. Such a study is achieved through what in literature is called *groups*. Once we have learnt a bit about groups, we study *group action*. This study helps us in defining an equivalence relation on the set of color configurations for a given necklace. And it turns out that the number of distinct color configurations is same as the number of equivalence classes.

11.1 Groups

Before coming to the definition and its properties, let us look at the properties of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. We know that the set S, which may be $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, satisfies the following:

Binary operation: For all $a, b \in S,\ a + b$, called the addition of a and b, is an element of S.

Addition is associative: For all $a, b, c \in S,\ (a + b) + c = a + (b + c)$.

Additive identity: S contains an element, called zero, denoted 0, so that for each $a \in S,\ a + 0 = a = 0 + a$.

Additive inverse: For every element $a \in S$, there exists an element $-a \in S$ such that $a + (-a) = 0 = -a + a$.

Addition is commutative: For all $a, b \in S,\ a + b = b + a$.

Write $S^* = S \setminus \{0\}$. Correspondingly, we write $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}, \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. As in the previous case, we see that similar statements hold true for S^* with respect to the multiplication operation, with one exception. They are as follows:

Binary operation: For all $a, b \in S^*,\ a \cdot b$, called the multiplication of a and b, is an element of S^*.

Multiplication is associative: For all $a, b, c \in S^*$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Multiplicative identity: S^* contains an element, called a unit element, or one, denoted 1, is such that for each $a \in S^*$, $a \cdot 1 = a = 1 \cdot a$.

Multiplication is commutative: For all $a, b \in S^*$, $a \cdot b = b \cdot a$.

Observe that if we choose $a \in \mathbb{Z}^*$ with $a \neq 1, -1$, then there does not exist an element $b \in \mathbb{Z}^*$ such that $a \cdot b = 1 = b \cdot a$. Whereas, for the sets $\mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ one can always find a b such that $a \cdot b = 1 = b \cdot a$.

Based on the above examples, an abstract notion called a *group* is defined. Formally, one defines a group as follows.

Definition 11.1.1. Let G be a nonempty set and let $*$ be a binary operation on G. The pair $(G, *)$ is called a **group** if the following are satisfied:

1. For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$. (*Associativity Property* holds in G.)
2. There exists $\mathbf{e} \in G$ such that for each $a \in G$, $a * \mathbf{e} = a = \mathbf{e} * a$. (*Existence of Identity* in G.)
3. For each $a \in G$, there exists $b \in G$ such that $a * b = \mathbf{e} = b * a$. (*Existence of Inverse* in G.)

In addition, if the statement "For all $a, b \in G$ $a * b = b * a$" is true, then the group $(G, *)$ is called an **an abelian (commutative)** group.

Observe that once $*$ is a binary operation on G, it is assumed that for each pair of elements $a, b \in G$, the element $a * b$ is also an element of G.

When $(G, *)$ is a group, we say informally that G is a group with the operation as $*$. For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are groups with the binary operation as addition. Also, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are groups with the binary operation as multiplication. In general, if the binary operation $*$ is understood from the context, we say that G is a group; and write ab instead of $a * b$ when $a, b \in G$.

Before proceeding with examples of groups that concerns us, we state a few basic results in group theory in the following remark. Those may be proved without much difficulty.

Remark 11.1.2. Let $(G, *)$ be a group. Then the following hold:

1. The identity element of G is unique. Hence, keeping a definite notation such as $\mathbf{e}$ for the identity element is meaningful.
2. Corresponding to any $a \in G$, the element $b \in G$ that satisfies $a * b = \mathbf{e} = b * a$ is unique. So, we denote such a b by a^{-1}, and call it the inverse of a.
3. $\mathbf{e}^{-1} = \mathbf{e}$.
4. For each $a \in G$, $(a^{-1})^{-1} = a$.
5. If $a * b = a * c$ for some $a, b, c \in G$, then $b = c$. Similarly, if $b * d = c * d$ for some $b, c, d \in G$, then $b = c$. That is, the *cancellation laws* hold in G.
6. For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
7. By convention, we assume $a^0 = \mathbf{e}$ for each $a \in G$; and define $a^n = a^{n-1} \cdot a$ for $n \in \mathbb{N}$. Then $a^n = a \cdot a^{n-1}$.
8. For each $a \in G$, $(a^n)^{-1} = (a^{-1})^n$ for all $n \in \mathbb{W}$. We write both $(a^n)^{-1}$ and $(a^{-1})^n$ as a^{-n}.
9. Last two statements define a^m for each $a \in G$ and for each $m \in \mathbb{Z}$.

In the remaining part of this chapter, the binary operation may not be explicitly mentioned as it will be clear from the context. We now look at a few examples that will be used later in this chapter.

Example 11.1.3. **[Symmetric Group on n letters/symbols]** Write $N = \{1, 2, \ldots, n\}$. Recall that a bijection $f : N \to N$ is called a permutation on n elements. The set of all permutations on n elements is denoted by $\mathcal{S}_n$, *i.e.*,

$$\mathcal{S}_n = \{f : N \to N \mid f \text{ is one to one and onto}\}.$$

We observe the following:

1. Suppose $f, g, h \in \mathcal{S}_n$. Then $f, g, h : N \to N$ are one-to-one and onto functions.
   (a) Hence $f \circ g$, the composition of f and g, is also one-to-one and onto. Thus, $f \circ g \in \mathcal{S}_n$. So, "composition of functions", denoted $\circ$, defines a binary operation in $\mathcal{S}_n$.
   (b) It is well known that $\circ$ is an associative operation, *i.e.*, $(f \circ g) \circ h = f \circ (g \circ h)$.
   (c) The identity function $\mathbf{e} : N \to N$ defined by $\mathbf{e}(i) = i$ for all $i = 1, 2, \ldots, n$ is a one-to-one and onto function. Further, $f \circ \mathbf{e} = f = \mathbf{e} \circ f$ for all $f \in \mathcal{S}_n$. The permutation $\mathbf{e}$ is called the **identity** permutation.
   (d) As f is a one-to-one and onto function, $f^{-1} : N \to N$ defined by $f^{-1}(i) = j$, whenever $f(j) = i$, for all $i = 1, 2, \ldots, n$, is a one-one and onto function. So, for each $f \in \mathcal{S}_n$, $f^{-1} \in \mathcal{S}_n$ and $f \circ f^{-1} = \mathbf{e} = f^{-1} \circ f$.
2. Thus $(\mathcal{S}_n, \circ)$ is a group. This group is called the **Symmetric group** or the **Permutation group** on n letters/symbols.
3. **[Product of permutations]** Let $\sigma, \tau \in \mathcal{S}_n$. Then $\sigma \circ \tau$ (the composition of σ and τ) is popularly called the **product of σ and τ**. From now onwards, we will just use $\sigma\tau$ in place of $\sigma \circ \tau$, *i.e*, we will not use the symbol $\circ$ unless it becomes necessary for the sake of clarity.
4. If $\sigma \in \mathcal{S}_n$ then one represents this by writing $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$. This representation of an element of $\mathcal{S}_n$ is called a **two row notation**.
5. Since $\sigma : N \to N$ is one-to-one and onto, $\{\sigma(1), \sigma(2), \ldots, \sigma(n)\} = N$. Hence, there are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$ (all elements of N except $\sigma(1)$) and so on. Thus, $|\mathcal{S}_n| = n!$.

Before discussing other examples, let us try to understand the group $\mathcal{S}_n$. As seen above, any element $\sigma \in \mathcal{S}_n$ can be represented using a two-row notation. There is another notation for permutations that is often very useful. This notation is called the *cycle notation* which we define next.

Definition 11.1.4. Let $\sigma \in \mathcal{S}_n$ and let $S = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$. If σ satisfies

$$\sigma(i_\ell) = i_{\ell+1} \text{ for each } \ell = 1, 2, \ldots, k-1, \; \sigma(i_k) = i_1, \text{ and } \sigma(r) = r \text{ for } r \notin S$$

then σ is called a **k-cycle** and is denoted by $\sigma = (i_1, i_2, \ldots i_k)$ or $(i_2, i_3, \ldots, i_k, i_1)$ and so on.

Example 11.1.5.
1. The permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$ in cycle notation can be written as (1234), (2341), (3412), or (4123) as $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 1$ and $\sigma(5) = 5$.
2. The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$ in cycle notation equals $(123)(65)$ as $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$; $\sigma(4) = 4$; and $\sigma(5) = 6$, $\sigma(6) = 5$. That is, this element is formed with the help of two cycles (123) and (56).

3. Consider two permutations $\sigma = (143)(27)$ and $\tau = (1357)(246)$. Then, their product is obtained as follows:
   $(\sigma\tau)(1) = \sigma\big(\tau(1)\big) = \sigma(3) = 1,\ (\sigma\tau)(2) = \sigma\big(\tau(2)\big) = \sigma(4) = 3,\ (\sigma\tau)(3) = \sigma\big(\tau(3)\big) = \sigma(5) = 5, (\sigma\tau)(4) = \sigma\big(\tau(4)\big) = \sigma(6) = 6,\ \ (\sigma\circ\tau)(5) = 2,\ (\sigma\tau)(6) = 7$ and $(\sigma\tau)(7) = 4$. Hence
   $$\sigma\tau = (143)(27)(1357)(246) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 6 & 2 & 7 & 4 \end{pmatrix} = (235)(467).$$
4. Similarly, verify that $(1456)(152) = (16)(245)$.
5. Let $\sigma = (123)$ and $\tau = (56)$. Then, σ, τ can be thought of as elements of $\mathcal{S}_6$ with $\sigma(i) = i$ for $4 \le i \le 6$. Similarly, $\tau \in \mathcal{S}_6$ with $\tau(i) = i$ for $1 \le i \le 4$. Further, the permutation $(123)(56)$ is the product of σ and τ.
6. Note that the identity permutation $\mathbf{e} \in \mathcal{S}_n$ satisfies $\mathbf{e}(i) = i$ for $1 \le i \le n$. So, we sometimes write $\mathbf{e} = (1)(2)\cdots(n)$.

Definition 11.1.6. Two cycles $\sigma = (i_1, i_2, \ldots, i_t)$ and $\tau = (j_1, j_2, \ldots, j_s)$ are said to be **disjoint** if
$$\{i_1, i_2, \ldots, i_t\} \ \cap\ \{j_1, j_2, \ldots, j_s\} = \varnothing.$$

The proof of the following theorem can be obtained from any standard book on abstract algebra.

Theorem 11.1.7. [Permutation as product of disjoint cycles] *Let $\sigma \in \mathcal{S}_n$. Then σ can be written as a product of disjoint cycles.*

Remark 11.1.8. Observe that the representation of a permutation as a product of disjoint cycles, none of which is the identity, is unique up to the order of the disjoint cycles. The representation of an element $\sigma \in \mathcal{S}_n$ as product of disjoint cycles is called the *cyclic decomposition* of σ.

Example 11.1.9. 1. Symmetries of regular n-gons in plane.

(a) Let A be the square in the XY-plane with it's vertices labeled as $1, 2, 3$ and 4 and placed at the points $(0,1,0), (0,0,0), (1,0,0)$ and $(1,1,0)$, respectively. (Since each side of A measures to 1 unit, we say that A is a unit square.) Our aim is to move the square in space so that each vertex may change its place, but altogether, the vertices are placed at these points only. Verify that whichever way we move the square (using only such movements), the square is moved to one of the following configurations (see Figure 11.1):

Now, let $\mathbf{e}$ denote the initial position of A. Then, one can obtain the possible 8 positions (see Figure 11.1) by repeated application of either the counter-clockwise rotation of A by $90°$, denoted by r, or by flipping of A along the vertical axis passing through the midpoint of opposite horizontal edges, denoted by f. So, we have a set $G = \{\mathbf{e}, r, r^2, r^3, f, rf, r^2f, r^3f\}$ whose elements are functions that sends A to a particular configurations in Figure 11.1. Thus, with the composition of functions as the binary operation
$$G = \{\mathbf{e}, r, r^2, r^3, f, rf, r^2f, r^3f\} \ \text{ with relations } r^4 = \mathbf{e} = f^2 \ \text{ and } \ fr^3 = rf \qquad (11.1)$$
forms a group. Further, using (11.1), observe that $(rf)^2 = (rf)(rf) = r(fr)f = r(r^3f)f = r^4f^2 = \mathbf{e}$. Similarly, it can be checked that $(r^2f)^2 = (r^3f)^2 = \mathbf{e}$, *i.e.*, the elements f, rf, r^2f and r^3f are flips.

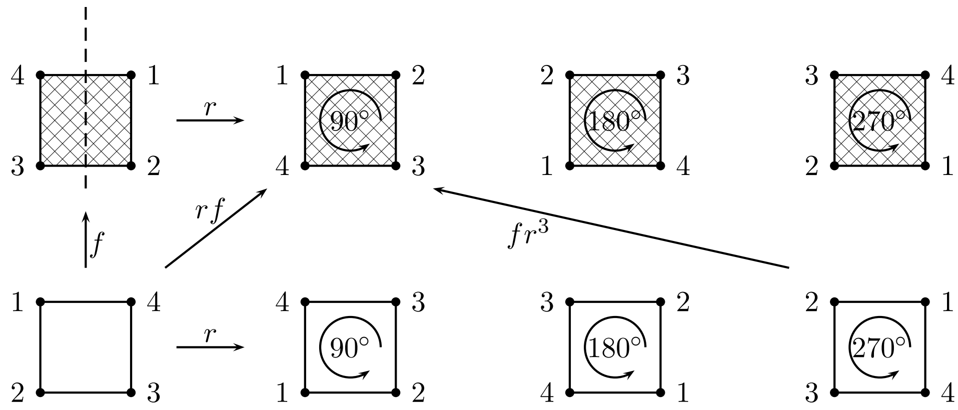


Figure 11.1: Symmetries of a square.

The group G is generally denoted by D_4 and is called the **Dihedral group** with 8 elements or the **symmetries of a square**. This group can also be represented by

$$H = \{e, (1234), (13)(24), (1432), (14)(23), (24), (12)(34), (13)\} \tag{11.2}$$

where the elements are obtained using the position of the vertices of the square in it's new position with respect to the position of vertices in A.

For another understanding, observe that if r and f in G are mapped to (1234) and $(14)(23)$, respectively, in H, then using the respective binary operations, the different elements of G and H can be identified. For example, rf is mapped to the product $(1234)(14)(23) = (24)$.

(b) In the same way, one can define the symmetries of an equilateral triangle (see Figure 11.2). This group is denoted by D_3 and is represented as

$$D_3 = \{\mathbf{e}, r, r^2, f, rf, r^2f\} \text{ with relations } r^3 = \mathbf{e} = f^2 \text{ and } fr^2 = rf, \tag{11.3}$$

where r is a counter-clockwise rotation by $120° = \dfrac{2\pi}{3}$ and f is a flip. Using Figure 11.2, one can check that the group D_3, consisting of 6 elements, can also be represented by

$$D_3 = \{\mathbf{e}, (ABC), (ACB), (BC), (CA), (AB)\}.$$

The readers should verify that $(ABC)^2 = (ABC)(ABC) = (ACB)$, $(ABC)^3 = \mathbf{e}$, $(AB)^2 = \mathbf{e}$, $(ABC)(AB) = (AC)$ and so on.

(c) For a regular pentagon, it can be verified that the group of symmetries of a regular pentagon is given by $G = \{\mathbf{e}, r, r^2, r^3, r^4, f, rf, r^2f, r^3f, r^4f\}$ with $r^5 = \mathbf{e} = f^2$ and $rf = fr^4$, where r denotes a counter-clockwise rotation through an angle of $72° = \dfrac{2\pi}{5}$ and f is a flip along a line that passes through a vertex and the midpoint of the opposite edge. Or equivalently, if we label the vertices of a regular pentagon, counter-clockwise, with the numbers $1, 2, 3, 4$ and 5 then

$$\begin{aligned} G &= \{\mathbf{e}, (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2), (2,5)(3,4), \\ &\qquad (1,3)(4,5), (1,5)(2,4), (1,2)(3,5), (1,4)(2,3)\}. \end{aligned}$$

(d) In general, one can define symmetries of a regular n-gon. This group is denoted by D_n, has $2n$ elements and is represented as

$$\{\mathbf{e}, r, r^2, \ldots, r^{n-1}, f, rf, \ldots, r^{n-1}f\} \text{ with } r^n = \mathbf{e} = f^2 \text{ and } fr^{n-1} = rf. \tag{11.4}$$

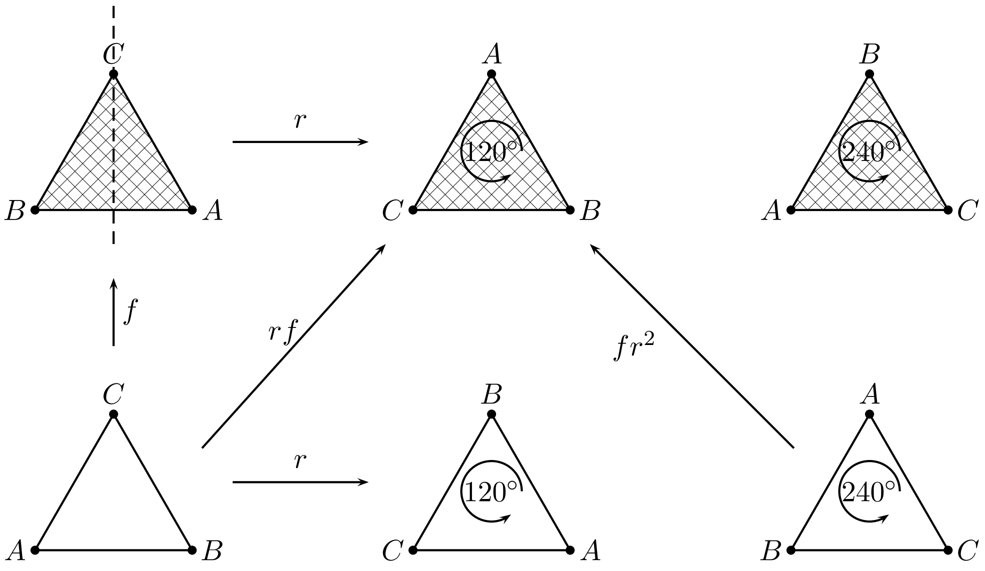


Figure 11.2: Symmetries of an Equilateral Triangle.

Here the symbol r stands for a counter-clockwise rotation through an angle of $\dfrac{2\pi}{n}$ and f stands for a vertical flip.

2. Symmetries of regular platonic solids.

   (a) Recall from geometry that a tetrahedron is a 3-dimensional regular object having 6 edges, 4 vertices and 4 faces, each face being an equilateral triangle (see Figure 11.1). If we denote the vertices of the tetrahedron with numbers $1, 2, 3$ and 4, then the symmetries of the tetrahedron is the following group:

$$T = \{\mathbf{e}, (234), (243), (124), (142), (123), (132), (134), (143), (12)(34), (13)(24), (14)(23)\},$$

   where, for distinct numbers i, j, k and ℓ, the element (ijk) is formed by a rotation of 120° along the line that passes through the vertex ℓ and the centroid of the equilateral triangle with vertices i, j and k. Similarly, the group element $(ij)(k\ell)$ is formed by a rotation of 180° along the line that passes through mid-points of the edges (ij) and $(k\ell)$.

   (b) Consider the Cube and the Octahedron given in Figure 11.3. It can be checked that the group of symmetries of the two figures has 24 elements. We give the group elements for the symmetries of the cube, when the vertices of the cube are labeled. The readers are required to compute the group elements for the symmetries of the octahedron. For the cube (see Figure 11.3), the group elements are

      i. $\mathbf{e}$, the identity element;

      ii. $3 \times 3 = 9$ elements that are obtained by rotations along lines that pass through the center of opposite faces (3 pairs of opposite faces and each face is a square: corresponds to a rotation of 90°). In terms of the vertices of the cube, the group elements are

$$(1234)(5678), (13)(24)(57)(68), (1432)(5876), (1265)(3784), (16)(25)(38)(47),$$
$$(1562)(3487), (1485)(2376), (18)(45)(27)(36), (1584)(2673).$$

      iii. $2 \times 4 = 8$ elements that are obtained by rotations along lines that pass through opposite vertices (4 pairs of opposite vertices and each vertex is incident with 3 edges:

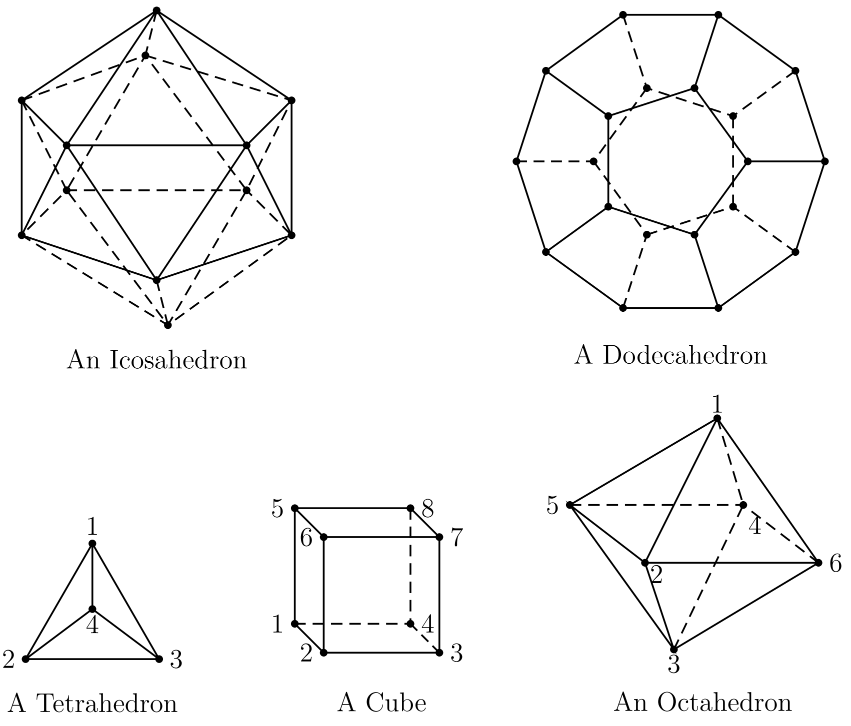


Figure 11.3: Regular Platonic solids.

corresponds to a rotation of 120°). The group elements in terms of the vertices of the cube are

$$(254)(368), (245)(386), (163)(457), (136)(475), (275)(138),$$
$$(257)(183), (168)(274), (186)(247).$$

iv. $1 \times 6 = 6$ elements that are obtained by rotations along lines that pass through the midpoint of opposite edges (6 pairs of opposite edges: corresponds to a rotation of 180°). The corresponding elements in terms of the vertices of the cube are

$$(14)(67)(28)(35), (23)(58)(17)(46), (15)(37)(28)(64), (26)(48)(17)(35),$$
$$(12)(78)(36)(45), (34)(56)(17)(28).$$

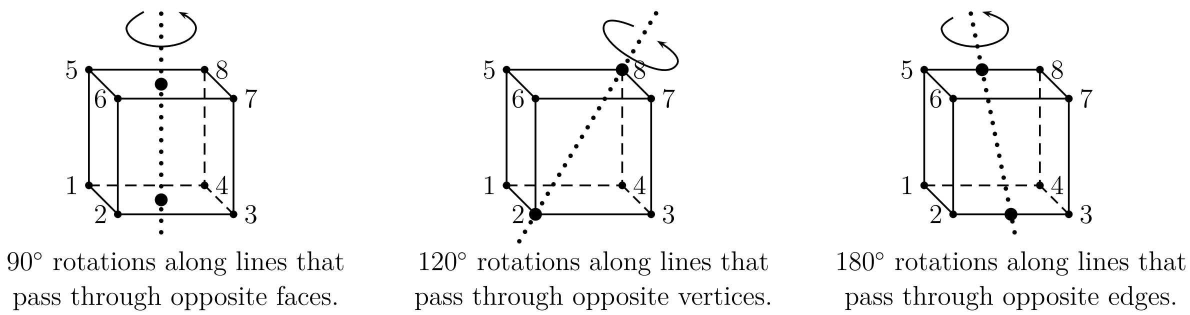


Figure 11.4: Understanding the group of symmetries of a cube.

(c) Consider now the icosahedron and the dodecahedron (see Figure 11.3). Note that the icosahedron has 12 vertices, 20 faces and 30 edges and the dodecahedron has 20 vertices, 12 faces and 30 edges. It can be checked that the group of symmetries of the two figures has 60 elements. We give the idea of the group elements for the symmetries of the icosahedron. The readers are required to compute the group elements for the symmetries of the dodecahedron. For the icosahedron, one has

i. $\mathbf{e}$, the identity element;

ii. $2 \times 10 = 20$ elements that are obtained by rotations along lines that pass through the center of opposite faces (10 pairs of opposite faces and each face is an equilateral triangle: corresponds to a rotation of 120°);

iii. $6 \times 4 = 24$ elements that are obtained by rotations along lines that pass through opposite vertices (6 pairs of opposite vertices and each vertex is incident with 5 edges: corresponds to a rotation of 72°);

iv. $1 \times 15 = 15$ elements that are obtained by rotations along lines that pass through the midpoint of opposite edges (15 pairs of opposite edges: corresponds to a rotation of 180°).

Exercise **11.1.10.** *Determine the group of symmetries of a parallelogram, a rectangle, a rhombus and an octahedron?*

By now, we have already come across lots of examples of groups that arise as symmetries of different objects. To proceed further, we study the notion of subgroup of a given group.

Definition 11.1.11. Let $(G, *)$ be a group. A nonempty subset H of G is said to be a **subgroup** of G, if $(H, *)$ is a group.

Note that the binary operation $*$ on H is the restriction of $*$ on G to the subset H. We informally say that the binary operation on H is *same* as that in G, and use the notation $*$ for the restriction of $*$ to H. Thus, H is a subgroup of G if and only if $H \subseteq G$, $H \neq \emptyset$ and H forms a group with the same binary operation of the group G.

Example 11.1.12. 1. Let G be a group with identity element $\mathbf{e}$. Then G and $\{\mathbf{e}\}$ are themselves groups and hence are subgroups of G. These two subgroups are called **trivial subgroups**.

2. Both $\mathbb{Z}$ and $\mathbb{Q}$ are subgroups of $\mathbb{R}$ with addition as the binary operation.

3. The sets $\{\mathbf{e}, f\}$ and $\{\mathbf{e}, r^2, f, r^2 f\}$ form subgroups of D_4.

4. Let $\sigma \in \mathcal{S}_4$. Then, using Theorem 11.1.7, we know that σ has a cycle representation. With this understanding, verify that D_4 is a subgroup of $\mathcal{S}_4$.

5. Verify that $H = \{\mathbf{e}, r, r^2, \ldots, r^{n-1}\}$ is a subgroup of D_n.

We leave the proof of the next result to the readers.

Lemma 11.1.13. *Let G be a group and let $a \in G, a \neq \mathbf{e}$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.*

In view of the above result, we give the following definition.

Definition 11.1.14. Let G be a group and let $a \in G$, $a \neq \mathbf{e}$. The **subgroup generated by** a, denoted by $\langle a \rangle$, is the subgroup $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$.

The following two results help us in proving whether a given nonempty set H of a group G is a subgroup or not.

Theorem 11.1.15 (Two-Step Subgroup Test)**.** *Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if the following two conditions are satisfied:*

1. *For all $a, b \in H$, $ab \in H$ (H is closed with respect to the binary operation of G).*
2. *For each $a \in H$, $a^{-1} \in H$. (H is closed with respect to taking inverse.)*

Proof. If H is a subgroup, then clearly the two conditions are satisfied. Conversely, suppose that the two conditions are satisfied.

Since $H \neq \varnothing$, let $a \in H$. The second condition implies that $a^{-1} \in H$. By the first condition, $\mathbf{e} = aa^{-1} \in H$. As in G, $x\mathbf{e} = \mathbf{e}x = x$ for each $x \in H$. Hence $\mathbf{e}$ is the identity element of H and $\mathbf{e} \in H$.

Then for each $x \in H$, $x^{-1} \in H$ implies that x^{-1} is the inverse element of x in H, and $x^{-1} \in H$.

The associativity condition is directly inherited from G to H.

Therefore, H is a subgroup of G. ∎

Theorem 11.1.16. [**Subgroup test**] *Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if for each pair of elements $a, b \in H$, $ab^{-1} \in H$.*

Proof. If H is a subgroup, then $a, b \in H$ implies $ab^{-1} \in H$. Conversely, suppose that for each pair of elements $a, b \in H$, $ab^{-1} \in H$. Since $H \neq \varnothing$, let $x \in H$. As in G, $\mathbf{e} = xx^{-1}$ shows that $\mathbf{e} \in H$.

First, if $x \in H$, then with $a = \mathbf{e}$ and $b = x$, we have $ab^{-1} = \mathbf{e}x^{-1} = x^{-1} \in H$.

Second, if $x, y \in H$, then by what we have just proved, $y^{-1} \in H$. As $y = (y^{-1})^{-1}$, we see that $xy = x(y^{-1})^{-1} \in H$.

By Theorem 11.1.15, H is a subgroup of G. ∎

Example 11.1.17. 1. The subsets of $\mathbb{Z}$ given below are not subgroups of $(\mathbb{Z}, +)$.

(a) Let $H = \{0, 1, 2, 3, \ldots\} \subseteq \mathbb{Z}$. Note that, for each $a, b \in H$, $a + b \in H$ and the identity element $0 \in H$. But H is not a subgroup of $\mathbb{Z}$, as for all $n \neq 0$, $-n \notin H$.

(b) Let $H = \mathbb{Z} \setminus \{0\} = \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\} \subseteq \mathbb{Z}$. Note that the identity element $0 \notin H$ and hence H is not a subgroup of $\mathbb{Z}$.

(c) Let $H = \{-1, 0, 1\} \subseteq \mathbb{Z}$. Then H contains the identity element 0 of $\mathbb{Z}$ and for each $h \in H$, $h^{-1} = -h \in H$. But H is not a subgroup of $\mathbb{Z}$ as $1 + 1 = 2 \notin H$.

2. Let G be an abelian group with identity $\mathbf{e}$. Write $H = \{x \in G : x^2 = \mathbf{e}\}$ and $K = \{x^2 : x \in G\}$. Prove that H and K are subgroups of G.

Answer: Clearly $\mathbf{e} \in H$; so $H \neq \varnothing$. Let $x, y \in H \subseteq G$. Then $x^2 = \mathbf{e} = y^2$. Since G is abelian,

$$\left(xy^{-1}\right)^2 = xy^{-1}xy^{-1} = x^2(y^{-1})^2 = \mathbf{e}\,(y^2)^{-1} = \mathbf{e}^{-1} = \mathbf{e}.$$

So, $xy^{-1} \in H$. By Theorem 11.1.16, H is a subgroup of G.

Again, $\mathbf{e} \in K$; so, $K \neq \varnothing$. Let $x, y \in K$. There exist $a, b \in G$ such that $x = a^2$ and $y = b^2$. Notice that $b^{-1} \in G$. Since G is abelian,

$$xy^{-1} = a^2(b^2)^{-1} = a^2(b^{-1})^2 = aab^{-1}b^{-1} = (ab^{-1})^2 \in K.$$

By Theorem 11.1.16, K is a subgroup of G.

As a last result of this section, we prove that the condition of the above theorems can be weakened if we assume that H is a finite, nonempty subset of a group G.

Theorem 11.1.18. [**Finite subgroup test**] *Let H be a nonempty finite subset of a group G. Then, H is a subgroup of G if and only if for each pair of elements $a, b \in H$, $ab \in H$.*

Proof. Suppose for each pair of elements $a, b \in H$, $ab \in H$. Due to Theorem 11.1.15, we need to show that for each $a \in H$, $a^{-1} \in H$. Notice that if $a = \mathbf{e} \in H$ then $a^{-1} = \mathbf{e}^{-1} = \mathbf{e} \in H$. So, assume that $a \neq \mathbf{e}$ and $a \in H$. Consider the set $S = \{a, a^2, a^3, \ldots, a^n, \ldots\}$. As H is closed with respect to the binary operation of G, $S \subseteq H$. But H has only finite number of elements. Hence, all these elements of S cannot be distinct. That is, there exist positive integers, say m, n with $m > n$, such that $a^m = a^n$. Thus, using Remark 11.1.2, one has $a^{m-n} = \mathbf{e}$. Hence, $a^{-1} = a^{m-n-1} \in H$. ■

EXERCISE **11.1.19.** 1. *Consider the group D_3. Does the subset $\{\mathbf{e}, rf\}$ form a subgroup of D_3?*

2. *Determine all subgroups of D_4.*

3. *Fix a positive integer n and consider the group D_n. Now, for each integer i, $0 \le i \le n-1$, does the set $\{\mathbf{e}, r^i f\}$ form a subgroup of D_n? Justify your answer.*

4. *Determine all subgroups of the group of symmetries of a tetrahedron.*

5. *Determine all subgroups of the group of symmetries of a cube.*

11.2 Lagrange's Theorem

In this section, we prove the first fundamental theorem for groups having finitely many elements. First, consider the following example.

Example 11.2.1. On $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ define addition component wise. That is, for (x_1, y_1), $(x_2, y_2) \in \mathbb{R}^2$ we take $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. Then $\mathbb{R}^2$ with component wise addition is a group. If H is a subgroup of $\mathbb{R}^2$, then H represents a line passing through $(0, 0)$.

For instance, $H_1 = \{(x, y) \in \mathbb{R}^2 : y = 0\}$, $H_2 = \{(x, y) \in \mathbb{R}^2 : x = 0\}$ and $H_3 = \{(x, y) \in \mathbb{R}^2 : y = 3x\}$ are subgroups of $\mathbb{R}^2$. Notice that H_1 represents the X-axis, H_2 represents the Y-axis and H_3 represents the line that passes through the origin and has slope 3.

Fix the element $(2, 3) \in \mathbb{R}^2$. Then

1. $(2, 3) + H_1 = \{(2, 3) + (x, y) : y = 0\} = \{(2 + x, 3) : x \in \mathbb{R}\}$. It is the line that passes through the point $(2, 3)$ and is parallel to the X-axis.

2. Verify that $(2, 3) + H_2$ represents the line that passes through the point $(2, 3)$ and is parallel to the Y-axis.

3. Similarly, $(2, 3) + H_3 = \{(2 + x, 3 + 3x) : x \in \mathbb{R}\} = \{(x, y) \in \mathbb{R}^2 : y = 3x - 3\}$ represents the line that has slope 3 and passes through the point $(2, 3)$.

In general, if H is a subgroup of $\mathbb{R}^2$ and $(x_0, y_0) \in \mathbb{R}^2$, then the set $(x_0, y_0) + H$ is the line that is a parallel shift of the line represented by H containing the point (x_0, y_0). Further,

1. (x_1, y_1) lies on the line $(x_0, y_0) + H$ if and only if $(x_0, y_0) + H = (x_1, y_1) + H$;

2. for any two points $(x_0, y_0), (x_1, y_1) \in \mathbb{R}^2$, either $(x_0, y_0) + H = (x_1, y_1) + H$ or they represent two parallel lines; each is parallel to the line H; and

3. $\bigcup\limits_{x \in \mathbb{R}} \bigcup\limits_{y \in \mathbb{R}} \big[(x, y) + H\big] = \mathbb{R}^2$.

That is, if we define a relation, denoted $\sim$, in $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$, whenever $(x_1 - x_2, y_1 - y_2) \in H$, then the above observations imply that this relation is an equivalence relation. Hence, as (x, y) vary over all the points of $\mathbb{R}^2$, we get a partition of $\mathbb{R}^2$. Moreover, the equivalence class containing the point (x_0, y_0) is the set $(x_0, y_0) + H$.

We see that given a subgroup H of a group G, it may be possible to partition the group G into subsets in the form gH or Hg, each of which is similar to H in some sense.

Definition 11.2.2. Let H be a subgroup of a group G. Let $g \in G$.

1. The set $gH = \{gh : h \in H\}$ is called a **left coset** of H in G.
2. The set $Hg = \{hg : h \in H\}$ is called a **right coset** of H in G.

Remark 11.2.3. Since the identity element $\mathbf{e} \in H$, for each fixed $g \in G$, $g = g\mathbf{e} \in gH$. Hence, we often say that gH is the left coset of H containing g. Similarly, $g \in Hg$ and hence Hg is said to be the right coset of H containing g.

Example 11.2.4. Consider the subgroups $H = \{\mathbf{e}, f\}$ and $K = \{\mathbf{e}, r^2\}$ of the group D_4. We observe the following:

1. $H = \{\mathbf{e}, f\} = Hf$, $\quad Hr = \{r, fr\} = Hfr$, $\quad Hr^2 = \{r^2, fr^2\} = Hfr^2$ and $Hr^3 = \{r^3, fr^3\} = Hfr^3$.
2. $H = \{\mathbf{e}, f\} = fH$, $\quad rH = \{r, rf\} = rfH$, $\quad r^2H = \{r^2, r^2f\} = r^2fH$ and $r^3H = \{r^3, r^3f\} = r^3fH$.
3. $K = \{\mathbf{e}, r^2\} = Kr^2 = r^2K$, $\quad Kr = \{r, r^3\} = rK = Kr^3 = r^3K$, $Kf = \{f, r^2f\} = fK = Kr^2f = r^2fK$ and $Kfr = \{fr, fr^3\} = frK = Kfr^3 = fr^3K$.

From Items 1 and 2, we see that Hg need not be equal to H, for each $g \in D_4$. Whereas in Item 3, $Kg = gK$, for each $g \in D_4$. So, there is a need to distinguish between these two subgroups of D_4. This leads to study of normal subgroups and beyond. The interested reader can look at any standard book in abstract algebra to go further in this direction.

Some important information about cosets are listed in the following theorem, which the reader can prove with a little labor.

Theorem 11.2.5. **[Cosets are equal or disjoint]**

1. *Let H be a subgroup of a group G. Suppose $a, b \in G$. Then the following results hold for left cosets of H in G:*
   (a) *$aH = H$ if and only if $a \in H$.*
   (b) *aH is a subgroup of G if and only if $a \in H$.*
   (c) *Either $aH = bH$ or $aH \cap bH = \varnothing$.*
   (d) *$aH = bH$ if and only if $a^{-1}b \in H$.*
   (e) *Each left coset is an equivalence class of the equivalence relation given by "$a \sim b$ if $a^{-1}b \in H$"; and the collection of all left cosets is a partition of G.*

2. *The following statements hold for right cosets of H in G:*
   (a) *$Ha = H$ if and only if $a \in H$.*
   (b) *Ha is a subgroup of G if and only if $a \in H$.*
   (c) *Either $Ha = Hb$ or $Ha \cap Hb = \varnothing$.*
   (d) *$Ha = Hb$ if and only if $ab^{-1} \in H$.*
   (e) *Each right coset is an equivalence class of the equivalence relation given by "$a \sim b$ if $ab^{-1} \in H$"; and the collection of all right cosets is a partition of G.*

3. *Further, $aH = Ha$ if and only if $H = aHa^{-1} = \{aha^{-1} : h \in H\}$.*

To proceed further, we need the following definition.

Definition 11.2.6. Let G be a group. As a set if G is finite, then $|G|$ is called the **order of the group** G. In such a case, G is said to be a finite group, or a group of finite order. As a set, if G is infinite, then G is said to be an infinite group.

Theorem 11.2.7. **[Lagrange Theorem]** *Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G equals $\dfrac{|G|}{|H|}$.*

Proof. We give the proof for left cosets. A similar proof holds for right cosets. Since G is a finite group, the number of left cosets of H in G is finite. Let $g_1H, g_2H, \ldots, g_mH$ be the collection of all left cosets of H in G. Then by Theorem 11.2.5, G is a disjoint union of the sets $g_1H, g_2H, \ldots, g_mH$.

Also, $|aH| = |bH|$, for each $a, b \in G$. Hence, $|g_iH| = |H|$, for all $i = 1, 2, \ldots, m$. Thus, $|G| = \left|\bigcup\limits_{i=1}^{m} g_iH\right| = \sum\limits_{i=1}^{m} |g_iH| = m|H|$ (the disjoint union gives the second equality). Thus, $|H|$ divides $|G|$ and the number of left cosets equals $m = \dfrac{|G|}{|H|}$. ∎

Remark 11.2.8.

1. The number m in Theorem 11.2.7 is called *the index* of H in G, and is denoted by $[G : H]$ or $i_G(H)$.
2. Theorem 11.2.7 is a statement about any subgroup of a finite group. It is quite possible that both the group G and its subgroup H are infinite but the number of left (right) cosets of H in G is finite. In this case, one still talks of index of H in G. For example, let $G = \mathbb{Z}$ and $H = 10\mathbb{Z} = \{10m : m \in \mathbb{Z}\}$, with the group operation as addition. Then the left cosets are $H,\ 1 + H, \ldots, 9 + H$ so that $[\mathbb{Z} : H] = 10$.
3. In general, if $m \in \mathbb{N}$, then $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ and $[\mathbb{Z} : m\mathbb{Z}] = m$.

Definition 11.2.9. Let G be a group and let $g \in G$. Then the smallest positive integer m such that $g^m = \mathbf{e}$ is called the **order** of g. If there is no such positive integer then g is said to have an **infinite order**. The order of an element is denoted by $\mathfrak{o}(g)$.

Example 11.2.10.

1. The only element of order 1 in a group G is the identity element of G.
2. In D_4, each of the elements r^2, f, rf, r^2f, r^3f has order 2, whereas the elements r and r^3 have order 4.

EXERCISE **11.2.11.**

1. *Prove that for each $a \in G$, $\mathfrak{o}(a) = \mathfrak{o}(a^{-1})$.*
2. *Determine the index of each subgroup that were obtained in Exercise 11.1.19.*
3. *Let G be a finite group and $a \in G, a \neq \mathbf{e}$. If $H = \{a^n : n \in \mathbb{Z}\}$ then prove that $|H| = \mathfrak{o}(a)$.*
4. *Let $a \in G$, a finite group. Show that $\mathfrak{o}(a) \in \mathbb{N}$.*

We now state some important corollaries of Lagrange's Theorem, whose proofs are easy.

Corollary 11.2.12. *Let G be a finite group and let $a \in G$. Then $\mathfrak{o}(a)$ divides $|G|$ as $H = \{a^n : n \in \mathbb{Z}\}$ is a finite subgroup of G.*

Corollary 11.2.12 implies that the possible orders of elements of a finite group G are the divisors of $|G|$. For example, if $|G| = 30$ then for each $g \in G$, $\mathfrak{o}(g) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$.

Further, Let $g \in G$, a finite group. Then, $|G| = m \cdot \mathfrak{o}(g)$ for some $m \in \mathbb{N}$. Hence

$$g^{|G|} = g^{m \cdot \mathfrak{o}(g)} = (g^{\mathfrak{o}(g)})^m = e^m = e.$$

We thus obtain the following corollary.

Corollary 11.2.13. *Let G be a finite group. Then for each $g \in G, g^{|G|} = e$.*

We now use the above understanding to digress towards modular arithmetic. Recall that for $a, b \in \mathbb{Z}$, the notation "$a \equiv b \pmod{m}$" means that m divides $a - b$.

Let p be an odd prime. Write $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$. Verify that $(\mathbb{Z}_p^*, \odot_p)$ is a group, where

$$a \odot_p b = \text{the remainder when } ab \text{ is divided by } p.$$

Applying Corollary 11.2.13 to $\mathbb{Z}_p^*$ gives the following result.

Corollary 11.2.14. **[Fermat's Little Theorem]** *Let $a \in \mathbb{N}$ and let p be a prime.*

1. *If p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$.*
2. *In general, $a^p \equiv a \pmod{p}$.*

We now state without proof a generalization of Fermat's Little Theorem. Let $n \in \mathbb{N}$. Consider

$$U_n = \{k : 1 \le k \le n, \gcd(k, n) = 1\}.$$
$$a \odot_n b = \text{the remainder when } ab \text{ is divided by } n.$$

Then $(U_n, \odot_n)$ is a group with $|U_n| = \varphi(n)$, where $\varphi(n)$ is Euler's totient function that denotes the the number of integers between 1 and n, coprime to n.

By Corollary 11.2.13, we obtain the following result.

Corollary 11.2.15. **[Euler's Theorem]** *If $a \in \mathbb{Z}$, $n \in \mathbb{N}$ and $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Example 11.2.16.

1. Find the digit in the unit place of 13^{1001} written in decimal notation.

   Ans: Observe that $13 \equiv 3 \pmod{10}$. So, $13^{1001} \equiv 3^{1001} \pmod{10}$. Also, $3 \in U_{10}$ and therefore by Corollary 11.2.13, $3^{|U_{10}|} = 1 \pmod{10}$. But $|U_{10}| = 4$ and $1001 = 4 \cdot 250 + 1$. Thus,

   $$13^{1001} \equiv 3^{1001} \equiv 3^{4 \cdot 250 + 1} \equiv (3^4)^{250} \cdot 3^1 \equiv 1 \cdot 3 \equiv 3 \pmod{10}.$$

   Hence, the digit in the unit place of 13^{1001} is 3.

2. Find the digits in the unit and tens places of 23^{1002} written in decimal notation.

   Ans: Observe that $23 \in U_{100}$ and $23^{|U_{100}|} = 1 \pmod{100}$. But $|U_{100}| = 40$ and $1002 = 40 \cdot 25 + 2$. Hence

   $$23^{1002} \equiv 23^{40 \cdot 25 + 2} \equiv (23^{40})^{25} \cdot 23^2 \equiv 1 \cdot 23^2 \equiv 529 \equiv 29 \pmod{100}.$$

   Therefore, in the decimal representation of 23^{1002}, the digit in the unit place is 9 and the digit in the tens place is 2.

In general, the converse of Lagrange's Theorem is not true. That is, there exists a group of order mn but it has no subgroup of order m for some $m, n \in \mathbb{N}$. See the following example.

Example 11.2.17. Let T be the group of symmetries of the tetrahedron as discussed in Example 11.1.9.2a. This group has 12 elements. From Exercise 11.1.19(4), we see that there is no subgroup of T with 6 elements.

If you have not completed that exercise, then let us show that there is no subgroup of T consisting of 6 elements. On the contrary, suppose H is a subgroup of T and $|H| = 6$. We know that

$$T = \{\mathbf{e}, (234), (243), (124), (142), (123), (132), (134), (143), (12)(34), (13)(24), (14)(23)\}.$$

Observe that T has exactly 8 elements of order 3; each of them is of the form (ijk) for distinct numbers i, j and k. Let a be any one of these 8 elements. That is, $a \in T$ with $\mathfrak{o}(a) = 3$. The possible cosets could be H, aH and a^2H (as $a^3 = \mathbf{e}$, no other coset exists). Using Theorem 11.2.5, we see that cosets of H in T will be exactly 2 in number. Hence, at most two of the cosets H, aH and a^2H are distinct; so that at least two of them are equal. By Theorem 11.2.5, it follows that $a \in H$. Therefore, all the 8 elements of order 3 must be elements of H. That is, H must have at least 9 elements (8 elements of order 3 and one identity). This is absurd as $|H| = 6$.

11.3 Group action

Recall that when $f : A \times B \to C$ is a function and $a \in A,\ b \in B$, the value of the function at the point (a, b) is written as $f(a, b)$. This is called the *outfix* notation. In the infix notation, we write the same value $f(a, b)$ as afb. For example, $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and we write $+(3, 5)$ as $3 + 5$. When we use the infix notation, the function f is referred to as an *operator*. It is another name for a function.

Definition 11.3.1. Let $(G, \cdot)$ be a group with identity $\mathbf{e}$. Then G is said to act on a set X if there exists an operator $\star : G \times X \to X$ satisfying the following two conditions:

1. For each $x \in X$, $\mathbf{e} \star x = x$.
2. For all $x \in X$, and $g, h \in G$, $g \star (h \star x) = (g \cdot h) \star x$.

In such a case, the operator $\star$ is called an action of the group G on the set X.

Remark 11.3.2. 1. Let us assume that X consists of a set of points and let us suppose that the group G acts on X by moving the points. Then Definition 11.3.1 can be interpreted as follows:

   (a) The first condition implies that the identity element of the group does not move any element of X. That is, the points in X remain fixed when they are acted upon by the identity element of G.

   (b) The second condition implies that if a point, say $x_0 \in X$, is first moved by an element $h \in G$ and then by an element $g \in G$, then the final position of x_0 is same as the position it would have reached if it was moved by the element $g \cdot h \in G$.

2. Suppose a group G acts on a set X with the group action as $\star$. Fix an element $g \in G$. Define functions $\phi, \psi : X \to X$ by $\phi(x) = g \star x,\ \psi(x) = g^{-1} \star x$ for each $x \in X$. Then

$$(\psi \circ \phi)(x) = g^{-1} \star (g \star x) = (g^{-1} \cdot g)(x) = \mathbf{e} \star x = x.$$

   Similarly, it follows that $(\phi \circ \psi)(x) = x$. Hence the function ϕ is a bijection on X. That is, g just permutes the elements of X. In particular, $\{g \star x : x \in X\} = X$.

3. There may exist $g, h \in G$, with $g \neq h$ such that $g \star x = h \star x$, for all $x \in X$,.

Example 11.3.3. 1. Consider the dihedral group $D_6 = \{\mathbf{e}, r, \ldots, r^5, f, rf, \ldots, r^5 f\}$, with $r^6 = \mathbf{e} = f^2$ and $rf = fr^5$. Here, f stands for the vertical flip and r stands for counter clockwise rotation by an angle of $\frac{\pi}{3}$. Then D_6 acts on the labeled edges/vertices of a regular hexagon by permuting the labeling of the edges/vertices (see Figure 11.5).

2. Let X denote the set of ways of coloring the vertices of a square with two colors, say, red and blue. Then X equals the set of all functions $h : \{1, 2, 3, 4\} \to \{red, blue\}$, where the vertices south-west, south-east, north-east and north-west are respectively, labeled as $1, 2, 3$ and 4. Then observe that $|X| = 16$. The distinct colorings have been depicted in Figure 11.6, where R stands

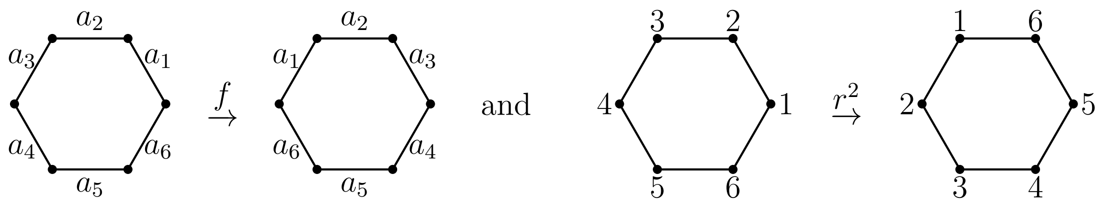


Figure 11.5: Action of f on labeled edges and of r^2 on labeled vertices of a regular hexagon.

for the vertex colored "red " and B stands for the vertex colored "blue". For example, the figure labeled x_9 in Figure 11.6 corresponds to $h(1) = R = h(4)$ and $h(2) = B = h(3)$. Now, let us denote the permutation (1234) by r and the permutation $(12)(34)$ by f. Then the dihedral group $D_4 = \{\mathbf{e}, r, r^2, r^3, f, rf, r^2f, r^3f\}$ acts on the set X. For example,

(a) x_1 and x_{16} are mapped to itself under the action of every element of D_4. That is, $g \star x_1 = x_1$ and $g \star x_{16} = x_{16}$, for all $g \in G$.

(b) $r \star x_2 = x_5$ and $f \star x_2 = x_3$.

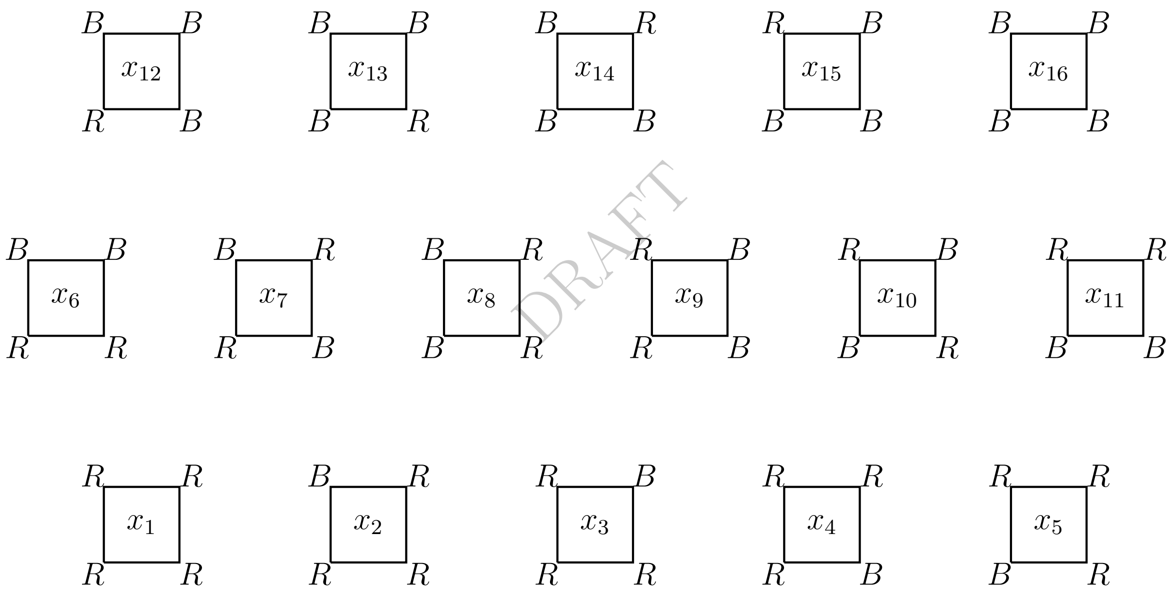


Figure 11.6: Coloring the vertices of a square.

There are three important sets associated with a group action. We first define them and then try to understand them using an example.

Definition 11.3.4. Let G act on a set X with the action as $\star$.

1. For each $x \in X$, $\mathcal{O}(x) := \{g \star x : \ g \in G\} \subseteq X$ is called the orbit of x.
2. For each $x \in X$, $G_x := \{g \in G : g \star x = x\} \subseteq G$ is called the stabilizer of x in G.
3. For each $g \in G$, $F_g := \{x \in X : g \star x = x\} \subseteq X$ is called the fix of g.

Example 11.3.5. Consider the set X given in Example 11.3.3.2. Then using the depiction of the set X in Figure 11.6, we have

$$\mathcal{O}(x_2) = \{x_2, x_3, x_4, x_5\}, \ G_{x_2} = \{e, rf\}, \ \text{ and } \ F_{rf} = \{x_1, x_2, x_4, x_7, x_{10}, x_{13}, x_{15}, x_{16}\}.$$

We now state a few results associated with the above definitions without proof as they can be easily verified.

Proposition 11.3.6. *Let G act on a set X with action as $\star$.*

1. *Then for each $x \in X$, the stabilizer G_x of x is a subgroup of G.*
2. *Define the relation $\sim$ on X by $x \sim y$ if there exists $g \in G$ such that $g \star x = y$. Then $\sim$ is an equivalence relation on X, and $[x] = \mathcal{O}(x)$. That is, the equivalence class containing x equals the orbit of x.*
3. *In particular, for each $x \in X$, if $t \in \mathcal{O}(x)$, then $\mathcal{O}(x) = \mathcal{O}(t)$.*
4. *For all $x, t \in X$, if $g \star x = t$ then $G_x = g^{-1} G_t g$.*

Proposition 11.3.6 helps us to relate the distinct orbits of X under the action of G with the cosets of G. This is stated and proved as the next result. Recall that the number of left cosets of a subgroup H of a group G equals $[G : H]$, the index of H in G.

Theorem 11.3.7. [Orbit stabilizer theorem] *Let a group G act on a set X. Then for each $x \in X$, there is a bijection between $\mathcal{O}(x)$ and the set of all left cosets of G_x in G. In particular, $|\mathcal{O}(x)| = [G : G_x]$. Moreover, if G is a finite group then for each $x \in X$, $|G| = |\mathcal{O}(x)| \cdot |G_x|$.*

Proof. Let S be the set of distinct left cosets of G_x in G. Write $S := \{gG_x : g \in G\}$. Then $|S| = [G : G_x]$. Consider the map $\tau : S \to \mathcal{O}(x)$ by $\tau(gG_x) = g \star x$, where $\star$ is the group action. Let us first check that τ is well-defined.

Suppose the left cosets gG_x and hG_x are equal. That is, $gG_x = hG_x$. Then, using Theorem 11.2.5 and the definition of group action, one obtains the following sequence of assertions:

$$gG_x = hG_x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow (h^{-1}g) \star x = x \Leftrightarrow h^{-1} \star (g \star x) = x \Leftrightarrow g \star x = h \star x \Leftrightarrow \tau(gG_x) = \tau(hG_x).$$

Hence, τ is well-defined and also a one-one map. To show τ is onto, note that for each $y \in \mathcal{O}(x)$, there exists an $h \in G$, such that $h \star x = y$. Also, for this choice of $h \in G$, the coset $hG_x \in S$. Therefore, for this choice of $h \in G$, $\tau(hG_x) = h \star x = y$ holds. Hence, τ is onto.

Therefore, τ is a bijection between $\mathcal{O}(x)$ and S. The second statement follows by observing that whenever $|G|$ is finite, $[G : G_x] = \dfrac{|G|}{|G_x|}$, for each subgroup G_x of G. ∎

The following results are immediate consequences of Proposition 11.3.6 and Theorem 11.3.7. We give the proof for the sake of completeness.

Lemma 11.3.8. *Let G be a finite group acting on a set X. Then for each $y \in X$,*

$$\sum_{x \in \mathcal{O}(y)} |G_x| = |G|.$$

Proof. Recall that, for each $x \in \mathcal{O}(y)$, $|\mathcal{O}(x)| = |\mathcal{O}(y)|$. Hence, using Theorem 11.3.7, one has $|G| = |G_x| \cdot |\mathcal{O}(x)|$, for all $x \in X$. Therefore,

$$\sum_{x \in \mathcal{O}(y)} |G_x| = \sum_{x \in \mathcal{O}(y)} \frac{|G|}{|\mathcal{O}(x)|} = \sum_{x \in \mathcal{O}(y)} \frac{|G|}{|\mathcal{O}(y)|} = \frac{|G|}{|\mathcal{O}(y)|} \sum_{x \in \mathcal{O}(y)} 1 = \frac{|G|}{|\mathcal{O}(y)|} |\mathcal{O}(y)| = |G|.$$ ∎

The next theorem is the generalization of Discussion 5.5.12 where we had calculated the number of distinct circular arrangements.

Theorem 11.3.9. *Let G be a finite group acting on a set X. Let N denote the number of distinct orbits of X under the action of G. Then*

$$N = \frac{1}{|G|} \sum_{x \in X} |G_x|.$$

Proof. By Lemma 11.3.8, $\sum\limits_{x \in \mathcal{O}(y)} |G_x| = |G|$ for all $y \in X$. Let $x_1, x_2, \ldots, x_N$ be the representative of the distinct orbits of X under the action of G. Then

$$\frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} \sum_{i=1}^{N} \sum_{y \in \mathcal{O}(x_i)} |G_{x_i}| = \frac{1}{|G|} \sum_{i=1}^{N} |G| = \frac{1}{|G|} N \cdot |G| = N. \qquad \blacksquare$$

Example 11.3.10. For Example 11.3.3.2, check that the number of distinct colorings are

$$\frac{1}{|G|} \sum_{i=1}^{16} |G_{x_i}| = \frac{1}{8} (8+2+2+2+2+2+4+2+2+4+2+2+2+2+2+8) = 6.$$

As the above example illustrates, the distinct configurations are obtained by listing out elements of X. If we color the vertices of the square with 3 colors, then $|X| = 3^4 = 81$, whereas the number of elements of the group of symmetries of a square, that is, of D_4, is only 8. Clearly, it will be advantageous to relate the number of distinct orbits with the elements of the group, in place of the elements of the set X. Our next result does this.

Theorem 11.3.11. **[Burnside's Lemma]** *Let G be a finite group acting on a set X. Let N be the number of distinct orbits of X under the action of G. Then*

$$N = \frac{1}{|G|} \sum_{g \in G} |F_g|.$$

Proof. Write the group action as $\star$. Consider the set $S = \{(g,x) \in G \times X \ : g \star x = x\}$. We calculate $|S|$ by two methods. First, for each fixed $x \in X$, G_x gives the collection of elements of G that satisfy $g \star x = x$. So, $|S| = \sum\limits_{x \in X} |G_x|$.

Second, for each $g \in G$, F_g is the collection of elements of X that satisfy $g \star x = x$. So, $|S| = \sum\limits_{g \in G} |F_g|$.

Thus $\sum\limits_{x \in X} |G_x| = |S| = \sum\limits_{g \in G} |F_g|$. By Theorem 11.3.9, we have $N = \dfrac{1}{|G|} \sum\limits_{g \in G} |F_g|$. $\blacksquare$

Example 11.3.12. In Example 11.3.3.2, verify that

$$|F_{\mathbf{e}}| = 16, \ |F_r| = 2, \ |F_{r^2}| = 4, |F_{r^3}| = 2, \ |F_f| = 4, \ |F_{rf}| = 8, |F_{r^2 f}| = 4 \text{ and } |F_{r^3 f}| = 8.$$

Hence, the number of distinct configurations are

$$\frac{1}{|G|} \sum_{g \in G} |F_g| = \frac{1}{8} (16+2+4+2+4+8+4+8) = 6.$$

It seems that we may still need to know all the elements of X to compute the above terms. In the next section, it will be shown that to compute $|F_g|$, for any $g \in G$, we just need to find a proper n such that $g \in \mathcal{S}_n$ and decompose g as product of disjoint cycles.

11.4 The Cycle index polynomial

Let G be a finite group acting on a set X. Then as mentioned at the end of the previous section, we need to understand the cycle decomposition of each $g \in G$ as product of disjoint cycles. red field and Polya observed that elements of G with the same cyclic decomposition made the same contribution to the sets of *fixed points*. They defined the notion of cycle index polynomial to keep track of the cycle decomposition of the elements of G. We first state the following result of Cayley which implies that every group element can be written as an element of a symmetric group. We start with the following definition.

Definition 11.4.1. Let $(G_1, \star)$ and $(G_2, \odot)$ be two groups. Then, an **isomorphism** is a function $f : G_1 \to G_2$ satisfying

1. f is one-to-one,
2. f is onto, and
3. $f(\sigma \star \tau) = (\sigma) \odot f(\tau)$, for each $\sigma, \tau \in G_1$.

Example 11.4.2. Observe the following:

1. The function that sent $r \mapsto (1234)$ and $f \mapsto (14)(23)$ gave an isomorphism between the two groups that appear in Example 11.1.9.1a.
2. The function that sends $r \mapsto (12345)$ and $f \mapsto (13)(45)$ gives an isomorphism between the two groups that appear in Example 11.1.9.1c.

Theorem 11.4.3. **[Cayley's Theorem]** *Let G be a group. Then G is isomorphic to a subgroup of the symmetric group acting on G.*

Proof. Let S be the set of all bijections on G. Notice that S is a group with the operation as composition of maps. Corresponding to $x \in G$, let λ_x be the function $\lambda_x : G \to G$ given by $\lambda_x(g) = xg$ for each $g \in G$. Now, if $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$ implies $a = b$. So, λ_x is one-one. If $y \in G$, then $\lambda_x(x^{-1}y) = xx^{-1}y = y$ shows that λ_x is onto. Thus, $\lambda_x \in S$.

Define the function $\phi : G \to S$ by $\phi(x) = \lambda_x$ for each $x \in G$. Then $\phi : G \to \mathsf{rng}\,\phi \subseteq S$ is a bijection. Also, observe that $\mathsf{rng}\,\phi$ For any $g \in G$,

$$\phi(xy)(g) = \lambda_{xy}(g) = xyg = x(yg) = x(\lambda_y(g)) = \lambda_x(\lambda_y(g)) = (\phi(x) \circ \phi(y))(g).$$

It shows that $\mathsf{rng}\,\phi$ is closed under the operation of composition of maps; that is, $\mathsf{rng}\,\phi$ is a subgroup of S. It also shows that ϕ is a homomorphism. Therefore, G is isomorphic to $\mathsf{rng}\,\phi \subseteq S$. ∎

Let us now start with a few definitions and examples to better understand the use of cycle decomposition of an element of a permutation group.

Definition 11.4.4. A permutation $\sigma \in \mathcal{S}_n$ is said to have the cycle structure $1^{k_1}\, 2^{k_2} \cdots n^{k_n}$, if the cycle representation of σ has k_i cycles of length i, for $1 \le i \le n$. Observe that $\sum\limits_{i=1}^{n} i \cdot k_i = n$.

Example 11.4.5.

1. Let $\mathbf{e}$ be the identity element of $\mathcal{S}_n$. Then $\mathbf{e} = (1)\ (2)\ \cdots (n)$ and hence the cycle structure of $\mathbf{e}$, as an element of $\mathcal{S}_n$ equals 1^n.
2. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 6 & 7 & 10 & 14 & 1 & 2 & 13 & 15 & 4 & 11 & 5 & 8 & 12 & 9 \end{pmatrix} \in S_{15}$. We see that $\sigma = (1\ 3\ 7\ 2\ 6)\ (4\ 10)\ (5\ 14\ 12)\ (8\ 13)\ (9\ 15)\ (11)$. Thus, the cycle structure of σ is $1^1 2^3 3^1 5^1$.

3. Consider the group G of symmetries of the tetrahedron (see Example 11.1.9.2a). The elements of G have the following cycle structures:

$$\begin{array}{rll} 1^4 & \text{for exactly} & 1 \text{ element corresponding to the identity element;} \\ 1^1 3^1 & \text{for exactly} & 8 \text{ elements corresponding to 3 cycles;} \\ 2^2 & \text{for exactly} & 3 \text{ elements corresponding to } (12)(34), (13)(24) \text{ and } (14)(23). \end{array}$$

Definition 11.4.6. Let G be a permutation/symmetric group on n symbols. For any $g \in G$, let $\ell_k(g)$ denote the number of cycles of length $k, 1 \le k \le n$, in the cycle representation of g. Then the cycle index polynomial of G is a polynomial in n variables $z_1, z_2, \ldots, z_n$ given by

$$P_G(z_1, z_2, \ldots, z_n) = \frac{1}{|G|}\Big(\sum_{g \in G} z_1^{\ell_1(g)}\ z_2^{\ell_2(g)}\ \cdots z_n^{\ell_n(g)}\Big).$$

Notice that for each $g \in G$, the condition that g has exactly $\ell_k(g)$ cycles of length $k, 1 \le k \le n$, implies that $1 \cdot \ell_1(g) + 2 \cdot \ell_2(g) + \cdots + n \cdot \ell_n(g) = n$.

Example 11.4.7. 1. Let G be the dihedral group D_4 (see Example 11.1.9.2). Then

$$e = (1)(2)(3)(4) \to z_1^4,\ r = (1234) \to z_4,\ r^3 = (1432) \to z_4,\ r^2 = (13)(24) \to z_2^2,$$
$$f = (14)(23) \to z_2^2,\ rf = (1)(3)(24) \to z_1^2 z_2,\ r^2 f = (12)(34) \to z_2^2,\ r^3 f = (13)(2)(4) \to z_1^2 z_2.$$

Thus, $P_G(z_1, z_2, z_3, z_4) = \frac{1}{8}\left(z_1^4 + 2z_4 + 3z_2^2 + 2z_1^2 z_2\right)$.

2. Let G be the dihedral group D_5 (see Example 11.1.9.1c). Then $P_G(z_1, z_2, z_3, z_4, z_5) = \frac{1}{10}\left(z_1^5 + 4z_5 + 5z_1 z_2^2\right)$.

3. Verify that the cycle index polynomial of the symmetries of a cube induced on the set of vertices is given by
$$P_G(z_1, z_2, \ldots, z_8) = \frac{1}{24}\left(z_1^8 + 6z_4^2 + 9z_2^4 + 8z_1^2 z_3^2\right).$$

Let S be an object, for example, say a geometrical figure, and let X be the finite set of vertices, edges and faces etc. of S. Also, let C be a finite set (say, of colors). Consider the set Ω that denotes the set of all functions from X to C. Observe that an element of Ω gives a color pattern on the object S. Let G be a subgroup of the group of permutations of the object S. Hence, G acts on the elements of X. Let us denote this action by $\star$. So, $g \star x \in X$, for all $x \in X$.

One can also obtain an action of G on Ω, denoted $\circledast$, by the following rule:
Fix an element $x \in X$. Then, for each $\phi \in \Omega$ and $g \in G$, $g \circledast \phi$ is an element of Ω and hence it gives a function from X to C. Hence, one defines

$$(g \circledast \phi)(x) = \phi(g^{-1} \star x), \text{ for all } \phi \in \Omega.$$

We claim that $\circledast$ indeed defines a group action on the set Ω. To do so, note that for each $h, g \in G$ and $\phi \in \Omega$, the definition of the action on X and Ω gives

$$\begin{aligned} (h \circledast (g \circledast \phi))(x) &= (g \circledast \phi)(h^{-1} \star x) = \phi\left(g^{-1} \star (h^{-1} \star x)\right) = \phi\left(g^{-1}h^{-1} \star x\right) \\ &= \phi\left((hg)^{-1} \star x\right) = (hg \circledast \phi)(x). \end{aligned}$$

Since, $(h \circledast (g \circledast \phi))(x) = (hg \circledast \phi)(x)$, for all $x \in X$, one has $h \circledast (g \circledast \phi) = hg \circledast \phi$, for each $h, g \in G$ and $\phi \in \Omega$. Hence, the proof of the claim is complete. Now, using the above notations, we have the following theorem.

Theorem 11.4.8. *Let C, S, X and Ω be as defined above. Also, let G be a subgroup of the group of permutations of the object S. Then the number of distinct color patterns (distinct elements of Ω), distinct up to the action of G, is given by*

$$P_G(|C|, |C|, \ldots, |C|).$$

Proof. Let $|X| = n$. Then observe that G is a subgroup of $\mathcal{S}_n$. So, each $g \in G$ can be written as a product of disjoint cycles. Also, by Burnside's Lemma (Theorem 11.3.11), N, the number of distinct color patterns (distinct orbits under the action of G), equals $\frac{1}{|G|} \sum\limits_{g \in G} |F_g|$, where

$$F_g = \{ \phi \in \Omega \ : (g \circledast \phi)(x) = \phi(x), \ \text{ for all } \ x \in X\}.$$

We claim that "$g \in G$ fixes a color pattern (or an element of Ω) if and only if ϕ colors the elements in a given cycle of g with the same color".

Suppose that $g \circledast \phi = \phi$. That is, $(g \circledast \phi)(x) = \phi(x)$, for all $x \in X$. So, using the definition, one has $\phi(g^{-1} \star x) = \phi(x)$, for all $x \in X$. In particular, for a fixed $x_0 \in X$, one also has

$$\phi(x_0) = \phi(g \star x_0) = \phi\big(g^2 \star x_0\big) = \cdots .$$

Note that, for each fixed $x_0 \in X$ and $g \in G$, the permutation $(x_0, \ g \star x_0, \ g^2 \star x_0, \ldots)$ corresponds to a cycle of g. Therefore, if g fixes a color pattern ϕ, *i.e.*, $g \circledast \phi = \phi$, then ϕ assigns the same color to each element of any cycle of g.

Conversely, fix an element $g \in G$ and let ϕ be a color pattern (a function) that has the property that every point in a given cycle of g is colored with the same color. That is, $\phi(x) = \phi(g \star x)$, for each $x \in X$. Or equivalently, $\phi(x) = \phi\big(g^{-1} \star x\big) = (g \circledast \phi)(x)$, for all $x \in X$. Hence, by definition, $g \circledast \phi = \phi$. Thus, g fixes the color pattern ϕ. Hence, the proof of the claim is complete.

Therefore, we observe that for a fixed $g \in G$, a cycle of g can be given a color independent of another cycle of g. Also, the number of distinct colors equals $|C|$. Hence, for a fixed $g \in G$, $|F_g| = |C|^{\ell_1(g)} \cdot |C|^{\ell_2(g)} \ \cdots |C|^{\ell_n(g)}$, where for each k, $1 \le k \le n$, $\ell_k(g)$ denotes the number of cycles of g of length k. Thus,

$$N = \frac{1}{|G|} \sum_{g \in G} |F_g| = \frac{1}{|G|} \sum_{g \in G} |C|^{\ell_1(g)} \cdot |C|^{\ell_2(g)} \ \cdots |C|^{\ell_n(g)} = P_G(|C|, |C|, \ldots, |C|). \qquad \blacksquare$$

We now give a few examples to indicate the importance of Theorem 11.4.8.

Example 11.4.9.

1. Determine the number of distinct color patterns, when the vertices of a pentagon are colored with 3 colors.

   Answer: We know that the group D_5, is the group of symmetries of a pentagon. Hence, D_5 acts on the color patterns. Verify that

   $$P_{D_5}(z_1, z_2, \ldots, z_5) = \frac{1}{|D_5|}(z_1^5 + 4z_5 + 5z_1 z_2^2) = \frac{z_1^5 + 4z_5 + 5z_1 z_2^2}{10}.$$

   Thus, by Theorem 11.4.8, the required number equals $N = \frac{1}{10}(3^5 + 4 \cdot 3 + 5 \cdot 3 \cdot 3^2) = 39.$

2. Suppose we are given beads of 3 different colors and that there are at least 6 beads of each color. Determine the distinct necklace patterns that are possible using the 6 beads.

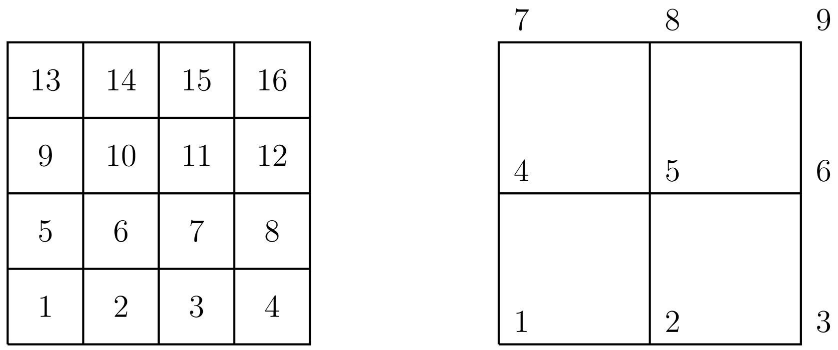
   Answer : Since we are forming a necklace using 6 beads, the group D_6 acts on the 6 beads of the necklace. Also, the cycle index polynomial of D_6 equals

   $$P_{D_6}(z_1, z_2, \ldots, z_5, z_6) = \frac{1}{|D_6|}(z_1^6 + 2z_6 + 2z_3^2 + z_2^3 + 3z_2^3 + 3z_1^2 z_2^2).$$

Hence, by Theorem 11.4.8, the number of distinct necklace patterns equals $\frac{1}{12}(3^6 + 2 \cdot 3 + 2 \cdot 3^2 + 4 \cdot 3^3 + 3 \cdot 3^2 \cdot 3^2) = 92$.

3. Consider the 2×2 square given in Figure 11.7. Determine the number of distinct color patterns, when the vertices of the given figure are colored with two colors.

   Answer: Observe that D_4 is the group of symmetries of the 2×2 square and it needs to act on 9 vertices. So, we need to write the elements of D_4 as a subgroup of $\mathcal{S}_9$. Hence, the cycle index polynomial is given by $P_{D_4}(z_1, \ldots, z_9) = \dfrac{z_1^9 + 2z_1z_4^2 + z_1z_2^4 + 4z_1^3z_2^3}{8}$ and the number of distinct color patterns equals 102.



The 4×4 Square   The 2×2 Square

Figure 11.7: Faces and Vertices of Squares

4. Determine the number of distinct color patterns when the faces of a cube are colored with 2 colors.

   Answer: Using the group of symmetries of the cube given on Page 236, the cycle index polynomial corresponding to the faces equals $P_G(z_1, \ldots, z_{12}) = \dfrac{z_1^{12} + 6z_4^3 + 3z_2^6 + 8z_3^4 + 6z_1^2z_2^5}{24}$. Thus, the required number is 218.

Exercise **11.4.10.** *Determine the number of distinct color patterns when*

1. *the faces of the 4×4 square given in Figure 11.7 are colored with 2 colors.*

2. *the edges of a cube are colored with 2 colors. Hint: The cycle index polynomial equals* $P_G(z_1, z_2, \ldots, z_6) = \frac{1}{24}\left(z_1^6 + 6z_1^2z_4 + 3z_1^2z_2^2 + 6z_2^3 + 8z_3^2\right)$.

11.5 Polya's inventory polynomial

In this section, the ideas of the previous subsection are generalized. This generalization allows us to count the distinct number of necklaces even if there are not sufficient number of beads of each color. To do this, each element of C is assigned a *weight*, that in turn gives weight to each color pattern. This weight may be a number, a variable or in general, an element of a commutative ring with identity. The setup for our study remains the same. To start with, we have the following definitions.

Definition 11.5.1. Let A be a commutative ring with identity (the elements of A are called weights). Let $w : C \to A$ be a map that assigns weight to each color. Then the **weight of a color pattern** $\phi : X \to C$, with respect to the weight function w is given by $w(\phi) = \prod\limits_{x \in X} w\big(\phi(x)\big)$.

Fix $g \in G$. Then we have seen that g fixes a color pattern $\phi \in \Omega$ if and only if ϕ colors the elements in a given cycle of g with the same color. Similarly, for each fixed $g \in G$ and $\phi \in \Omega$, one has

$$w(g \circledast \phi) = \prod_{x \in X} w\big(g \circledast \phi(x)\big) = \prod_{x \in X} w\big(\phi(g^{-1} \star x)\big) = \prod_{y \in X} w\big(\phi(y)\big) = w(\phi), \tag{11.5}$$

as $\{g \star x : x \in X\} = X$ (see Remark 11.3.2). That is, for a fixed $\phi \in \Omega$, the weight of each element of $\mathcal{O}(\phi) = \{g \circledast \phi : g \in G\}$ is the same and it equals $w(\phi)$. That is, $w(\phi) = w(\psi)$, whenever $\psi = g \circledast \phi$, for some $g \in G$.

Example 11.5.2. Let X consist of the set of faces of a cube, G be the group of symmetries of the cube and let C consist of two colors 'red' and 'blue'. Thus, if the weights R and B are assigned to the two elements of C then the weight

1. B^6 corresponds "all faces being colored blue";
2. R^2B^4 corresponds to "any two faces being colored 'red' and the remaining four faces being colored 'blue';
3. R^3B^3 corresponds to "any three faces being colored 'red' and the remaining three faces being colored 'blue' and so on.

The above examples indicate that different color patterns need not have different weights. We also need the following definition to state and prove results in this area.

Definition 11.5.3. Let G be a group acting on the set Ω, the set of color patterns and let $w : C \to A$ be a weight function. The pattern inventory, denoted I, under the action of G on Ω, with respect to w, is the sum of the weights of the orbits. That is, $I = \sum\limits_{\Delta} w(\Delta)$, where the sum runs over all the distinct orbits Δ obtained by the action of G on Ω.

With the above definitions, we are ready to prove the Polya's Enumeration Theorem. To do so, we first need to prove the weighted Burnside's Lemma. This Lemma is the weighted version of the Burnside's Lemma.

Lemma 11.5.4. *With the definitions and notations as above,*

$$I = \sum_{\Delta} w(\Delta) = \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{\phi \in \Omega \\ g \circledast \phi = \phi}} w(\phi),$$

where the sum runs over all the distinct orbits Δ obtained by the action of G on Ω.

Proof. As G acts on Ω, for each $\alpha \in \Omega$, the application of Lemma 11.3.7 gives $|G_\alpha| \cdot |\mathcal{O}(\alpha)| = |G|$. Since Δ is an orbit under the action of G, for each $\phi \in \Delta$, $|G_\phi| \cdot |\Delta| = |G|$. Also, by definition, $w(\Delta) = w(\phi)$, for all $\phi \in \Delta$. Thus,

$$w(\Delta) = w(\phi) = \frac{1}{|\Delta|} \sum_{\phi \in \Delta} w(\phi) = \sum_{\phi \in \Delta} \frac{1}{|\Delta|} w(\phi) = \sum_{\phi \in \Delta} \frac{|G_\phi|}{|G|} w(\phi) = \frac{1}{|G|} \sum_{\phi \in \Delta} |G_\phi| \cdot w(\phi).$$

Let $F_g = \{\phi \in \Omega : g \circledast \phi = \phi\}$. Then $\sum\limits_{\phi \in \Omega} \sum\limits_{g \in G_\phi} w(\phi) = \sum\limits_{g \in G} \sum\limits_{\phi \in F_g} w(\phi)$ and hence

$$\begin{aligned} I &= \sum_{\Delta} w(\Delta) = \sum_{\Delta} \frac{1}{|G|} \sum_{\phi \in \Delta} |G_\phi| \cdot w(\phi) = \frac{1}{|G|} \sum_{\Delta} \sum_{\phi \in \Delta} |G_\phi| \cdot w(\phi) = \frac{1}{|G|} \sum_{\phi \in \Omega} |G_\phi| \cdot w(\phi) \\ &= \frac{1}{|G|} \sum_{\phi \in \Omega} \sum_{g \in G_\phi} w(\phi) = \frac{1}{|G|} \sum_{g \in G} \sum_{\phi \in F_g} w(\phi). \end{aligned}$$

∎

We are now in a position to prove the Polya's Enumeration Theorem. Before doing so, recall that F_g consists precisely of those color schemes which color each cycle of g with just one color (see the argument used in the second paragraph in the proof of Theorem 11.4.8).

Theorem 11.5.5. [Polya's enumeration theorem] *With the definitions and notations as above,*

$$I = \sum_{\Delta} w(\Delta) = P_G(x_1, x_2, \ldots, x_n),$$

where the sum runs over all the distinct orbits Δ obtained by the action of G on Ω and $x_i = \sum\limits_{c \in C} w(c)^i$, is the i^{th} power sum of the weights of the colors. In particular, $I = P_G(|C|, |C|, \ldots, |C|)$, if weight of each color is 1.

Proof. Using the weighted Burnside Lemma 11.5.4, we need to prove that

$$\sum_{g \in G} \sum_{\phi \in F_g} w(\phi) = \sum_{g \in G} x_1^{\ell_1(g)} x_2^{\ell_2(g)} \cdots x_n^{\ell_n(g)},$$

where $\ell_i(g)$ is the number of cycles of length i in the cycle representation of g.

Now, fix a $g \in G$. Suppose g has exactly t disjoint cycles, say $g_1, g_2, \ldots, g_t$. As F_g consists precisely of those color schemes which color each cycle of g with just one color, we just need to determine the weight of such a color pattern. To do so, for $1 \le i \le t$, define X_i to be that subset of X whose elements form the cycle g_i. Then, it is easy to see that $X_1, X_2, \ldots, X_t$ defines a partition of X. Also, the condition that x and $g \star x$ belong to the same cycle of g, one has $w(\phi(s_i)) = w(\phi(g \star s_i))$, for each $s_i \in X_i, 1 \le i \le t$. Thus, for each $\phi \in F_g$,

$$w(\phi) = \prod_{x \in X} w(\phi(x)) = \prod_{i=1}^{t} \prod_{x \in X_i} w(\phi(x)) = \prod_{i=1}^{t} w(\phi(s_i))^{|X_i|}.$$

Note that if we pick a term from each factor in $\prod\limits_{i=1}^{t} \left(\sum\limits_{c \in C} w(c)^{|X_i|} \right)$ and take the product of these terms, we obtain all the terms of $\prod\limits_{i=1}^{t} \left(\sum\limits_{c \in C} w(c)^{|X_i|} \right)$. All these terms also appear in $\sum\limits_{\phi \in F_g} \prod\limits_{i=1}^{t} w(\phi(s_i))^{|X_i|}$ because as ϕ is allowed to vary over all elements of F_g, the images $\phi(s_i)$, for $1 \le i \le t$, take all values in C. The argument can also be reversed and hence it follows that

$$\sum_{\phi \in F_g} w(\phi) = \sum_{\phi \in F_g} \prod_{i=1}^{t} w(\phi(s_i))^{|X_i|} = \prod_{i=1}^{t} \left(\sum_{c \in C} w(c)^{|X_i|} \right).$$

Now, assume that g has $\ell_k(g)$ cycles of length k, $1 \le k \le n$. This means that in the collection $|X_1|, |X_2|, \ldots, |X_t|$, the number 1 appears $\ell_1(g)$ times, the number 2 appears $\ell_2(g)$ times and so on till the number n appears $\ell_n(g)$ times (note that some of the $\ell_i(g)$'s may be zero). Consequently, $\prod\limits_{i=1}^{t} \left(\sum\limits_{c \in C} w(c)^{|X_i|} \right)$ equals $\prod\limits_{k=1}^{n} x_k^{\ell_k(g)}$, as $x_1 = \sum\limits_{c \in C} w(c)$, $x_2 = \sum\limits_{c \in C} w(c)^2$ and so on till $x_n = \sum\limits_{c \in C} w(c)^n$. Hence, $\sum\limits_{\phi \in F_g} w(\phi) = \prod\limits_{k=1}^{n} x_k^{\ell_k(g)}$ and thus, the required result follows. ∎

Example 11.5.6. 1. Consider a necklace consisting of 6 beads. If there are 3 color choices, say R, B and G, then determine

(a) the number of necklaces that have at least one R bead.

(b) the number of necklaces that have three R, two B and one G bead.

Ans: Recall that D_6 acts on a regular hexagon and its cycle index polynomial equals

$$P_{D_6}(z_1, z_2, \ldots, z_6) = \frac{1}{12}(z_1^6 + 4z_2^3 + 2z_3^2 + 2z_6 + 3z_1^2 z_2^2).$$

So, for the first part, at least one R needs to be used and the remaining can be any number of B and/or G. So, we define the weight of the color R as x and that of B and G as 1. Therefore, by Polya's Enumeration Theorem 11.5.5,

$$\begin{aligned} I &= \frac{1}{12}\left((x+1+1)^6 + 4(x^2+1+1)^3 + 2(x^3+1+1)^2 \right. \\ &\qquad \left. +2(x^6+1+1) + 3(x+1+1)^2(x^2+1+1)^2\right) \\ &= x^6 + 2x^5 + 9x^4 + 16x^3 + 29x^2 + 20x + 15. \end{aligned}$$

So, the required answer is $1 + 2 + 9 + 16 + 29 + 20 = 77$.

For the second part, define the weights as R, B and G itself. Then

$$\begin{aligned} I &= \frac{1}{12}\left((R+B+G)^6 + 4(R^2+B^2+G^2)^3 + 2(R^3+B^3+G^3)^2 \right. \\ &\qquad \left. +2(R^6+B^6+G^6) + 3(R+B+G)^2(R^2+B^2+G^2)^2\right). \end{aligned}$$

The required answer equals the coefficient of R^3B^2G in I, which equals

$$\frac{1}{12}\left(C(6;3,2,1) + 3\cdot 2\cdot 2\right) = \frac{1}{12}\left(\frac{6!}{3!2!} + 6\right) = 6.$$

We end this chapter with a few Exercises. But before doing so, we give the following example with which Polya started his classic paper on this subject.

Example 11.5.7. Suppose we are given 6 similar spheres in three different colors, say, three red, two blue and one yellow (spheres of the same color being indistinguishable). In how many ways can we distribute the six spheres on the 6 vertices of an octahedron freely movable in space?

Ans: Here $X = \{1,2,3,4,5,6\}$ and $C = \{R, B, Y\}$. Using Example 11.1.9.2b on Page 236 the cycle index polynomial corresponding to the symmetric group of the octahedron that acts on the vertices of the octahedron is given by

$$\frac{1}{24}\left(z_1^6 + 6z_1^2 z_4 + 3z_1^2 z_2^2 + 8z_3^2 + 6z_2^3\right).$$

Hence, the number of patterns of the required type is the coefficient of the term R^3B^2Y in

$$\begin{aligned} I &= \frac{1}{24}\left((R+B+Y)^6 + 6(R+B+Y)^2(R^4+B^4+Y^4) + 3(R+B+Y)^2(R^2+B^2+Y^2)^2 \right. \\ &\qquad \left. +8(R^3+B^3+Y^3)^2 + 6(R^2+B^2+Y^2)^3\right). \end{aligned}$$

Verify that this number equals 3.

Exercise **11.5.8.** 1. *Three black and three white beads are strung together to form a necklace. If the beads of the same color are indistinguishable, determine the number of distinct necklace patterns, if the necklace can only be rotated. What is the number if the necklace can be rotated and turned over?*

2. *Suppose the edges of a regular tetrahedron are being colored with white and black. Then determine the number of patterns that have exactly four black edges and two white edges.*

3. *Consider the molecules CH_4, C_2H_6 and C_6H_6 given in Figure 11.8. In each case, determine the number of possible molecules that can be formed, if the hydrogen atoms can be replaced by either Fluorine, Chlorine or Bromine.*

4. *In essentially how many different ways can we color the vertices of a cube if n colors are available?*

5. *Three ear-rings are shown in Figure 11.8. In each case, the ear-ring can be rotated along the horizontal axis passing through the central vertex (highlighted with dark circle). Then determine the following:*
   (a) *The group that acts on the ear-rings.*
   (b) *Write the elements of the group as a subgroup of $\mathcal{S}_n$, for a proper choice of n.*
   (c) *Determine the number of distinct color patterns when there are sufficient number of beads of both the colors "RED" and "BLUE".*

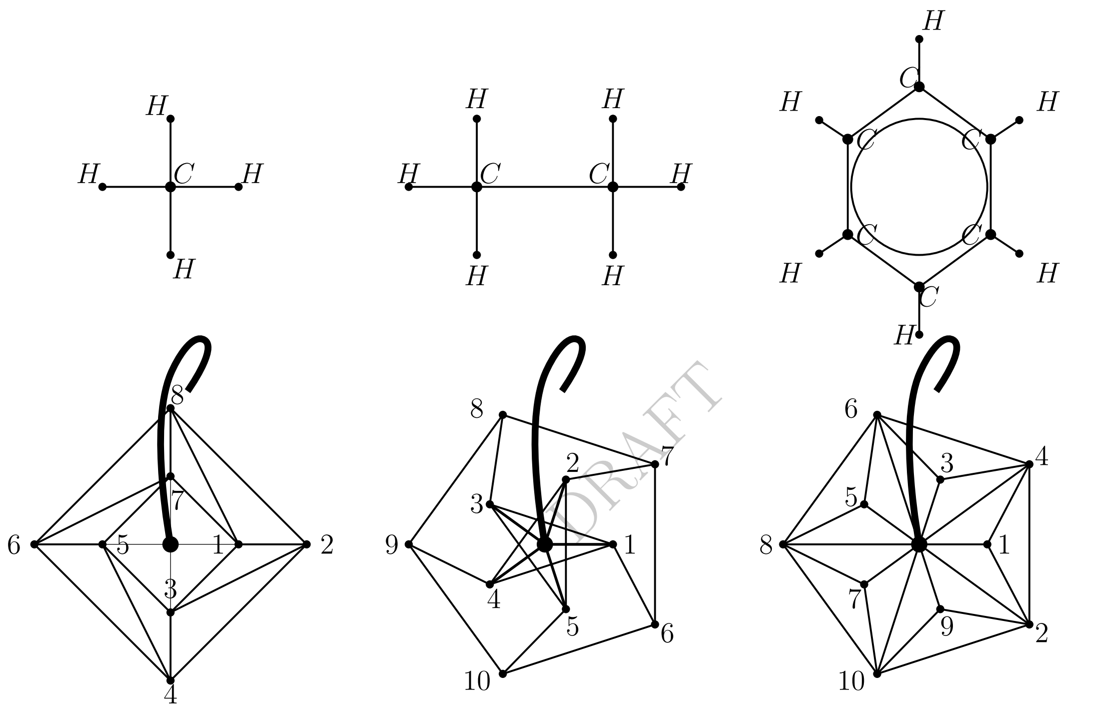


Figure 11.8: Three ear-rings and three molecules, CH_4, C_2H_6 and C_6H_6.

6. *Let p be a prime suppose that we want to make a necklace consisting of p beads. If for each bead, one has n choices of colors, then determine the number of distinct necklace patterns. Use this number to prove the Fermat's little theorem.*

7. *Prove that the cycle index polynomial for the vertices, edges and faces of the octahedron is respectively, equal to*

$$\begin{aligned}
P(z_1,\ldots,z_6) &= \frac{1}{24}\left(z_1^6+6z_1^2z_4+3z_1^2z_2^2+8z_3^2+6z_2^3\right),\\
P(z_1,\ldots,z_{12}) &= \frac{1}{24}\left(z_1^{12}+6z_4^3+3z_2^6+8z_3^4+6z_1^2z_2^5\right),\\
P(z_1,\ldots,z_8) &= \frac{1}{24}\left(z_1^8+6z_4^2+9z_2^4+8z_1^2z_3^2\right).
\end{aligned}$$

8. *Consider the following problems that appeared in Section 5.5. Note that we need to consider only the rotations to form the group.*
   (a) *Find the number of circular arrangements of $\{A, B, B, C, C, D, D, E, E\}$.*

(b) *Find the number of circular arrangements of* $S = \{A, A, B, B, C, C, D, D, E, E\}$.

(c) *How many circular arrangements of* $\{A, A, A, B, B, B, C, C, C\}$ *are there?*

(d) *Determine the number of circular arrangements of size* 5 *using the alphabets* A, B *and* C.

(e) *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, in the following cases.*

   i. *The flowers can have colors 'red' or 'blue'.*

   ii. *The flowers can have the colors 'red', 'blue' or 'green'.*

   iii. *The flowers can have* k *colors.*

(f) *Determine the number of distinct garlands that can be formed using* 6 *flowers,* 4 *of which are blue and* 2 *are red.*

(g) *Find the number of circular permutations of* $\{A, A, B, B, C, C, C, C\}$.

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] D. M. Cvetkovic, Michael Doob and Horst Sachs, *Spectra of Graphs: theory and applications*, Academic Press, New York, 1980.

[4] D. I. A. Cohen, *Basic Techniques of Combinatorial Theory*, John Wiley and Sons, New York, 1978.

[5] William Dunham, *Euler: The Master of Us All*, Published and Distributed by The Mathematical Association of America, 1999.

[6] F. Harary, *Graph Theory*, Addison-Wesley Publishing Company, 1969.

[7] T. J. Jech, *The Axiom of Choice*, Dover, 2008.

[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] G. H. Moore, *Zermelo's Axiom of Choice: Its Origins, Development and Influence*, Dover, 2013.

[12] J. Riordan, *Introduction to Combinatorial Analysis*, John Wiley and Sons, New York, 1958.

[13] R. P. Stanley, *Enumerative Combinatorics, vol. 2*, Cambridge University Press, 1999.

[14] H. S. Wilf, *Generatingfunctionology*, Academic Press, 1990.

Index