Contents

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.

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

$[0] = \{\ldots, -3n, -2n, -n, 0, n, 2n, \ldots\}$.
$[1] = \{\ldots, -3n+1, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}$.
$[2] = \{\ldots, -3n+2, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\}$.
$\vdots$
$[n-2] = \{\ldots, -2n-2, -n-2, -2, n-2, 2n-2, 3n-2, \ldots\}$.
$[n-1] = \{\ldots, -2n-1, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}$.

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.

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 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 $X = \{k \in \mathbb{N} :$ 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

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

$\ell = 1, 2, \ldots, n$. 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 $\mathbb{N}\backslash\{1, 2, \ldots, n_0\}$ (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 $n = k$. 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* $n = 5x + 9y$.

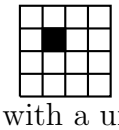
11. *Prove that, for all* $n \geq 40$, *there exist non-negative integers* x *and* y *such that* $n = 5x + 11y$.

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.*

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

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

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.*

the condition $-x \leq y$ is equivalent to the condition $0 \leq y + x$ which in turn is equivalent to $-y \leq x$. Hence $|y| = -y \leq x$. Thus, the required result follows. ∎

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

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

Proof. Using Lemma 2.6.12, one has $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$. Hence,

$$-|x| + (-|y|) \leq x + y \leq |x| + |y|.$$

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 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.

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.

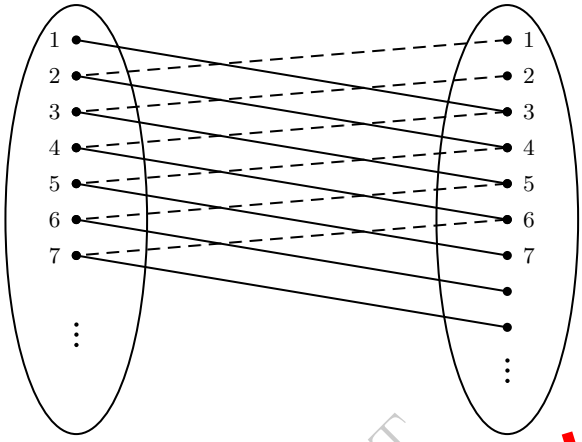


Figure 3.1: Graphic representation of functions f and g

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 $\mathsf{rng}\, f$. Since f is not an onto function, there are elements in $Y \setminus \mathsf{rng}\, f$. 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 $y \notin \mathsf{rng}\, f$. 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 $\mathsf{rng}\, f$. 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 $g(x) = x + 2$.*

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

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

2. Fix $N \in \mathbb{N}, N \geq 2$. 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 $a_1 b_1 d = ab/d = a_1 b$, 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.

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.

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 $1 \leq k \leq n-1$ 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 $x = x_1x_2\ldots x_n \in X$, 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, $C(0; 0, \ldots, 0) = 1$.

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 $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

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:

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 $\mathsf{rng}\, f$, and $\mathsf{rng}\, f$ 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. ∎

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 $1 \leq i \leq k$, 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.*

Theorem 5.8.8. **[Recurrence relation for C_n]** *Let $n \in \mathbb{N}$. Then $C_n = \sum_{i=1}^{n} C_{i-1}C_{n-i} = \sum_{i=0}^{n-1} C_i C_{n-1-i}$.*

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,

$$C_n = \sum_{i=1}^{n} C_{i-1}C_{n-i} = \sum_{i=0}^{n-1} C_i C_{n-1-i}.$$

■

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.

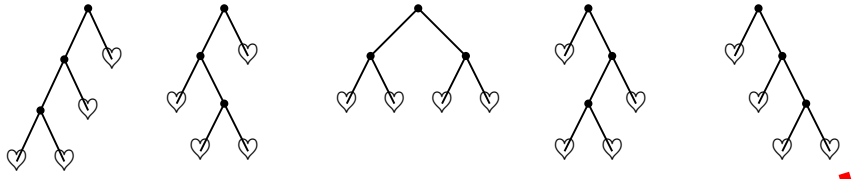


Figure 5.4: Full binary trees on 7 vertices (or 4 leaves)

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, $f(n) = \sum_{k=0}^{n-1} f(k)f(n-k-1)$. 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 $C_n = \sum_{i=1}^{n} C_{i-1}C_{n-i}$ 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 $\sum_{k=0}^{n} C(n,k) = 2^n$.*
4. *Use lattice paths to give a combinatorial proof of $\sum_{k=0}^{n} C(n,k)^2 = C(2n,n)$. [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).]*

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:

$$n, n-1, \cdots, 1, 2n, 2n-1, \ldots, n+1, 3n, 3n-1, \ldots, 2n+1, \ldots, mn, mn-1, \cdots, mn-n+1.$$

■

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 $px \geq b$, then $(a,b) \subseteq \big((p-1)x, px\big)$ and so $b - a \leq x < \frac{1}{n}$, which is not possible. So, $px \in (a,b)$ and $px \in S$ as well. Thus, $(a.b) \cap S \neq \emptyset$. ∎

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 $\bigcup_i P_i = X$. 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 $\prod_{i=1}^{n} \big(i - p(i)\big)$ 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.*

4. Evaluate $S := \sum_{k=0}^{\infty} \frac{k}{2^k} = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots$.

   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

$$\begin{array}{l} \frac{1}{2} \qquad\qquad + \\ \frac{1}{4} + \frac{1}{4} \qquad + \\ \frac{1}{8} + \frac{1}{8} + \frac{1}{8} \quad + \\ \vdots \\ \hline 1 + \frac{1}{2} + \cdots = 2. \end{array}$$

EXERCISE **6.3.12.** *1. Determine a closed form expression for $\sum_{n\geq 0} nx^n \in \mathbb{Q}[[x]]$. Or in other words, write $\sum_{n\geq 0} nx^n = \frac{p(x)}{q(x)}$, 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 $\sum_{n\geq 0} \frac{n^2 + 5n + 16}{n!}$.*
5. *Determine a closed form expression for $\sum_{k=1}^{N} k^3$.*
6. *For $n, r \in \mathbb{N}$ determine the number of non-negative solutions to $x_1 + 2x_2 + \cdots + nx_n = r$ in the unknowns x_i's.*
7. *Determine $\sum_{k=0}^{\infty} \frac{1}{2^k} C(n+k-1, k)$.*
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.*

We show that there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ such that $u(n) = \sum_{i=1}^{r} \alpha_i x_i^n$ 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 $u(n) = \sum_{i=1}^{r} \alpha_i x_i^n$ 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 $u(n) = \sum_{i=1}^{r} \alpha_i x_i^n$ 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 $u(n) = \sum_{i=1}^{r} \alpha_i x_i^n$ 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, $x_i^k = \sum_{j=1}^{r} c_j x_i^{k-j}$. 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, $u(n) = \sum_{i=1}^{r} \alpha_i x_i^n$ 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, $y(n) = \sum_{i=1}^{r} \gamma_i x_i^n$ 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 α is replaced by γ. 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

$$a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]. \tag{6.6}$$

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 $C_0 = \lim_{x\to 0} g(x) = 1$. 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, $g(x) = \sum_{n=0}^{\infty} C_nx^n$. Then, for $n \geq 1$,

$$\text{CF}\left[x^{n-1}, g(x)^2\right] = \text{CF}\left[x^{n-1}, \left(\sum_{n=0}^{\infty} C_nx^n\right)^2\right] = \sum_{i=0}^{n-1} C_iC_{n-1-i} = C_n \text{ using Equation (6.9).}$$

That is, $\text{CF}\left[x^n, xg(x)^2\right] = C_n$. 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 $\lim_{x\to 0} g(x) = C_0 = 1$, 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 $\sum_{k=0}^{n} a_ka_{n-k} = C(n+r, r)$ for all $n \geq 1$. Determine a_n.

   Answer: Let $g(x) = \sum_{n\geq 0} a_nx^n$. Using $C(n+r, r) = C(n+(r+1)-1, n)$, we obtain

$$g(x)^2 = \sum_{n\geq 0}\left(\sum_{k=0}^{n} a_ka_{n-k}\right)x^n = \sum_{n\geq 0} C(n+r, r)x^n = \sum_{n\geq 0} C(n+r, n)x^n = \frac{1}{(1-x)^{r+1}}.$$

   Hence, $a_n = \text{CF}\left[x^n, \frac{1}{(1-x)^{(r+1)/2}}\right]$. For example, when $r = 2$

$$a_n = (-1)^nC(-3/2, n) = \frac{3\cdot 5\cdot 7\cdots(2n+1)}{2^n\ n!} = \frac{(2n+1)!}{2^{2n}n!n!}.$$

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

$$f(n,m) = f(n-1,m) + f(n-1,m-1) \quad \text{for } n > 0,\ m > 0. \tag{6.10}$$

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 $\neg$, $\wedge$, $\vee$, $\rightarrow$ and $\leftrightarrow$, respectively. Then the complex statements are made using these symbols along with parentheses by following some specified rules.

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)
$$\begin{aligned} p \leftrightarrow p \wedge q &\equiv \big(\neg p \vee (p \wedge q)\big) \wedge \big(p \vee \neg(p \wedge q)\big) && \text{Biconditional} \\ &\equiv \big(\neg p \vee (p \wedge q)\big) \wedge (p \vee (\neg p \vee \neg q)) && \text{De Morgan} \\ &\equiv (\neg p \vee p) \wedge (\neg p \vee q) \wedge (p \vee (\neg p \vee \neg q)) && \text{Distributivity} \\ &\equiv \neg p \vee q && \text{Constants} \\ &\equiv p \to q && \text{Implication} \end{aligned}$$

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 $\forall x \big(P(x) \to B(x) \vee M(x)\big)$.

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 $\exists x \big(S(x) \wedge (H(x) \vee E(x))\big)$.

   Note that $\exists x \big(S(x) \to H(x) \vee E(x)\big)$ is not the correct 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 $Q(x)$.

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.

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.

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 laws 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.

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 $\bigcup_{\alpha\in I} A_\alpha$. Similarly, the product of this family consists of all functions f from I to $\bigcup_{\alpha\in I} A_\alpha$, 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 $\bigcup_{Y\in\mathcal{C}} Y$; 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 $f : \mathcal{C} \to \bigcup_{Y\in\mathcal{C}} Y$, 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 $f : \{B_\alpha : \alpha \in I\} \to \bigcup_{\alpha\in I} B_\alpha$ 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.

This is a contradiction.

(Tukey's lemma ⇒ 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 ⇒ 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 ⇒ 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

$$B \subseteq C, \quad \leq_B \subseteq \leq_C, \quad \text{if } b \in B \text{ and } c \in C \setminus B, \text{ then } (b, c) \in \leq_C.$$

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

$$W = \bigcup\{A : (A, \leq_A) \in \mathcal{C}\}, \quad \leq_W = \bigcup\{\leq_A : (A, \leq_A) \in \mathcal{C}\}.$$

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, $E \not\subseteq D$. 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 ⇒ AC). Assume that Zermelo's well ordering principle is true. Let $\{X_\alpha\}_{\alpha \in L}$ be a nonempty family of nonempty sets. Write $X = \bigcup_{\alpha \in L} X_\alpha$. By Zermelo's well ordering

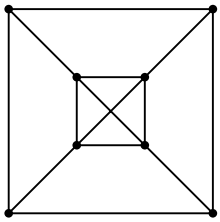
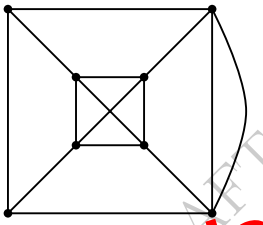
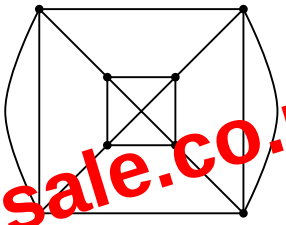
Chapter 9

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-element subsets 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.

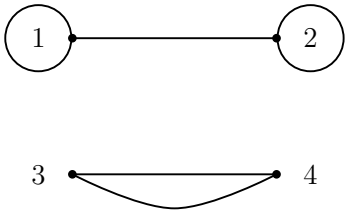


Figure 9.1: A pseudograph

1. **Complete graph**, denoted K_n, if each pair of vertices in G are adjacent.
2. **Path graph**, denoted P_n, if $E = \{\{i, i+1\} : 1 \leq i \leq n-1\}$.
3. **Cycle graph**, denoted C_n, if $E = \{\{i, i+1\} : 1 \leq i \leq n-1\} \cup \{n, 1\}$.
4. **Bipartite graph** if $V = V_1 \cup V_2$ such that $|V_1|, |V_2| \geq 1$, $V_1 \cap V_2 = \varnothing$ 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 $E = \{\{i, j\} : 1 \leq i \leq r, 1 \leq j \leq s\}$.

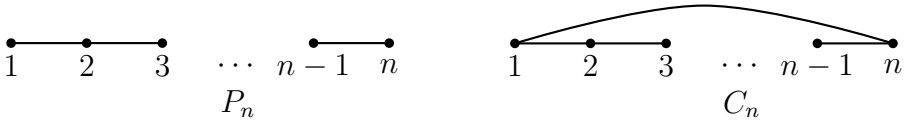


Figure 9.3: P_n and C_n.

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.

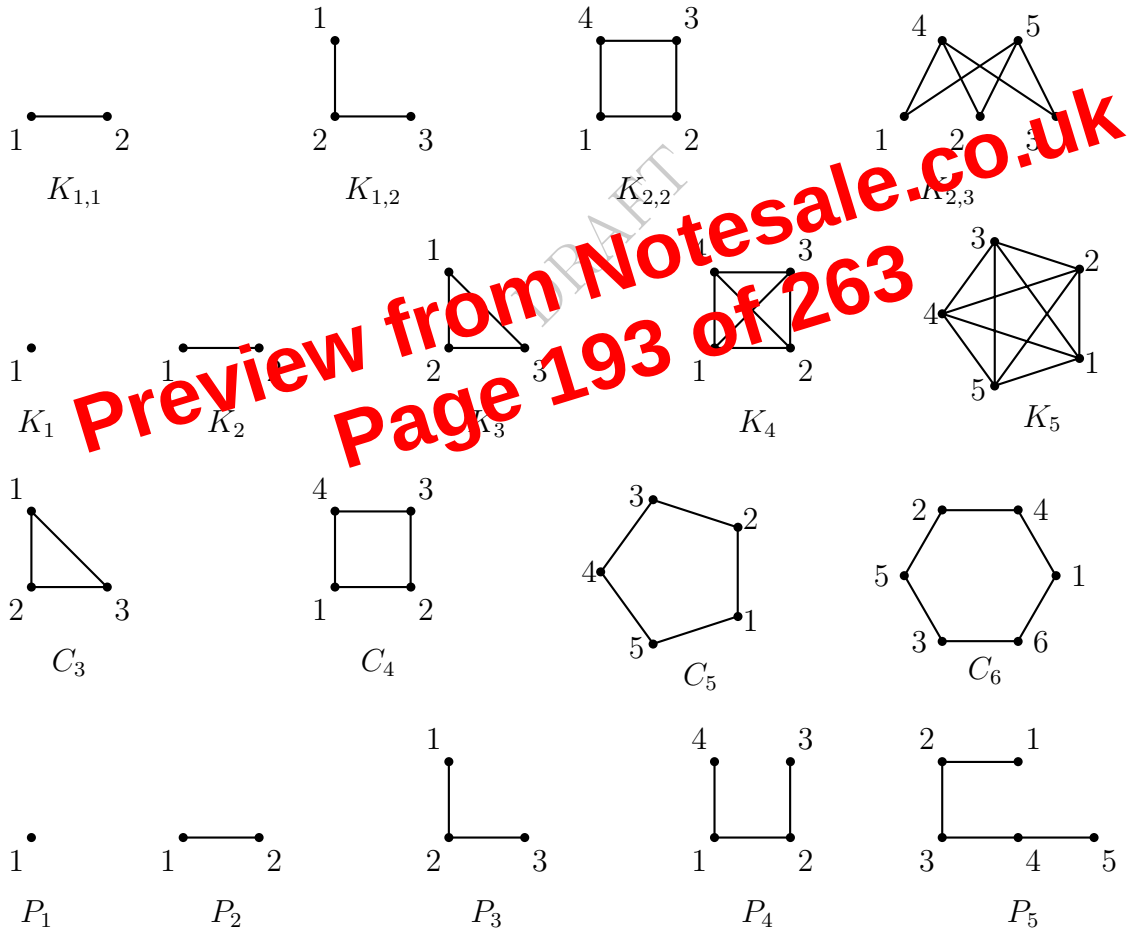


Figure 9.4: Some well known family of graphs

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, $\sum_{v \in V} d(v) = 2|E|$. Thus, the number of vertices of odd degree is even.*

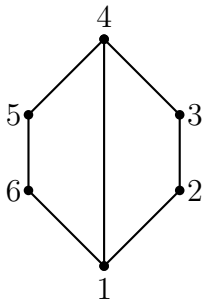
Example 9.3.15. Notice that $\Gamma(C_5)$ has a subgroup $\Gamma_1 = \{\mathbf{e}, \sigma, \sigma^2, \sigma^3, \sigma^4\}$, with $\sigma^5 = \mathbf{e}$, of order 5. Let G be a subgraph of C_5 obtained by deleting some (zero allowed) edges. If $\|G\| = 5$, then $|\Gamma(G)| = 10$. If $\|G\| = 0$, then $|\Gamma(G)| = |S_5| = 5!$. 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 $1, \ldots, n$.*

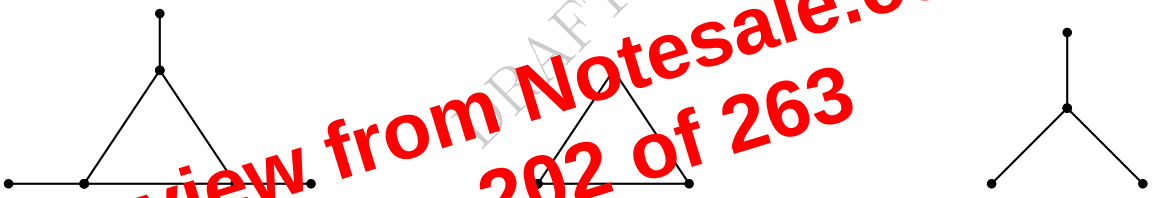
2. Compute $\Gamma(G)$ for some graphs of small order.

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?*

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)⇔(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)⇔(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)⇔(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 $\sum_{i=1}^{k} n_i = n$. As $k \geq 2$, we have $\|G\| = \sum_{i=1}^{k}(n_i - 1) = n - k < n - 1 = \|G\|$, a contradiction.

(1)⇔(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 $\|G\| = n-1$.

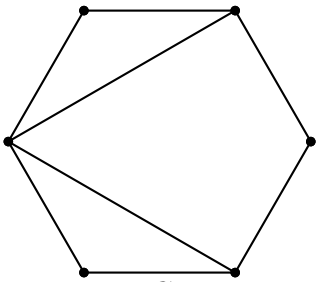
(1)⇔(6). Let G be a tree. Since G is connected, between any two distinct vertices of G there exists a path. If there exist more than one path between $u, v \in V(G)$, then by Proposition 9.2.8 any two of these u-v paths will contain a cycle. This is not possible as G is acyclic. Hence the uniqueness 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. ∎

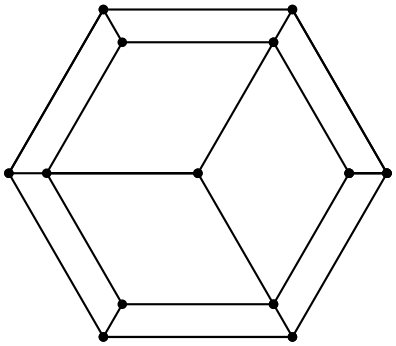
Proposition 9.4.12. *The center of a tree is either a singleton or has at most two vertices.*

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 $\|P(x, w)\| < \|P(x, v)\| \leq k$.



G



H

(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.*

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 $\left[I + A(G)\right]^{n-1}$ 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

$$q_{ij} = \begin{cases} 1 & \text{if edge } e_j \text{ originates at } i, \\ -1 & \text{if edge } e_j \text{ terminates at } i, \\ 0 & \text{if edge } e_j \text{ is not incident with } i. \end{cases}$$

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 $m \in \mathbb{Z}$.

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 $\frac{|G|}{|H|}$.*

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, $|G| = \left|\bigcup_{i=1}^{m} g_iH\right| = \sum_{i=1}^{m} |g_iH| = m|H|$ (the disjoint union gives the second equality). Thus, $|H|$ divides $|G|$ and the number of left cosets equals $m = \frac{|G|}{|H|}$. ∎

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.