Lecture Notes on Discrete Mathematics

S. K. Panda

IIT Kharagpur

April 22, 2020

Relation and Partial ordered Relation

Definition 0.1. [**Cartesian Product**] Let X and Y be two sets. Then their Cartesian product, denoted by $X \times Y$, is defined as $X \times Y = \{(a, b) \ : \ a \in X, b \in Y\}$. The elements of $X \times Y$ are also called ordered pairs with the elements of X as the first entry and elements of Y as the second entry. Thus,

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

Example 0.1.

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

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

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

2. The Euclidean plane, denoted by $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \ : \ x, y \in \mathbb{R}\}$.
3. By convention, $\phi \times X = X \times \phi = \phi$. In fact $X \times Y = \phi$ if and only if either $X = \phi$ or $Y = \phi$.

Theorem 0.1. *Let X, Y, Z and W be nonempty sets. Then, the following statements are true.*

1. *The product construction can be used on sets several times, for example,*

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

2. $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$
3. $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$
4. $(X \times Y) \cap (Z \times W) = (X \cap Z) \times (Y \cap W)$
5. $(X \times Y) \cup (Z \times W) \subseteq (X \cup Z) \times (Y \cup W)$

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

Definition 0.2. [**Relation**] Let X and Y be two nonempty sets. A relation R from X to Y is a subset of $X \times Y$, i.e., it is a collection of certain ordered pairs. We write xRy to mean $(x, y) \in R \subseteq X \times Y$. Thus, for any two sets X and Y, the sets ϕ and $X \times Y$ are always relations from X to Y . A **relation** from X to X is called a relation on X.

Example 0.2. 1. Let X be any nonempty set and consider the set $\mathcal{P}(X)$. Define a relation R on $\mathcal{P}(X)$ by $R = \{(S,T) \in \mathcal{P}(X) \times \mathcal{P}(X) \;:\; S \subseteq T\}$.

2. Let $A = \{a,b,c,d\}$. Some relations R on A are:

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

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

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

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

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

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

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

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

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

3. Let $A = \{1,2,3\}$, $B = \{a,b,c\}$ and let $R = \{(1,a),(1,b),(2,c)\}$.

4. Let $R = \{(x,y) \;:\; x,y \in Z \text{ and } y = x + 5m \text{ for some } m \in Z\}$ is a relation on Z.

Definition 0.3. Let A be a nonempty set. Then, a relation R on A is said to be

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

2. **symmetric:** if for each pair of elements $a,b \in A$, $(a,b) \in R$ implies $(b,a) \in R$.

3. **transitive:** if for each triple of elements $a,b,c \in A$, $(a,b),(b,c) \in R$ imply $(a,c) \in R$.

Definition 0.4. 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 0.3. 1. Consider the relations on A of Example 0.2

   (a) The relation in Example 0.2(1) is not an equivalence relation; it is not symmetric.

   (b) The relation in Example 0.2(2a) is an equivalence relation with $[a] = \{a,b,c,d\}$ as the only equivalence class.

(c) Other relations in Example 0.2(2) are not equivalence relations.

(d) The relation in Example 0.2(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. $[4] = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}$.

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 $[b] = \{b\}$.

Theorem 0.2 (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 $\sim$.*

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

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

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

Definition 0.5. Let X be a nonempty set. Then a **partition** of X is a collection of disjoint, nonempty subsets of X whose union is X.

Example 0.4. Let $X = \{a,b,c,d,e\}$.

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

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

2. Consider the partition $\{\{a\},\{b,c,d\},\{e\}\}$ of X. Verify that the relation $R = \{(a,a),(b,b),(c,c),(d,d),(e,e),(b,c),(c,d),(b,d),(c,b),(d,c),(d,b)\}$ is an equivalence relation on X with equivalence classes $[a] = \{a\}$, $[b] = \{b,c,d\}$ and $[e] = \{e\}$.

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

Theorem 0.3 (**Constructing equivalence relation from equivalence classes**)**.** *Let $\mathcal{P}$ be a partition of a nonempty set X. Let $\sim$ be the relation on X defined by for each pair of elements $x,y \in X$, $x \sim y$ if and only if both x and y are elements of the same subset A in $\mathcal{P}$.*

Proof. The construction of $\sim$ says that if A and B are two distinct elements of $\mathcal{P}$, then all elements of A are related to each other by $\sim$, all elements of B are related to each other by $\sim$, but no element of A is related to any element of B by $\sim$. Let $x \in X$. Since $\mathcal{P}$ is a partition, $x \in A$ for some $A \in \mathcal{P}$. Then $x \sim x$. So,$\sim$ is reflexive.

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

To complete the proof, we show that

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

2. each element of P is an equivalence class of $\sim$.

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

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

Definition 0.6. [**Inverse Relation**] Let X and Y be two nonempty sets and let R be a relation from X to Y. Then, the inverse relation, denoted by R^1, is a relation from Y to X, defined by $R^1 = \{(y,x) \in Y \times X \ : \ (x,y) \in R\}$. So, for all $x \in X$ and $y \in Y$ $(x,y) \in R$ if and only if $(y,x) \in R^1$

Example 0.5. 1. If $R = \{(1,a),(1,b),(2,c)\}$ then $R^1 = \{(a,1),(b,1),(c,2)\}$.

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

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

    1. $(x, y) \notin R$ for all $y \in Y$.

    2. There is a unique $y \in Y$ such that $(x, y) \in R$.

    3. There exists at least two elements $y_1, y_2 \in Y$ such that $(x, y_1), (x, y_2) \in R$.

Definition 0.7. Let R be a nonempty relation from X to Y. Then,

1. the set **dom** $R := \{x : (x, y) \in R\}$ is called the domain of R, and

2. the set **rng** $R := \{y \in Y : (x, y) \in R\}$ is called the range of R.

Example 0.6. Let a, b, c and d be distinct symbols and let $R = \{(1, a), (1, b), (2, c)\}$. Then,

1. **dom** $R = \{1, 2\}$, **rng** $R = \{a, b, c\}$,

2. **dom** $R^1 = \{a, b, c\}$, **rng** $R^1 = \{1, 2\}$,

Definition 0.8. Let X be a nonempty set. A relation R on X is called antisymmetric if $(a, b) \in R$ and $(b, a) \in R$ imply $a = b$.

Example 0.7. 1. Let $X = \mathbb{R}$ and xRy if and only if x is less than or equal to y. Then R is a partially order relation.

2. Let $X = \mathbb{N}$ and xRy if and only if x divides y. Then R is a partial order relation.

3. Let X be a non-empty set. Let R is a relation on $\mathcal{P}(x)$ defined by ARB if and only if $A \subseteq B$. Then R is a partial order relation on $\mathcal{P}(X)$.

4. Let $X = \{1, 2, 3\}$. $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$. Then R is a partial order relation on R.

A partial order relation is denoted by ‘ $\leq'$.

Let ‘ $\leq'$ be a partial order relation on X. Then $(x, \leq)$ is called partially ordered set.

Definition 0.9. Let $(x, \leq)$ be a partially ordered set. Let $x, y \in X$. Then x and y are comparable if $x \leq y$ or $y \leq x$.

Remark: Let $(x, \leq)$ be a partially ordered set. Let $x, y \in X$. If $x \leq y$, then we say x is less than equal to y or y is getter than equal to x.

Definition 0.10. Let $(x, \leq)$ be a partially ordered set. Then $(x, \leq)$ is called **totally ordered set** if any two elements in X are comparable.

Definition 0.11. Let $(x, \leq)$ be a partially ordered set. Let $A \subseteq X$. An element $a \in A$ is called **maximal element** of A if a is not smaller than any other element of A. That is there is no $b \in A - \{a\}$ such that $a \leq b$.

Remark:

1. Maximal element of a set if it exists must be an element of that set.

2. Maximal element of a set may not be unique.

Example 0.8. 1. Let $X = \{1, 2, 3\}$. $R = \{(1, 1), (2, 2), (3, 3)\}$. You can easily check that R is a partial order relation on X. Let $A = \{1, 2\}$. Then $1, 2$ ~~and 3~~ are the maximal elements of A.

2. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (0, 1)$. Then A does not have any maximal element.

3. Let $(\mathbb{N}, \leq)$ be a poset where the relation $x \leq y$ iff x divides y. Let $A = \{2, 4, 6, 8, 10\}$. Then 10 is the only maximal of A.

Definition 0.12. Let $(x, \leq)$ be a partially ordered set. Let $A \subseteq X$. An element $a \in A$ is called **minimal element** of A if a is not ~~smaller~~ greater than any other element of A. That is there is no $b \in A - \{a\}$ such that $a \leq b$.

Remark:

1. Minimal element of a set if it exists must be an element of that set.

2. Minimal element of a set may not be unique.

Example 0.9. 1. Let $X = \{1, 2, 3\}$. $R = \{(1, 1), (2, 2), (3, 3)\}$. You can easily check that R is a partial order relation on X. Let $A = \{1, 2\}$. Then $1, 2$ ~~and 3~~ are the minimal elements of A.

2. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (0, 1)$. Then A does not have minimal element.

3. Let $(\mathbb{N}, \leq)$ be a poset where the relation $x \leq y$ iff x divides y. Let $A = \{2, 4, 6, 8, 10\}$. Then 2 is the only minimal elements of A.

Definition 0.13. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. An element $a \in A$ is called **maximum element** of A if $b \leq a$ for all $b \in A$.

Remark:

1. Maximum element of a set if it exists must be an element of that set.

2. Maximum element of a set if it exists is unique.

3. For totally ordered set maximum and maximal concepts are same.

Definition 0.14. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. An element $a \in A$ is called **minimum element** of A if $a \leq b$ for all $b \in A$.

Remark:

1. Minimum element of a set if it exists must be an element of that set.

2. Minimum element of a set if it exists is unique.

3. For totally ordered set minimum and minimal concepts are same.

Definition 0.15. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. An element $a \in X$ is called **upper bound** of A if $b \leq a$ for all $b \in A$.

Remark:

1. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. If A has upper bound, then A is called bounded above.

2. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. The set may or may not have upper bound.

3. Upper bound of a set may not be unique.

4. Maximum element is always an upper bound but upper bound may not be maximum.

Example 0.10. 1. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (0, 1)$. Then $[1, \infty)$ is the set of all upper bounds of A.

2. Let $(\mathbb{N}, \leq)$ be a poset where the relation $x \leq y$ iff x divides y. Let $A = \{2, 4, 6, 8, \ldots\}$. Then A does not have supremum.

3. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (-\infty, 0)$. Then $[0, \infty)$ A are the upper bounds of A.

Definition 0.16. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. An element $a \in X$ is called **lower bound** of A if $b \leq a$ for all $b \in A$.

Remark:

1. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. If A has lower bound, then A is called bounded below.

2. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset. The set may or may not have lower bound.

3. Lower bound of a set may not be unique.

4. Minimum element is always a lower bound but lower bound may not be minimum.

Example 0.11. 1. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (0, 1)$. Then $(-\infty, 0]$ is the set of all lower bounds of A.

2. Let $(\mathbb{N}, \leq)$ be a poset where the relation $x \leq y$ iff x divides y. Let $A = \{2, 4, 6, 8, \ldots\}$. Then 2 and 1 are the lower bounds of A.

3. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (-\infty, 0)$. Then A does not have lower bound.

Definition 0.17. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset and let A be bounded above. Let S be the set of all upper bound of A. Then minimum element of S is called **supremum or least upper bound** of A.

Remark:

1. Supremum of a set is unique.

2. Supremum of a set may not be the element of that set.

3. Maximum is always supremum but supremum may not be maximum. If supremum of a set is an element of that set, then supremum is maximum.

4. If a subset of $\mathbb{R}$ (with usual less than or equal to relation) is bounded above, then that set must have supremum.

Example: Let $X = \mathbb{Q}$ and $\leq$ be usual less than equal. You can easily check that $\mathbb{Q}$ is totally ordered set. Let $S = \{1, 1 + \frac{1}{1!}, 1 + \frac{1}{1!} + \frac{1}{2!}, \ldots\}$. You can easily check that S is bounded above and 3 is one upper bound. But it has no supremum in $\mathbb{Q}$. But S has supremum in $\mathbb{R}$ which is e.

Example 0.12. 1. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (0, 1)$. Then 1 is the supremum of A but 1 is not the maximum of A. A does not have maximum.

2. Let $(\mathbb{N}, \leq)$ be a poset where the relation $x \leq y$ iff x divides y. Let $A = \{2, 4, 6, 8, \ldots\}$. Then A does not have supremum.

3. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (-\infty, 0]$. Then 0 is the supremum as well as maximum of A.

Definition 0.18. Let $(X, \leq)$ be a partially ordered set. Let $A \subseteq X$ be a totally ordered subset and let A be bounded below. Let S be the set of all lower bound of A. Then maximum element of S is called **infimum or greatest upper bound** of A.

Remark:

1. Infimum of a set is unique.

2. Infimum of a set may not be the element of that set.

3. Minimum is always infimum but infimum may not be minimum. If infimum of a set is an element of that set, then infimum is minimum.

4. If a subset of $\mathbb{R}$ (with usual less than or equal to relation) is bounded below, then that set must have infimum.

Example: Let $X = \mathbb{Q}$ and $\leq$ be usual less than equal. You can easily check that $\mathbb{Q}$ is totally ordered set. Let $S = \{-1, -1 - \frac{1}{1!}, 1 - \frac{1}{1!} - \frac{1}{2!}, \ldots\}$. You can easily check that S is bounded below and -3 is one lower bound. But it has no infimum in $\mathbb{Q}$. But S has infimum in $\mathbb{R}$ which is $-e$.

Example 0.13. 1. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (0, 1)$. Then 0 is the infimum of A but 0 is not the minimum of A. A does not have minimum.

2. Let $(\mathbb{N}, \leq)$ be a poset where the relation $x \leq y$ iff x divides y. Let $A = \{2, 4, 6, 8, \ldots\}$. Then 2 is the infimum and minimum of A.

3. Let $(\mathbb{R}, \leq)$ be a poset where the relation $\leq$ is usual less than or equal on $\mathbb{R}$. Let $A = (-\infty, 0)$. Then A does not have infimum.

Definition 0.19. Let $(X, \leq)$ be a partially ordered set. A subset A of X is called **chain** if A is totally ordered set.

Zorn's Lemma: Let $(X, \leq)$ be a partially ordered set. Let every chain have upper bound. Then X has a maximal element.

You can prove that every non-empty vector space has basis by using Zorn's lemma.

Lattice: In a poset, it is not necessary that two elements x, y should have a common upper bound. For instance, consider the poset $\{1, 2, \ldots, 6\}$ with "$a \leq b$ if and only if a

Similarly, in a poset, if a pair $\{x, y\}$ has at least one upper bound, it is not necessary that the set $\{x, y\}$ has an lub.

Definition 0.20. A poset $(X, \leq)$ is called a lattice if each pair $x, y \in X$ has an lub and also a glb. An lub of x, y is also written as $x \vee y$ (read as 'x or y' / 'join of x and y') and a glb of x, y as $x \wedge y$ (read as 'x and y' / 'meet of x and y').

Definition 0.21. A lattice is called a distributive lattice if for all pairs of elements x, y the following conditions, called distributive laws, are satisfied :

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Example 0.14.

1. Consider the poset $X = \{0, 1\}$, where $0 < 1$. So, X is a linearly ordered set. In this case, $a \vee b = max\{a, b\}$ and $a \wedge b = min\{a, b\}$. Hence, X is a lattice.

2. Let $S = \{a, b, c\}$. Consider the poset $calP(S)$ (power set) with the partial order as $\subseteq$. Then $A = A \cup B$ and $A \wedge B = A \cap B$. Verify that $\mathcal{P}(\mathcal{S})$ is a distributive lattice.

Functions

In this notes, Definition of function, one-one(injection) function, onto function, bijection function, inverse function, composite of two functions (notation of composite of two functions $f \circ g$), domain and range of a function.

Definition 0.22. Let X and Y be nonempty sets and let f be a relation from X to Y.

1. f is called a **partial function** from X to Y, denoted by $f : X \rightharpoonup Y$, if for each $x \in X$, $f(\{x\})$ is either a singleton or ϕ.
2. For an element $x \in X$, if $f(\{x\}) = \{y\}$, a singleton, we write $f(x) = y$. Hence, y is referred to as the **image** of x under f; and x is referred to as the **pre-image** of y under f. $f(x)$ is said to be undefined at $x \in X$ if $f(\{x\}) = \phi$.
3. If f is a partial function from X to Y such that for each $x \in X$, $f(\{x\})$ is a singleton then f is called a **function** and is denoted by $f : X \to Y$.

Remark 0.1. Observe that for any partial function $f : X \rightharpoonup Y$, the condition $(a, b), (a, b') \in f$ implies $b = b'$. Thus, if $f : X \rightharpoonup Y$, then for each $x \in X$, either $f(x)$ is undefined, or there exists a unique $y \in Y$ such that $f(x) = y$. Moreover, if $fX \to Y$ is a function, then $f(x)$ exists for each $x \in X$, i.e., there exists a unique $y \in Y$ such that $f(x) = y$.

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

Example 0.15. Let $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ and $X = \{3, 4, b, c\}$.

1. Consider the relation $R_1 = \{(a, 1), (b, 1), (c, 2)\}$ from A to B. The following are true.

   (a) R_1 is a partial function.

   (b) $R_1(a) = 1$, $R_1(b) = 1$, $R_1(c) = 2$. Also, $R_1(\{d\}) = \phi$; thus $R_1(d)$ is undefined.

   (c) $R_1(X) = \{1, 2\}$.

   (d) $R_1^{-1} = \{(1, a), (1, b), (2, c)\}$. So, $R_1^{-1}(\{1\}) = \{a, b\}$ and $R_1^{-1}(2) = c$. For any $x \in X$, $R_1^{-1}(x) = \phi$. Therefore, $R_1^{-1}(x)$ is undefined.

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

   (a) R_2 is a partial function.

   (b) $R_2(a) = 1$, $R_2(b) = 4$, $R_2(c) = 2$ and $R_2(d) = 3$.

   (c) $R_2(X) = \{2, 4\}$.

(d) $R_2^{-1}(1) = a$, $R_2^{-1}(2) = c$, $R_2^{-1}(3) = d$ and $R_2^{-1}(4) = b$. Also, $R_2^{-1}(X) = \{b, d\}$.

Remark 0.2.

1. If $X = \phi$, then by convention, one assumes that there is a function, called the empty function, from X to Y.
2. If $Y = \phi$ and $X \neq \phi$, then by convention, we say that there is no function from X to Y
3. Individual relations and functions are also sets. Therefore, one can have equality between relations and functions, i.e., they are equal if and only if they contain the same set of pairs. For example, let $X = \{-1, 0, 1\}$. Then, the functions $f, g, h : X \to X$ defined by $f(x) = x$, $g(x) = x|x|$ and $h(x) = x^3$ are equal as the three functions correspond to the relation $R = \{(-1, -1), (0, 0), (1, 1)\}$ on X.
4. A function is also called a map.
5. Throughout the book, whenever the phrase 'let $f : X \to Y$ be a function' is used, it will be assumed that both X and Y are nonempty sets.

Definition 0.23. Let X be a nonempty set.

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

Definition 0.24. 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 0.16.

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. There is no one-one function from the set $\{1, 2, 3\}$ to its proper subset $\{1, 2\}$.
4. The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not one-one as $f(-1) = f(1) = 1$.

Definition 0.25. Let $f : X \to Y$ be a function. Let $A \subsetneqq X$ and $A \neq \phi$. 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 0.17. 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.

Definition 0.26. A function $f : X \to Y$ is said to be **surjective** (also called **onto** or a **surjection**) if $f^{-1}(\{b\}) \neq \phi$ 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 0.18.

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. There does not exist any onto function from the set $\{a, b\}$ to its proper superset $\{a, b, c\}$.

Definition 0.27. 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 **equinumerous1** with the set Y if there exists a bijection $f : X \to Y$.

Remark 0.3. Clearly, if a set X is equinumerous with a set Y then Y is also equinumerous with X. Hence, X and Y are said to be equinumerous sets.

Example 0.19.

1. The function $f : \{1, 2, 3\} \to \{a, b, c\}$ defined by $f(1) = c$, $f(2) = b$ and $f(3) = a$, is a bijection. Thus, $f^{-1} : \{a, b, c\} \to \{1, 2, 3\}$ is a bijection; and the set $\{a, b, c\}$ is equinumerous with $\{1, 2, 3\}$.
2. Let X be a nonempty set. Then the identity map on X is a bijection. Thus, the set X is equinumerous with itself.
3. The set $\mathbb{N}$ is equinumerous with $\{2, 3, \ldots\}$. Indeed the function $f : \mathbb{N} \to \{2, 3, \ldots\}$ defined by $f(1) = 3$, $f(2) = 2$ and $f(n) = n + 1$, for all $n \geq 3$ is a bijection.

Definition 0.28. Let f and g be two relations such that $\mathbf{rng}f \subseteq \mathbf{dom}g$. Then, the composition of f and g, denoted by $g \circ f$, is defined

$$g \circ f = \{(x, z) : (x, y) \in f \text{ and } (y, z) \in g \text{ for some } y \in rngf \subseteq domg\}$$

.

Example 0.20. Let $f = \{(\beta, a), (3, b), (3, c)\}$ and $g = \{(a, 3), (b, \beta), (c, \beta)\}$. Then, $g \circ f = \{(3, \beta), (\beta, 3)\}$ and $f \circ g = \{(a, b), (a, c), (b, a), (c, a)\}$.

Theorem 0.4. *Let $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ be functions.*

1. *If f and g are injections then $g \circ f : X \to Z$ is an injection.*
2. *If f and g are surjections then $g \circ f : X \to Z$ is a surjection.*
3. *If f and g are bijections then $g \circ f : X \to Z$ is a bijection.*

Theorem 0.5. *Let $f : X \to Y$ and $g : Y \to X$ be functions such that $(g \circ f)(x) = x$ for each $x \in X$. Then f is one-one and g is onto.*

Countable and Uncountable Sets

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

Prerequisite: Definition of function, one-one(injection) function, onto function, bijection function, inverse function, composite of two functions (notation of composite of two functions $f \circ g$), domain and range of a function. All these things are known to you, so I do not write here. We use $\mathbf{rng} f$ to denote the range of f.

---

least for finite sets. Since the set $\{1, 2, \ldots, m\}$ will be used often, we give a notation for this set.

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

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

Theorem 0.6. *Let $n \in \mathbb{N}$. There exists no one-one function from $[n]$ to any of its proper subsets.*

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

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

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

Case I $m + 1 \in \mathbf{rng} f$.

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

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

$$g(k) = l, g(x) = f(x) \text{ for } x \neq k$$

.

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

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

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

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

Theorem 0.7. *Let $m, n \in \mathbb{N}$. Then the following are true:*

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

Proof. (1) Suppose $m \leq n$. Then the function $Id : [m] \to [n]$ given by $Id(x) = x$ is a one-one function. Conversely, let $f : [m] \to [n]$ be a one-one function. If $m > n$, then $[n]$ is a proper subset of $[m]$. Now, f is one-one function from $[m]$ to a proper subset of $[m]$ contradicting Theorem 0.6. Hence $m \leq n$.

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

Definition 0.29. Two sets are said to be **equinumerous** if there is a bijection between them.

Definition 0.30.

1. A set X is called **finite** if either $X = \phi$ or there exists a bijection from X to $[m]$ for some $m \in \mathbb{N}$; this number m is called the **cardinality** of X and is denoted by $|X|$. We write $|\phi| = 0$.
2. A set which is not finite is called an **infinite set**.

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

If $\mathbb{N}$ is a finite set, then there is a bijection $f : \mathbb{N} \to [n]$ for some $n \in \mathbb{N}$. In that case, the restriction function $f_{[n+1]} : [n+1] \to [n]$ is one-one. It contradicts Theorem 0.6. Therefore, $\mathbb{N}$ is an infinite set. We give some characterization of finite and infinite sets, where the requirements are seemingly weaker than those mentioned in their definitions.

Theorem 0.8. *1. A nonempty set X is finite if and only if there exists a one-one function $f : X \to [m]$ for some $m \in \mathbb{N}$.*

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

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

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

---

1 Families of sets

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

Definition 1.1. Let I be a set. For each $\alpha \in I$, take a set A_α. The set

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

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

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

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

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

[**Convention**] The union of sets in an empty family is ϕ. The intersection of sets in an empty family of subsets of a set S is S.

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

Example 1.1. 1. Take $A = \{1, 2, 3\}$, $B_1 = \{1, 2\}$, $B_2 = \{2, 3\}$ and $B_3 = \{4, 5\}$. Then the family $\{B_\alpha : \alpha \in A\} = \{B_1, B_2, B_3\} = \{\{1, 2\}, \{2, 3\}, \{4, 5\}\}$.

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

2. Take $A = \mathbb{N}$ and $B_n = \{n, n+1, \ldots\}$. Then the family $\{B_\alpha : \alpha \in A\} = \{B_1, B_2, \ldots\} = \{\{1, 2, \ldots\}, \{2, 3, \ldots\}, \ldots\}$

Thus, $\bigcup\limits_{\alpha \in A} B_\alpha = \mathbb{N}$ and $\bigcap\limits_{\alpha \in A} B_\alpha = \phi$.

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

Theorem 1.1. *Let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of subsets of X and let B be any set. For any subset Y of X, write $Y^c = X \setminus Y$. Then*

1. $B \bigcup \left(\bigcap\limits_{\alpha\in I} A_\alpha \right) = \bigcap\limits_{\alpha\in I} \left(B \bigcup A_\alpha \right)$.
2. $B \bigcap \left(\bigcup\limits_{\alpha\in I} A_\alpha \right) = \bigcup\limits_{\alpha\in I} \left(B \bigcap A_\alpha \right)$.
3. $\left(\bigcap\limits_{\alpha\in I} A_\alpha \right)^c = \left(\bigcup\limits_{\alpha\in I} A_\alpha^c \right)$
4. $\left(\bigcup\limits_{\alpha\in I} A_\alpha \right)^c = \left(\bigcap\limits_{\alpha\in I} A_\alpha^c \right)$

Proof. Exercise. □

Definition 1.2. Let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of sets. Assume that A_α is nonempty for each $\alpha \in I$. The product of the sets in the family is defined as

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

In case $A_\alpha = \phi$ for some $\alpha \in I$, then $\prod\limits_{\alpha\in I} A_\alpha = \phi$

2 Cantor-Schoder-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?

Notations: Let $f : X \to Y$ be a function. We use $(x, y) \in f$ to denote $f(x) = y$.

Experiment: Creating a bijection from injection.

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

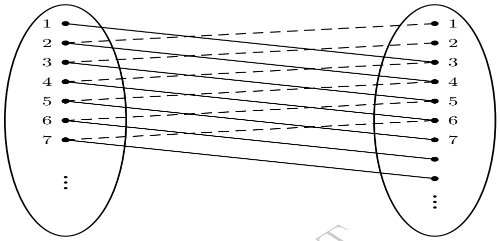


Figure 3.1: Graphic representation of functions f and g

a solid line joining x and y. If $(y, x) \in g$, we draw a dotted line joining y and x.

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 **rng**f. Since f is not an onto function, there are elements in Y **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 $y \in$ **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 **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

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

Theorem 2.1 (Cantor-Schroder-Bernstein (CSB)). *Let X and Y be nonempty sets and let $f : X \to Y$ and $g : Y \to X$ be one-one functions. Then there exists a bijection $h : X \to Y$.*

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

$$\phi(B) \bigcup \left(\bigcup_{n=2}^{\infty} \phi^n(B) \right)$$

.

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

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

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

is a bijection map. □

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

Theorem 2.2. *The set $\mathbb{N} \times \mathbb{N}$ is equinumerous $\mathbb{N}$.*

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

We show that $\mathbb{Q}$ is equinumerous with $\mathbb{N}$. For this, write $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$, where $\mathbb{Q}^+ = \{\frac{m}{n} : m, n \in \mathbb{N}, gcd(m, n) = 1\}$ and $\mathbb{Q}^- = \{-x : x \in \mathbb{Q}^+\}$.

Theorem 2.3. *Prove that $\mathbb{Q}^+$ is equinumerous with $\mathbb{N}$.*

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

Theorem 2.4. *Prove that $\mathbb{Q}^-$ is equinumerous with $\mathbb{N}$.*

Proof. Using above result you can easily prove this one. □

Theorem 2.5. *Prove that $\mathbb{Q}$ is equinumerous with $\mathbb{N}$.*

Proof. Using above two results you can easily prove this. □

---

3 Countable and uncountable sets

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

Definition 3.1.

1. A set which is equinumerous with $\mathbb{N}$ is called a **denumerable set**. A denumerable set is also called a **countably infinite set.**
2. A set which is either finite or denumerable is called a **countable set.**
3. A set which is not countable is called an **uncountable set.**

Example 3.1. 1. Set of integers $\mathbb{Z}$ is countable set.

2. $\mathbb{N} \times \mathbb{N}$ is countable.

3. $\mathbb{Q}$ is countable.

Theorem 3.1. *Let X be a nonempty set.*

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

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

Proof. 1. Let X be a countable set. If X is finite, then there exists a bijection $f : X \to [m]$ for some $m \in \mathbb{N}$. This bijection gives a one-one function $f : X \to \mathbb{N}$. Else, X is denumerable, so that there is a bijection $g : X \to \mathbb{N}$. In this case, the function g is one-one. Conversely, suppose there exists a one-one function $f : X \to \mathbb{N}$. If X is finite, then it is countable. So, suppose that X is infinite. Then, by Theorem 0.8, there exists a one-one function $g : \mathbb{N} \to X$. By CSB-theorem, there exists a bijection $h : X \to \mathbb{N}$. Hence X is denumerable; thus countable.

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

Theorem 3.2. 1. *Each subset of a denumerable set is countable.*

2. *Each infinite subset of a denumerable set is denumerable.*

3. *A set is infinite if and only if it has a denumerable subset.*

4. *Any subset of a countable set is countable; and any superset of an uncountable set is uncountable.*

5. *A countable union of countable sets is countable.*

6. *For any $k \in \mathbb{N}$, the Cartesian product $\mathbb{N}^k$ is denumerable.*

7. *A finite product of countable sets is countable*

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

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

3. Let X be an infinite set. Then, by Theorem 3.1, there is a one-one function $f : \mathbb{N} \to X$. Thus, $f : \mathbb{N} \to \mathbf{rng} f$ is a bijection. Hence, $\mathbf{rng} f$ is a denumerable subset of X.

Conversely, let X be a set and let $Y \subseteq X$ be denumerable. There exists a bijection $f : Y \to \mathbb{N}$. The function $f^{-1} : \mathbb{N} \to X$ is one-one. By Theorem 0.8, X is an infinite set.

4. Let X be a countable set and let $Y \subseteq X$. If $Y = \phi$, then it is finite, thus countable. So, suppose that $Y \neq \phi$. As X is countable, by Theorem 3.1, there exists a one-one function $f : X \to \mathbb{N}$. The restriction of f to Y is also a one-one function from Y to $\mathbb{N}$. Hence Y is countable. Let X be an uncountable set and let $X \subseteq Y$. If X is countable, then by what we have just proved, X would be countable. Hence, Y is uncountable.

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

If X is finite, then it is countable. So, let X be infinite. By Theorem 0.8, there is a one-one function $f : \mathbb{N} \to X$. Now, let $x \in X$. Then, there exists at least one $i \in \mathbb{N}$ such that $x \in A_i$. Further, since A_i is countable, we may assume that A_i has been enumerated. So, suppose x appears at the kth position in this enumeration of A_i. Thus, corresponding to each $x \in X$, we have a unique pair (i, k) of natural numbers. Define $g : X \to \mathbb{N}$ by $g(x) = 2^i 3^k$, where i is the smallest natural number for which $x \in A_i$ and x appears at the k-th position in the enumeration of A_i. Then g is one-one. Therefore, by CSB-theorem, A is equinumerous with $\mathbb{N}$.

6. For $k = 1$, the result is obvious. Suppose the result is true for $k = m$. That is, there exists a bijection $f : \mathbb{N}^m \to \mathbb{N}$. From Theorem 2.2, we have a bijection $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Define $h : \mathbb{N}^{m+1} \to \mathbb{N}$ by $h(x_1, \ldots, x_m, x_{m+1}) = g\Big(f(x_1, \ldots, x_m), x_{m+1}\Big)$. Then h is a bijection. Thus, by the PMI the result holds.

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

Theorem 3.3 **(Cantor).** *There exists no surjection from a set to its power se* set

---

Remark 3.1. Cantor's theorem implies that one cannot have a bijection between a set and its power set. In particular, the sets $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ cannot be equinumerous. However, $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ given by $f(x) = \{x\}$ is one-one. Thus the set $\mathcal{P}(\mathbb{N})$ is infinite but not denumerable, i.e., $\mathcal{P}(\mathbb{N})$ is an uncountable set. It follows that any set equinumerous with $\mathcal{P}(\mathbb{N})$ is uncountable. In general, the following result hold

Theorem 3.4. *The power set of any infinite set is uncountable*

Proof. Let X be an infinite set. By Theorem 0.8, there exists a one-one function $f : \mathbb{N} \to X$. Define the function $g : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathcal{X})$ by $g(A) = \{f(i) : i \in A\}$ for each $A \in \mathcal{P}(\mathbb{N})$. Then, g is one-one. As Remark 3.1 shows, $\mathcal{P}(\mathbb{N})$ is uncountable. Thus $g(\mathcal{P}(\mathbb{N}))$ is uncountable. The set $\mathcal{P}(\mathcal{X})$, being a superset of $g(\mathcal{P}(\mathbb{N}))$ is uncountable. □

4 Cardinality of Sets

This section is all about cardinality of sets. At first this looks like a very simple concept. To find the cardinality of a set, just count its elements. If $A = \{a, b, c, d\}$, then $|A| = 4$ ($|A|$ is the notation of cardinality of A) ;if $B = \{n \in Z : 5 \leq n \leq 5\}$, then $|B| = 11$. In this case $|A| < |B|$.

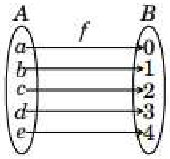
What could be simpler than that? Actually, the idea of cardinality becomes quite subtle when the sets are infinite. The main point of this chapter is to explain how there are numerous different kinds of infinity, and some infinities are bigger than others. Two sets A and B can both have infinite cardinality, yet $|A| < |B|$.

4.1 Sets with Equal Cardinalities

We begin with a discussion of what it means for two sets to have the same cardinality. Up until this point we've said $|A| = |B|$ if A and B have the same number of elements: Count the elements of A, then count the elements of B. If you get the same number, then $|A| = |B|$.

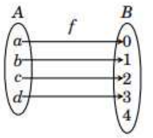
Although this is a fine strategy if the sets are finite (and not too big!), it doesn't apply to infinite sets because we'd never be done counting their elements. We need a new approach that applies to both finite and infinite sets. Here it is:

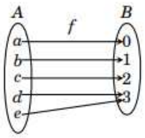
Definition 4.1. Two sets A and B have the **same cardinality**, written $|A| = |B|$, if there exists a bijective function $f : A \to B$. If no such bijective function exists, then the sets have **unequal cardinalities**, that is, $|A| \neq |B|$.



The above picture illustrates our definition. There is a bijective function $f : A \to B$, so $|A| = |B|$. The function f matches up A with B. Think of f as describing how to overlay A onto B so that they fit together perfectly.

On the other hand, if A and B are as indicated in either of the following figures, then there can be no bijection $f : A \to B$. (The best we can do is a function that is either injective or surjective, but not both). Therefore the definition says $|A| \neq |B|$ in these cases.





Remark 4.1. Several comments are in order. First, if $|A| = |B|$, there can be lots of bijective functions from A to B. We only need to find one of them in order to conclude $|A| = |B|$. Second, as bijective functions play such a big role here, we use the word **bijection** to mean bijective function. Also, an **injective** function is called an injection and a **surjective** function is called a surjection.

We emphasize and reiterate that Definition 13.1 applies to finite as well as infinite sets. If A and B are infinite, then $|A| = |B|$ provided there exists a bijection $f : A \to B$. If no such bijection exists, then $|A \neq |B|$.

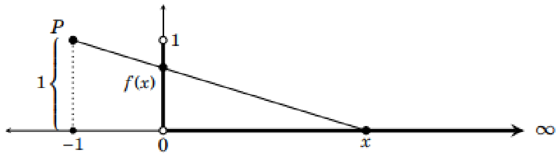
Theorem 4.1. *There exists a bijection* $f : \mathbb{N} \to \mathbb{Z}$*. Therefore* $|\mathbb{N}| = |\mathbb{Z}|$*.*

Theorem 4.2. *There exists no bijection* $f : \mathbb{N} \to \mathbb{R}$*. Therefore* $|\mathbb{N}| \neq |\mathbb{R}|$*.*

This is our first indication of how there are different kinds of infinities. Both $\mathbb{N}$ and $\mathbb{R}$ are infinite sets, yet $|\mathbb{N}| \neq |\mathbb{R}|$. We will continue to develop this theme throughout this chapter. The next example shows that the intervals $(0, \infty)$ and $(0, 1)$ on $\mathbb{R}$ have the same cardinality.

Example 4.1. Show that $|(0, \infty)| = |(0, 1)|$.

Proof. Consider the following function. $f(x) = \frac{x}{x+1}$. You can easily check that f is bijection from $(0, \infty)$ to $(0, 1)$. See the following figure. □



Example 4.2. Show that $|\mathbb{R}| = |(0, 1)|$.

Proof. Consider the map $f : \mathbb{R} \to (0, \infty)$ where $f(x) = 2^x$. You can easily check that f is bijection. Hence $|\mathbb{R}| = |(0, \infty)|$. Since $|(0, \infty)| = |(0, 1)|$. Therefore $|\mathbb{R}| = |(0, 1)|$. □

Definition 4.2. The cardinality of the natural numbers is denoted as $\aleph_0$. That is, $|\mathbb{N} = \aleph_0$. Thus any countably infinite set has cardinality $\aleph_0$.

The symbol $\aleph$ is the first letter in the Hebrew alphabet, and is pronounced "aleph." The symbol $\aleph_0$ is pronounced "aleph naught." The summary of facts at the beginning of this section shows $|\mathbb{Z}| = \aleph_0$ and $|\mathbb{R}| \neq \aleph_0$.

Theorem 4.3. *A set* A *is countably infinite if and only if its elements can be arranged in an infinite list* $a_1, a_2, a_3, a_4, \ldots$*.*

Proof. Since A is countably infinite, Definition 13.2 says there is a bijection $f : \mathbb{N} \to A$. This allows us to list out the set A as an infinite list $f(1), f(2), f(3), f(4), \ldots$. Conversely, if the elements of A can be written in list form as $a_1, a_2, a_3, \ldots$, then the function $f : N \to A$ defined as $f(n) = a_n$ is a bijection, so A is countably infinite. □

Definition 4.3. Suppose A and B are two sets.

1. $|A| = |B|$ means there is a bijection $A \to B$.

2. $|A| < |B|$ means there is an injection $A \to B$, but no surjection $A \to B$.

3. $|A| \leq |B|$ means either $|A| < |B|$ or $|A| = |B|$.

Remark 4.2. If $|A| \leq |B|$ and $|B| \leq |A|$, then by using Cantor Bernstein Schroder theorem, $|A| = |B|$

Theorem 4.4. *If A is any set, then $|A| < |\mathcal{P}(A)|$ (power set of A).*

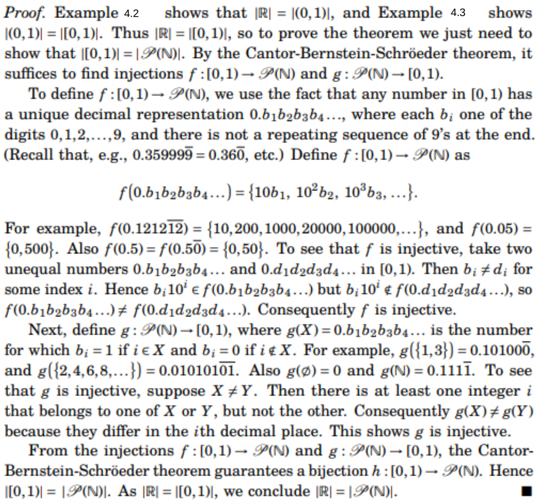
Problem 1. *Let $A = \{0,1\}^{\mathbb{N}}$ be the set of all possible sequences of 0's and 1's. Prove that A is uncountable.*

Sol: Suppose A was countable. This means, we would have been able to list all the elements of A as $A = \{p_1, p_2, \ldots\}$. By definition of A, each element p_i is a sequence of 0's and 1's. Let us make a new sequence $a = (a_k)_{k \in \mathbb{N}}$, defined by $a_k = 0$ if the sequence p_k has a 1 in the kth place, and $a_k = 1$ if the sequence p_k has a 0 in the kth place. This new sequence is also an element of P, and it cannot coincide with any of the sequences p_k, because its kth term is different. We have arrived at the contradiction.

Example 4.3. The intervals $[0,1)$ and $(0,1)$ in $\mathbb{R}$ have equal cardinalities.

Sol: Let $f(x) = \frac{x}{2} + \frac{1}{4}$ be a function $[0,1) \to (0,1)$. You can easily check that f is an injection. Let $g(x) = x$ be a function $(0,1) \to [0,1)$. You can easily check that g is an injection. By using CSB, there is a bijection from $[0,1)$ to $(0,1)$. Hence $|[0,1)| = |(0,1)|$.

Theorem 4.5. *The set $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$ have the same cardinality.*



Proof. Example 4.2 shows that $|\mathbb{R}| = |(0,1)|$, and Example 4.3 shows $|(0,1)| = |[0,1)|$. Thus $|\mathbb{R}| = |[0,1)|$, so to prove the theorem we just need to show that $|[0,1)| = |\mathscr{P}(\mathbb{N})|$. By the Cantor-Bernstein-Schröeder theorem, it suffices to find injections $f : [0,1) \to \mathscr{P}(\mathbb{N})$ and $g : \mathscr{P}(\mathbb{N}) \to [0,1)$.

To define $f : [0,1) \to \mathscr{P}(\mathbb{N})$, we use the fact that any number in $[0,1)$ has a unique decimal representation $0.b_1b_2b_3b_4\ldots$, where each b_i one of the digits $0,1,2,\ldots,9$, and there is not a repeating sequence of 9's at the end. (Recall that, e.g., $0.35999\overline{9} = 0.36\overline{0}$, etc.) Define $f : [0,1) \to \mathscr{P}(\mathbb{N})$ as

$$f(0.b_1b_2b_3b_4\ldots) = \{10b_1,\ 10^2b_2,\ 10^3b_3,\ \ldots\}.$$

For example, $f(0.1212\overline{12}) = \{10, 200, 1000, 20000, 100000, \ldots\}$, and $f(0.05) = \{0, 500\}$. Also $f(0.5) = f(0.5\overline{0}) = \{0, 50\}$. To see that f is injective, take two unequal numbers $0.b_1b_2b_3b_4\ldots$ and $0.d_1d_2d_3d_4\ldots$ in $[0,1)$. Then $b_i \neq d_i$ for some index i. Hence $b_i10^i \in f(0.b_1b_2b_3b_4\ldots)$ but $b_i10^i \notin f(0.d_1d_2d_3d_4\ldots)$, so $f(0.b_1b_2b_3b_4\ldots) \neq f(0.d_1d_2d_3d_4\ldots)$. Consequently f is injective.

Next, define $g : \mathscr{P}(\mathbb{N}) \to [0,1)$, where $g(X) = 0.b_1b_2b_3b_4\ldots$ is the number for which $b_i = 1$ if $i \in X$ and $b_i = 0$ if $i \notin X$. For example, $g(\{1,3\}) = 0.10100\overline{0}$, and $g(\{2,4,6,8,\ldots\}) = 0.010101\overline{01}$. Also $g(\emptyset) = 0$ and $g(\mathbb{N}) = 0.111\overline{1}$. To see that g is injective, suppose $X \neq Y$. Then there is at least one integer i that belongs to one of X or Y, but not the other. Consequently $g(X) \neq g(Y)$ because they differ in the ith decimal place. This shows g is injective.

From the injections $f : [0,1) \to \mathscr{P}(\mathbb{N})$ and $g : \mathscr{P}(\mathbb{N}) \to [0,1)$, the Cantor-Bernstein-Schröeder theorem guarantees a bijection $h : [0,1) \to \mathscr{P}(\mathbb{N})$. Hence $|[0,1)| = |\mathscr{P}(\mathbb{N})|$. As $|\mathbb{R}| = |[0,1)|$, we conclude $|\mathbb{R}| = |\mathscr{P}(\mathbb{N})|$. ■

Remark 4.3. Using Cantor set theorem, we have $\mathcal{P}(\mathbb{N})$ is uncountable. We have seen that $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$ have the same cardinality. Hence $\mathbb{R}$ is uncountable.

Interesting Story: We know that $|\mathbb{R}| \neq |\mathbb{N}|$ and $|\mathbb{R}| = |\mathbb{P}(\mathbb{N})|$. This suggests that the cardinality of $\mathbb{R}$ is not "too far" from $|\mathbb{N}| = \aleph_0$. We close with a few informal remarks on this mysterious relationship between $\aleph_0$ and $|\mathbb{R}|$.

We established earlier in this chapter that $\aleph_0 < |\mathbb{R}|$. For nearly a century after Cantor formulated his theories on infinite sets, mathematicians struggled with the question of whether or not there exists a set A for which

$$\aleph_0 < |A| < |\mathbb{R}|$$

.

It was commonly suspected that no such set exists, but no one was able to prove or disprove this. The assertion that no such A exists came to be called the **continuum hypothesis.**

$\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| \cdots .$

From this, we can see that the continuum hypothesis asserts that no set has a cardinality between that of $\mathbb{N}$ and its power set.

Although this may seem intuitively plausible, it eluded proof since Cantor first posed it in the 1880s. In fact, the real state of affairs is almost paradoxical. In 1931, the logician Kurt Gödel proved that for any sufficiently strong and consistent axiomatic system, there exist statements which can neither be proved nor disproved within the system. Later he proved that the negation of the continuum hypothesis cannot be proved within the standard axioms of set theory. This meant that either the continuum hypothesis is false and cannot be proven false, or it is true. In 1964, Paul Cohen discovered another startling truth: Given the laws of logic and the axioms of set theory, no proof can deduce the continuum hypothesis. In essence he proved that the continuum hypothesis cannot be proved. Taken together, Gödel and Cohens' results mean that the standard axioms of mathematics cannot "decide" whether the continuum hypothesis is true or false; that no logical conflict can arise from either asserting or denying the continuum hypothesis. We are free to either accept it as true or accept it as false, and the two choices lead to different—but equally consistent—versions of set theory.

5 Permutation

Definition 5.1. Let A be a non-empty set. A **permutation** on A is a bijective map from A to A.

Example 5.1. Let $A = \{1, 2, 3\}$. Let $f : A \to A$ be a map, defined by $f(1) = 2, f(2) = 1, f(3) = 3$. Since f is a bijection, f is an example of permutation on A.

Example 5.2. Consider a set X containing 3 objects, say a triangle, a circle and a square. A permutation of $X = \{\triangle, \circ, \square\}$ might send for example $\triangle \to \triangle$, $\circ \to \square$, $\square \to \circ$ and we observe that what just did is exactly to define a bijection on the set X, namely a map $f : X \to X$ defined as $f(\triangle) = \triangle$, $f(\circ) = \square$ and $f(\square) = \circ$.

Remark 5.1. Since what matters for a permutation is how many objects we have and not the nature of the objects, we can always consider a permutation on a set of n objects where we label the objects by $\{1, 2, \ldots, n\}$. The permutation of the previous example can be rewritten as $f : \{1, 2, 3\} \to \{1, 2, 3\}$ be a map, defined by $f(1) = 1, f(2) = 3, f(3) = 2$. It is denoted by $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

If it is given $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, this one is a permutation on $\{1, 2, 3, 4\}$. The first row of the matrix is domain of that bijective mapping and second row is co-domain of that bijective mapping. So the image of 1 is 1 , 2 is 3, 3 is 4 and 4 is 2.

Definition 5.2. The permutation $\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & 2 & 3 & \cdots & n-1 & n \end{pmatrix}$ is called **identity permutation**.

Remark 5.2. 1. We have seen that a permutation is a bijective map. Hence inverse of that map is also a permutation.

Consider the following permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$. The inverse permutation of this permutation is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ where inverse image of 1 is 1, 2 is 4, 3 is 2 and 4 is 2.

2. We know that composition of two bijective maps is bijective map. Hence composition of two permutations on $\{1, 2, \ldots, n\}$ is again a permutation on $\{1, 2, \ldots, n\}$.

Consider the following two permutations $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$. Then $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

The following question is immediate. How many permutations are there on $\{1, 2, \ldots, n\}$? That is, how many bijective maps are there from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$?

Ans: There are $n!$ number of permutations on $\{1, 2, \ldots, n\}$. Hint (method of induction).

That is there are 6 permutations on $\{1, 2, 3\}$. The following are total list of them.

$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

The following table is called the composition table.

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

The set of all permutations on $\{1, 2, \dots, n\}$ is denoted by S_n. So $S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$.

Remark 5.3. Let σ be a permutation on $\{1, 2, 3, 4\}$ such that $\sigma = (123)$. That means $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

Definition 5.3. A cycle is a permutation which maps a finite subset $\{x_1, x_2, \dots, x_n\}$ by $x_1 \to x_2 \to x_3 \to x_4 \dots \to x_n \to x_1$.

This cycle will be denoted $(x_1 x_2 \dots x_n)$. The cycle $(x_1 x_2 \dots x_n)$ has **length** n.

Example 5.3. 1. Write the cycle $(425) \in S_5$ in permutation notation.

2. Write the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$.

Answer: 1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$.

2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} = (15342)$.

Example 5.4. The following permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is not a cycle but the product of cycle.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (135)(24)$, here (135) and (24) are two cycles (they are disjoint).

Theorem 5.1. *Every permutation on a finite set can be written as a product of disjoint cycles.*

Proof. Proof is not required. □

Lemma 5.1. *Disjoint cycles commute.*

Proof. Proof is not required. □

Definition 5.4. A **transposition** is a permutation which interchanges two elements and leaves everything else fixed.

Example 5.5. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (135)(24) = (15)(13)(24)$. Carefully check how to write $(135) = (15)(13)$, 1 is fixed in each transpose and start with the last element 5. But the following expression is not true. $(135) \neq (13)(15)$.

Theorem 5.2. *Every permutation is a product of transpositions.*

Proof. Proof is not required. □

Remark 5.4. While the decomposition of a permutation into disjoint cycles is unique up to order and representation of the cycles (i.e. $(123) = (231)$), a permutation may be written as a product of transpositions in infinitely many ways. You can always tack on trivial terms of the form $(ab)(ab)$ is identity permutation.

Example 5.6. $(2745) = (25)(24)(27)$ and $(2745) = (25)(24)(27)(36)(36)$.

Definition 5.5. A permutation is **even** if it can be written as a product of an even number of transpositions; a permutation is **odd** if it can be written as a product of an odd number of transpositions.

Example 5.7. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (135)(24) = (15)(13)(24)$. Hence $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is odd permutation.

Theorem 5.3. *A permutation cannot be written as a product of both an odd and an even number of transpositions.*

Proof. Proof is not required. □

6 Classes of residues of integers modulo n

Let n be a positive integers and let us consider the equivalence relation R on $\mathbb{Z}$ defined by "aRb if and only if $a-b$ is divisible by n" for $a, b \in \mathbb{Z}$. There are n classes $cl(0), cl(1), \ldots, cl(n-1)$. These are also called the **classes of residues of integers modulo** n. We use the notation $\bar{a}$ to denote the class $cl(a)$. Let $\mathbb{Z}_n$ be the set of residue classes $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

We define a binary composition $+_n$, called addition modulo n, on the set $\mathbb{Z}_n$ by $\overline{a} +_n \overline{b} = \overline{(a+b)(\text{ mod } n)}$, where $+$ is the usual addition. In the problem set 3, I have discussed What is $a+b(\text{ mod } n)$.

For example, consider $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. I am showing how to calculate $\overline{4} +_5 \overline{3}$.

We know that $\overline{4} +_5 \overline{3} = \overline{(4+3)(\text{ mod } 5)} = \overline{7(\text{ mod } 5)}$. We have seen in problem set 3, $7(\text{ mod } 5) = 2$. Hence $\overline{4} +_5 \overline{3} = \overline{2}$.

The following table is called the composition table.

$+_5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Similarly, We define a binary composition $._n$, called multiplication modulo n, on the set $\mathbb{Z}_n$ by $\overline{a} \cdot_n \overline{b} = \overline{(a \cdot b)(\text{ mod } n)}$, where $\cdot$ is the usual multiplication. In the problem set 3, I have discussed What is $a.b(\text{ mod } n)$.

For example, consider $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. I am showing how to calculate $\overline{4} \cdot_5 \overline{3}$.

We know that $\overline{4}._5\overline{3} = \overline{(4 \cdot 3)(\text{ mod } 5)} = \overline{12(\text{ mod } 5)}$. We have seen in problem set 3, $12(\text{ mod } 5) = 2$. Hence $\overline{4} \cdot_5 \overline{3} = \overline{2}$.

7 Group Theory

Introduction: A group is an algebraic structure like vector space. You have seen in Maths-II, to define a vector space you need two types of binary operation one is vector addition and another one is scalar multiplication. Similarly to define a group we need a binary operation like vector addition. First four condition with respect to vector addition to be a vector space are actually the conditions to be a group. So every vector space is a group with respect to respective vector addition. I recall those four conditions to be a vector space. Let V be a nonempty set and $\circ$ is a vector addition on V.

1. Closed under vector addition $\circ$.

2. Vector addition $\circ$ is associative.

3. There is an element $e \in V$ such that $e \circ a = a \circ e$ for all $a \in V$. This e is called identity element.

4. For each element a, there is an element $b \in V$ such that $a \circ b = e$. This b is called inverse of a.

In this chapter we will deal with an algebraic structure which satisfying above four properties.

Definition 7.1. Let X, Y and Z be three non-empty sets. A binary operation is a mapping from $X \times Y$ to Z. That is, a **binary operation** is a calculation that combines two elements to produce another element.

Example 7.1. 1. Let $\circ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R} \setminus \mathbb{Q}$, defined by $m * n = \sqrt{2}(m + n)$ for all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.

2. To define a vector space we need two binary operations, vector addition and scalar multiplication.

3. Dot product and cross product of two vectors are binary operations.

4. Addition, subtraction and multiplications of two real numbers are binary operations.

Binary operations are the keystones of most algebraic structure, that are studied in algebra, in particular in group, ring, fields and vector spaces. Usually we $\circ$ to denote a binary operation. But sometimes we use the following symbols $*, + \cdot ., \bigoplus, \bigodot$ to denote a binary operation.

Definition 7.2. A binary operation $\circ$ is said to be **closed** on a non empty set A if $a \circ b \in A$ for all $a, b \in A$.

Example 7.2. 1. Addition, subtraction, multiplication on $\mathbb{R}$ are closed.

2. Addition, subtraction, multiplication on $\mathbb{Z}$ are closed.

3. Addition and multiplication on $\mathbb{N}$ are closed but subtraction is not closed on $\mathbb{N}$.

4. Addition, subtraction, multiplication on $\mathbb{R} \setminus \mathbb{Q}$ are not closed.

5. Composition of two permutations is closed.

6. Addition modulo n on $\mathbb{Z}_n$ is closed.

7. Matrix multiplication of two matrices is closed.

8. Let X be a non-empty set and $\mathcal{P}(X)$ be the power set of X. Then union, intersection and symmetric differences are closed binary operations on $\mathcal{P}(X)$.

9. Matrix multiplication is closed.

Definition 7.3. A binary operation $\circ$ is said to be **associative** on a non empty set A if $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in A$.

Example 7.3. 1. Addition and multiplication on $\mathbb{R}$ are associative but subtraction is not associative.

2. Addition and multiplication on $\mathbb{Z}$ are associative but subtraction is not associative.

3. Addition and multiplication on $\mathbb{N}$ are associative but not subtraction.

4. Addition and multiplication on $\mathbb{R} \setminus \mathbb{Q}$ are associative.

6. Composition of two permutations is associative.

7. Addition modulo n and multiplication modulo n on $\mathbb{Z}_n$ is associative.

8. Matrix multiplication of two matrices is associative.

9. Let X be a non-empty set and $\mathcal{P}(X)$ be the power set of X. Then union, intersection and symmetric differences are associative binary operations on $\mathcal{P}(X)$.

Definition 7.4. A binary operation $\circ$ is said to be **commutative** on a non empty set A if $a \circ b = b \circ c$ for all $a, b \in A$.

Example 7.4. 1. Addition and multiplication on $\mathbb{R}$ are commutative but subtraction is not commutative.

2. Addition and multiplication on $\mathbb{Z}$ are commutative but subtraction is not commutative.

3. Addition and multiplication on $\mathbb{N}$ are commutative but not subtraction.

4. Addition and multiplication on $\mathbb{R} \setminus \mathbb{Q}$ are commutative.

6. Composition of two permutations is not commutative.

7. Addition modulo n and multiplication modulo n on $\mathbb{Z}_n$ are commutative.

8. Matrix multiplication of two matrices is not commutative.

9. Let X be a non-empty set and $\mathcal{P}(X)$ be the power set of X. Then union, intersection and symmetric differences are commutative binary operations on $\mathcal{P}(X)$.

Definition 7.5. Let G be a non-empty set and $\circ$ be a binary operation on G. Then $(G, \circ)$ is called **groupoid** if $\circ$ is closed binary operation on G.

Example 7.5. 1. $(\mathbb{Z}, +)$ and $(\mathbb{Z}, -)$ are both groupoid.

2. $(\mathbb{Q}, +)$,$(\mathbb{Q}, -)$, $(\mathbb{Q}, \cdot)$,$(\mathbb{R}, +)$, $(\mathbb{R}, -)$, $(\mathbb{R}, \cdot)$ are groupiod.

3. $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n, \cdot)$ are groupiod.

4. $(\mathbb{N}, -)$ is not groupoid.

5. $(M_2(\mathbb{R}), +)$ is groupiod, where $+$ is the matrix addition.

Definition 7.6. A groupoid $(G, \circ)$ is called **semigroup** if $\circ$ is associative binary operation on G.

Example 7.6. 1. $(\mathbb{Z}, +)$ is semigroup but$(\mathbb{Z}, -)$ is not semigroup.

2. $(\mathbb{Q}, +)$, $(\mathbb{Q} \cdot)$,$(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$ are semigroup.

3. $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n, \cdot)$ are semigroup.

4. $(M_2(\mathbb{R}), +)$ is semigroup, where $+$ is the matrix addition.

5. $(\mathbb{Q}, -)$ and $(\mathbb{R} -)$ are not semigroup.

Definition 7.7. A semigroup $(G, \circ)$ is called **monoid** if there exists an element e in G such that $e \circ a = a \circ e = a$ for all $a \in G$. This element e is called identity element. Identity element depends on the binary operation $\circ$. For different different binary operation you may have different different identity element.

Example 7.7. 1. $(\mathbb{Z}, +)$ is monoid 0 is the identity.

2. $(\mathbb{Q}, +)$ is monoid 0 is the identity but $(\mathbb{Q}, .)$ is not monoid as there is no identity with respect to multiplication.

3. $(\mathbb{R}, +)$ is monoid 0 is the identity element. But $(\mathbb{R}, .)$ is not monoid as there is no identity element with respect to multiplication. → 1

4. $(\mathbb{Z}_n, +)$ is monoid $\bar{0}$ is the identity element and $(\mathbb{Z}_n, .)$ is not monoid. → $\bar{1}$

5. $(M_2(\mathbb{R}), +)$ is monoid and identity matrix is the identity element, where $+$ is the matrix addition.

Remark 7.1. A monoid is always a semigroup but not true other way. A semigroup is groupoid but not true other way.

---

8 Group

Definition 8.1. A non-empty set G is said to form a **group** with respect to binary operation $\circ$, if

1. G is closed under $\circ$,
2. $\circ$ is associative,
3. there exists an element e in G such that $e \circ a = a \circ e = a$ for all in G,
4. for each element a in G , there exists an element a' in G such that $a' \circ a = a \circ a' = e$.

The group is denoted by the symbol $(G, \circ)$.

Remark 8.1. 1. The element e is said to be an identity element in the group. We shall prove that there is only one such element in the group and therefore e will be said to be the identity element.

2. The element a' is said to be an inverse of a. We shall prove that each element a has only one inverse and therefore a' will be said to be the inverse of a.

Definition 8.2. A group $(G, \circ)$ is said to be a **commutative group** or an **abelian group** (after the name of Norwegian mathematician N. Abel) if $\circ$ is commutative.

Example 8.1. 1. $(\mathbb{Z}, +)$ is commutative group.

2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are commutative group.
3. $(\mathbb{N}, +)$ is not a group as it has no identity element.
4. Let $m\mathbb{Z} = \{0, \pm m, \pm 2m, \pm 3m, \ldots\}$, where m is a positive integer. Then $(m\mathbb{Z}, +)$ is commutative group.
5. $(\mathbb{Z}, \cdot)$ is not a group as the inverse of no element other than 1 and -1 in $\mathbb{Z}$ exists.
6. $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ are not a group as the inverse of 0 does not exist in each case. But $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ are commutative groups.

7. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices whose elements are real numbers. $(M_2(\mathbb{R}), +)$ is a commutative group, where $+$ is matrix addition.

8. $(M_2(\mathbb{R}), \cdot)$ is not a group, where $\cdot$ is matrix addition as many elements in $M_2(\mathbb{R})$ have no inverse.

9. Let S be the set of all 2×2 non-singular matrices whose elements are real numbers. S is a proper subset of $M_2(\mathbb{R})$. $(S, \cdot)$ is a non-commutative group.

   This group is called **general linear group of degree 2** over $\mathbb{R}$ and is denoted by $GL(2, \mathbb{R})$. Similarly, the group $GL(n, \mathbb{R})$ is the group of all $n \times n$ real matrices under matrix multiplication.

The following two groups are quite important for advance mathematics as well as for engineering branch.

Example 8.2. Let S_n be the set of all permutation on $\{1, 2, \ldots, n\}$ and $\circ$ is composition of two functions. We can easily check that $(S_n, \circ)$ is a non-commutative group. This group has special name, **symmetric group**. I am considering S_3 and the composition table for S_3.

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

Using this composition table you can easily show that S_3 is a non commutative group.

Example 8.3. Let $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n}\}$. You can easily check that $(\mathbb{Z}_n, +_n)$ is a commutative group. This group is called **modulo group.** I am considering $\mathbb{Z}_5$ and its composition table under $+_n$.

$+_5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Theorem 8.1. *A group $(G, \circ)$ contains only one identity element.*

Proof. Let e and f be two identity element in the group. Then $e \circ a = a \circ e = a$ and $f \circ a = a \circ f = a$ for all $a \in G$. We have $e \circ f = f$ by the property of e; and also $e \circ f = e$ by the property of f. Therefore $e = f$ and this proves uniqueness of identity element. □

Theorem 8.2. *In a group $(G, \circ)$ each element has only one inverse.*

Proof. Let $a \in G$ and a', a'' be two inverses of a. Then $a' \circ a = a \circ a' = e$ and $a'' \circ a = a \circ a'' = e$, e being the identity element. We have $a' \circ (a \circ a'') = (a' \circ a) \circ a''$, since $\circ$ is associative. But $a' \circ (a \circ a'') = a' \circ e = a'$ and $(a' \circ a) \circ a'' = e \circ a'' = a''$. Therefore $a' = a''$ and this proves that the inverse of a is unique.

Remark 8.2. The inverse of a is denoted by a^{-1}. Therefore for each $a \in G$, $a \circ a^{-1} = a^{-1} \circ a = e$.

You cannot write $ab = ac \implies b = c$ always. The following theorem gives you the sufficient condition to cancel from left and right.

Theorem 8.3. *In a group $(G, \circ)$, for all $a, b, c \in G$,*

i) $a \circ b = a \circ c$ implies $b = c$ (left cancellation)

ii) $b \circ a = c \circ a$ implies $b = c$ (right cancellation)

Proof. Since $a \in G$, $a^{-1} \in G$.

(i) $a \circ b = a \circ c \implies a^{-1} \circ (a \circ b) = a^{-1}(a \circ c) \implies (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$ (using associativity) $\implies e \circ b = e \circ c. \implies b = c.$

Similarly you can show ii). □

Definition 8.3. The **order** of a group $(G, \circ)$ is the number of elements it contains. It is denoted by $o(G)$.

Remark 8.3. This number is, of course, most interesting when it is finite. In that case we say that $(G, \circ)$ is a **finite** group. Otherwise we say $(G, \circ)$ is a **infinite** group.

Example 8.4. We check the groups given in Example 8.1 are finite or infinite.

1. Since $\mathbb{Z}$ contains infinite number of elements. Hence this group is infinite.

2. Those are infinite group.

3. This one is not a group.

4. This one is infinite group.

5. This one is not a group.

6. Those are not groups for first part. Those are infinite group for second part.

7. This one is infinite group.

8. This one is infinite group.

9. The group given in Example 8.2 is finite. Hence $o(G) = 6$.

10. The group given in Example 8.3 is finite. Hence $o(G) = 5$.

Definition 8.4. If $(G, \circ)$ is a group and $a \in G$, the order of a is the least positive integers m such that $a^m = e$ and denote it by $o(a) = m$. Here $a^m = a \circ a \circ \cdots \circ a$ (m times). If such m does not exist then the order of a is infinite.

Remark 8.4. 1. Here $a^m = a \circ a \circ \cdots \circ a$ (m times). That is, if your binary operation $\circ$ is addition $+$, then $a^m = a \circ a \circ \cdots \circ a = a + a + +a = ma$. If your binary operation $\circ$ is multiplication, then $a^m = a \circ a \circ \cdots \circ a = a.a..a$. So a^m is dependent on the binary operation, a^m is just a notation.

2. Let $a \in G$, a group. Then $a^{-m} = a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}$($m$ times).

3. $a^0 = e$.

4. i) $a^m \circ a^n = a^{m+n}$. ii) $(a^m)^n = a^{mn}$ iii) $(a^n)^{-1} = a^{-n}$

Remark 8.5. The order of the identity element of any group is 1 and no other element in a group is of order 1.

Example 8.5. 1. The order of any element except 0 is infinite in $(\mathbb{R}, +)$. Same thing is true for $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{C}, +)$.

2. Consider the group $(S_3, \circ)$. Then $o(\rho_0) = 1$, $o(\rho_1) =$ ~~2,~~ 3 $o(\rho_2) =$ ~~2~~ 3 $o(\rho_3) =$ ~~3~~ 2, $o(\rho_4) =$ ~~3~~ 2 and $o(\rho_5) =$ ~~3~~. 2

3. In the group $(\mathbb{Z}_{\cancel{6}}, +_n)$, $o(\overline{0}) = 1$, $o(\overline{1}) = 6$, $o(\overline{2}) = 3$ $o(\overline{4}) = 3$, $o(\overline{5}) = 6$.

Theorem 8.4. *Let a be an element of a group $(G, \circ)$. Then*

1. *$o(a) = o(a^{-1})$;*

2. *if $o(a) = n$ and $a^m = e$, then n is divisor of m;*

3. *if $o(a) = n$, then $a, a^2, a^3, \ldots, a^n (= e)$ are distinct elements of G;*

4. *if $o(a) = n$, then for a positive integer m, $o(a^m) = \frac{n}{gcd(m,n)}$;*

5. *if $o(a)$ is infinite and p is a positive integer, then $o(a^p)$ is infinite.*

Proof. The proof is not required. □

Theorem 8.5. *Each element of a* **finite** *group is of finite order.*

Proof. Let a be an element of a finite group $(G, \circ)$. Then $a, a^2, a^3, \ldots$ are all elements of G. Since G is finite, these elements are not all distinct. Therefore $a^m = a^n$ must hold for some positive integers $m, n (m > n)$. Therefore $a^m \circ (a^n)^{-1} = e_G$, or, $a^{m-n} = e_G$. □

Remark 8.6. The order of an element in a **finite** group cannot exceed the order of the group.

9 Subgroups

Introduction: The concept of subgroup of a group is similar to the concept of subspace of a vector space. It is known to you how to check whether a non-empty subset of a vector space is subspace or not. Similar type result is also exist to check whether a subset of a group is subgroup or not.

Definition 9.1. Let $(G, \circ)$ be a group and H be a non-empty subset of G. If H is itself a group with respect to the same binary operation $\circ$, then $(H, \circ)$ is called subgroup of $(G, \circ)$.

Example 9.1.

1. Let $(G, \circ)$ be a group. G being a subset of G, $(G, \circ)$ is a subgroup of $(G, \circ)$. This subgroup $(G, \circ)$ is said to be the **improper** subgroup of $(G, \circ)$. $(\{e_G\}, \circ)$ (identity element of G) is also a subgroup of $(G, \circ)$. This subgroup is called trivial subgroup.

2. $(\mathbb{Q}, +)$ is a group. $(\mathbb{Z}, +)$ is a subgroup $(\mathbb{Q}, +)$.

3. $(\mathbb{Q}, +)$ and $(\mathbb{Q} - \{0\}, +)$ both are groups and $\mathbb{Q} - \{0\} \subsetneqq \mathbb{Q}$ but $(\mathbb{Q} - \{0\}, +)$ is not a subgroup of $(\mathbb{Q}, +)$.

4. Let A_3 be the set of all even permutation on $\{1, 2, 3\}$. Therefore $A_3 \subseteq S_3$. You can check from the composition table of S_3, $(A_3, \circ)$ is a group. Hence $(A_3, \circ)$ is a subgroup of $(S_3, \circ)$.

5. Let $S = \{\overline{0}, \overline{2}\} \subseteq \mathbb{Z}_4$. You can easily check that $(S, +_4)$ is a subgroup of $(\mathbb{Z}_4, +_4)$.

The following theorem gives you the way how to check a subset is subgroup or not.

Theorem 9.1. *Let $(G, \circ)$ be a group and $H \subsetneqq G$. Then $(H, \circ)$ is a subgroup of $(G, \circ)$ if and only if $a \circ b^{-1} \in H$ for all $a, b \in H$.*

Proof. We first consider $(H, \circ)$ subgroup of $(G, \circ)$. Therefore $(H, \circ)$ is a group. Let $a, b \in H$. Since $(H, \circ)$ is a group, $b^{-1} \in H$ and $a \circ b^{-1} \in H$.

We now consider $a \circ b^{-1} \in H$ for all $a, b \in H$. We have to show that $(H, \circ)$ is a group.

i) $a \circ a^{-1} = e \in H$ by using given condition. Hence identity element is in H.

ii) $e \circ a^{-1} = a^{-1} \in H$ for all $a \in H$ by using given condition. Hence each element in H has inverse.

iii) Since H is subset of G. Hence $\circ$ is associative in H.

iv) Let $a, b \in H$. Then $b^{-1} \in H$. Using above condition $a \circ (b^{-1})^{-1} \in H \implies a \circ b \in H$. Hence $\circ$ is closed in H.

Therefore, $(H, \circ)$ is a group. Hence $(H, \circ)$ is a subgroup of $(G, \circ)$. □

Theorem 9.2. **??** *Let $(G, \circ)$ and let $a \in G$. Let $o(a) = m$. Let $H = \{a, a^2, a^3, \dots, a^m\}$. Then $(H, \circ)$ is a subgroup.*

Proof. The proof is trivial. □

---

10 Important Theorem:

In this section we discuss a theorem which is quite important in group theory. To state and prove that theorem we need the following definition.

Definition 10.1. Let $(G, \circ)$ be a group and $(H, \circ)$ be a subgroup of $(G, \circ)$. Define $aH = \{a \circ h \mid h \in H\}$, this is called **left cosets** and $Ha = \{h \circ a \mid h \in H\}$, this called **right cosets**

Example 10.1. Let $H = \{\rho_0, \rho_1\}$ and $(H, \circ)$ be a subgroup of $(G, \circ)$. $\rho_0 H = \{\rho_0 \circ \rho_0, \rho_0 \circ \rho_1\} = \{\rho_0, \rho_1\}$.
$\rho_3 H = \{\rho_3 \circ \rho_0, \rho_3 \circ \rho_1\} = \{\rho_3, \rho_4\}$. These are examples of left cosets.

$H\rho_0 = \{\rho_0 \circ \rho_0, \rho_1 \circ \rho_0\} = \{\rho_0, \rho_1\}$.
$H\rho_3 = \{\rho_0 \circ \rho_3, \rho_1 \circ \rho_3\} = \{\rho_3, \rho_5\}$. These are examples of right cosets.

Remark 10.1. 1. Left cosets may not be equal to right cosets, we have seen in the previous example. If they are equal then $(H, \circ)$ is called normal subgroup of $(G, \circ)$. We are not going to discuss in details here. You will see the details in Modern Algebra Course.

2. Two left cosets are either disjoint or identical.

Theorem 10.1. *Let $(G, \circ)$ be a group and H be a subgroup of G. Let R be a relation on R defined by xRy if and only if $x^{-1} \circ y \in H$. Prove that R is equivalence relation.*

Proof. Reflexive: Let $a \in G$. $a^{-1} \circ a = e \in H$. Hence aRa for all $a \in G$.

Symmetric: Let aRb. Then $a^{-1} \circ b \in H$. H is a group, the inverse of $a^{-1} \circ b$ is $b^{-1} \circ a$ (check!) in H. Hence bRa. Hence R symmetric.

Transitive: Let aRb and bRc. Then $a^{-1} \circ b \in H$ and $b^{-1} \circ c \in H$. Since $(H, \circ)$ is group, $a^{-1} \circ b \circ b^{-1} \circ c in H$ this implies, $a^{-1} \circ c \in H$. Therefore aRc. Hence R is transitive.

Hence R is equivalence relation on $(G, \circ)$. □

Remark 10.2. The set G is partitioned into equivalence classes and each class is a left cosets of H, because $[a] = \{x \in G : aRx\} = \{x \in G : a^{-1}x \in H\} = \{x \in G : x \in aH\} = aH$.

The following is the main theorem of this section, Lagrange's theorem.

Theorem 10.2. *The order of every subgroups of a* **finite** *group G divides the order of G.*

Proof. Let $(H, \circ)$ be a subgroup of $(G, \circ)$. Let $o(H) = m$ and $o(G) = n$. Since G is finite, there are finite number of disjoint left cosets. Let $x_1, \ldots, x_p$ in G such that $x_1H, \ldots, x_pH$ are the disjoint left cosets. We consider the previous equivalence relation on G and we have seen that $aH = [a]$ for each $a \in G$. Since $x_1H, \ldots, x_pH$ are the only disjoint left cosets in $(G, \circ)$, therefore $G = \bigcup\limits_{i=1}^{n} x_iH$. Hence $|G| = |\bigcup\limits_{i=1}^{n} x_iH| \implies n = pm$ as each left cosets are disjoint with same cardinality. Therefore m divides n. Hence $o(H)$ divides $o(G)$. □

Corollary 1. *Let $(G, \circ)$ be a* **finite** *group and let $a \in G$. Then $o(a)$ divides $o(G)$.*

Proof. Let $o(a) = k$. By using Theorem **??**, $(H, \circ)$ is a subgroup of $(G, \circ)$, where $H = \{a, a^2, \ldots, a^k\}$ and $o(H) = k$. By using Lagrange's theorem, $o(H)$ divides $o(G)$, that is, k divides $o(G)$, that is $o(a)$ divides $o(G)$. □

11 Cyclic Groups

In this section we define generator of a group which is similar to the concept of basis of a vector space.

Definition 11.1. Let $(G, \circ)$ be a group and let $a \in G$. Then a is called generator of $(G, \circ)$ if for each $y \in G$, there exists an integer m such that $y = a^m$, here $a^m = a \circ a \circ \ldots \circ a$ (m times).

Example 11.1.

1. Consider the group $(\mathbb{Z}, +)$. Here 1 is a generator of $(\mathbb{Z}, +)$ because ...
2. In the group $(S_3, \circ)$, there is no generator.
3. In the group $(\mathbb{Z}_4, +_4)$, $\overline{1}$ is a generator.
4. In the group $(\mathbb{Z}_5, +_5)$, $\overline{1}$ is a generator.

Remark 11.1. We have seen that each vector space has basis but each group may not have generator, see Example 11.1(2).

Definition 11.2. A group $(G, \circ)$ is said to be **cyclic** if $(G, \circ)$ has generator, that is $G = \{a^n : n \in \mathbb{Z}\}$. If G is a finite cyclic group of order n, then $G = \{a, a^2, a^3, \ldots, a^n\}$.

Example 11.2.

1. The group $(\mathbb{Z}, +)$ is cyclic as it has generator.
2. The group $(S_3, \circ)$ is not cyclic as it has no generator.

3. The group $(\mathbb{Z}_4, +_4)$ is cyclic as it has generator.
4. The group $(\mathbb{Z}_5, +_5)$ is cyclic as it has generator.
5. The group $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are not cyclic as it has no generator.
6. The group $(M_n(\mathbb{R}), +)$ is not cyclic as it has no generator.
7. The group $(GL_n(\mathbb{R}), \cdot)$ is not cyclic as it has no generator.

Definition 11.3. The total number of generators of a finite cyclic group of order n is $\phi(n)$, $\phi(1) = 1$ and for $n \geq 2$, $\phi(n) =$ the number of positive integers less than n and prime to$n$.

Example 11.3. We have seen that $\mathbb{Z}_6, +_n$ is cyclic of order 6. Here $\phi(6) = 2$, the number of positive integers less than 6 and prime to 6 (there are two elements 1 and 5 which are less than 6 and prime to 6).

Theorem 11.1. *The following are true.*

1. *If a is generator of a group $(G, \circ)$, then a^{-1} is also a generator.*
2. *Every cyclic group is commutative, but the converse is not true.*
3. *Let $(G, \circ)$ be a* **finite** *group. Then $(G, \circ)$ is cyclic if and only if there is an element $a \in G$ such that $o(a) = o(G)$.*
4. *Subgroup of a cyclic group is cyclic.*

Proof. 1. Let $b \in G$. Since a is generator, there exists integer m such that $b = a^m$. Then the inverse of b is equal to the inverse $(a^m)^{-1}$, that is, $b^{-1} = (a^m)^{-1}$. We know that $(a^m)^{-1} = (a^{-1})^m$, then $b^{-1} = (a^{-1})^m$. again $(b^{-1})^{-1} = ((a^{-1})^m)^{-1} \implies b = (a^{-1})^{-m})$. Hence a^{-1} is generator.

2. Let a is a generator of the cyclic group $(G, \circ)$. Let $x, y \in G$. Then $x = a^{m_1}$ and $y = a^{m_2}$ for some integers m_1 and m_2. $x \circ y = a^{m_1} \circ a^{m_2} = a^{m_1+m_2} = a^{m_2+m_1} = a^{m_2} \circ a^{m_1} = y \circ x$. Hence $(G, \circ)$ is commutative.

3. We first assume that $(G, \circ)$ is cyclic. Let a be a generator of $(G, \circ)$. Let k be the order of a. Then $\{a, a^2, a^3, \ldots, a^k\} = \{a^n : n \in \mathbb{Z}\}$(How?). Since a is a generator of G, $G = \{a^n : n \in \mathbb{Z}\}$. Hence $G = \{a, a^2, a^3, \ldots, a^k\}$. Then $o(G) = k = o(a)$.
We now assume that there is an element b such that $o(b) = o(G) = n$. We now show that $(G, \circ)$ is cyclic. To show that it is enough to show b is a generator of G. Since $o(b) = n$, $b, b^2, b^3, \ldots, b^n$ are distinct elements. Then $G = \{b, b^2, b^3, \ldots, b^n\}$. Therefore b is a generator of G. Hence G is cyclic.

4. the proof is not required. □

Theorem 11.2. *Every finite group of prime order is cyclic.*

Proof. Let $o(G) = p$, p is a prime number. Let $a \in G$ such that $a \neq e$. We have seen that $o(a)$ is a divisor of p and p has exactly two divisors, 1 and p. So $o(a)$ is either 1 or p. Since $a \neq e$, $o(a) = p = o(G)$. By using previous theorem, $(G, \circ)$ is cyclic. □

---

12 Group Homomorphism

In this section we define group homomorphism from a group to another group which is similar to linear transformation from a vector space to another vector space.

Definition 12.1. Let $(G, \circ)$ and $(G', *)$ be two groups. A map $\phi : G \to G'$ is called **group homomorphism** if $\phi(a \circ b) = \phi(a) * \phi(b)$ for all $a, b \in G$.

Example 12.1. 1. Let $G = (\mathbb{Z}, +)$ and $G' = (\mathbb{Z}_n, +)$ and $\phi : G \to G'$ be defined by $\phi(m) = \overline{m}$, $m \in \mathbb{Z}$, where $\overline{m}$ is the remainder of $m($ mod $n)$.

2. Let $G = (\mathbb{Z}, +)$ and $G' = (2\mathbb{Z}, +)$ and a mapping $\phi : G \to G'$ be defined by $\phi(a) = 2a$, $a \in G$.

Definition 12.2. Let $\phi : G \to G'$ be a group homomorphism from $(G, \circ)$ to $(G', *)$. $ker(\phi) = \{x \in G : \phi(x) = e_{G'}\}$ and $Img(\phi) = \{\phi(x) : x \in G\}$.

Theorem 12.1. *Let $\phi : G \to G'$ be a group homomorphism from $(G, \circ)$ to $(G', *)$. The following are true.*

1. *$\phi(e_G) = e_{G'}$, where $e_G, e_{G'}$ are the identity elements of G and G', respectively.*
2. *$\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.*
3. *$ker(\phi)$ is a subgroup of $(G, \circ)$.*
4. *$Img(\phi)$ is a subgroup of $(G', *)$.*

Proof. 1. $\phi(e_G) = \phi(e_G \circ e_G) = \phi(e_G) * \phi(e_G)$ (using homomorphism definition).

$$\phi(e_G) = \phi(e_G) * \phi(e_G) \implies \phi(e_G) * \phi^{-1}(e_G) = \phi(e_G) \implies e_{G'} = \phi(e_G).$$

2. Let $x \in G$. Then $x \circ x^{-1} = e_G$. $\phi(x \circ x^{-1}) = \phi(e_G) \implies \phi(x) * \phi(x^{-1}) = e_{G'} \implies \phi(x^{-1}) = \phi(x)^{-1} * e_{G'} \implies \phi(x^{-1}) = \phi(x)^{-1}$.

3. Let $a, b \in ker(\phi)$. Then $\phi(a) = \phi(b) = e_{G'}$. Take $a \circ b^{-1}$. We show that $a \circ b^{-1}$ in $ker(\phi)$. $\phi(a \circ b^{-1}) = \phi(a) * \phi(b^{-1}) = \phi(a) * \phi(b)^{-1} = e_{G'} * e_{G'} = e_{G'}$. Therefore $a \circ b^{-1} \in ker(\phi)$. Hence $ker(\phi)$ is a subgroup of $(G, \circ)$.

4. Similarly you can show that $Img(\phi)$ is a subgroup of $(G', *)$. □

---

13 Definition and Examples

In this section we are going to define few things but we are not going to discuss in details. Those will be taught in your Modern Algebra Course.

Definition 13.1. A nonempty set R is said to be a **ring** if in R there are defined two binary operations, denoted by $+$ and $\cdot$, respectively, such that for all a, b, c in R

1. $a + b$ is in R

2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. There is an element 0 (this a notation of identity element with respect to $+$) in R such that $a + 0 = a$
5. For each $a \in R$ there exists an element $-a$ (this is a notation of inverse element) in R such that $a + (-a) = 0$.
6. $a \cdot b \in R$
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Axiom 1 through 5 merely state that R is an abelian group under the operation $+$, which is call addition. Axiom 6 and 7 insist that R be closed under and associative operations $\cdot$, which we call multiplication.

Remark 13.1. Here 0 not actual zero. This just a notation of identity element of R with respect to $+$. $+$ and $\cdot$ are not usual addition and multiplication, these are just a notation of two operations. If R has identity element with respect to ., then it is denoted by 1 and $(R, +, \cdot)$ is called **ring with unity.**

Example 13.1. 1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ are example of rings, where $+$ and $\cdot$ are usual addition and multiplication.

2. $(\mathbb{Z}_n, +_n, \cdot_n)$ is an example of ring.
3. $(M_n(\mathbb{R}), +, \cdot)$ is an example of ring where $+$ and $\cdot$ are matrix addition and matrix multiplication, respectively.

Definition 13.2. A nonempty set R is said to be a **field** if in R there are defined two binary operations, denoted by $+$ and $\cdot$, respectively, such that

1. $(R, +)$ is abelian group, the identity element is denoted by zero.
2. $(R \setminus \{0\}, \cdot)$ is abelian group, the identity element is denoted 1.
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$

Example 13.2. 1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ and are example of fields, where $+$ and $\cdot$ are usual addition and multiplication.

2. $(\mathbb{Z}_n, +_n, \cdot_n)$ is field if and only if n is prime.
3. $(M_n(\mathbb{R}), +, \cdot)$ is not a field where $+$ and $\cdot$ are matrix addition and matrix multiplication, respectively.
4. $(\mathbb{Z}, +, \cdot)$ is not a field.

End