"Set, Relation and Function"

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirement for the award of the degree of Master of Science in Mathematics

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

Department of Mathematics

Submitted By:

Jangam Jyoti Saikia

Roll No: MAT-20/23

Registration No: MSSV-0023-101-001355

Department of Mathematics MSSV, Nagaon

Under The Guidance:

Dr. Raju Bordoloi, HOD

Department of Mathematics, MSSV, Nagaon

Contents

SET,RELATION AND FUNCTION

Jangam Jyoti Saikia

03.07.20253

Chapter 1

Chapter-I(SET,RELATION AND FUNCTION)

1.1 Set:

Here we shall not try to explore the groundwork for the axiomatic theory of sets;rather we use our intuitive approach for a set to be a collection of some well defined objects.To be honest we can consider a set as primitive notion which one does not define.In an axiomatic development of any mathematical theory, it is a common practice to take for granted certain undefined concepts. For instance during the axiomatic development of elementary geometry we were never offered the definition of **point,line** etc.; rather we were simply taught what can be done with these objects. However it must be clear that our intention is not to lead our readers within the twilight of some uncertainty. Here the basic undefined concept with which we shall be concerned is that of a **set**. The words collection, family or class are sometimes used synonyms for the word set.
A set is a collection of some **well defined objects**. By the use of the words well defined objects we mean that one must be in a position to decide firmly whether an object belong to the collection or not. A set is denoted by capital letters while the elements of a set are denoted by small letters. In case an object x(say) is an element of a set A, then we write $x \in A$ and we read it as "x belongs to A" or "x is in A". In the same tune, whenever we write $x \notin A$, will be read as " x is not an element of A" or "x is not in A".
In order to present a set we do have two distinct ways at our hand, what we call **tabular** form of presentation and **builder** form of presentation. In case of tabular form of presentation of a set A(say) we shall display the elements of the set within brackets {} separating any two of them by commas. Sup-

pose that A be the set of positive integers with single digit. Then the set A can be presented in tabular form as

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

One important point to be note here that the position the elements in the tabular presentation do not posses any meaning. It means that one can alter the positions of the elements in the list at their will. Further, the repetition of an element in the list does not affect the presentation of the set.
In case of builder presentation of a set, we present a set by

$$A = \{x \mid P(x), Q(x), \cdots\}$$

where $P(x), Q(x)$ etc. are some statements concerning an elements x in the set A which must give us the guarantee whether an object x belong to the set A or not. For instance,

$$S = \{x \mid x \text{ is a natural number and } 1 \leq x \leq 9\}$$

is the same set as displayed above in tabular form.
In case every element of a set A is also an element of another set X then we say that " A is a sub-set of the set X" or "A is contained in X" or "X contains the set A" and in such a situation we write $A \subseteq X$. We must note that by the relation $A \subseteq X$ we always include the possibility of their equality. In fact,

$$A = X \Leftrightarrow A \subseteq X \text{ and } X \subseteq X$$

A sub-set A of a set X is said to be a proper sub-set of X if $A \subseteq X$ and $A \neq X$, what we denote by $A \subset X$.
The empty set or null set ϕ contains no elements and it is sub-set of every set.
The number of distinct elements in a set A is said to be the order of the set and we denote it by $\circ(A)$ or by $|A|$. For instance $\circ(\phi) = 0$.

Definition 1. *In any application of set theory, all the sets that appeared are considered to be sub-set of a fixed set what we call the* ***Universal set*** *and we denote it by U.*
For any two given sets. in a number of ways we can combine them to produce a new set. These process of combination can be extended to any given number of sets, finite or infinite whatsoever. Here we define combination of any two sets, ultimately this will lead us into the general environment.

Definition 2. *The union of any two sets A and B is the set $\{x \mid x \in A \text{ or } x \in B\}$ and we denote it by $A \cup B$.*

$$\therefore A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

Please note that the word "or" used here always in inclusive sense. It means that in order to qualify for an element x to be an element of $A \cup B$, we need $x \in A$ or $x \in B$ or x belong to both of the sets A and B.

Definition 3. *The intersection of any two sets A and B is the set $\{x \mid x \in A \text{ and } x \in B\}$ and we denote it by $A \cap B$.*

$$\therefore A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

In case $A \cap B = \phi$, the sets A and B are said to be disjoint.

Definition 4. *The difference of any two sets A and B is the set $\{x \mid x \in A \text{ and } x \notin B\}$ and we denote it by $A - B$.*

$$\therefore A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

In case $B \subseteq A$, we call $A - B$ is the complement of B in the set A. As a special case the difference $U - A$, where U is the Universal set, is said to be the complement of the set A and we denote it by A^c. From the definition of difference of sets it follows that,

$$A^c = \{x \mid x \notin A\}$$

Definition 5. *The Cartesian product of any two sets A and B is the set $\{(x, y) \mid x \in A \text{ and } y \in B\}$ and we denote it by $A \times B$.*

$$\therefore A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$$

Please note that the sets $A \times B$ and $B \times A$ are distinct sets. The Cartesian product of a set A with itself ie. $A \times A$ will be denoted by A^2. The elements of the form (a, a) in A^2 are said to be the diagonal elements and the collection of all the diagonal elements is said to be the diagonal of A^2. If the set A is a finite set and $\circ(A) = n$ then the set A^2 is also finite and $\circ(A^2) = n^2$.

Indexed family of sets: *During the course of our journey we may encounter a set A whose elements are set itself. For instance if we consider a set whose elements are the inhabitant of different countries of the World. Suppose I represent the set of all Indians then $I \in A$. Thus the elements of the set A are set itself. In such an environment we call A as a collection of*

sets.
Let us consider a collection of sets given by.

$$A = \{A_1, A_2, \cdots, A_{100}\}$$

Our natural instinct certainly tempted us to represent the set A by,

$$A = \{A_i \mid i \in I\} \text{ where } I = \{1, 2, \cdots, 100\}$$

In this process, actually we have used a box of labels in the form of I and we convinced ourselves that corresponding to each label (an element) i in I there exists an element A_i in A. This is how the concept of indexed family coming in to play in human mind.
A collection of sets

$$A = \{A_\alpha \mid \alpha \in \Lambda\}$$

is said to be an indexed family of sets, where the set Λ (the box of labels) is said to be the indexed set.
Please note that the union and intersection of the members of the indexed family of set A are denoted by

$$\cup_{\alpha\in\Lambda} A_\alpha, \quad \text{and} \quad \cap_{\alpha\in\Lambda} A_\alpha$$

respectively and we define them by,

$$\cup_{\alpha\in\Lambda} A_\alpha = \{x \mid x \in A_\alpha \text{ for some } \alpha \in \Lambda\}$$
$$\cap_{\alpha\in\Lambda} A_\alpha = \{x \mid x \in A_\alpha \ \forall \alpha \in \Lambda\}$$

In case $A_\alpha \cap A_\beta = \phi$ whenever $\alpha \neq \beta$, then the collection A is said to be a collection of mutually disjoint sets.
At this point we would like to state a few results in respect of distributive property.The following result shows how $\cup$ and $\cap$ are distributive over one another and how $\times$ is distributive over $\cup$ and $\cap$.

Theorem 1. *For any three sets A, B, C we have,*

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
3. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
4. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Proof: *For any* $x \in A \cap (B \cup C)$ *we have,*

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \ \textit{and} \ x \in (B \cup C) \\ &\Leftrightarrow x \in A \ \textit{and} \ (x \in B \ \textit{or} \ x \in C) \\ &\Leftrightarrow (x \in A \ \textit{and} \ x \in B) \ \textit{or} \ (x \in A \ \textit{and} \ x \in C) \\ &\Leftrightarrow x \in (A \cap B) \ \textit{or} \ x \in (A \cap C) \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

It follows that,

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

For an element $(x, y) \in A \times (B \cup C)$ *we have,*

$$\begin{aligned} (x, y) \in A \times (B \cup C) &\Leftrightarrow x \in A \ \textit{and} \ y \in (B \cup C) \\ &\Leftrightarrow x \in A \ \textit{and} \ (y \in B \ \textit{or} \ y \in C) \\ &\Leftrightarrow (x \in A \ \textit{and} \ y \in B) \ \textit{or} \ (x \in A \ \textit{and} \ y \in C) \\ &\Leftrightarrow (x, y) \in (A \times B) \ \textit{or} \ (x, y) \in (A \times C) \\ &\Leftrightarrow (x, y) \in (A \times B) \cup (A \times C) \end{aligned}$$

It follows that,

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

The proof of the other two parts are left as an Exercise.
Remark: *Here we can afford to state the above results in a more general set-up as follows:*
For any set B *and for a collection of sets* $A = \{A_\alpha \mid \alpha \in \Lambda\}$ *with* Λ *as the indexed set, the following results hold good.*

1. $B \cap (\cup_{\alpha \in \Lambda} A_\alpha) = \cup_{\alpha \in \Lambda} (B \cap A_\alpha)$
2. $B \cup (\cap_{\alpha \in \Lambda} A_\alpha) = \cap_{\alpha \in \Lambda} (B \cup A_\alpha)$
3. $B \times (\cup_{\alpha \in \Lambda} A_\alpha) = \cup_{\alpha \in \Lambda} (B \times A_\alpha)$
4. $B \times (\cap_{\alpha \in \Lambda} A_\alpha) = \cap_{\alpha \in \Lambda} (B \times A_\alpha)$

Proof: *For any* $x \in B \cup (\cap_{\alpha \in \Lambda} A_\alpha)$ *we have,*

$$\begin{aligned} x \in B \cup (\cap_{\alpha \in \Lambda} A_\alpha) &\Leftrightarrow x \in B \ \textit{or} \ x \in (x \in \cap_{\alpha \in \Lambda} A_\alpha) \\ &\Leftrightarrow x \in B \ \textit{or} \ (x \in A_\alpha \ \forall \ \alpha \in \Lambda) \\ &\Leftrightarrow (x \in B \ \textit{or} \ x \in A_\alpha) \ \forall \alpha \in \Lambda \\ &\Leftrightarrow x \in (B \cup A_\alpha) \ \forall \alpha \in \Lambda \\ &\Leftrightarrow \cap_{\alpha \in \Lambda} (B \cup A_\alpha) \end{aligned}$$

It follows that,

$$B \cup (\cap_{\alpha\in\Lambda} A_\alpha) = \cap_{\alpha\in\Lambda}(B \cup A_\alpha)$$

The proof of the other parts readily follows.

Theorem 2. *(De-Morgan Laws) For any two sets A and B we always have,*

$$(A \cup B)^c = A^c \cap B^c$$
$$(A \cap B)^c = A^c \cup B^c$$

Proof: *For any $x \in (A \cup B)^c$ we have,*

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \\ &\Leftrightarrow x \notin A \ \text{and} \ x \notin B \\ &\Leftrightarrow x \in A^c \ \text{and} \ x \in B^c \\ &\Leftrightarrow x \in (A^c \cap B^c) \end{aligned}$$

It follows that,

$$(A \cup B)^c = A^c \cap B^c$$

In the same line for any $x \in (A \cap B)^c$ we have,

$$\begin{aligned} x \in (A \cap B)^c &\Leftrightarrow x \notin A \cap B \\ &\Leftrightarrow x \notin A \ \text{or} \ x \notin B \\ &\Leftrightarrow x \in A^c \ \text{or} \ x \in B^c \\ &\Leftrightarrow x \in (A^c \cup B^c) \end{aligned}$$

It follows that,

$$(A \cap B)^c = A^c \cup B^c$$

Remark: *For an indexed collection of sets $A = \{A_\alpha \mid \alpha \in \Lambda\}$ with Λ as the indexed set, the following are the generalised form of De-Morgan laws:*

$$(\cup_{\alpha\in\Lambda} A_\alpha)^c = \cap_{\alpha\in\Lambda} A^c$$
$$(\cap_{\alpha\in\Lambda} A_\alpha)^c = \cup_{\alpha\in\Lambda} A^c$$

Proof: *For an element $x \in (\cup_{\alpha\in\Lambda} A_\alpha)^c$ we have,*

$$\begin{aligned} x \in (\cup_{\alpha\in\Lambda} A_\alpha)^c &\Leftrightarrow x \notin \cup_{\alpha\in\Lambda} A_\alpha \\ &\Leftrightarrow x \notin A_\alpha \ \ \forall \alpha \in \Lambda \\ &\Leftrightarrow x \in A_\alpha^c \ \ \forall \alpha \in \Lambda \\ &\Leftrightarrow x \in \cap_{\alpha\in\Lambda} A_\alpha^c \end{aligned}$$

It follows that,

$$(\cup_{\alpha\in\Lambda} A_\alpha)^c = \cap_{\alpha\in\Lambda} A_\alpha^c$$

In the same line one can proceed for the proof of the other part of the result. Here we would like to state a few simple but interesting results in respect of the operations as already defined to combine sets.

Theorem 3. *For any sets A, B, C, D, S, T etc.(all are considered to be subsets of the universal set U) it can be seen that,*

1. $A \subseteq (A \cup B)$, $B \subseteq (A \cup B)$; $(A \cap B) \subseteq A$, $(A \cap B) \subseteq B$
2. $A \cup A = A$, $A \cap A = A$ *[Idempotent property]*
3. $(A \cup B) = (B \cup A)$; $(A \cap B) = (B \cap A)$ *[Commutative property]*
4. $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$ *[Associative property]*
5. $A \cup \phi = A$; $A \cap \phi = \phi$ *while* $A \cup U = U$; $A \cap U = A$
6. $A - A = \phi$; $A - \phi = A$
7. $(A - B) \subseteq A$ *as a consequence* $(A - B) \cup A = A$
8. $(A - B) \cap B = \phi$; $A \cap A^c = \phi$; $U^c = \phi$ *and* $\phi^c = U$
9. $A \subseteq B \subseteq C \Rightarrow A^c \supseteq B^c \supseteq C^c$

The simplicity in the proof of the results motivate us to left it as an Exercise.

Example: *Let us consider the collection of sets $\mathbb{A} = \{A_\alpha \mid \alpha \in \mathbb{N}\}$ with the set of natural number $\mathbb{N}$ as the indexed set, where*

$$A_\alpha = \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{\alpha}\right\}$$

Determine the union and intersection of the members of $\mathbb{A}$. Further verify De-Morgan laws for the collection $\mathbb{A}$ with the universal set $U = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$.

Solution: *For $\alpha = 1, 2, 3, \cdots$ we have,*

$$A_1 = \{1\} \ , \ A_2 = \left\{1, \frac{1}{2}\right\} \ , \ A_3 = \left\{1, \frac{1}{2}, \frac{1}{3}\right\} \ \textit{etc.}$$

It follows that,

$$\cup_{\alpha\in\mathbb{N}}A_\alpha = \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{\alpha}, \frac{1}{\alpha+1}, \cdots\right\}$$

Further for any $x \in \cap_{\alpha\in\mathbb{N}}A_\alpha$ *we have,*

$$\begin{aligned} x \in \cap_{\alpha\in\mathbb{N}}A_\alpha &\Leftrightarrow x \in A_\alpha \ \forall\alpha \in \mathbb{N} \\ &\Leftrightarrow x = 1 \\ &\Leftrightarrow x \in \{1\} \end{aligned}$$

It follows that,

$$\cap_{\alpha\in\mathbb{N}}A_\alpha = \{1\}$$

From the definition of the universal set U *it is clear that* $U = [0, 1]$. *Further from the definition of complement it is clear that,*

$$A_1^c = [0, 1)$$

For any $\alpha(\neq 1) \in \mathbb{N}$ *it is clear that,*

$$A_\alpha^c = [0, 1] - \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{\alpha}\right\} \subset [0, 1) = A_1^c$$

It follows that,

$$\cup_{\alpha\in\mathbb{N}}A_\alpha^c = A_1^c \tag{1.1}$$

On the other hand,

$$(\cap_{\alpha\in\mathbb{N}}A_\alpha)^c = A_1^c \tag{1.2}$$

From (1.1) *and* (1.2) *it follows that,*

$$(\cap_{\alpha\in\mathbb{N}}A_\alpha)^c = \cup_{\alpha\in\mathbb{N}}A_\alpha^c$$

From the definition of A_α *it is clear that,*

$$A_1 \subset A_2 \subset A_3 \cdots \Rightarrow A_1^c \supset A_2^c \supset A_3^c \supset \cdots \tag{1.3}$$

From (1.3) *it follows that,*

$$\begin{aligned} &A_1^c \cap A_2^c \cap A_3^c \cap \cdots \cap A_\alpha^c \cap A_{\alpha+1}^c \cap \cdots = A_{\alpha+1}^c \cap \cdots \\ &\Rightarrow \cap_{\alpha\in\mathbb{N}}A_\alpha^c = [0, 1] - \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{\alpha}, \frac{1}{\alpha+1}, \cdots\right\} \\ &\Rightarrow \cap_{\alpha\in\mathbb{N}}A_\alpha^c = (\cup_{\alpha\in\mathbb{N}}A_\alpha)^c \end{aligned}$$

Thus we have verified De-Morgan laws for the members of the collection of sets $\mathbb{A}$.

Example: *A finite set A has n distinct elements, prove that A has exactly 2^n distinct sub-sets.*
Solution: *Suppose that $A = \{x_1\}$. Then the sub-sets of A are $\phi, \{x_1\}$, which means that the result is true for $n = 1$ as the number of subsets of A is $2 = 2^1$. In case $A = \{x_1, x_2\}$, the sub-sets of A are $\phi, \{x_1\}, \{x_2\}, \{x_1, x_2\}$, which means that the result is true for $n = 2$, as the number of sub-sets of A is $4 = 2^2$. Further we notice that the number of sub-sets of A where x_2 appear as an element is 2^1. In the same line it can be seen that in case of $A = \{x_1, x_2, x_3\}$ the number of sub-sets of A is $8 = 2^3$ and the number of sub-sets of A in which $x_3$appears as an element is 2^2.*
Let us assume that the result is true for $n = k$ ie. any set having k number of elements will have 2^k number of sub-sets. Suppose that $A = \{x_1, x_2, \cdots, x_k, x_{k+1}\}$. According to our assumption the number of sub-sets of the set A which are also sub-sets of the set $\{x_1, x_2, \cdots, x_k\}$ is 2^k. Further, the number of sub-sets of the set A where x_{k+1} will appear as an element is 2^k. Thus the total number of sub-sets of the set A is $2^k + 2^k = 2^{k+1}$. It follows that the result is true for $n = k + 1$. Thus by mathematical induction the result is true for any positive integer n.

Example: *For any two sets A and B, their symmetric difference is defined as $(A - B) \cup (B - A)$. Prove that the symmetric difference of A and B equals $(A \cup B) - (A \cap B)$.*
Solution: *For an arbitrary element $x \in (A - B) \cup (B - A)$ we have,*

$$\begin{aligned} x \in (A - B) \cup (B - A) &\Leftrightarrow x \in (A - B) \text{ or } x \in (B - A) \\ &\Leftrightarrow (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and} x \notin A) \\ &\Leftrightarrow x \in A \text{ or } (x \in B \text{ and} x \notin A) \text{ and } x \notin B \text{ or } (x \in B \text{ and} x \notin A) \\ &\Leftrightarrow (x \in A \text{ or } x \in B) \text{ and } (x \notin B \text{ and } x \notin A) \\ &\Leftrightarrow x \in (A \cup B) \text{ and } x \notin (A \cap B) \\ &\Leftrightarrow x \in (A \cup B) - (A \cap B) \end{aligned}$$

It follows that,

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

Remark: *If we denote the symmetric difference of the sets A and B by $A \triangle B$ then it can be seen that,*

1. $A \triangle B = B \triangle A$

2. $A \triangle (B \triangle C) = (A \triangle B) \triangle C$

3. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

1.2 Relation:

In our day to day life we always come across a good number of relations among ourselves. For instance we often use the phrases like "Lakshay is the son of Naruttam", "Lakshay is friend of Naba", "Nilay is the uncle of Khanin" etc. etc. In fact any one will accept that such a phrase define a relation of someone with the other within our society. The relationship whichever are coming to us in our day to day life are quite informal in nature but readily acceptable to everyone. Let us try to explore this field of informal definitions to provide a formal shape so that it can draw a clear picture in respect of relationships at our hand.
Here we notice that we need two objects to have a relation between them and these two objects must come from some sets of objects. Please note that, in order to display all possible pair of objects between two sets A and B we can consider their Cartesian product $A \times B$. It is not that all the objects in the set A must have relation with all of the objects in the set B. It means some objects in the set A will have relation with some objects in the set B. Thus a relation R (say) from a set A to another set B is simply a sub-set of the Cartesian product $A \times B$, what provide us the clue in order to derive a formal definition of a relation from a set A to another set B.

Definition 6. *A relation R from a set A to another set B is nothing but a sub-set of the set $A \times B$. Thus,*

$$R \text{ is a relation from the set } A \text{to the set } B \iff R \subseteq A \times B$$

For an element $a \in A$ and $b \in B$ if $(a, b) \in R$ then we read it as "the element a is related to b by virtue of the relation R" and we write it as

$$(a, b) \in R \Leftrightarrow aRb$$

Similarly for an element $a \in A$ and $b \in B$ if $(a, b) \notin R$ then we read it as "the element a is not related to b by virtue of the relation R" and we write it as

$$(a, b) \notin R \Leftrightarrow a \not{R} b$$

To have a relation from a set A to another set B the basic need is that some objects must be there in both the sets and therefore we presume that both the

sets A and B are non-empty sets.
For a non-empty set A, if $R \subseteqq A \times A$ then we read it as "R is a relation in the set A" or "R is a relation on the set A" instead of R is a relation from the set A to the set A.

Definition 7. *A relation R in a set A is said to be an* ***equivalence relation*** *in the set A if and only if*
1. R is reflexive ie. $aRa \quad \forall a \in A$
2. R is symmetric ie. $aRb \Rightarrow bRa$ for any $a, b \in A$ and
3. R is transitive ie. aRb and $bRc \Rightarrow aRc$ for any $a, b, c \in A$

The concept of ***equivalence relation*** *is really very important one and it plays central role in all parts of mathematics. In this direction we need one more important concept related to an equivalence relation, what we can call it as* ***equivalence class****.*

Definition 8. *For an element $a \in A$ the equivalence class determined by the element a with respect to an equivalence relation R in the set A is denoted by $[a]$ or by $cl(a)$ and it is defined as the sub-set of the set A by,*

$$[a] = \{x \in A \mid xRa\}$$

Because of the reflexivity of R we always have aRa as a consequence of which we can conclude that $a \in [a]$. Thus we are always assured that an equivalence class $[a]$ is a non-empty sub-set of the set A.

Further, any two equivalence classes are either disjoint or identical. In simple word for any $a, b \in A$ either $[a] \cap [b] = \phi$ or $[a] = [b]$. One can establish this result with the simple argument as follows:
Suppose that $[a] \cap [b] \neq \phi$ then there must exists some element x (say) in $[a] \cap [b]$. In this situation we have,

$$\begin{aligned} x \in [a] \cap [b] &\Leftrightarrow x \in [a] \quad and \quad x \in [b] \\ &\Leftrightarrow xRa \quad and \quad xRb \\ &\Leftrightarrow aRx \quad and \quad xRb \quad [using \quad symmetry \quad of \quad R] \\ &\Leftrightarrow aRb \quad [using \quad transitivity \quad of \quad R] \end{aligned}$$

Now for any $y \in [a]$ we have,

$$\begin{aligned} y \in [a] &\Leftrightarrow yRa \\ &\Leftrightarrow yRb \quad [since \quad aRb] \\ &\Leftrightarrow y \in [b] \end{aligned}$$

This shows that,

$$[a] = [b]$$

Definition 9. *A relation R in a set A is said to be anti-symmetric if for any $a, b \in A$,*

$$aRb \text{ and } bRa \Rightarrow a = b$$

Thus in case of an anti-symmetric relation R we never have both aRb and bRa except when $a = b$.

At this point we would like to introduce one more important concept what we call ***partition*** *of a set, so that we can establish a relation between* ***partition*** *and* ***equivalence relation****.*

Definition 10. *A collection, $\mathbb{P} = \{G_\alpha \mid G_\alpha \subseteq G \text{ and } \alpha \in \Lambda\}$ where Λ be an indexed set, is said to be a partition of the set G if and only if the members of $\mathbb{P}$ are mutually disjoint and union of its' members will cover the entire set G. In other sense,*

$$\begin{aligned}&\mathbb{P} = \{G_\alpha \mid G_\alpha \subseteq G \text{ and } \alpha \in \Lambda\} \text{ is a partition of } G\\ &\quad \Leftrightarrow G = \cup_{\alpha\in\Lambda} G_\alpha \text{ and } G_\alpha \cap G_\beta = \phi \text{ for any two distinct } \alpha, \beta \in \Lambda\end{aligned}$$

We hope this is the right place to establish our most desired result which certainly unfold the relationship between an equivalence relation and a partition on a set A.

Theorem 4. *The distinct equivalence classes of an equivalence relation on a set A provide us a partition of the set A. Conversely, for a given partition $\mathbb{P}$ of a set A, it is always possible to define an equivalence relation on the set A for which the the members of the given partition $\mathbb{P}$ are exactly the equivalence classes.*

Proof: *Suppose that $\sim$ be an equivalence relation on a set A. Let us consider the collection,*

$$\mathbb{P}_1 = \{[a] \mid a \in A\}$$

We note that for any $a \in A$ by the reflexivity of the relation $\sim$ we have $a \sim a$, as a consequence of which $a \in [a]$. This shows that the members of $\mathbb{P}_1$ are non-empty sub-sets of the set A. As we know that any two equivalence classes

are either disjoint or identical (prove!), the members of the collection $\mathbb{P}_1$ *are mutually disjoint sub-sets of the set* A*. Obviously,*

$$A = \cup_{a \in A}[a]$$

This shows that $\mathbb{P}_1$ *is a partition of the set* A*.*
Conversely, suppose that,

$$\mathbb{P} = \{A_\alpha \mid A_\alpha \subseteq A \ \ and \ \ \alpha \in \Lambda\}$$

be a partition of the set A *with* Λ *as an indexed set. Since* $\cup_{\alpha \in \Lambda} A_\alpha = A$ *and the members of* $\mathbb{P}$ *are mutually disjoint, for any* $a \in A$ *it must be exactly in one* A_α*. Let us define a relation* $\sim$ *on the set* A *by,*

$$a \sim b \Leftrightarrow a, b \in A_\alpha \ \ for some \ \ \alpha \in \Lambda$$

As $\cup_{\alpha \in \Lambda} A_\alpha = A$*, for any* $a \in A$*, we must have* $a, a \in A_\alpha$ *for some* $\alpha \in \Lambda$ *and consequently* $a \sim a$*, which proves the reflexivity of* $\sim$*.*
Now, for any $a, b \in A$ *we have,*

$$\begin{aligned} a \sim b &\Rightarrow a, b \in A_\alpha \ \ for\ some \ \ \alpha \in \Lambda \\ &\Rightarrow b, a \in A_\alpha \ \ for\ some \ \ \alpha \in \Lambda \\ &\Rightarrow b \sim a \end{aligned}$$

This proves the symmetry of the relation $\sim$*.*
Suppose that, $a, b, c \in A$ *such that* $a \sim b \ \ and \ \ b \sim c$*.*
We now have,

$$\begin{aligned} a \sim b \ \ and \ \ b \sim c &\Rightarrow a, b \in A_\alpha \ \ and \ \ b, c \in A_\beta \ \ for some \ \ \alpha, \beta \in \Lambda \\ &\Rightarrow a, c \in A_\alpha \ \ [since \ \ A_\alpha = A_\beta, \ \ for \ \ b \in A_\alpha \cap A_\beta] \\ &\Rightarrow a \sim c \end{aligned}$$

This proves the transitivity of the relation $\sim$*.*
Thus the relation $\sim$ *so defined is an equivalence relation on the set* A*.*
Finally, let us consider an equivalence class $[a]$ *with respect to the equivalence relation* $\sim$*, determine by the element* $a \in A$*. We now have,*

$$\begin{aligned} a \in A &\Rightarrow a \in A_\alpha \ \ for some \ \ \alpha \in \Lambda \\ &\Rightarrow a \in [a] \cap A_\alpha \ \ [since \ \ a \in [a]] \\ &\Rightarrow [a] = A_\alpha \end{aligned}$$

Thus the equivalence classes with respect to the equivalence relation $\sim$ *are exactly the members of the partition* $\mathbb{P}$*.*

Definition 11. *For a fixed positive integer n in the set of integers $\mathbb{Z}$ we define a relation,*

$$a \equiv b(mod\ n) \Leftrightarrow n \mid (a-b)$$

The relation so defined is said to be ***"congruence modulo n"****, n is called* ***modulus*** *of the relation. Whenever $a \equiv b(mod\ n)$ we read it as "a is congruent to b modulo n".*
Without exaggeration this relation in the set of integers $\mathbb{Z}$ is probably the single most important as it plays pivotal role in number theory, group theory etc. This is why we would like to focus our special attention to this relation.
1. The relation congruence modulo n is an equivalence relation on the set of integers $\mathbb{Z}$.
2. This equivalence relation has exactly n distinct equivalence classes.
3.If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then $a+c \equiv b+d(mod\ n)$ and $ac \equiv bd(mod\ n)$.
4. If $ab \equiv ac(mod\ n)$ and a is relatively prime to n then $b \equiv c(mod\ n)$.
Proof: *For any $a \in \mathbb{Z}$, since $n \mid (a-a)$, $a \equiv a(mod\ n)$ which proves the reflexivity of the congruence relation in $\mathbb{Z}$.*
For any $a, b \in \mathbb{Z}$ we have,

$$\begin{aligned} a \equiv b(mod\ n) &\Rightarrow n \mid (a-b) \\ &\Rightarrow n \mid (b-a) \\ &\Rightarrow b \equiv a(mod\ n) \end{aligned}$$

This proves the symmetry of the congruence relation in $\mathbb{Z}$.
For $a, b, c \in \mathbb{Z}$ we have,

$$\begin{aligned} a \equiv b(mod\ n)\ and\ b \equiv c(mod\ n) &\Rightarrow n \mid (a-b)\ and\ n \mid (b-c) \\ &\Rightarrow n \mid (a-c) \\ &\Rightarrow a \equiv c(mod\ n) \end{aligned}$$

This proves the transitivity of the congruence relation in the set $\mathbb{Z}$ and hence the relation in question is an equivalence relation.
For the proof of the second part of the result let us consider an equivalence class $[a]$ determined by the element $a \in \mathbb{Z}$ with respect to the equivalence

relation in question. Then by Euclidean algorithm we have,

$a = nk + r$ *where* $0 \leq r < n$
$\Rightarrow (a - r) = nk$
$\Rightarrow n \mid (a - r)$
$\Rightarrow a \equiv r(mod\ n)$
$\Rightarrow a \in [r]$
$\Rightarrow [a] = [r]$ *[since any two equivalence classes are either disjoint or identical]*

Since $0 \leq r < n$ *therefore we can have at most* n *number of congruent classes, namely* $[0], [1], \cdots [n-1]$.
We are to prove that all these n *congruent classes are distinct. On the contrary suppose that* $[i] = [j]$ *with* $0 \leq i < j < n$. *But then* $n \mid (j-i)$ *as* $i \in [j]$ *which is impossible as* $j - i$ *is a positive integer less than* n.
Thus all the congruent classes $[0], [1], \cdots [n-1]$ *are distinct.*
For the proof of the third part, it is given that $a \equiv b(mod\ n)$ *and* $c \equiv d(mod\ n)$. *We now have,*

$$\begin{aligned} a \equiv b(mod\ n)\ and\ c \equiv d(mod\ n) &\Rightarrow n \mid (a-b)\ and\ n \mid (c-d) \\ &\Rightarrow n \mid (a-b) + (c-d) \\ &\Rightarrow n \mid (a+c) - (b+d) \\ &\Rightarrow a + c \equiv b + d(mod\ n) \end{aligned}$$

Further,

$$\begin{aligned} n \mid (a-b)\ and\ n \mid (c-d) &\Rightarrow n \mid (a-b)c + (c-d)b \\ &\Rightarrow n \mid (ac - bd) \\ &\Rightarrow ac \equiv bd(mod\ n) \end{aligned}$$

We now proceed to prove the last part of the result. Here we have,

$$\begin{aligned} ab \equiv ac(mod\ n) &\Rightarrow n \mid a(b-c) \\ &\Rightarrow n \mid (b-c)\ \textit{[since } a \textit{ is relatively prime to } n\textit{]} \\ &\Rightarrow b \equiv c(mod\ n) \end{aligned}$$

This complete the proof of the required results.

1.3 Function:

Here we intend to introduce the concept of function or mapping from a set A *to another set* B. *In fact the practice used by men during their nomadic life to*

keep a pebble against one thing to be counted is directly related to an one-one and onto mapping which plays a predominant role in modern mathematics. One can presume that it is not just a new concept as we are using it from early days of our schooling life. For instance, whenever we were asked to plot the relation $y = x^2$ we were simply being asked to study the particular mapping which takes every real number on to its square. One can consider a mapping or a function f from a set A to a set B just as a relation with a special condition that it must relate ***every element*** *of the set A to* ***an unique element*** *of the set B. Because of its speciality we shall use the notation $f : A \to B$ instead of $f \subseteq A \times B$ and if an element $x \in A$ related to the element $y \in B$ by virtue of the relation f then we shall use the notation $y = f(x)$ instead of xfy.*

Definition 12. *A function or a mapping f from a set A to a set B is a relation from the set A to the set B which associates each element $x \in A$ with an unique element B and we denote it by $f : A \to B$.*

In case of an element $x \in A$ is associated to the element $y \in B$ by virtue of the function $f : A \to B$,we write $f(x) = y$. In such a situation we pronounce it as "$y \in B$ is the image of $x \in A$" and "$x \in A$ is a pre-image of $y \in B$. We must note that an element $x \in A$ has unique image $y \in B$ whereas an element $y \in B$ may have more than one pre-image $x \in A$. In simple words for a function $f : A \to B$ it may so happen that for an element $y \in B, \exists\ x_1, x_2 \in A$ such that,

$$x_1 \neq x_2 \ \text{ whereas } \ f(x_1) = y \ \text{ and } \ f(x_2) = y$$

It means $x_1, x_2 \in A$ are two distinct pre-images of the element $y \in B$.

In case of a function $f : A \to B$, the sets A, B are said to be ***domain*** *and* ***co-domain*** *respectively of the function f. The* ***range*** *of the function f is the subset of B(co-domain) containing those elements of B which has some pre-image in A and we shall denote it by $f(A)$.*

$$\therefore f(A) = \{y \in B \mid f(x) = y \ \text{ for some } \ x \in A\}$$

In case $f(A) = B$ ie. every element of B has some pre-image in A, we say that the function $f : A \to B$ is an ***onto*** *function.*

A function $f : A \to B$ is said to an one-one function if any two distinct elements of A has distinct images in B ie. for $x_1, x_2 \in A$ and $x_1 \neq x_2$ must implies $f(x_1) \neq f(x_2)$.

Working rules:
1.In order to establish a function $f : A \to B$ to be an onto function we shall show that for any $y \in B$ there exists some $x \in A$ such that,

$$f(x) = y$$

2.In order to establish a function $f : A \to B$ to be an one-one function we shall show that for any $x_1, x_2 \in A$

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Remark: *An one-one function is sometime called as* ***injection*** *or* ***injective*** *one. An onto function is sometime called as* ***surjection****or* ***surjective*** *one. An one-one and onto function is sometime called as* ***bijection*** *or a* ***bijective*** *one.*

Equality of two functions: *Any two functions with the same domain, $f : A \to B$ and $g : A \to C$ are said to be equal if and only if*

$$f(x) = g(x) \ \forall x \in A$$

Thus for the functions f and g with the same domain A

$$f = g \Leftrightarrow f(x) = g(x) \ \forall x \in A$$

Let us design an environment wherein we have two functions $f : A \to B$ and $g : B \to C$. Please note that the co-domain of the function f and domain of the function g is the same set, namely the set B. In such an environment we can compose both the functions f and g which will result a new function from the set A to the set C what we call the composition of the functions f and g and we denote this new function by $f \circ g$. We note that for any $x \in A$ we always have $f(x) \in B$ and since B is the domain of the function g therefore $g(f(x)) \in C$. Thus for any $x \in A$ we can provide an unique element $g(f(x)) \in C$. This provide us sufficient clue to construct the composite function $f \circ g : A \to C$.

Definition 13. *For the functions $f : A \to B$ and $g : B \to C$ it is always possible to define a function $f \circ g : A \to C$ such that*

$$f \circ g(x) = g(f(x)) \ \forall x \in A$$

Definition 14. *A function $I : A \to A$ is said to be the* ***identity function*** *on the set A if and only if*

$$I(x) = x \ \forall x \in A$$

Definition 15. *A function $f : A \to B$ is said to be a* ***constant function*** *if for some fixed $k(say) \in B$*

$$f(x) = k \ \forall x \in A$$

Please note that the range of the constant function f defined above is a single tone ie. $f(A) = \{k\} \subseteq B$.

For a given function $f : A \to B$ one can ask a very natural question like- " Is it possible to construct a function $g(say) : B \to A$ with the help of the function $f : A \to B$". However the answer to such a question is not always affirmative. Please note that in case the range of the function f is a proper sub-set of its' co-domain B then it will not be possible to assign the image of each element in B. Thus to define the function $g : B \to A$ situation demand an environment wherein $f(A) = B$ ie. the function $f : A \to B$ must be an onto function. Further to maintain the uniqueness of the images of an element in B under g the basic requirement is that the function $f : A \to B$ must be an one-one function.
Thus for an one-one and onto function $f : A \to B$ it is always possible to construct a function $g : B \to A$ such that

$$f(x) = y \Leftrightarrow g(y) = x \text{ for any } x \in A, \ y \in B$$

The function $g : B \to A$ so obtain with the help of the one-one and onto function $f : A \to B$ is said to be the ***inverse function*** *of f and we denote it by f^{-1}.*

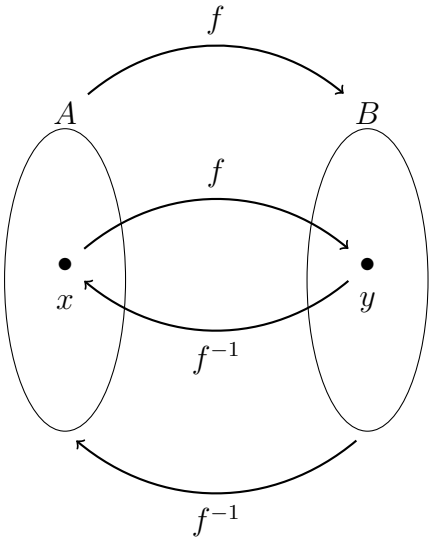

Figure 1.

Definition 16. *For a given one-one and onto function $f : A \to B$ it is always possible to define a function $f^{-1} : B \to A$ what we call the inverse function of f, such that*

$$f(x) = y \Leftrightarrow f^{-1}(y) = x \ \ \forall x \in A \ \text{and} \ \forall y \in B$$

Definition 17. *Suppose that A be a subset of a set X then the* ***characteristic function*** *of the set A is denoted by χ_A such that $\chi_A : X \to \{0, 1\}$ defined by,*

$$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

We note that the characteristic function of the empty set ϕ is a constant function with $\{0\}$ as its range set. Further for any two sub-sets A, B of the set X it is easy to verify that,

$$\chi_A = \chi_B \Leftrightarrow A = B$$

In some special situations the characteristic function plays very important role to verify the equality of sub-sets of the set X. Further we notice that there exists a bijection between the collection of all characteristic functions on X and the collection of all sub-sets of X ie. the power set of X.

Here we would like to state a few simple but important results in respect of composition and inverse of functions. One will certainly realise the importance of these simple results in due course of mathematical training.

1. Composition of functions satisfy associative property.

2. For the functions $f : A \to B$ and $g : B \to C$, $f \circ g$, will be one-one and onto provided f and g both are one-one and onto. Further in such a situation,

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

3. For a function $f : A \to B$ if $f^{-1} : B \to A$ exists then the function f^{-1} is also one-one and onto.Further,

$$(f^{=1})^{-1} = f$$

Furthermore in case of a bijective function $f : A \to A$

$$f \circ f^{-1} = f^{-1} \circ f = I$$

where I is the identity function on the set A.

4. A function $f : A \to B$ will be an one-one and onto function if and only if there exists a function $g : B \to A$ such that both $f \circ g$ and $g \circ f$ are identity functions on A and B respectively.

Proof of part 1: *Suppose that $f : A \to B$, $g : B \to C$ and $h : C \to D$ are three given functions. We are to show that*

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Here we note that the domain of both the functions $f \circ (g \circ h)$ and $(f \circ g) \circ h$ is the same set, namely the set A. Now for any $x \in A$ we have

$$f \circ (g \circ h)(x) = g \circ h(f(x)) = h(g(f(x)))$$
$$(f \circ g) \circ h(x) = h(f \circ g(x)) = h(g(f(x)))$$

The required equality follows from the above results.

Proof of part 2: *Suppose that both the functions $f : A \to B$ and $g : B \to C$ are one-one and onto. We need to show that $f \circ g : A \to C$ is also one-one and onto.*
For any $x_1, x_2 \in A$ we have,

$$\begin{aligned} f \circ g(x_1) = f \circ g(x_2) &\Rightarrow g(f(x_1)) = g(f(x_2)) \\ &\Rightarrow f(x_1) = f(x_2) \ [since \ \ g \ \ is \ \ one - one] \\ &\Rightarrow x_1 = x_2 \ [since \ \ f \ \ is \ \ one - one] \end{aligned}$$

This prove that the function $f \circ g : A \to C$ is one-one.

Suppose that z be an arbitrary element of C. Since the function $g : B \to C$ is suppose to be onto,$\exists$ $y \in B$ such that, $g(y) = z$. Since the function $f : A \to B$ is onto, $\exists$ $x \in A$ such that $f(x) = y$. It follows that,

$$\begin{aligned} g(y) = z &\Rightarrow g(f(x)) = z \ [since \ \ y = f(x)] \\ &\Rightarrow f \circ g(x) = z \end{aligned}$$

Thus for any $z \in C$ $\exists$ $x \in A$ such that $f \circ g(x) = z$. This prove that the function $f \circ g : A \to C$ is onto.

We notice that $g^{-1} : C \to B$ and $f^{-1} : B \to A$. It follows that the domain of both the functions $g^{-1} \circ f^{-1}$ and $(f \circ g)^{-1}$ is the same set, namely

the set C. For any $z \in C$ we have,

$$\begin{aligned} g^{-1} \circ f^{-1}(z) &= f^{-1}(g^{-1}(z)) \\ &= f^{-1}(y) \ [where \ y \in B \ suchthat \ g(y) = z] \\ &= x \ where \ x \in A \ suchthat \ f(x) = y \end{aligned}$$

On the other hand, $z = g(y) = g(f(x)) = f \circ g(x)$. It follows that $(f \circ g)^{-1}(z) = x$. Thus we have,

$$(f \circ g)^{-1}(z) = g^{-1} \circ f^{-1}(z) \ \forall z \in C$$

This proves the required equality.

Remark: *Please note that we cant' comment on one-one and onto character of the functions f and g from one-one and onto character of the composite function $f \circ g$.*
Suppose that $f \circ g : A \to C$ is one-one and onto. For any $x_1, x_2 \in A$ we have,

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow g(f(x_1)) = g(f(x_2)) \ [since f(x_1), f(x_2) \in B(domain \ of \ g)] \\ &\Rightarrow f \circ g(x_1) = f \circ g(x_2) \\ &\Rightarrow x_1 = x_2 \ [since \ f \circ g \ is \ one - one] \end{aligned}$$

This shows that the function $f : A \to B$ is one-one. However we do not have any assurance in respect of the other one.

Proof of part 3: *Suppose that the function $f : A \to B$ is one-one and onto, so that $f^{-1} : B \to A$ exists. We are to show that the function f^{-1} is also one-one and onto. For any $y_1, y_2 \in B$ suppose that $f^{-1}(y_1) = x_1(say) \in A$ and $f^{-1}(y_2) = x_2(say) \in A$ such that $f^{-1}(y_1) = f^{-1}(y_2)$. We now have,*

$$\begin{aligned} f^{-1}(y_1) = f^{-1}(y_2) &\Rightarrow x_1 = x_2 \\ &\Rightarrow f(x_1) = f(x_2) \ [For \ uniqueness \ of \ image \ under \ a \ function] \\ &\Rightarrow y_1 = y_2 \ [Since \ f^{-1}(y_i) = x_i \Rightarrow f(x_i) = y_i \ for \ i = 1, 2] \end{aligned}$$

This shows that the function $f^{-1} : B \to A$ is one-one.

We note that for any $x \in A$, $f(x) = y(say) \in B$ which means that $f^{-1}(y) = x$. Thus for any $x \in A \ \ \exists \ y \in B$ such that $f^{-1}(y) = x$, as a consequence of which we can conclude that the function $f^{-1} : B \to A$ is onto.

It is clear that the domain of both the functions f and $(f^{-1})^{-1}$ is the same set, namely the set A. For any $x \in A$ we have,

$$\begin{aligned}(f^{-1})^{-1}(x) = y &\Rightarrow f^{-1}(y) = x \\ &\Rightarrow y = f(x) \\ &\Rightarrow (f^{-1})^{-1}(x) = f(x)\end{aligned}$$

It follows that,

$$(f^{-1})^{-1}(x) = f(x) \ \forall x \in A \Rightarrow (f^{-1})^{-1} = f$$

We are assured in respect of the existence of the function $f^{-1} : A \Rightarrow A$, as because the information in respect of the bijective character of the function $f : A \Rightarrow A$ is available at our hand. Here we note that the domains of both the functions $f \circ f^{-1}$ and $f^{-1} \circ f$ are same, namely the set A. Now for any $x \in A$ we have,

$$\begin{aligned}&f \circ f^{-1}(x) = f^{-1}(f(x)) = f^{-1}(y) \ \text{ where } \ f(x) = y \\ &\Rightarrow f \circ f^{-1}(x) = x = I(x) \ \forall x \in A\end{aligned}$$

Similarly it can be seen that

$$f^{-1} \circ f(x) = I(x) \ \forall x \in A$$

It follows that

$$f \circ f^{-1}(x) = f^{-1} \circ f(x) = I(x) \ \forall x \in A \Rightarrow f \circ f^{-1} = f^{-1} \circ f = I$$

Proof of part 4: *If we assume that the function $f : A \to B$ is one-one and onto then the required result follows with $g = f^{-1}$ (Prove!).*
Suppose that $f : A \Rightarrow B$ and $g : B \Rightarrow A$ are functions such that,

$$f \circ g = g \circ f = I \tag{1.4}$$

where I be the identity function on the set A. For any $x_1, x_2 \in A$ we have,

$$\begin{aligned}f(x_1) = f(x_2) &\Rightarrow g(f(x_1)) = g(f(x_2)) && [\text{Since } f(x_1), f(x_2) \in B \ (\text{Domain of } g)] \\ &\Rightarrow f \circ g(x_1) = f \circ g(x_2) \\ &\Rightarrow I(x_1) = I(x_2) && [\text{Using } (1)] \\ &\Rightarrow x_1 = x_2 && [\text{Since } I \text{ is the identity function on the set } A]\end{aligned}$$

It follows that the function $f : A \to B$ is one-one.
For any $y \in B$ it is clear that $g(y) = x(say) \in A$ such that,

$$\begin{aligned}f(g(y)) = f(x) &\Rightarrow g \circ f(y) = f(x) \\ &\Rightarrow I(y) = f(x) && [\text{since } g \circ f = I] \\ &\Rightarrow f(x) = y\end{aligned}$$

Thus for any $y \in B$ $\exists$ $x \in A$ such that $f(x) = y$, as a result we can conclude that the function $f : A \to B$ is onto.
This complete the proof of the required result.

At this point we prefer to consider the collection of all the one-one and onto functions (bijections) defined on a set X what we denote by $A(X)$. To be honest we are interested to consider this set because of its beautiful mathematical structure under the composition of functions. Thus for a non-empty set X we define,

$$A(X) = \{f \mid f \ \ f is\ a\ bijection\ on\ X\}$$

Suppose that $X = \{x_1, x_2, x_3\}$ and $\alpha \in A(X)$ such that $\alpha(x_1) = x_2, \alpha(x_2) = x_3$ and $\alpha(x_3) = x_1$ then we would like to use a special notation for α by,

$$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$$

Here we place the image of each element of X just below of it in the list as displayed under the function α. However some Algebraist prefer to use another more simple notation like $\alpha = (x_1, x_2, x_3)$ wherein we consider the image of each element of X is the next one in the list as displayed under the function α. and the image of the last element in the list is the first one. In this form of notation the missing elements are understood to be image of itself under α. With the results what we have already established in this section one can readily put forward his or her signature on the proof of the following result.

Theorem 5. *If $\alpha, \beta, \gamma \in A(X)$ then*
1. $\alpha \circ \beta \in A(X)$ ie. $A(X)$ is closed with respect to the binary operation $\circ$.
2. $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ ie. the associativity hold in $A(X)$ under $\circ$.
3. There exists an element I(the identity function) $\in A(X)$ such that

$$\alpha \circ I = I \circ \alpha = \alpha.$$

4. There exists an element $\alpha^{-1} \in A(X)$ such that $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = I$.

One of the natural question is that can we enjoy the commutative environment in $A(X)$ under the binary operation within our consideration. Of-course yes provided the number of elements in the set is at most two. However the answer to this question is no if the number of elements in the set X more than two. For instance let us consider the set $X = \{x_1, x_2, x_3, \cdots\}$ and consider

the elements $\alpha = (x_1, x_2, x_3)$ *and* $\beta = (x_2, x_3)$ *in* $A(X)$. *Please note that according to our notation,*

$\alpha(x_1) = x_2, \alpha(x_2) = x_3, \alpha(x_3) = x_1$ *and* $\alpha(x) = x$ *for any other elements in* X

and

$$\beta(x_2) = x_3, \beta(x_3) = x_2 \text{ and } \alpha(x) = x \text{ for any other elements in } X$$

Now from the definition of composition of functions we have,

$$\alpha \circ \beta(x) = \beta(\alpha(x)) \ \forall x \in X$$

It follows that $\alpha \circ \beta(x_1) = \beta(\alpha(x_1)) = \beta(x_2) = x_3$; $\alpha \circ \beta(x_2) = \beta(\alpha(x_2)) = \beta(x_3) = x_2$; $\alpha \circ \beta(x_3) = \beta(\alpha(x_3)) = \beta(x_1) = x_1$. *Thus we can write* $\alpha \circ \beta = (x_1, x_3)$.
On the other hand $\beta \circ \alpha(x_1) = \alpha(\beta(x_1)) = \alpha(x_1) = x_2$; $\beta \circ \alpha(x_2) = \alpha(\beta(x_2)) = \alpha(x_3) = x_1$; $\beta \circ \alpha(x_3) = \alpha(\beta(x_3)) = \alpha(x_2) = x_3$. *Thus we can write* $\beta \circ \alpha = (x_1, x_2)$.
It follows that

$$\alpha \circ \beta \neq \beta \circ \alpha$$

1.4 Well Ordering principle:

We believe that this is the proper time and place to introduce two very important but basic principles what we call well ordering principle and the principle of Mathematical induction. What we notice from our experience that there are some people who tries and rather does to use the mathematical induction to prove ***well ordering principle*** *to establish mathematical induction. However we are not interested to proceed in this direction, rather we shall try to establish the well ordering principle to establish mathematical induction.*
Well ordering principle*: Every non-empty subset of the set of natural number* $\mathbb{N}$*(equivalently the set of positive integers) has a minimal (least or smallest) element i.e if* $S(\neq \phi) \subseteq \mathbb{N}$ *then there exists an element* $m \in S$ *s.t*

$$m \leq s, \quad \forall s \in S$$

Proof. Suppose that S is a non empty subset of $\mathbb{N}$. As S is non empty there exists at least on $k \in S$. If we consider the set T define by,

$$T = \{s \in S \colon s \leq k\}$$

It follows that $T \subseteq \{1, 2, 3, \ldots, k\}$, as a result of which T is a finite subsetof $\mathbb{N}$ and consequently T has a minimal element m(say). Then for an arbitrary element $s \in S$, we consider the following two cases:
Case-I: If $s \leq k$ then $s \in T$ and since m is the minimal element of T, it follows that $m \leq S$
Case-II: If $s \geq k$ and since $m \leq k \leq s$ therefore $m \leq s$.
It follows that $m \leq s$ for every $s \in S$ and consequently m is the minimal element of the set S. □

Mathematical induction(First form): *If S is a subset of $\mathbb{N}$ such that,*

$$(a)\ 1 \in S$$
$$\text{and } (b)\ k+1 \in S, \text{ whenever } k \in S$$

then $S = \mathbb{N}$

Proof. Here we suppose that S is a subset of $\mathbb{N}$ which satisfies both the conditions.We have to show that $S = \mathbb{N}$.
If possible let us suppose that $S \neq \mathbb{N}$ i.e S is a proper subset of $\mathbb{N}$. It follows that $\mathbb{N} - S = S^c$[considering $\mathbb{N}$ as our universal set] is a non empty subset of $\mathbb{N}$.
By well ordering principle S^c has a minimal element m(say). we observe that $m \in S^c$ and consequently $m \notin S$.
Furthermore m is the minimal element of S^c means $(m-1) \notin S^c$ and so $(m-1) \in S$. By the given condition S,

$$(m-1) + 1 \in S \quad [\because k+1 \in S, whenever \ \ k \in S]$$
$$\Rightarrow m \in S$$

But this contradicts the given fact that $m \notin S$.
This contradiction leads us into the conclusion that $S = \mathbb{N}$. □

Mathematical induction (Second form): *Suppose that n_0 is a fixed but arbitrarly element of $\mathbb{N}$ and $P(n)$ is a property such that*
(a) $P(n_0)$ is true
(b) $P(k+1)$ is true whenever $P(k)$ is true.
Then the property $P(n)$ is true for every $n \geq n_0$.

Proof. Suppose that,

$$S = \mathbb{N} - \{1, 2. \ldots, n_0 - 1\}$$

In order to prove our desired result it is enough to show that the statement $P(n)$ is true $\forall n \in \mathbb{N}$.

On the contrary, let us assume that the property $P(n)$ is not true for some $m \in S$. It follows that $m \geq n_0$.As $P(n_0)$ is true,we must have $m > n_0$. But then there exists some $k \in \mathbb{N}$ such that $m = n_0 + k$ and consequently $P(m-k) = P(n_0)$ is true. But then $P(m-k+1)$ is true. Again by the given condition $P(m-k+2)$ is true. Continuing this process in the kth step we ultimately obtain that $P(m-k+k) = P(m)$ is true which contradicts our initial assumption that P(m) is not true. This contradicts leads us into the conclusion that $P(n)$ is true foe every $n \geq n_0$. This completes the proof of required result.

Remark: A good number of Mathematics followers consider the above form of Mathematical induction as redundent one as because taking $n_0 = 1$, the second form of induction immediately transform into the first form of Mathematical induction. In fact this is not true in general. For instance the inequality $2^n \geq 2n + 1$ is not true for $n = 1 or 2$. If we consider $n_0 = 3$ then it can be seen that this inequality will hold for every $m \geq n_0$.

Here we observe that, $2^3 \geq 2 \times 3 + 1 = 7$. Let us assume that this inequality hold good for $m = k$

i.e

$$\begin{aligned}
& 2^k > 2k + 1 \\
\Rightarrow\ & 2^{(k+1)} \geq 4k + 2 = 2k + 2(k+1) \\
\Rightarrow\ & 2^t \geq 2(t-1) + 2t \quad [considering\, t = k+1] \\
=\ & 2t + (2t - 2) \\
>\ & 2t + 1 \quad [\because 2t - 2 > 1\ for\ t = 4, 5, ...]
\end{aligned}$$

Thus the inequality hold good for $(k+1)$ whenever it hold good for k. Thus by Mathematical induction (second form) the inequality hold good for any $m \geq n_0$ i.e

$$2^m > 2m + 1, \quad \forall m \geq n_0 (= 3)$$

□

Mathematical induction (Third form): *Suppose S is a subset of $\mathbb{N}$ such that*

$$\begin{aligned}
& (a) 1 \in S \\
and \quad & (b) K + 1 \in S\ whenever \{1, 2, ...k\} \subseteq S,\ \ forevery\ k \in \mathbb{N}
\end{aligned}$$

Then $S = \mathbb{N}$.

Proof. On the contrary suppose that $S \neq \mathbb{N}$ so that $\mathbb{N} - S = S^c$ (considering $\mathbb{N}$ as the universal set) is non empty subset of $\mathbb{N}$. Thus by well ordering principle S^c has minimal element m(say). It follows that $m \in S^c$ or equivalently $m \notin S$ and $m \leq k$, $\forall k \in S^c$.
Since m is the minimal element of S^c, for any $k \in \mathbb{N}$

$$\begin{aligned} & m - r \notin S^c, \quad \forall r = 1, 2, ...k \\ & \Rightarrow m - r \in S, \quad \forall r = 1, 2, ...r \\ & \Rightarrow \{m-1, m-2, ...m-k\} \subseteq S \end{aligned}$$

According to our hypothesis $(m - k + 1) \in S$ and consequently

$$\{m-1, m-2, ...m-k, m-k+1\} \subseteq S$$

But then $m - k + 2 \in S$ and as a consequence

$$\{m-1, m-2, ...m-k, m-k+1, m-k+2\} \subseteq S$$

Continuing the same process ultimately at the k^{th} step we shall get
$m - k + k = m \in S$
But this contradicts the given fact that $m \notin S$
This contradiction leads us into the conclusion that $S = \mathbb{N}$
This completes the proof of the result. □

At this point we would like to introduce the concept of equivalence relation between two sets, which ultimately lead us to the concept of countable and uncountable sets.

Definition 18. *Two set A and B are said to be equivalent if there exists a bijection f between the sets and we denote it by $A \sim B$.*
$\therefore A \sim B \iff \exists f : A \to B$ which is a bijection.
NB : It can be seen that $\sim$ is an equivalence relation in the collection of all sets.

Definition 19. *A set S is said to be a finite set if for some $n \in \mathbb{N}$*
$S \sim \{1, 2, 3...n\}$ In such a case the number n is defined to be the cardenility of the set S.

Definition 20. *A set is said to be an infinite set if it is not finite.*

Definition 21. *An infinite set S is said to be a denumerable set if it is equivalent to the set of positive integers $\mathbb{N}$ i.e $\exists$ a bijection $f : S \to \mathbb{N}$.*

Definition 22. *A set S is said to be countable if it is either finite or it is denumerable.*

Definition 23. *A set is said to be countable if it is either finite or it is denumerable.*

Definition 24. *A set is S is said to be uncountable if it is not countable .*
Examples: (a) The set $E = 2n : n \in \mathbb{N}$ of all even natural numbers is a countable(denumerable) set. This is because the function $f : \mathbb{N} \to \mathbb{E}$ defined by $f(n) = 2n$, $\forall n \in \mathbb{N}$ or the function $g : \mathbb{E} \to \mathbb{N}$ define by $g(m) = \frac{m}{2}$, $\forall m \in \mathbb{E}$ are bijections.
(b) The set $O = \{2n - 1 : n \in \mathbb{N}\}$ of all odd natural numbers is a countable(denumerable) set. This is because $f : \mathbb{N} \to O$ define by $f(n) = 2n - 1$, $\forall n \in \mathbb{N}$ or $g : O \to \mathbb{N}$ define by $g(m) = \frac{m+1}{2}$, $\forall m \in O$ are bijections.
(c) The set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$ is denumerable.
Here we define a function $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(x) = \begin{cases} 2m, & \text{if } m > 0 \\ 1 - 2m, & \text{if } m \leq 0 \end{cases}$$

For any $m.m' \in \mathbb{Z}$ if $f(m) = f(m')$ then either both m, m' are positive or both are negative. In case $m, m' > 0$,

$$\begin{aligned} f(m) = f(m') &\Rightarrow 2m = 2m' \\ &\Rightarrow m = m' \end{aligned}$$

In case $m, m' \leq 0$,

$$\begin{aligned} f(m) = f(m') &\Rightarrow 1 - 2m = 1 - 2m' \\ &\Rightarrow m = m' \end{aligned}$$

It follows that $f : \mathbb{Z} \to \mathbb{N}$ is one one.
Suppose that $n \in \mathbb{N}$
If $n = 1$ then $0 \in \mathbb{Z}$ such that $f(0) = 1 - 2.0 = 1$
In case $n \geq 2$ and n is even then $m = \frac{n}{2} (> 0) \in \mathbb{Z}$. But then,

$$f(m) = 2m = 2.\tfrac{n}{2} = n$$

In case $n \geq 3$ and n is odd then $n = 1 - 2m$ where $m = -1, -2, -3, \ldots$
From the definition of f we have

$$f(m) = 1 - 2m = 1 - 2.\frac{(1-n)}{2} = n$$

It follows that the function f is onto.
Hence $f : \mathbb{Z} \to \mathbb{N}$ is a bijection and consequently $\mathbb{Z} \sim \mathbb{N}$ and hence $\mathbb{Z}$ is denumerable and hence countable.

Theorem 6. *The Cartesian product $\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. Let us consider the function $\psi : \mathbb{N} \longrightarrow \mathbb{N}$defined by,

$$\psi(k) = \frac{k(k+1)}{2} \qquad \forall k \in \mathbb{N}$$

From the definition of the function ψ one can note two important properties of it. First, for any $k \in \mathbb{N}$,

$$\psi(k) = \psi(k-1) + k$$

Secondly for any $k_1, k_2 \in \mathbb{N}$,

$$k_1 < k_2 \Rightarrow \psi(k_1) < \psi()k_2$$

We now consider a function $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ define by,

$$f(m,n) = \psi(m+n-2) + m \qquad \forall (m,n) \in \mathbb{N} \times \mathbb{N}$$

We will be through if we can prove that the function f as defined above is a bijection.
Suppose that $(m,n), (m',n') \in \mathbb{N} \times \mathbb{N}$ such that $(m,n) \neq (m',n')$. Then either $m+n \neq m'+n'$ or $m+n = m'+n'$ but $m \neq m'$.
In case $m+n \neq m'+n'$, without loss of generality we can assume that,

$$\begin{aligned} m+n < m'+n' &\Rightarrow m+n-2 < m'+n'-2 \\ &\Rightarrow \psi(m+n-2) < \psi(m'+n'-2) \qquad [\because \psi \ \textit{is monotone}] \\ &\Rightarrow \psi(m+n-2) + m < \psi(m'+n'-2) + m' \\ &\Rightarrow f(m,n) < f(m',n') \\ &\Rightarrow f(m,n) \neq f(m',n') \end{aligned}$$

In case $m+n = m'+n'$ but $m \neq m'$. We can assume that $m < m'$.
Now,

$$\begin{aligned} m+n = m'+n' &\Rightarrow \psi(m+n-2) = \psi(m'+n'-2) \\ &\Rightarrow \psi(m+n-2) + m < \psi(m'+n'-2) + m' \\ &\Rightarrow f(m,n) < f(m',n') \\ &\Rightarrow f(m,n) \neq f(m',n') \end{aligned}$$

It follows that the function $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ is one-one.
Let $p \in \mathbb{N}$. For $p \in \mathbb{N}$ we consider the set E_p define by,

$$E_p = \{k \in \mathbb{N} \mid p \leq \psi(k)\}$$

Since $p \in \mathbb{N}$ and $p \leq \psi(p)$ therefore $p \in E_p$ and hence E_p is a nonempty subset of $\mathbb{N}$. Thus by well ordering principle E_p has a least element k_p (say). It follows that $k_p \in E_p$ and $k_p - 1 \notin E_p$. Now,

$$\begin{aligned} k_p - 1 \notin E_p \text{ and } k_p \in E_p &\Rightarrow \psi(k_p - 1) < p \text{ and } p \leq \psi(k_p) \\ &\Rightarrow \psi(k_p - 1) < p \leq \psi(k_p - 1) + k_p \\ &\Rightarrow 1 \leq p - \psi(k_p - 1) \leq k_p \\ &\Rightarrow 1 \leq m_p \leq k_p \text{ where } m_p = p - \psi(k_p - 1) \\ &\Rightarrow 1 \leq k_p - m_p + 1 \leq k_p \\ &\Rightarrow 1 \leq n_p \leq k_p \text{ where } n_p = k_p - m_p + 1 \end{aligned}$$

It follows that,

$$\begin{aligned} f(m_p, n_p) &= \psi(m_p + n_p - 2) + m_p \\ &= \psi(k_p - 1) + m_p \\ &= p \end{aligned}$$

It follows that the function $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ is onto.
Hence the function $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ is a bijection.This complete the proof. □

Corollary 1. *Countable union of countable sets is countable*

Proof. Suppose that $\sigma = \{A_1, A_2, \cdots\}$ is a countable collection of countable sets and $A = \cup_{i=1}^{\infty} A_i$. We are to show that A is countable.
Suppose,

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13} \cdots\} \\ A_2 &= \{a_{21}, a_{22}, a_{23} \cdots\} \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \cdots\} \\ &\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

Let us define a function $f : A \to \mathbb{N} \times \mathbb{N}$ defined by,

$$f(a_{ij}) = (i, j) \qquad \forall a_{ij} \in A$$

It can be readily verified that $f : A \to \mathbb{N} \times \mathbb{N}$ so defined is bijection and hence A is countable. □

Corollary 2. *The Cartesian product of any two countable sets is a countable set.*

Proof. Suppose that A and B be any two countable sets and suppose that,

$$\begin{aligned} A &= \{a_1, a_2, a_3, \cdots\} \\ B &= \{b_1, b_2, b_3, \cdots\} \\ \therefore A \times B &= \{(a_i, b_j) \mid i, j \in \mathbb{N}\} \end{aligned}$$

If we consider a function $f : A \times B \to \mathbb{N} \times \mathbb{N}$ defined by,

$$f(a_i, b_j) = (i, j)$$

then it is matter of simple verification that the function $f : A \times B \to \mathbb{N} \times \mathbb{N}$ is a bijection and consequently $A \times B$ is countable being equivalent to a countable set $\mathbb{N} \times \mathbb{N}$. □

Corollary 3. *The set of rationals $\mathbb{Q}$ is countable.*

Proof. Let us consider the countable sets $A_1, A_2, A_3, \cdots$ defined as,

$$\begin{aligned} A_1 &= \left\{\frac{0}{1}, \frac{-1}{1}, \frac{1}{1}, \frac{-2}{1}, \frac{2}{1}, \frac{-3}{1}, \frac{3}{1}, \cdots\right\} \\ A_2 &= \left\{\frac{0}{2}, \frac{-1}{2}, \frac{1}{2}, \frac{-2}{2}, \frac{2}{2}, \frac{-3}{2}, \frac{3}{2} \cdots\right\} \\ A_3 &= \left\{\frac{0}{3}, \frac{-1}{3}, \frac{1}{3}, \frac{-2}{3}, \frac{2}{3}, \frac{-3}{3}, \frac{3}{3} \cdots\right\} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

It is clear that,

$$\mathbb{Q} = \cup_{i=1}^{\infty} A_i$$

Each A_i is denumerable being equivalent to $\mathbb{Z}$ and hence $\mathbb{Q}$ is denumerable and hence countable being equal to countable union of countable sets. □

Alternative:

Proof. Let us consider a function $f_n : \mathbb{N} \to A_n$ defined by,

$$f_n(x) = \begin{cases} \frac{-m}{2n}, & \text{if } m \text{ is even} \\ \frac{m-1}{2n}, & \text{if } m \text{ is odd} \end{cases}$$

For $m, m' \in \mathbb{N}$ suppose that $f_n(m) = f_n(m')$. It follows that either both m, m' are even or odd.
In case both m, m' are even,

$$f_n(m) = f_n(m') \Rightarrow \frac{-m}{2n} = \frac{-m'}{2n} \Rightarrow m = m'$$

In case both m, m' are odd,

$$f_n(m) = f_n(m') \Rightarrow \frac{m-1}{2n} = \frac{m'-1}{2n} \Rightarrow m = m'$$

It follows that the function $f_n : \mathbb{N} \to A_n$ is one one.
Suppose that $\frac{m}{n} \in A_n$. If $\frac{m}{n} = 0$ then $f_n(1) = \frac{1-1}{n} = 0$.
Let us assume that $\frac{m}{n} \neq 0$
In case m is even, $-2m \in \mathbb{N}$ such that $f_n(-2m) = \frac{-(-2m)}{2n} = \frac{m}{n}$
In case m is odd, $2m + 1 \in \mathbb{N}$ such that $f_n(2m + 1) = \frac{2m+1-1}{2n} = \frac{m}{n}$
It follows that $f_n : \mathbb{N} \to A_n$ is onto and hence it is a bijection and consequently A_n is countable $\forall n = 1, 2, \ldots$. It follows that $\mathbb{Q}$ is countable being equal to the union of a countable collection of countable sets. □

Theorem 7. *Every infinite set has a denumerable subset.*

Proof. Let A be an infinite set and $a_1 \in A$. Since A is infinite $A \neq \{a_1\}$ and therefore there exists $a_2 \in A \setminus \{a_1\}$.
Since A is infinite $A \neq \{a_1, a_2\}$ and therefore there exists $a_3 \in A \setminus \{a_1, a_2\}$.
Since A is infinite $A \neq \{a_1, a_2, a_3\}$ and therefore there exists $a_4 \in A \setminus \{a_1, a_2, a_3\}$.
We now consider the set $B = \{a_1, a_2, a_3, \cdots\}$ which is clearly a denumerable subset of the set A.
This complete the proof. □

Theorem 8. *Every infinite set is equivalent to a proper subset of it.*

Proof. Let A be an infinite set.Then A must have an denumerable subset C(say) and let $C = \{a_1, a_2, a_3, \cdots\}$.
Let D be a subset of the set A given by $D = A \setminus \{a_1\}$.
Let us consider the set B given by,

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

Clearly $a_1 \notin B$ but $a_1 \in A$ for which one can infer that B is a proper subset of the set A.
We now consider a function $f : A \longrightarrow B$ define by,

$$\begin{aligned} f(x) &= x && \forall x \in A \setminus C \\ f(a_i) &= a_{i+1} && \forall a_i \in C \end{aligned}$$

For any $x, y \in A \setminus C$ it is clear that $f(x) = f(y) \Rightarrow x = y$. On the other hand, for any $a_i, a_j \in C$ we have,

$f(a_i) = f(a_j) \Rightarrow a_{i+1} = a_{j+1} \Rightarrow i+1 = j+1 \Rightarrow a_i = a_j$.
It follows that the function $f : A \longrightarrow B$ is one-one.
For any $y \in B$ implise that either $y \in A \setminus C$ or $y \in D$.
In case $y \in A \setminus C$ there exists $y \in A$ such that $f(y) = y$.
In case $y \in D$ we must have $y = a_i$ where $i \geq 2$. Then there exists
$a_{i-1} \in C \subseteq A$ such that $f(a_{i-1}) = a_i = y$.
It follows that the function $f : A \longrightarrow B$ is a bijection and consequently A is equivalent to B which is a proper subset of the set A.
This complete the proof. □

Theorem 9. *The close interval* $[0, 1]$ *is uncountable.*

Proof. On the contray let us assume that the close interval $[0, 1]$ is countable and $[0, 1] = \{a_1, a_2, a_3 \cdots\}$.
It follows that,

$$\begin{aligned} a_1 &= 0.a_{11}a_{12}a_{13}\cdots \\ a_2 &= 0.a_{21}a_{22}a_{23}\cdots \\ a_3 &= 0.a_{31}a_{32}a_{33}\cdots \\ &\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

Let us consider $b = 0.b_1b_2b_3\cdots \in [0, 1]$ in such a way that,

$$\begin{aligned} &b_1 = 1 \ a_{11} \neq 1 \ and \ b_1 = 2 \ if \ a_{11} = 1 \ so \ that \ b_1 \neq a_{11}. \\ &b_2 = 1 \ a_{22} \neq 1 \ and \ b_2 = 2 \ if \ a_{22} = 1 \ so \ that \ b_2 \neq a_{22}. \\ &b_3 = 1 \ a_{33} \neq 1 \ and \ b_3 = 2 \ if \ a_{33} = 1 \ so \ that \ b_3 \neq a_{33}. \end{aligned}$$

Continuing this one can easily infer that $b \neq a_i \ \forall i = 1, 2, 3, \cdots$.
It follows that $b \in [0, 1]$ whereas $b]notin\{a_1, a_2, a_3, \cdots\}$.
This shows that the elements in the close interval $[0, 1]$ can not be listed out and hence the close interval $[0, 1]$ is uncountable. □

Corollary 4. *The set of real numbers* $\mathbb{R}$ *is uncountable.*

Proof. Since $[0, 1] \subset \mathbb{R}$ and since $[0, 1]$ is uncountable therefore $\mathbb{R}$ is uncountable. □

Corollary 5. *The set of irrationals* $\mathbb{Q}^c$ *is uncountable.*

Proof. If possible suppose that the set of irrationals $\mathbb{Q}^c$ is countable. Since the set of rationals $\mathbb{Q}$ is countable and $\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c$ therefore according to our assumption $\mathbb{R}$ is countable being equal to the union of two countable sets. This contradicts the fact that $\mathbb{R}$ is uncountable. This contradiction leads us to the conclusion that the set of irrationals $\mathbb{Q}^c$ is uncountable. □