Chapter four Functions:

Definition: A ***Function*** (mapping) from A to B is the order triple (f, A, B) where A and B are two nonempty sets and $\boldsymbol{f}$ is a subset of $A \times B$ satisfying the following conditions:

1) $\forall\, x \in A, \exists\, y \in B$ such that $(x, y) \in f$.

2) If (x, y_1) and $(x, y_2) \in f$, then $y_1 = y_2$.

The set A is called the ***Domain of*** f and the set B is called the ***Co-domain of*** f.

Example: let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ and

$\boldsymbol{f_1} = \{ (1, a), (2, b), (3, c)\}$, $\boldsymbol{f_2} = \{ (1, a), (1, b), (2, c), (3, c), (4, c)\}$

$\boldsymbol{f_3} = \{ (1, a), (2, a), (3, a), (4, a)\}$, $\boldsymbol{f_4} = \{ (2, b), (2, c)\}$.

f_1 is not function from A to B since $4 \in A$ but $\nexists y \in B$ such that $(4, y) \in f_1$.

f_2 is not function from A to B since $(1, a)$ and $(1, b) \in f_2$ but $a \neq b$.

f_3 is a function from A to B.

f_4 is not function from A to B since $1, 3, 4 \in A$ but $\nexists y \in B$ such that $(1, y)(3, y), (4, y) \in f_4$.

Definition: Let f be a function from A to B then Range of function f is the set of all elements b∈B, such that (a, b) ∈ f for some a∈A, that is Range f ={b∈B ; (a, b) ∈ f for some a∈A}and Range of function f is denoted by Ran f.

Remark:

1. It is customary to write the function (f, A, B) as $f : A \rightarrow B$.
2. If $(x, y) \in f$, then we usually write $y = f(x)$, and call y the image of x under$f$.
3. In the function $f : A \rightarrow B$, x is called independent variable and y is is called dependent variable.
4. The range of f is always a subset of the codomain.
5. $f(x)$ is an element of the codomain.

Example: Let A={a, b, c} and B={1, 2, 3, 4} consider the following functions:

f_1= { (a, 2), (b, 3), (c, 3)} , f_2= { (a, 2), (b, 3), (c, 1)}, f_1(a)=2, f_1(b)=3, f_1(c)=3 and f_2(a)=2, f_2(b)=3, f_2(c)=1. Then Ran f_1= {2, 3} and Ran f_2= {1, 2, 3}.

Definition: Let f: A→B be a function. Then f is called ***injective(one-to-one)function***

If $f(x_1)= f(x_2)$, then $x_1=x_2$ $\forall x_1, x_2 \in A$; or if $x_1 \neq x_2$,then $f(x_1) \neq f(x_2)$ $\forall x_1, x_2 \in A$;

Definition:

A function $f: A \to B$ is called ***Surjective (on to) function*** if $\forall y \in B, \exists x \in A$, such that $f(x) = \boldsymbol{y}$**.**

Remark:

A function f from A to B is surjective if Range of f is equal to codomain(B).

Definition:

A function f: A→B is called Bijective ***(one to one correspondence) function*** if f is injective(one-to-one) and surjective (on to) function from A to B.

Example:

Let A= {1, 2, 3, 4} and B= {a, b, c, d} consider the following functions:

$f_1 = \{(1,a),(2,a),(3,b),(4,c)\}$ and $f_2 = \{(1,a),(2,b),(3,c),(4,d)\}$

f_1 is not injective function since $f_1(1) = f_1(2) =$ a but 1≠2;

f_1 is not surjective function since d $\in B, but \nexists x \in A; f(x) =$d

So that the function f_1 is not bijective function.

f_2 is injective function because if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$ $\forall x_1, x_2 \in A$.

f_2 is surjective function. So that the function f_2 is bijective function.

Example: Let $f: \mathbb{R} \to \mathbb{R}$ be a function defined by $f(x) = |x| = \begin{cases} x & if\ x \geq 0 \\ -x & if\ x < 0 \end{cases}$

f is not surjective function since if y$\in \mathbb{R}^-$, $but \nexists x \in R \ni f(x) = y$.

f is not injective function since $f(-1) = f(1) = 1$ but $1 \neq -1$.

Definition:

A function f from A to B ($f: A \to B$) is called ***invertible function*** iff f^{-1} from B to A is a function.

Remark: A function $f: A \to B$ is ***invertible*** *iff*

1. $(x, y) \in f$ if and only if $(y, x) \in f^{-1}$
2. $f(x) = y$ if and only if $f^{-1}(y) = x$.

Example: Let A={1, 2, 3} and B={a, b, c} consider the following functions:

$f_1 = \{(1,a),(2,b),(3,b)\}$ is not invertible since $f_1^{-1} = \{(a,1),(b,2),(b,3)\}$ is not function.

$f_2 = \{(1,b),(2,a),(3,c)\}$ is invertible since $f_2^{-1} = \{(b,1),(a,2),(c,3)\}$ is invertible.

Theorem: A function f: A→B is invertible if and only if f is bijective function.

Proof: Suppose that f is invertible function to prove f is bijective function.

Injective: Let $f(x_1) = f(x_2) = y$ where x_1 and x_2 belongs to A. Then $f(x_1) = y$ and $f(x_2) = y$

Then $(x_1, y) \in f$ and $(x_2, y) \in f$. Then $(y, x_1), (y, x_2) \in f^{-1}$ [why?]Then $x_1 = x_2$ [since f^{-1} is a function from B to A]. Hence, f is injective (one to one) function.

Surjective: Let y ∈B, since f^{-1}: B→A is a function (f is invertable)

$\rightarrow \exists$ x ∈ A, $\ni f^{-1}(y) = x \rightarrow (y, x) \in f^{-1}$ then $(x, y) \in f$ [by the definition of inverse relation]

$\rightarrow f(x) = y$, therefore, $\forall\, y \in B, \exists x \in A, \ni f(x) = y$. Hence f is surjective function.

Therefore, f is bijective function.

Conversely: Suppose that f is a bijective function to prove f is invertible.

That is we have to prove f^{-1}: B→A satisfy the following two conditions

1. $\forall\, y \in B, \exists\, x \in A$ such that $(y, x) \in f^{-1}$
2. If (y, x_1) and $(y, x_2) \in f^{-1}$, then $x_1 = x_2$.

Let $y \in B$ then, $\exists x \in A$, such that $f(x) = y$ [since f is surjective function from A to B]

then $(x, y) \in f$, then $(y, x) \in f^{-1}$ [by the definition of inverse relation]

then $f^{-1}(y) = x$, therefore, $\forall y \in B, \exists x \in A$ such that $f^{-1}(y) = x$.

Let $(y, x_1), (y, x_2) \in f^{-1}$, then $(x_1, y), (x_2, y) \in f$ [by the definition of inverse relation]. Then $f(x_1) = y$ and $f(x_2) = y$, then $f(x_1) = f(x_2)$, then $x_1 = x_2$ [since f is injective function].

Thus f^{-1} is a function from B to A. Therefore, f^{-1} is an invertible function.

Theorem: Let $f: A \rightarrow B$, $g: B \rightarrow C$ and $gof: A \rightarrow C$, be functions. Then

1. If $f: A \rightarrow B$ and $g: B \rightarrow C$ are injective functions, then $gof: A \rightarrow C$ is injective function.
2. If $f: A \rightarrow B$ and $g: B \rightarrow C$ are surjective function, then $gof: A \rightarrow C$ is surjective function.
3. If $gof: A \rightarrow C$ is injective function, then $f: A \rightarrow B$ injective functions
4. If $gof: A \rightarrow C$ is surjective function , then $g: B \rightarrow C$ is surjective function

Proof (1): suppose that $f: A \rightarrow B$ and $g: B \rightarrow C$ are injective functions to prove $gof: A \rightarrow C$ is injective function. Let $(gof)(x_1) = (gof)(x_2)$, then $g(f(x_1)) = g(f(x_2))$, then $f(x_1) = f(x_2)$ [since g is injective function]. Then $x_1 = x_2$ [since f is injective function].

Therefore, $gof: A \rightarrow C$ is injective function.

Proof (2): Suppose that $f: A \to B$ and $g: B \to C$ are surjective functions to prove $gof: A \to C$ is surjective function. Let $z \in C$, then there exist $y \in B$, such that $g(y) = z$ [since g is surjective function].Then there exist $x \in A$, such that $f(x) = y$ [Since f is surjective function]

Since $g(y) = z$ and $f(x) = y$ then $g(f(x)) = (gof)(x) = z$, Thus, $\forall z \in c, \exists x \in A, \ni$ $(gof)(x) = z$. Therefore, $gof: A \to C$ is surjective function.

Proof (3): suppose that $gof: A \to C$ is an injective function to prove $f: A \to B$ is injective function. Let $f(x_1)= f(x_2)$ for some x_1, $x_1 \in A$. Then $g(f(x_1))= g(f(x_2))$ [since $f(x_1)$, $f(x_2) \in B$ and $g: B \to C$ is a function]. Then $(gof)(x_1)= (gof)(x_2)$, then $x_1=x_2$ [since $gof: A \to C$ is injective function]. Therefore, $f: A \to B$ is injective function.

Proof (4): Suppose that $gof: A \to C$ is surjective function to prove $g: B \to C$ is surjective function. Let $z \in C$, then $\exists x \in A$, such that $(gof)(x) = z$, then $g\big(f(x)\big) = z$. This means that $\forall z \in C, \exists f(x) \in B$, such that $g\big(f(x)\big) = z$. Therefore, g: B→C is surjective function.

Theorem:

Let $f: A \to B$ and $g: B \to A$ be two functions. Then

1. $f = g$ if and only if $f(x) = g(x) \; \forall \; x \in A$.
2. If $gof = I_A$, then f: A→B is injective function.
3. If $fog = I_B$, then f: A→B is surjective function.
4. If gof=I_A and fog=I_B then f: A→B and g: B→A are bijective function and $f=g^{-1}$.

Proof(1): Suppose that $f = g$ to prove $f(x) = g(x) \; \forall \; x \in A$.

let $f(x) = y, \leftrightarrow \; (x, y) \in f \; \leftrightarrow \; (x, y) \in g \; , \leftrightarrow \; g(x) = y$. Therefore, $f(x) = g(x) \; \forall \; x \in A$.

Conversely, suppose that $f(x) = g(x) \; \forall \; x \in$ A, we have to prove that $f = g$.

Let $(x, y) \in f \; \leftrightarrow \; f(x) = y \; \leftrightarrow \; g(x) = y$ [since $(x) = g(x) \; \forall$ x ∈ A] $\leftrightarrow (x, y) \in g$.

Therefore, $f = g$.

Proof(2): suppose that gof=I_A to prove f: A→B is injective function.

Let $f(x_1) = f(x_2)$ where x_1 and $x_2 \in A$, then $g\big(f\,(x_1)\big) = g\big(f\,(x_2)\big)$ [since $f(x_1)$and $f(x_2) \in B$] Then $gof\,(x_1) = gof\,(x_2)$, then $I_A(x_1) = I_A(x_2)$ [since $gof = I_A$]

Then $x_1 = x_2$[by the definition of identity function]. Therefore, f: A→B is injective function.

Proof(3): Suppose that fog=I_B to prove f: A→B is surjective function.

Let y∈ B, $\exists x \in A; g(y) = x$ [since $y \in B$ and g: B → A is a functions.]

Then $f(g(y)) = f(x)$ [since g(y), x∈ A and f: A→B is a function]

Then $fog\ (y) = f(x)$, then $I_B(y) = f(x)$[since fog=I_B]

Then $y = f(x)$ [by def. of identity function]

This means that ∀ y∈ B, $\exists x \in A$ such that $f(x) = y$. Therefore, f: A→B is surjective function.

Theorem:

Let f: A→B be a function if f is invertible function, then $f^{-1}\ of = I_A$ and $fof^{-1} = I_B$

Proof: Let f: A→B be an invertible function, (f^{-1}: B → A is a function), we have to prove $f^{-1}\ of = I_A$ and $fof^{-1} = I_B$. Let (a, c)∈ $f^{-1}\ of$, then ∃ $b \in B, \ni (a, b) \in f$and $(b, c) \in f^{-1}$, then $(b, a) \in f^{-1}$ and$(\mathrm{b}, \mathrm{c}) \in \mathrm{f}^{-1}$ [by def.of f^{-1}], then $a = c$ [since f^{-1}: B → A is a function] th
$(a, c) \in \mathrm{I_A}$, therefore $f^{-1}\ of \subseteq \mathrm{I_A}$. To prove $\mathrm{I_A} \subseteq \mathrm{f}^{-1}$of (H.W.)

Chapter five

Cardinality of Sets

We say that two sets are **equivalent** (denoted by A ~ B) iff there exists a bijection f: A $\rightarrow$ B.

It is not hard to check that ~ is an equivalence relation on the class of all sets:

(1) **A ~ A** for all sets A. (I_A: A $\rightarrow$ A is a bijection for all sets A)

(2) If **A ~ B** then **B ~ A**. (If f: A $\rightarrow$ B is a bijection, f^{-1}: B $\rightarrow$ A is also)

(3) If **A ~ B** and **B ~ C** then **A ~ C**. (If f: A $\rightarrow$ B is a bijection and g: B $\rightarrow$ C is a bijection, then g ∘ f: A $\rightarrow$ C is a bijection).

The equivalence classes under this relation are called **cardinalities.**

Example 1:

1. If $A = \{1,2,3,4,5\}$ and $B = \{4,8,12,16,20\}$ then there exists at least a bijective function f: A → B where $f(x) = 4x$. Then A ~ B.
2. If $C = \{2,3,4,\ldots\}$ since there exists at least a bijective function f: ℕ → C. where $f(x) = x$-1. Then ℕ ~ C.
3. If $D = [0,1] = \{x \in \mathbb{R}; 0 \leq x \leq 1\}$ and $E = [1,3] = \{x \in \mathbb{R}; 1 \leq x \leq 3\}$ then there exists at least a bijective function f: D → E where $f(x) = 2x + 1$. Then **D ~ E**.
4. ℝ ~ (0, ∞) Since there exists a bijective function $f: \mathbb{R} \to (0,\infty)$ where $f(x) = 2^x$.
5. $(0,1)$ ~ $(1,\infty)$ Since there exists a bijective function $f: (0,1) \to (1,\infty)$ where $f(x) = \frac{1}{x}$.

Example 2:

Consider three sets $A_1 = \left\{\frac{1}{n+1}; n \in \mathbb{N}\right\}$=$\{\frac{1}{2},\frac{1}{3},\ldots\}$, $B_1 = \left\{\frac{1}{n}; n \in \mathbb{N}\right\} = A_1 \cup \{1\} = \{1,\frac{1}{2},\frac{1}{3},\ldots\}$, $C_1 = A_1 \cup \{0\} = \{0,\frac{1}{2},\frac{1}{3},\ldots\}$ and $D_1 = A_1 \cup \{0,1\} = \{0,1,\frac{1}{2},\frac{1}{3},\ldots\}$.

1. $\mathbb{N} \sim \mathbf{A_1}$ since there exists at least a bijective function $f: \mathbb{N} \to A_1$ where $f(n) = \frac{1}{n+1}$.

2. $\mathbf{A_1} \sim \mathbf{B_1}$ since there exists at least a bijective function $f: A_1 \to B_1$ where $f(\frac{1}{n}) = \frac{1}{n+1}$.

3. $\mathbf{A_1 \sim C_1}$ since there exists a bijective function $f: A_1 \to C_1$ where

$$f(x)=\begin{cases} 0 & \text{if } x = \frac{1}{2} \\ \frac{1}{n+1} & \text{if } x = \frac{1}{n+2}, n \in \mathbb{N} \end{cases}.$$

4. $\mathbf{A_1 \sim D_1}$ since there exists a bijective function $f: A_1 \to D_1$ where

$$f(x)=\begin{cases} 0 & \text{if } x = \frac{1}{2} \\ 1 & \text{if } x = \frac{1}{3} \\ \frac{1}{n+1} & \text{if } x = \frac{1}{n+3}, n \in \mathbb{N} \end{cases}.$$

5. Since $\mathbb{N} \sim \mathbf{A_1}$, $\mathbf{A_1 \sim B_1}$, $\mathbf{A_1 \sim C_1}$ and $\mathbf{A_1 \sim D_1}$ then $\mathbb{N} \sim \mathbf{A_1 \sim B_1 \sim C_1 \sim D_1}$.

Remark: Let $A = A_1 \cup A_2 \cup \ldots \cup A_n$, $A_i \cap A_j = \emptyset$ if $i \neq j$ and $B = B_1 \cup B_2 \cup \ldots \cup B_n$, $B_i \cap B_j = \emptyset$. If $A_i \sim B_i$ for all $i \in \{1, 2, \ldots n\}$ then $A \sim B$.

Example 3:

1. If A=(0,1) then $A = A_1 \cup A_2$ where $A_1 = \left\{\frac{1}{n+1}; n \in \mathbb{N}\right\}$ and $A_2 = \{x \in A; x \notin A_1\}$.
2. If B=(0,1] then $B = B_1 \cup B_2$ where $B_1 = \left\{\frac{1}{n}; n \in \mathbb{N}\right\}$ and $B_2 = \{x \in B; x \notin B_1\}$.
3. If C=[0,1) then $C = C_1 \cup C_2$ where $C_1 = \left\{\frac{1}{n+1}; n \in \mathbb{N}\right\} \cup \{0\}$ and $C_2 = \{x \in C; x \notin C_1\}$.
4. If D=[0,1] then $D = D_1 \cup D_2$ where $D_1 = \left\{\frac{1}{n}; n \in \mathbb{N}\right\} \cup \{0\}$ and $C_2 = \{x \in C; x \notin C_1\}$.

Since $A_1 \sim B_1 \sim C_1 \sim D_1$ and $A_2 = B_2 = C_2 = D_2$ then A~B~C~D. See example 2.

Finite Sets and Infinite sets:

We define some special sets of natural numbers:

$A_1=\{1\}$ $A_2=\{1,2\}$ $A_3=\{1,2,3\}$, ..., $A_m=\{1,2,...,m\}$

These sets are sometimes called **initial segments**.

Definition:

1. A set A is **finite** iff $A = \emptyset$ or $A \sim A_m$ for some $m \in \mathbb{N}$.
2. A set is **infinite** iff it is not finite.

3. We say that $\emptyset$ is of **cardinality 0**.
4. If $A \sim A_m$ we say that A is of **cardinality m**. This makes sense since A and A_m are in the same equivalence class, i.e., "are of the same cardinality".

Example 4:

If $A = \{a, b, c, d, e\}$ then $A \sim A_5$ so that the cardinality of A is equal to 5.

Remark: To find the cardinality of a finite set, just count its elements.

Example 5:

If $A = \{a, 1, \alpha, 2\}$ then $|A|=4$; If $B = \{x \in \mathbb{Z};\ \mathbf{-4 \leq x \leq 4}\}$ then $|B|=9$. Therefore, $|A| < |B|$.

Definition: A set A is **denumerable** if there exists a bijection function $f: \mathbb{N} \to A$. Or it's cardinality as $\mathbb{N}$ ($A \sim \mathbb{N}$).

Example 6: Each of the following set is **denumerable:**

1. A_1, B_1, C_1 and D_1 see example 2.
2. $2\mathbb{N} = \{2,4,6,8,\ldots\}$ since there exists at least a bijective function $f: \mathbb{N} \to 2\mathbb{N}$ where $f(x) = 2x$.
3. $\mathbb{Z}$ Since there exists at least a bijective function $f: \mathbb{N} \to \mathbb{Z}$ where $f(x) = \begin{cases} \frac{1-x}{2} & \text{if x is odd} \\ \frac{x}{2} & \text{if x is even} \end{cases}$.
4. The set $\mathbb{Q}$.

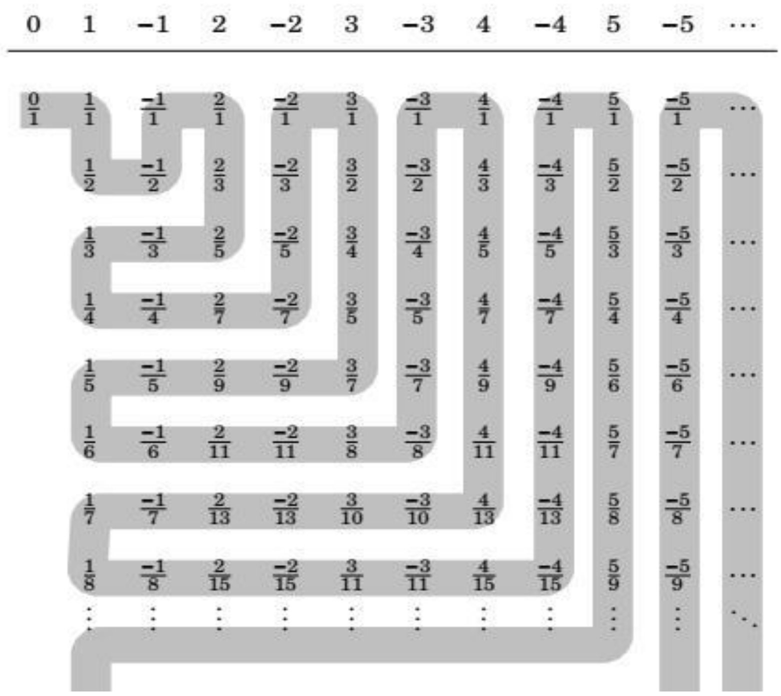
Explanation:

Theorem 13.4 The set $\mathbb{Q}$ of rational numbers is countably infinite.

Proof. To prove this, we just need to show how to write the set $\mathbb{Q}$ in list form. Begin by arranging all rational numbers in an infinite array. This is done by making the following chart. The top row has a list of all integers, beginning with 0, then alternating signs as they increase. Each column headed by an integer k contains all the fractions (in reduced form) with numerator k. For example, the column headed by 2 contains the fractions $\frac{2}{1}, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \ldots$, and so on. It does not contain $\frac{2}{2}$, $\frac{2}{4}$, $\frac{2}{6}$, etc., because those are not reduced, and in fact their reduced forms appear in the column headed by 1. You should examine this table and convince yourself that it contains all rational numbers in $\mathbb{Q}$.

0	1	−1	2	−2	3	−3	4	−4	5	−5	⋯
$\frac{0}{1}$	$\frac{1}{1}$	$\frac{-1}{1}$	$\frac{2}{1}$	$\frac{-2}{1}$	$\frac{3}{1}$	$\frac{-3}{1}$	$\frac{4}{1}$	$\frac{-4}{1}$	$\frac{5}{1}$	$\frac{-5}{1}$	⋯
	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{2}{3}$	$\frac{-2}{3}$	$\frac{3}{2}$	$\frac{-3}{2}$	$\frac{4}{3}$	$\frac{-4}{3}$	$\frac{5}{2}$	$\frac{-5}{2}$	⋯
	$\frac{1}{3}$	$\frac{-1}{3}$	$\frac{2}{5}$	$\frac{-2}{5}$	$\frac{3}{4}$	$\frac{-3}{4}$	$\frac{4}{5}$	$\frac{-4}{5}$	$\frac{5}{3}$	$\frac{-5}{3}$	⋯
	$\frac{1}{4}$	$\frac{-1}{4}$	$\frac{2}{7}$	$\frac{-2}{7}$	$\frac{3}{5}$	$\frac{-3}{5}$	$\frac{4}{7}$	$\frac{-4}{7}$	$\frac{5}{4}$	$\frac{-5}{4}$	⋯
	$\frac{1}{5}$	$\frac{-1}{5}$	$\frac{2}{9}$	$\frac{-2}{9}$	$\frac{3}{7}$	$\frac{-3}{7}$	$\frac{4}{9}$	$\frac{-4}{9}$	$\frac{5}{6}$	$\frac{-5}{6}$	⋯
	$\frac{1}{6}$	$\frac{-1}{6}$	$\frac{2}{11}$	$\frac{-2}{11}$	$\frac{3}{8}$	$\frac{-3}{8}$	$\frac{4}{11}$	$\frac{-4}{11}$	$\frac{5}{7}$	$\frac{-5}{7}$	⋯
	$\frac{1}{7}$	$\frac{-1}{7}$	$\frac{2}{13}$	$\frac{-2}{13}$	$\frac{3}{10}$	$\frac{-3}{10}$	$\frac{4}{13}$	$\frac{-4}{13}$	$\frac{5}{8}$	$\frac{-5}{8}$	⋯
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Next, draw an infinite path in this array, beginning at $\frac{0}{1}$ and snaking back and forth as indicated below. Every rational number is on this path.



Define f:N→ Q by f(1)=0, f(2)=1, f(3)= 1/2, f(4)=-1/2, f(5)=-1, and so on. It is not hard to check that f is a bijective function. Then Q is a denumerable and Countable set.

Example 7:

Each of the following sets are not **denumerable**

- The Set of real numbers $\mathbb{R}$
- $[a,b]$={ $x \in \mathbb{R}; a \leq x \leq b; a < b$} for example, [1,2].
- (a,b)={ x $\in \mathbb{R}$; a $< x < b$} for example, (0,1).
- The set of irrational numbers.

Definition:

A set A is called countably infinite (Or **denumerable)** if A $\sim \mathbb{N}$. We say that A is countable if A $\sim$ N or A is finite. If a set B is not countable it is uncountable.

Example 8:

$\mathbb{Q}$ is countable but $\mathbb{R}$ is not countable(uncountable).

Remark:

1) If A is countable and B $\subseteq$ A then B is countable.

2) If A and B are two countable sets then $A \cup B, A \cap B, A - B,$ and $A \triangle B$ are countable sets.

3) If B is uncountable and B $\subseteq$ A then A is uncountable.

Exercises: Show that each of pair of given sets have equal cardinality by describing a bijection from one to the other: ((0,1) and $\mathbb{R}$), (($\sqrt{2}$, ∞) and $\mathbb{R}$), (A={$\ldots\frac{1}{8},\frac{1}{4},\frac{1}{2},1,2,3,4,\ldots$}and $\mathbb{Z}$**), and (**The set of even integers and the set of odd integers).

Chapter six

Construction of Numbers (Part 1)

1-The Natural Numbers

The Peano Axioms

Thus far we have assumed those properties of the number systems necessary to provide examples and exercises in the earlier chapters. In this chapter we propose to develop the system of numbers assuming only few of its simpler properties. These simple properties known as the **Peano's** Axioms (Postulates) after the Italian mathematician who in 1889 inaugurated the program, may state as follows:

Peano's Axioms: $\mathbb{N}$ is a set with the following properties.

Axiom **I :** $1 \in \mathbb{N}$;

AxiomII : For each $n \in \mathbb{N}$ there exists a unique element $n^+ \in \mathbb{N}$, called Successor of n in $\mathbb{N}$. $(n \in \mathbb{N} \Rightarrow n^+ \in \mathbb{N})$

AxiomIII : For each $n \in \mathbb{N}, n^+ \neq 1$;

Axiom IV(injective**):** For every $m, n \in \mathbb{N}$, if $m^+ = n^+$, then $m = n$;

Axiom V(Principle of Induction): If A is a sub set of $\mathbb{N}$, such that $1 \in A$, and if $k \in A$ implies $k^+ \in A$, then $A = \mathbb{N}$.

ADDITION ON $\mathbb{N}$:

Addition(+) on $\mathbb{N}$defined by

I) $n^+ = n + 1$ for every $n \in \mathbb{N}$

II) $m + n^+ = (m + n)^+$ whenever $n + m$ is defined, $\forall m, n \in \mathbb{N}$.

MULTIPLICATION ON $\mathbb{N}$:

Multiplication on $\mathbb{N}$ is defined by

I) n.1=n for every $n \in \mathbb{N}$

II) $m.n^+ = mn + m$, whenever $n.m$ is defined, $\forall m, n \in \mathbb{N}$.

Lemma: If $n \in \mathbb{N}$ and $n \neq 1$, then there exists $m \in \mathbb{N}$ such that $n = m^+$.

Or every natural number different from 1 is a successor that is

Theorem(Closed):- $m + n \in \mathbb{N}$ for every $m, n \in \mathbb{N}$.

Proof: Let A be a subset of ℕ as follows: A = $\{n \in \mathbb{N}; \forall m \in \mathbb{N}, m+n \in \mathbb{N}\}$. To prove the theorem, we must prove A = ℕ.

Step 1: Let $n = 1$. Since $m \in \mathbb{N}$ then by axiom II, $m^+ \in \mathbb{N}$ and by the definition of addition part 1, $m^+ = m + 1$ so that $m + 1 \in \mathbb{N}$ Thus we obtained 1 ∈A.

Step 2: Suppose that k ∈A that is $m + k \in \mathbb{N}$

Step 3: To prove k^+ ∈A that is $m + k^+ \in \mathbb{N}$.

Since $m + k \in \mathbb{N}$ (By assumption)

then by axiom II, $(m+k)^+ \in \mathbb{N}$. But $(m+k)^+ = m + k^+$

So that $m + k^+ \in \mathbb{N}$ Thus by Axiom V, A=ℕ therefore, $\forall\, m, n \in \mathbb{N}; m+n \in \mathbb{N}$.

Theorem:- For any m, n and p in natural number

1- $(m+n)+p = m+(n+p)$ (Associative law)

2- $n+1 = 1+n$

3- $m+n = n+m$ (Commutative law)

4- $If\ m+p = n+p$ then $m = n$. (Cancelation law)

5- $m^+ + n = (m+n)^+$

Proof *1*: As before let us define a subset of ℕ as follows:

A = $\{p \in \mathbb{N}; \forall m, n \in \mathbb{N};\ (m+n)+p = m+(n+p)\}$

To prove the theorem, we must show that A = ℕ and again we plan to use the Principle of Induction. To apply the Principle, we must check three things and we will check them below.

Step 1: Let p=1 then L.H.S = $(m+n)+1 = (m+n)^+$ (By the definition of addition) $= m + n^+$ (By the definition of addition)= $m + (n+1)$ (By the definition of addition) =R.H.S Thus we get 1 ∈A.

Step 2: Suppose that k ∈A that is $(m+n)+k = m+(n+k)$.

Step 3: To prove k^+ ∈A that is $(m+n) + k^+ = m + (n+k^+)$.

L.H.S= $(m+n)+k^+ = \big((m+n)+k\big)^+$ (By the definition of addition)

$= \big(m+(n+k)\big)^+$ (By assumption) = $m + (n+k)^+$ (By the definition of addition)

$= m + (n+k^+)$ (By the definition of addition)

=R.H.S Thus by Axiom V, A=ℕ therefore, $\forall m, n, p \in \mathbb{N} \Rightarrow (m+n)+p = m+(n+p)$.

Proof *2:* Let A be a subset of ℕ as follows:

1- A = $\{n \in \mathbb{N}; n+1 = 1+n\}$

To prove the theorem, we must prove A = ℕ. Now we plan to use the Principle of Induction.

Step 1: Let $n = 1$ then L.H.S $= 1+1$ =R.H.S Thus we get 1 ∈A.

Step 2: Suppose that k ∈A that is $k+1 = 1+k$.

Step 3: To prove k^+ ∈A that is $k^+ + 1 = 1 + k^+$.

L.H.S= $k^+ + 1 = (k+1)+1$ (By the definition of addition) = $k + (1+1)$ (By associative law) $= k + 1^+$ (By the definition of addition) $= (k+1)^+$ (By the definition of addition) $= (1+k)^+$ (By assumption) =$1 + k^+$ (By the definition of addition)= R.H.S.

Or L.H.S= $k^+ + 1 = (k+1)+1$ (By the definition of addition) = $(1+k)+1$ (By assumption) $= 1 + (k+1)$ (By associative law)$= 1 + k^+$ = R.H.S.

Thus by Axiom V, A=ℕ therefore, $\forall\, n \in \mathbb{N} \Rightarrow n+1 = 1+n$.

3- $m+n = n+m$ (Commutative law) H.W

Hint A = $\{n \in \mathbb{N}; \forall\, m \in \mathbb{N}; m+n = n+m\}$

4-If $m+p = n+p$ then $m = n$. (Cancelation law) H.W

Hint A = $\{p \in \mathbb{N}; \forall\, m \in \mathbb{N};$ if $m+p = n+p$ then $m = n\}$

<u>Theorem(Closed):-</u> $m.n \in \mathbb{N}$ for every $m, n \in \mathbb{N}$.

Proof: Let A be a subset of ℕ as follows: A = $\{n \in \mathbb{N}; \forall m \in \mathbb{N}, m.n \in \mathbb{N}\}$. To prove the theorem, we must prove A = ℕ.

Step 1: Let $n = 1$. Since $m \in \mathbb{N}$ and $m.1 = m \in \mathbb{N}$(why?) Thus we get 1 ∈A.

Step 2: Suppose that k ∈A that is $m.k \in \mathbb{N}$

Step 3: To prove k^+ ∈A that is $m.k^+ \in \mathbb{N}$.

Since $m.k^+ = mk + m$ and $m, m.k \in \mathbb{N}$

then $mk + m \in \mathbb{N}$. (why?)

But $m.k^+ = mk + m$ So that $m.k^+ \in \mathbb{N}$. Thus by Axiom V, A=ℕ therefore, $\forall\, m, n \in \mathbb{N}; m.n \in \mathbb{N}$.

<u>Theorem: -</u> For any m, n and p in ℕ

1) $1.n = n.1$

2) $m^+.n = mn + n$

3) $m.n = n.m$ (Commutative law)

4) a- $m.(n + p) = mn + mp$ b- $(m + n).p = mp + np$

5) $(m.n).p = m.(n.p)$ (Associative law)

Proof 1: Let A be a subset of ℕ as follows:

A = $\{n \in \mathbb{N}; 1.n = n.1\}$. To prove the theorem, we must prove A = ℕ.

Step 1: Let $n = 1$ then L.H.S $= 1.1 = 1$ (By the definition of multiplication)

=R.H.S Thus we get 1 ∈A.

Step 2: Suppose that k ∈A that is $1.k = k.1$

Step 3: To prove k^+ ∈A that is $1.k^+ = k^+.1$

L.H.S= $1.k^+ = 1.k + 1$ (By the definition of multiplication) = $k + 1$ (why ?)

$= k^+$ (By the definition of addition) = $k^+.1$ (By the definition of multiplication)

= R.H.S. Thus by Axiom V, A=ℕ therefore, $\forall\, n \in \mathbb{N} \Rightarrow n + 1 = 1 + n$.

Proof 2: Let A be a subset of ℕ as follows: A = $\{n \in \mathbb{N}; \forall m \in \mathbb{N},\ m^+.n = mn + n\}$. To prove the theorem, we must prove A = ℕ.

Step 1: Let $n = 1$ then L.H.S $= m^+.n = m^+.1 = m^+$ (By n.1=n)

=$m + 1$ (By the definition of addition)= $m.1 + 1$ (By n.1=n)=R.H.S Thus we get 1 ∈A.

Step 2: Suppose that k ∈A that is $m^+.k = mn + k$

Step 3: To prove k^+ ∈A that is $m^+.\ k^+ = mn + \ k^+$

L.H.S= $m^+.\ k^+ = m^+.k + m^+$(By the definition of addition $m.n^+ = m.n + m$)

$= (mk + k) + m^+$(By Assumption) = $(mk + k) + (m + 1)$ (By the definition of addition)

=$mk + (k + (m + 1))$ (By associative law $(m + p) + n = m + (p + n)$)

$= m.k + ((k + m) + 1)$ (By associative law $(m + p) + n = m + (p + n)$)

$= m.k + ((m + k) + 1)$ (By commutative law $m + n = n + m$)

$= m.k + (m + (k + 1))$ (By associative law $(m + p) + n = m + (p + n)$)

$= (m.k + m) + (k + 1)$ (By associative law $(m + p) + n = m + (p + n)$)

$= mk^+ + k^+$ (By the definition of addition)

$= R.H.S$ Thus by Axiom V, A=ℕ therefore, $\forall\, m, n \in \mathbb{N}$; $m^+.n = mn + n$.

3. $m.n = n.m$ (Commutative law) **H.W**

Hint A = $\{n \in \mathbb{N}; \forall\, m \in \mathbb{N}; m.n = n.m\}$.

Step 3: L.H.S= $m.k^+ = mk + m$(why?) = $km + m$(why?)=$k^+.m$ (why?)=R.H.S

4.a- $m.(n + p) = mn + mp$ H.W

Hint A = $\{p \in \mathbb{N}; \forall\, m, n \in \mathbb{N}; m.(n + p) = mn + mp\}$.

Step 3: L.H.S=$m.(n + k^+)$= $m.(n + k)^+$= $m.(n + k) + m$

= $(mn + mk) + m$(why?) $mn + (mk + m)$(why?) $= mn + mk^+$ (why?)

4.b- $(m + n).p = mp + np$ H.W (Hint Same as 4.a)

5. $(m.n).p = m.(n.p)$ (Associative law)

Hint A = $\{p \in \mathbb{N}; \forall\, m, n \in \mathbb{N}; (m.n).p = m.(n.p)\}$.

Step 3: L.H.S=$(m.n).k^+$=$(m.n).k + (mn)$ (why?)

= $m.(n.k) + mn$ (why?) = $m.(n.k + n)$ (why?) $= m.(n.k^+)$ =R.H.S

Remark:

1. If $m = n$ and $n = k$ then $m = k$ (By substitution)
2. If $m = n$ then $m + p = n + p$ (By substitution)
3. $0^+ = 1$, $0 + k = k + 0$ and $0.k = k.0$.

<u>**Theorem:-**</u> For any $m \in \mathbb{N}$.

1. If $m + n = m$ then n=0
2. If $m.n = 0 \; then \; m = 0 \lor n = 0$
3. If $n.p = m.p \rightarrow n = m \; where \; p \neq 0$.

<u>**Exponentiation:-**</u>

For any $n \in \mathbb{N}$: $(1) n^0 = 1$; (2) $n^{m^+} = n^m.n$, $\forall m \in \mathbb{N}$ or $m = 0$; (3) $0^n = 0$.

Lemma: For any $n \in \mathbb{N}$: (1) $n^1 = n$. (2) $1^n = 1$.

Proof 1: Let A be a subset of ℕ as follows:

A = $\{n \in \mathbb{N};\ n^1 = n\}$. To prove the theorem, we must prove A = ℕ.

Step 1: Let $n = 1$ then L.H.S = $1^1 = 1^{0^+}$(By remark $0^+ = 1$) $= 1^0.1$(By **Definition** $n^{m^+} = n^m.n\ ,\ \forall m \in \mathbb{N}$ or $m = 0$) $= 1.1$(why?) $= 1$(why?) $= R.H.S$

Step 2: Suppose that k ∈A that is $k^1 = k$

Step 3: To prove k^+ ∈A that is $(k^+)^1 = k^+$

L.H.S= $(k^+)^1 = (k^+)^{0^+}$(why?)=$(k^+)^0.(k^+)$ (why?)=1.k^+(why?) =k^+ (why?)= R.H.S.

Thus by Axiom V, A=ℕ therefore, $\forall\, n \in \mathbb{N} \Rightarrow n^1 = n$.

Proof 2: Let A be a subset of ℕ as follows:

A = $\{n \in \mathbb{N}; 1^n = 1\}$. To prove the theorem, we must prove A = ℕ.

Step 1: Let $n = 1$ then L.H.S = $1^1 = 1$(By part 1) $= R.H.S$

Step 2: Suppose that k ∈A that is $1^k = 1$

Step 3: To prove k^+ ∈A that is $1^{k^+} = 1$

L.H.S=$1^{k^+} = 1^k.1$(why?) $= 1.1$(why?) $= 1$(why?)= $R.H.S$

Thus by Axiom V, A=ℕ therefore, $\forall\, n \in \mathbb{N} \Rightarrow 1^n = 1$.

<u>Theorem:</u> $\forall\, n, m$ & $z \in \mathbb{N}$

1)$n^{m+z} = n^m.n^z$ 2) $(n^m)^z = n^{mz}$ 3)$(n.m)^z = n^z.m^z$

The Order Relation on Natural Number

Definition: If $m, n \in \mathbb{N}$, we say that n is less than m, written $n < m$, if there exists a natural number k such that $m = n + k$. We also write $n \leq m$, read n is less than or equal to m, to mean that either $n = m$ or $n < m$.

<u>Theorem:-</u> For any $m, n, p\ and\ q \in \mathbb{N}$

1-If $m < n\ \wedge\ n < p\ then\ m < p$ (< is transitive relation)

2- If $n < m \wedge m \leq p \rightarrow n < p$.

3- If $n \leq m \wedge m \leq p \rightarrow n \leq p$

4- If $m \leq n \wedge n \leq m \rightarrow m = n$.

5- If $n < m \rightarrow n + p < m + p$.

6- If $n \leq m \rightarrow n + p \leq m + p$.

7- If $n < m \wedge p < q$ then the following: a) $n + p < m + q$ b) $n.p < m.q$

8- $\sim (\exists k \in \mathbb{N}\ such\ that\ n < k < n^{+})$.

9- If $m, n \in \mathbb{N}$ then only one of the following condition is true $m < n$, $m = n$, $m > n$

10. $n < m$ if and only if $n.p < m.p\ where\ p \neq 0$

Proof 1: Suppose that $m < n\ and\ n < p$ then $\exists z, w \in \mathbb{N}$ such that $m + z = n$ $and\ n + w = p$ (By the definition of order relation on $\mathbb{N}$)

$p = n + w = (m + z) + w$ (By substitution)

then $m + (z + w) = p$ (By associative law)

then $m < p$ (By the definition of order relation on $\mathbb{N}$ and closed theorem)

Proof 2: Suppose that $n < m \wedge m \leq p \Rightarrow (n < m) \wedge [(m < p) \vee (m = p)]$ (By definition of $\leq$) $\Rightarrow [(n < m) \wedge (m < p)] \vee [(n < m) \wedge (m = p)]$ (By distributive law in logic)

$\Rightarrow (n < p) \vee (n < p)$(< is transitive relation+ Substitution)

$\Rightarrow n < p$ (Idempotent Laws $P \vee P \equiv P$).

.Proof of 3, 4,5 and 6 are similar to 2

Proof 7-a: If $n < m \wedge p < q \rightarrow n + p < m + q$

Suppose that $n < m\ and\ p < q$ then $\exists r, s \in \mathbb{N}$ such that $m = n + r$ $and\ q = p + s$ (By the definition of order relation on $\mathbb{N}$). Then

$m + q = (n + r) + (p + s) = n + (r + (p + s)) = n + ((r + p) + s) = n + ((p + r) + s$ $= n + (p + (r + s)) = (n + p) + (r + s)$. Therefore $n + p < m + q$ (By the definition of order relation on $\mathbb{N}$ and closed theorem). ***Proof 7-b:*** If $n < m \wedge p < q \rightarrow n.p < m.q$ H.W

Suppose that $n < m\ and\ p < q$ then $\exists r, s \in \mathbb{N}$ such that $m = n + r$and $q = p + s$ (By the (definition of order relation on $\mathbb{N}$

then $m.q = (n + r).(p + s)$ ... H.W

Chapter six

Construction of Numbers (Part 2)

3-The Integers($\mathbb{Z}$): The system of integers can be construction from the system of natural numbers. For this purpose, we form the product set $\mathbb{N} \times \mathbb{N} = \{(p,q);\ p,q \in \mathbb{N}\}$.

<u>Definition</u>: Let the binary relation "$\sim$", read "wave" be defined on all $\big((m,n),(p,q)\big) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ by $(m,n) \sim (p,q)$ if and only if $m + q = p + n$.

Example:

$(1,5) \sim (4,8) \quad \leftrightarrow \quad 1 + 8 = 4 + 5$.

<u>Theorem:</u>

The relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ is an equivalence relation. H.W

<u>Definition:</u>

The set of all equivalence relation on $\mathbb{N} \times \mathbb{N}$ with respect to the relation $\sim$ is called set of integers and denoted by $(\mathbb{Z})$ that is

$\mathbb{Z} = \{[(m,n)]/(m,n) \in \mathbb{N} \times \mathbb{N}\}$ and $[(m,n)] = \{(p,q) \in \mathbb{N} \times \mathbb{N}\ |(m,n) \sim (p,q)\}$.

<u>Example:</u>-

$[(2,5)] = \{(p,q) \in \mathbb{N} \times \mathbb{N}\ |(2,5) \sim (p,q)\} = \{(3,6),(4,7),(2,5) \ldots\}$.

Note: We write $[m,n]$ instead $[(m,n)]$.

The Addition and Multiplication on $\mathbb{Z}$:

<u>Definition</u>: Addition and multiplication on $\mathbb{Z}$ will be defined respectively by

1) $[m,n] + [p,q] = [m + p, n + q]$.
2) $[m,n].[(p,q)] = [mp + nq, mq + np]$.

The Positive, Negative and Zero Integers

Since for every $m,n \in \mathbb{N}$, we have the following cases: $m = n$, $n < m$ or $m < n$

1) If $m = n$ then $[m,n] = [m,m] = [n,n]$ is called zero integer

2) If $m < n$ then $\exists u \in \mathbb{N}$ such that $m + u = n$, $[m,n] = [m,m+u]$ is called negative integer. That is $\mathbb{Z}^- = \{[m,n]: (m,n) \in \mathbb{N} \times \mathbb{N}, m < n\}$**.**

3) If $n < m$ then $\exists w \in \mathbb{N}$ such that $n + w = m, [m,n] = [n + w, n]$ is called positive integer. That is $\mathbb{Z}^+ = \{[m,n]: (m,n) \in \mathbb{N} \times \mathbb{N}, m > n\}$**.**

Remark: (1) $-[m,n] = [n,m]$. (2) $0 = [m,m]$. (3) $p = [m + p, m]$.

Example:-

[2,7]=[2, 2+5] is a negative integer,

[8,1]=[1+7, 1] is a positive integer and

[2, 2] is zero integer.

Theorem: Let x, y and $z \in \mathbb{Z}$**.**

1) $x + y = y + x$

2) $x.y = y.x$

3) $(x + y) + z = x + (y + z)$.

4) $(x.y).z = x.(y.z)$.

5) $x.(y + z) = (x.y) + (x.z)$.

6) $If\ x + y = x + z\ then\ y = z$

7) $If\ x \neq 0\ and\ if\ x.y = x.z\ then\ y = z$.

Proof 1:-Let $x = [(m,n)]$, and $y = [(p,q)]$ then

$L.H.S$= $x + y = [m,n] + [p,q] = [(m + p), (n + q)]$

$= [m + p, n + q]$(by the definition of addition in $\mathbb{Z}$)

$= [p + m, q + n]$(by commutative law in $\mathbb{N}$; $m + n = n + m$)

$= [p,q] + [m,n]$ (by the definition of addition in $\mathbb{Z}$)

$= y + x = R.H.S.$

$\boldsymbol{Proof\ 2}$: Let $x = [(m,n)]$, and $y = [(p,q)]$. Then

$L.H.R$=$[m,n].[p,q] = [mp + nq, mq + np]$(by the definition of multiplication in $\mathbb{Z}$)

$= [pm + qn, qm + pn]$(why?) $= [pm + qn, pn + qm]$(why?)

$= [p,q].[m,n]$(why?) $= R.H.S.$

Proof 3:-Let $x = [(m,n)], y = [(p,q)]$ and $z = [r,s]$. Then

$L.H.S$=$(x + y) + z = ([m,n] + [p,q]) + [r,s] = [(m + p), (n + q)] + [r,s]$

$= [(m+p)+r,(n+q)+s] = [m+(p+r),n+(q+s)] = [m,n] + [(p+r),(q+s)]$
$= [m,n] + ([p,q] + [r,s]) = x + (y+z) = R.H.S.$

Proof 4 and 5 are Home work.

Proof (6): Let $x = [m,n], y = [p,q]$ and $z = [r,s]$ and Suppose $x + y = x + z$. Then
$[m,n] + [p,q] = [m,n] + [r,s]$

$\to [m+p,n+q] = [m+r,n+s]$(By the definition of addition)

$\to ((m+p,n+q),(m+r,n+s)) \in \sim$ (By the definition of relation ∼)

$\to (m+p)+(n+s) = (n+q)+(m+r)$ (By the condition of the relation wave)

$(p+s)+(m+n) = (r+q)+(m+n)$ (by commutative law and associative law in ℕ)

$\to p+s = r+q$(By cancelation law)

$\to ((p,q),(r,s)) \in \sim$ $\to [p,q] = [r,s] \to y = z$.

<u>Theorem:</u>- For every $x, y \in \mathbb{Z}$

1) $x - x = 0$
2) $-(x-y) = y - x$.
3) $x - y = 0$ if and $only$ if $x = y$.
4) $x.y = 0$ $then$ $x = 0$ or $y = 0$.

Proof: (1) Let $x = [m,n]$ $then$

L.H.S=$x - x = x + (-x) = [m,n] + (-[m.n]) = [m,n] + [n,m]$
$= [m+n,n+m] = [m+n,m+n] = 0 = R.H.S.$

2) Let $x = [(m,n)]$, $y = [(p,q)]$ and $0 = [e,e]$.

Suppose $x - y = 0$ then $[m,n] + (-[p,q]) = [e,e] \to [m,n] + [q,p] = [e,e]$.

$\to [m+q,n+p] = [e,e]$ $\to \big((m+q,n+p),(e,e)\big) \in \sim$

$\to (m+q)+e = (n+p)+e$ [By the condition of relation wave]

$\to m+q = n+p$(By the cancelation law in ℕ)

$\to \big((m,n),(p,q)\big) \in \sim$ [by the definition of relation wave on ℕ × ℕ]

$\to [m,n] = [p,q] \to x = y$.

Conversely: Suppose that $x = y$ we have to prove that $x - y = 0$

$L.H.S = x - y = x - x$[By substitution because x=y]

$= 0$ [By the theorem $x - x = 0$) = R.H.S.

The Order Relation on Integers:

<u>Definition:</u> Let $x, y \in \mathbb{Z}$, where $x = [(m,n)]$ and $y = [(p,q)]$. We say that x is less than y, written $x < y$, if and only if $m + q < n + p$ and x is greater than y, written $x > y$ if and only if $m + q > n + p$.

Example:-

1. $[(5,2)] < [(8,4)]$ since $5 + 4 < 8 + 2$
2. $[(4,1)] > [(2,7)]$ since $4 + 7 > 2 + 1$

<u>Remark:</u>- $\forall\ x, y \in \mathbb{Z}$ we use

1) $x \leq y\ iff\ x < y\ or\ x = y$
2) $x \nleq y\ iff\ x \nless y\ and\ x \neq y.$
3) $x > y\ iff\ y < x.$
4) $x \geq y\ iff\ y \leq x.$

<u>Theorem</u>:-$Let\ x, y\ and\ w \in\ \mathbb{Z}$ then

1) $x \nless x.$
2) $If\ x < y\ and\ y < w,\ \ then\ x < w.$
3) $x < y\ \ or\ \ y < x\ \ or\ \ x = y.$
4) $If\ x < w\ \ then\ x + y < w + y$
5) $If\ x < y\ \wedge 0 < w\ \ then\ x.w < y.w.$

$\boldsymbol{Proof}$ **1**$: -$ Let $x = [(m,n)]$. Suppose that $x < x$ then $[(m,n)] < [(m,n)]$

$\rightarrow m + n < m + n$, which is contradiction with the theorem

[$m \nless m. \forall m \in \mathbb{N}$], therefore $x \nless x$.

$\boldsymbol{Proof}$ **2**$: -$ Let $x = [(m,n)]$, $y = [(p,q)]$ and $w = [(r,s)]$.

Suppose that $x < y\ and\ y < w$ then

$\rightarrow [(m,n)] < [(p,q)]$ and $[(p,q)] < [(r,s)]$

$\rightarrow m + q < p + n$ and $p + s < r + q$

$\rightarrow (m+q)+(p+s)<(p+n)+(r+q)$ [by theorem if $x<y$ and $n<m$ then $x+n<y+m$]

…H.W…

$\rightarrow (m+s)+(p+q)<(r+n)+(p+q)$

$\rightarrow m+s<r+n$ [By theorem if $x<y$ and $n<m$ then $x+n<y+m$]

$\rightarrow [(m,n)]<[(r,s)]$ $\rightarrow x<w$.

$\boldsymbol{Proof\ 3}:-$ Let $x=[(m,n)]$ and $y=[(p,q)]$.

Case 1: If $x<y$ and $x=y$ then

$[(m,n)]<[(p,q)]$ and$[(m,n)]=[(p,q)]$

$\rightarrow (m+q)<(p+n)$ $\wedge\big((m,n),(p,q)\big)\in\sim$(By …)

$\rightarrow (m+q)<(p+n)$ $\wedge(m+q)=(p+n)$ Which is contradiction (By …).

Case 2: Let $x<y$ and $y<x$ then

$\rightarrow [(m,n)]<[(p,q)]\wedge[(p,q)]<[(m,n)]$(By…)

$\rightarrow (m+q)<(n+p)\wedge(p+n)<(q+m)$(By the definition of order relation in $\mathbb{Z}$)

$\rightarrow (m+q)<(m+q)$Which is contradiction [by theorem $m\nless m$]

Case 3: Let $y<x$ and $y=x$ then $y<y$ (By substitution)

which is contradiction[by theorem $m\nless m$] . Hence $x<y$ or $y<x$ or $x=y$.

$\boldsymbol{Proof\ 4}:-$Let $x=[(m,n)]$, $y=[(p,q)]$ and $w=[(r,s)]$.

Let $x<w$ then $[(m,n)]<[(r,s)]\rightarrow m+s<n+r$ (By…)

$\rightarrow (m+s)+(p+q)<(n+r)+(p+q)$(By…)

… H.W…

$\rightarrow (m+p)+(s+q)<(n+q)+(r+p)$(By …)

$\rightarrow [(m+p),(n+q)]<[(r+p),(s+q)]$(By …)

$\rightarrow [(m,n)]+[(p,q)]<[(r,s)]+[(p,q)]$ $\rightarrow x+y<w+y$.

<u>Theorem:-</u>$For\ any\ x,y,w\ and\ u\in\mathbb{Z}$.

1) $[(x<y)\wedge(u<w)]\rightarrow x+u<y+w$
2) $[(x<y)\wedge(u\leq w)]\rightarrow x+u<y+w$
3) $[(x\leq y)\wedge(u<w)]\rightarrow x+u<y+w$

4) $[(x \leq y) \wedge (u \leq w)] \rightarrow x + u \leq y + w$

5) $[(0 < w) \wedge x.w < y.w] \rightarrow x < y$

Proof 1: $-$ Let $x = [(m,n)], y = [(p,q)], w = [(r,s)], and\ u = [(e,f)]$.

$where\ m,n,p,q,r,s,e\ and\ f \in \mathbb{N}$.

Suppose that $x < y\ and\ u < w$

$\rightarrow [(m,n)] < [(p,q)]$ and $[(e,f)], < [(r,s)]$

$\rightarrow (m + q < p + n)$ and $(e + s < r + f)$

$\rightarrow (m + q) + (e + s) < (p + n) + (r + f)$

$\rightarrow (m + e) + (q + s) < (p + r) + (n + f)$

$\rightarrow [(m + e, n + f)] < [(p + r), (q + s)]$

$\rightarrow [(m,n)] + [(e,f)] < [(p,q)] + [(r,s)] \rightarrow x + u < y + w$

Definition:-

Let $x, y \in \mathbb{Z}$. An integer x is positive if and only if $x > 0$ and

An integer y is negative if and only if $y < 0$.

Theorem:- *For any* $x, y, and\ w \in \mathbb{Z}$

1) $x < y$ if and only if $y - x$ is positive.

2) y is positive if and only if $-y$ is negative.

3) $x < y$ if and only if $-y < -x$

4) The sum and product of two positive integers are positive.

5) The product of two negative integers is positive.

6) The product of positive and negative integer is negative.

7) If $x \neq 0$, then $x^2 > 0$.

Proof 1:-Let $x = [(m,n)]$ and $y = [(p,q)]$.

Suppose that $x < y \leftrightarrow [(m,n)] < [(p,q)]$

$\leftrightarrow m + q < p + n$ (By definition of < in $\mathbb{Z}$**)**

$\leftrightarrow p + n > m + q$(By Remark, if $x < y$ iff $y > x$)

$\leftrightarrow p + n > q + m[by\ a + b = b + a, \forall a, b \in \mathbb{N}]$

$\leftrightarrow [(p+n, q+m)] > 0$[By remark, if $x = [(m,n)], x > 0\ iff\ m > n$]

$\leftrightarrow [(p,q)] + [(n,m)]$is a positive integer [By the definition of addition in $\mathbb{Z}$.]

$\leftrightarrow [(p,q)] - [(m,n)]$ is a positive integer.(By …) $\leftrightarrow y - x\ is\ positive$.

4) The product of two positive integers is positive.

Proof: Let $x = [m,n]$ and $y = [p,q]$ be two positive integers where $m,n,p,q \in N$.

Thus $m > n$ and $p > q$. Then there exist k_1, $k_2 \in N$ such that m= k_1+n and p= k_2+q.

Then xy=$[m,n]\ [p,q]$

= $[k_1 + \text{n}, n]\ [k_2 + \text{q}, q]$

=$[(k_1 + \text{n})(k_2 + \text{q}) + \text{nq}, (k_1 + \text{n})\text{q} + (k_2 + \text{q})\text{n}]$

=$[(k_1 + \text{n})k_2 + (k_1 + \text{n})\text{q} + \text{nq}, (k_1 + \text{n})\text{q} + (k_2 + \text{q})\text{n}]$

==$[(k_1k_2 + \text{n}k_2) + (k_1\text{q} + \text{nq}) + \text{nq}, (k_1\text{q} + \text{nq}) + (k_2\text{n} + \text{q n})]$

=$[k_1k_2 + (k_1\text{q} + \text{nq} + k_2\text{n} + \text{q n}), (k_1\text{q} + \text{nq} + k_2\text{n} + \text{q n})] > 0$

Hence the product of two positive integers is positive.

5) The product of two negative integers is positive.

Proof: Let $x = [m,n]$ and $y = [p,q]$ be two positive integers where $m,n,p,q \in N$.

Thus $m < n$ and $p < q$. Then there exist k_1, $k_2 \in N$ such that n= k_1+m and q= k_2+p.

Then xy=$[m,n]\ [p,q]$

= $[m, k_1 + \text{m}]\ [p, k_2 + \text{p}]$

=$[\text{mp} + (k_1 + \text{m})(k_2 + \text{p}), \text{p}(k_1 + \text{m}) + \text{m}(k_2 + \text{p})]$

=$[\text{mp} + ((k_1 + \text{m})k_2 + (k_1 + \text{m})\text{p}), \text{p}(k_1 + \text{m}) + \text{m}(k_2 + \text{p})]$

=$[\text{mp} + ((k_1k_2 + \text{m}k_2) + (k_1\text{p} + \text{mp})), (pk_1 + \text{pm}) + (mk_2 + \text{mp})]$

=$[k_1k_2 + (pk_1 + \text{pm} + mk_2 + \text{mp}), (pk_1 + \text{pm} + mk_2 + \text{mp})] > 0$

Hence the product of two negative integers is positive.

6) The product of positive and negative integer is negative.

Proof: Let $x = [m,n]$ be a positive integer and $y = [p,q]$ be a negative integer where $m,n,p,q \in N$. Thus $m > n$ and $p < q$. Then there exist k_1, $k_2 \in N$ such that m= k_1+n and q= k_2+p. Then xy=$[m,n]\ [p,q]$ = $[k_1 + \text{n}, n]\ [p, k_2 + \text{p}]$

=$[(k_1 + \text{n})\text{p} + \text{n}(k_2 + \text{p}), (k_1 + \text{n})(k_2 + \text{p}) + \text{np}]$

$=[(k_1\text{p} + \text{np})+(nk_2 + \text{np}), ((k_1 + \text{n})k_2 + (k_1 + \text{n})\text{p}) + \text{np}]$

$=[(k_1\text{p} + \text{np})+(nk_2 + \text{np}), ((k_1k_2 + \text{n}k_2) + (k_1\text{p} + \text{np})) + \text{np}]$

$=[(k_1\text{p} + \text{np}+nk_2 + \text{np}), (k_1\text{p} + \text{np} + nk_2 + \text{np}) + k_1k_2] <0$

Hence the product of positive and negative integer is negative.

Proof 7) Suppose that $xx \neq 0$ to prove that either $x > 0$ *or* $x < 0$.

Case 1: If $x < 0 \rightarrow x$ is a negative integer $\rightarrow x.x$ is a positive integers by branch 5]

x^2 is a positive integer then $x^2 > 0$.

Case 2: If $x > 0 \rightarrow x$ is a positive integer $\rightarrow x.x$ is a positive integer by branch 4

$\rightarrow x^2$ is a positive integer $\rightarrow x^2 > 0$.

Definition(Absolute Value): The Absolute value "|a|", of an integer a defined by

$|a| = \begin{cases} a & when\ a \geq 0 \\ -a & when\ a < 0 \end{cases}$ Thus, $|a| \in \mathbb{Z}^+$ when $a \neq 0$.

Theorem: *For any* $x, y \in \mathbb{Z}$

1) $|x| \geq 0$

2) $|x| = 0$ if and only if $x = 0$

3) $|-x| = |x|$

4) $|x - y| = |y - x|$

5) $|x.y| = |x|.|y|$

6) $-|x| \leq x \leq |x|$

7) $|x| < y$ *if and only if* $-y < x < y$

8) $|x + y| \leq |x| + |y|$.

9) $|x - y| \geq |x| - |y|$.

4-The Rational Numbers

The system of integers has an obvious defect in that, given integers, $m \neq 0$ and s, the equation mx=s may or may not have a solution. For example, 3x=6 has the solution x=2 but

4x=6 has no solution . This defect is remedied by adjoining to the integers additional numbers to form system $\mathbb{Q}$ of rational numbers.

Definition:

Let the binary relation "≈", read " Double wave" be defined on all $\big((m,n),(p,q)\big) \in (\mathbb{Z}\times\mathbb{Z}^*)\times(\mathbb{Z}\times\mathbb{Z}^*)$ by $(m,n) \approx (p,q)$ if and only if $m.q = p.n$. Where $\mathbb{Z}^* = \mathbb{Z} - \{0\}$.

Example:-

$\big((2,-3),(-2,3)\big) \in\approx$ since 2.3=-2.-3 and $\big((4,7),(4,7)\big) \in\approx$ because 4.7=4.7

Theorem:-

The relation $\approx$ is an equivalence relation on $\mathbb{Z}\times\mathbb{Z}^*$

Proof: 1) Let $(\mathrm{m}, \mathrm{n}) \in \mathbb{Z}\times\mathbb{Z}^* \rightarrow m.n = m.n \rightarrow \big((\mathrm{m},\mathrm{n}),(\mathrm{m},\mathrm{n})\big) \in \approx$ [by difintion of $\approx$ on $\mathbb{Z}\times\mathbb{Z}^*$]. Therefore $\approx$ is a reflexive relation on $\mathbb{Z}\times\mathbb{Z}^*$.

2) Let$\big((\mathrm{m},\mathrm{n}),(\mathrm{p},\mathrm{q})\big) \in \approx \rightarrow m.q = p.n \rightarrow p.n = m.q \rightarrow \big((\mathrm{p},\mathrm{q}),(\mathrm{m},\mathrm{n})\big) \in \approx$ [by difintion of $\approx$ on $\mathbb{Z}\times\mathbb{Z}^*$]. Therefore $\approx$ is a symmetric relation on $\mathbb{Z}\times\mathbb{Z}^*$.

3) Let $\big((\mathrm{m},\mathrm{n}),(\mathrm{p},\mathrm{q})\big) \in \approx$, and $\big((\mathrm{p},\mathrm{q}),(\mathrm{r},\mathrm{s})\big) \in \approx$

$\rightarrow m.q = p.n$ and $p.s = r.q$ [by difintion of $\approx$ on $\mathbb{Z}\times\mathbb{Z}^*$]

$\rightarrow (m.q).s = (p.n).s$ $[by\ theorem\ a = b \rightarrow a.z = b.z\ \ \forall a,b,z \in \mathbb{Z}\,]$

$\rightarrow (m.q).s = n.(p.s) \rightarrow (m.s).q = n.(r.q)$ $[by\ p.s = r.q]$.

$\rightarrow (m.s).q = (n.r).q \rightarrow m.s = n.r$ $[by\ theorem\ if\ a.c = b.c\ \rightarrow a = b \forall a,b,c \in \mathbb{Z}]$.

$\rightarrow \big((\mathrm{m},\mathrm{n}),(\mathrm{r},\mathrm{s})\big) \in \approx$ [by difintion of $\approx$ on $\mathbb{Z}\times\mathbb{Z}^*$].

Therefore $\approx$ is a transitive relation on $\mathbb{Z}\times\mathbb{Z}^*$.

Hence $\approx$ is an equivalence relation on on $\mathbb{Z}\times\mathbb{Z}^*$.

Definition:- The set of all equivalence classes with respected to the relation $\approx$ on $\mathbb{Z}\times\mathbb{Z}^*$called the set of all **rational number** and denoted by $\mathbb{Q}$

The Positive Negative and Zero rational number

1) Let [(m,n)] ∈ $\mathbb{Q}$, then [(m,n)] is called positive rational number if m.n>0, and denoted by $\mathbb{Q}^+$.

2) Let [(m,n)] ∈ $\mathbb{Q}$, then [(m,n)] is called negative rational number if m.n<0, and denoted by $\mathbb{Q}^-$.

3) Let [(m,n)] ∈ $\mathbb{Q}$, then [(m,n)] is called zero rational number if m=0.

Example:- [(-3,-3)] is a positive rational number,

[(-2,6)] is a negative rational number and [(0,6)] is a zero rational number.

Note:- $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$.

Definition

(i) Let [(m,n)] ∈ $\mathbb{Q}$, then –[(m,n)]=[(-m,n)].

(ii) Let [(m,n)] ∈ $\mathbb{Q}$, then $[(m,n)]^{-1}$=[(n,m)] provided that [(m,n)]≠ 0.

(iii) Let [(m,n)], [(p,q)] ∈ $\mathbb{Q}$, then

1) $[(m,n)] + [(p,q)] = [(mq + pn, nq)]$.

2) $[(m,n)].[(p,q)] = [(mp, nq)]$.

3) $[(m,n)] - [(p,q)] = [(m,n)] + [(-p,q)]$

4) $[(m,n)] \div [(p,q)] = [(m,n)].[(p,q)]^{-1}, provided\ [(p,q)] \neq 0$.

Theorem: Let x, y, w ∈ $\mathbb{Q}$

1) $x + (y + w) = (x + y) + w$

2) $x + y = y + x$

3) $x.(y + w) = x.y + x.y$

4) $x.(y.w) = (x.y).w$

5) For each $x \in \mathbb{Q} \exists -x \in \mathbb{Q}$ such that $x + (-x) = (-x) + x = 0$

6) $x.1 = 1.x = x$

7) For each $x \in \mathbb{Q} x^{-1} \in \mathbb{Q}$ such that $x.(x^{-1}) = (x^{-1}).x = 1$.

Proof:- 1) Let x=[(m,n)], y=[(p,q)], w=[(r,s)] .

L.H.S= $[(m,n)] + ([(p,q)] + [(r,s)]) \to [(m,n)] + [(ps + rq, qs)]$

$\to [(m(qs) + (ps + rq)n, n(qs)] \to \left[\left((mq)s + pns + rqn, (nq)s\right)\right]$

$\to \left[\left((mq)s + (pn)s + rqn, (qn)s\right)\right] \to \left[\left((mq + pn)s + rqn, (qn)s\right)\right]$

$\to [(mq + pn, qn)] + [(r,s)] \to ([(m,n)] + [(p,q)]) + [(r,s)]$ =R.H.S.

By similar way we can show that 2,3,4,5 and 6 .

Let x=[(m,n)] where m,n∈ ℤ then

–x=[-m,n] ∈ ℚ → $[(m,n)]+[(-m,n)]=[(mn+(-mn),n.n)]=[(0,n.n)]=0.$

Therefore for every x∈ ℚthere exists -x∈ ℚ such that x+(-x)=0.

9) Let x=[(m,n)] where m,n∈ $\mathbb{Z}^*$. Then x^{-1}=[n,m] ∈ ℚ**.**

L.H.S=[(m,n)].[(n,m)]=[(m.n,m.n)]=1=R.H.S

The order relation on rational number

Definition:- Let $[(m,n)],[(p,q)] \in \mathbb{Q}$ then $[(\boldsymbol{m},\boldsymbol{n})]<[(p,q)]$ iff $\boldsymbol{mq}.\boldsymbol{nq} < np.nq$.

Example: [(5,-3)]<[(0,6)] Since (5).(6).(-3).(6)<(-3).(0).(-3).(6) then

(-30).(18)<0. Therefore, $[(5,-3)]<[(0,6)]$.

Theorem: For every $x,y,w \in \mathbb{Q}$

1) $x \nless x$

2) If $x<y \wedge y<w$ $then$ $x<w$.

3) For every rational numbers x and y exactly one of the following holds

$x<y$, $x=y$, $y<x$.

4) If $x<y$ then If $x+w<y+w$

5) If $x<y$ and $w>0$ $then$ $x.w<y.w$.

Proof 1: Let $x=[(m,n)]$, where $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^*$.

Suppose that $x<x$ then $[(m,n)]<[(m,n)]$

$\rightarrow (m.n).(n.n)<(n.m).(n.n)$(Why?) $\rightarrow (m.n).(n.n)<(m.n).(n.n)$ (Why?)

Which is contradiction with theorem [c≮c for every c ∈ ℤ]. Hence $x \nless x$.

2) Let $x=[(m,n)],y=[(p,q)],w=[(r,s)]$, where m,p $r \in \mathbb{Z}$ and n , q , $s \in \mathbb{Z}^*$. Suppose that $x<y$ and $y<w$ then $[(m,n)]<[(p,q)]and$ $[(p,q)]<[(r,s)]$

$\rightarrow (m.q).(n.q)<(n.p).(n.q)$ and $(p.s).(q.s)<(q.r).(q.s)$ (Why?)

$\rightarrow (m.q).(n.q).(s.s)<(n.p).(n.q).(s.s)$ and $(p.s).(q.s).(n.n)<(q.r).(q.s).(n.n)$

$\rightarrow (m.q).(n.q).(s.s)<(q.r).(q.s).(n.n)$(Since $(n.p).(n.q).(s.s)=$ $(p.s).(q.s).(n.n)) \rightarrow (m.s).(n.s).(q.q)<(n.r).(n.s).(q.q)$ (Why?)

$\rightarrow (m.s).(n.s)<(n.r).(n.s)$ (Why?) $\rightarrow [(m,n)]<[(r,s)]$ (Why?). Hence $x<w$.

Chapter six **Construction of Numbers (Part 3)**

Real Numbers, Irrational Numbers and Complex numbers

A Sequence is a list of things (usually numbers) that are in order. When the sequence goes on forever it is called an **infinite sequence**, otherwise it is a **finite sequence**

Examples: {1, 2, 3, 4, ...} is a very simple sequence (and it is an **infinite sequence**)

{20, 25, 30, 35, ...} is also an infinite sequence

{1, 3, 5, 7} is the sequence of the first 4 odd numbers (and is a **finite sequence**)

{4, 3, 2, 1} is 4 to 1 **backwards**

{1, 2, 4, 8, 16, 32, ...} is an infinite sequence where every term doubles

{a, b, c, d, e} is the sequence of the first 5 letters **alphabetically**

{f, r, e, d} is the sequence of letters in the name "fred"

{0, 1, 0, 1, 0, 1, ...} is the sequence of **alternating** 0s and 1s (yes they are in order, it is an alternating order in this case)

When we say the terms are "in order", we are free to define **what order that is**! They could go forwards, backwards ... or they could alternate ... or any type of order we want!

A Sequence is like a Set, except: the terms are **in order** (with Sets the order does not matter)

and the same value can appear many times (only once in Sets)

Example: {0, 1, 0, 1, 0, 1, ...} is the **sequence** of alternating 0s and 1s.

Sequences also use the same **notation** as sets: list each element, separated by a comma, and then put curly brackets around the whole thing.

.

DEFINITION OF A SEQUENCE

A sequence is a set of numbers $u_1, u_2, u_3, \ldots$ in a definite order of arrangement (i.e., a *correspondence* with the natural numbers) and formed according to a definite rule. Each number in the sequence is called a *term*; u_n is called the nth *term*. The sequence is called *finite* or *infinite* according as there are or are not a finite number of terms. The sequence $u_1, u_2, u_3, \ldots$ is also designated briefly by $\{u_n\}$.

EXAMPLES. 1. The set of numbers $2, 7, 12, 17, \ldots, 32$ is a finite sequence; the nth term is given by $u_n = 2 + 5(n-1) = 5n - 3$, $n = 1, 2, \ldots, 7$.

2. The set of numbers $1, 1/3, 1/5, 1/7, \ldots$ is an infinite sequence with nth term $u_n = 1/(2n-1)$, $n = 1, 2, 3, \ldots$.

Unless otherwise specified, we shall consider infinite sequences only.

LIMIT OF A SEQUENCE

A number l is called the *limit* of an infinite sequence $u_1, u_2, u_3, \ldots$ if for any positive number ϵ we can find a positive number N depending on ϵ such that $|u_n - l| < \epsilon$ for all integers $n > N$. In such case we write $\lim_{n\to\infty} u_n = l$.

EXAMPLE . If $u_n = 3 + 1/n = (3n+1)/n$, the sequence is $4, 7/2, 10/3, \ldots$ and we can show that $\lim_{n\to\infty} u_n = 3$.

If the limit of a sequence exists, the sequence is called convergent; otherwise, it is called divergent. A sequence can converge to only one limit, i.e., if a limit exists, it is unique.

Example 1:

1. Consider the sequence $\{4\}$=4, 4, 4, … is converge to 4 since $\forall\varepsilon > 0$ take k=1 then $|4-4| < \varepsilon \forall n > 1$;

2. Consider the sequence $\{\frac{1}{n}\} = 1, \frac{1}{2}, \frac{1}{3}, \ldots$ is convergent to 0 since $\forall\varepsilon > 0, \exists k \in \mathbb{N}$ such that

$|\frac{1}{n} - 0| < \varepsilon, \forall n > k;$

$|\frac{1}{n}| < \varepsilon, \forall n > k$ then $\frac{1}{n} < \varepsilon, \forall n > k$ then $n > \frac{1}{\varepsilon}, \forall n > k$, take k $= [\![\frac{1}{\varepsilon}]\!] + 1$ therefor $|\frac{1}{n} - 0| < \varepsilon, \forall n > [\![\frac{1}{\varepsilon}]\!] + 1.$

Remark:

If a sequence $\{a_n\}$is not convergent then it is called divergent sequence.

For example $\{5n\}$ is a divergent sequence.

THEOREMS ON LIMITS OF SEQUENCES

If $\lim_{n\to\infty} a_n = A$ and $\lim_{n\to\infty} b_n = B$, then

1. $\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n = A + B$
2. $\lim_{n\to\infty}(a_n - b_n) = \lim_{n\to\infty} a_n - \lim_{n\to\infty} b_n = A - B$
3. $\lim_{n\to\infty}(a_n \cdot b_n) = (\lim_{n\to\infty} a_n)(\lim_{n\to\infty} b_n) = AB$

Definition:-

A sequence $\{a_n\}$ called **Cauchy sequence** if $\forall\varepsilon > 0, \exists k \in \mathbb{N}$ such that

$|a_m - a_n| < \varepsilon, \forall m, n > k$.

Definition:

Let the binary relation $\simeq$ be defined on A={$\{x_n\}$; rational Cauchy sequence}

as follows: $(\{x_n\},\{x_n\}) \in \simeq iff \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$. That is the relation $\simeq \subseteq (A \times A)$.

Theorem:-

The relation $\simeq$ is an equivalence relation on A × A.

Example:-

$\left\{\frac{1}{2^n}\right\} \simeq \left\{\frac{1}{3^n}\right\}$, since $\lim_{n\to\infty}\frac{1}{2^n} = \lim_{n\to\infty}\frac{1}{3^n} = 0$.

Remark:

$[\{x_n\}] = \{\{y_n\};\ \{x_n\} \simeq \{y_n\}\} = \{\{y_n\};\ \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n\}$.

Definition: - Let B be the set of all equivalence classes $[\{x_n\}]$ with respect to the equivalence relation $\simeq$, then the set of real numbers $\mathbb{R} = \{a = \lim_{n\to\infty} x_n\ ;\ [\{x_n\}] \in$B$\}$.

The real numbers (axioms)

1) For any $a, b \in \mathbb{R}$,$a + b \in \mathbb{R}$.
2) For any $a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$.
3) For any $a, b \in \mathbb{R}$, $a + b = b + a$.
4) There exists a unique real number (0) such that $a + 0 = 0 + a = a$, for any a$\in \mathbb{R}$.
5) For every $a \in \mathbb{R}$, there exists a unique $(-a) \in \mathbb{R}$. such that

$$a + (-a) = (-a) + a = 0$$

6) For any $a, b \in \mathbb{R}$, $a.b \in \mathbb{R}$.

7) For any $a, b \in \mathbb{R}$, $a.b = b.a$.

8) There exists a unique real number (1) such that $a.1 = 1.a = a$, for any $a \in \mathbb{R}$.

9) For every $a \in \mathbb{R} - \{0\}$, there exists a unique $(1/a) \in \mathbb{R}$. such that $a.(1/a) = (1/a).a = 1$.

10) For any $a, b, c \in \mathbb{R}$, $(a.b).c = a.(b.c)$.

11) For any $a, b, c \in \mathbb{R}$, $a.(b + c) = a.b + a.c$.

<u>Theorem:</u>

For any $a \in \mathbb{R}$, $a.0 = 0$

Proof: $a.0 = a.0 + 0$ $[By\ a + 0 = 0 + a = a]$

$= a.0 + \big(a + (-a)\big)[By\ a + (-a) = (-a) + a = 0]$.

$= (a.0 + a) + (-a)$ $[By\ a + (b + c) = (a + b) + c.]$

$= (a.0 + 1.a) + (-a)$ $[By\ a.1 = a]$

$= a.(0 + 1) + (-a)$ $[By\ a.(b + c) = a.b + a.c]$

$= a.1 + (-a)$ $[By\ a + 0 = a] = a + (-a)[By\ a.1 = a]$.

$= 0.$ $[By\ a + (-a) = (-a) + a = 0]$.

Exercise: For any $a, b, c, d \in \mathbb{R}$ and . $b, d \neq 0$ then $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$.

Irrational Numbers: A real number is irrational if it is not rational for example

$\sqrt{5}$, $\sqrt[4]{7}$, ... $e^2, \pi,$ ...are irrational number.

Complex Number: The system of complex number is the number of ordinary algebra . It is the smallest set in which for example, the equation $x^2=a$ can be solved when a is any element of $\mathbb{R}$. We begin with the product set $\mathbb{R} \times \mathbb{R}$. The binary relation "=" requires $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. Now each of the resulting equivalence classes contains but a single element. Hence, we denote a class as (a, b) and so, hereafter, denote $\mathbb{R} \times \mathbb{R}$ by $\mathbb{C}$. That is $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(x, y)|\ x, y \in \mathbb{R}\}$.

Remark:-

(1) $If\ (x, y) \in \mathbb{C}$ then $x + iy$ where $x, y \in \mathbb{R}$ and $i = \sqrt{-1}$ (2) $i = (0,1)$.

Chapter Seven

Group, Ring, Field

Definition :- Let S be a nonempty set , any function($*$) from cartesian product S×S in to S is called a binary operation . That is $*: S \times S \rightarrow S$ is a function.

Example:- 1)- Let $S = \{1, 2, 3\}$. Then $* : S \times S \rightarrow S$ is a function where $*(a, b) = a$ (Means $a * b = a$). Therefore, $*$ is a binary operation.

2- Usual addition + is a binary operation on the set $\mathbb{Z}$. Since $\mathbb{Z}$ is a non empty set and $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ satisfy function conditions.

Definition:- Anon empty set with one or two binary operations defined on this set is called a mathematical system.

Example:-

1. $(\mathbb{Z}, +, .)$is a mathematical system.
2. If $\mathbb{Z}_o$ ={…,-3, -1, 1, 3, 5,…} then $(\mathbb{Z}_o, +)$is not a mathematical system because 1, 3∈ $\mathbb{Z}$ but 1+3=4 ∉ $\mathbb{Z}$.

Definition:- Let $(S,*)$ be a mathematical system, then $*$ is called associative if and only if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Example:-

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

2) (p(x),∪) is associative.

Definition:- Let $(S,*)$ be a mathematical system, then * is commutative (abelian) if and only if $a * b = b * a$ for each $a, b \in S$.

Example:- 1) $(\mathbb{Z}, -)$ is not commutative 2. $(\mathbb{Z}, +)$ is commutative.

Definition:- Let $(S,*)$ be a mathematical system. The set S have left side identity if there exists an element $e \in S$ such that $e * a = a$ for all $a \in S$. The set S right side identity if there exists an element $e \in S$ such that $e * a = a$ for all $a \in S$. The set S have two side identity if there exists an element $e \in S$ such that $a * e = e * a = a$ for all $a \in S$.

Example:- $(\mathbb{Z}, +)$: 0 is identity element and in ($\mathbb{Z}$,.): 1 is identity element but in (p(x),∪): ∅ is identity element since A∪∅=A

Definition:- A mathematical system $(S,*)$ is said to be semigroup if

$$(a * b) * c = a * (b * c); \ \forall a, b, c \in S.$$

Example: 1 $(\mathbb{Z}, +)$ is a semigroup.

1- If $S = \{1, 2, 3\}$. Then $*$ is a binary operation where $*(a, b) = a$.
   Since $(a * b) * c = a * (b * c)$ therefore, $(S,*)$ is a semigroup.
2- $(\mathbb{Z}, *)$ is not semigroup if $*(a, b) = a + 2b$.

Definition:- A mathematical system (G,*) with the following axioms is said to be a group.

1- $\forall a, b, c \in G, (a * b) * c = a * (b * c)$

2- $\forall a \in G$, there exists $e \in G$ such that $a * e = e * a = a$

3- $\forall$a $\in G$, there exists $a^{-1} \in G$, such that $a*a^{-1}=a^{-1}*a=e$ (a^{-1} inverse element to a)

Example:- $(\mathbb{Z}, +)$ is a group since it has the following properties

1- $(\mathbb{Z}, +)$ is mathematical system
2- $\forall a \in \mathbb{Z}$, there exists $0 \in \mathbb{Z}$ such that $a + 0 = 0 + a = a$
3- $\forall a \in \mathbb{Z}$, there exists $-a \in \mathbb{Z}$, such that $a + (-a) = (-a) + a = 0$.

Remark: Some time we say that a non empty set is a group if it is satisfy four axioms such as closed, associative, identity and inverse.

Example:-

1- A set $S = \{-1, 0, 1\}$ is not closed set under usual addition because $1+1 \notin S$ but it is satisfy associative law, has identity such as o and each element has additive inverse.
2- A set $\mathbb{Z}$ is not satisfy associative law under $-$ because $1 - 3 \notin \mathbb{Z}$ but it is closed, has identity such as o and each element is additive inverse for itself.
3- $(\mathbb{Z}^*, +)$ is semigroup and each element has additive inverse but it has not identity.
4- $(\mathbb{Z}, .)$ is semigroup with identity but it is not group since every element $a \neq 1$ in $\mathbb{Z}$ has not multiplicative inverse.

Definition:-

Let $(S,*)$ be a group, then * is commutative if and only if $a * b = b * a$ for each $a, b \in S$.

Definition:- A mathematical system $(R, +, \times)$ is called a ring if and only if

1- $(R, +)$ is a commutative group;

2- $(R,\times)$ is a semigroup;

3- The distributive law hold in R: i.e for all a, b, c∈R ,

$$a\times(b\ +c)=a\ \times b\ +a\ \times c \quad \text{and} \quad (a\ +b)\times c=\ a\ \times c+\ b\ \times c.$$

Example:-

1- (ℤ,+, .) is a ring. Since

i. (ℤ,+) is commutative group.

ii. (ℤ, .) is semigroup

iii. $\forall a,b,c\in\mathbb{Z},\ a.(b+c)=a.b+a.c.$

2- $(\mathbb{R},+,.)$ is a ring. Since

a) (ℝ,+) is commutative group.

b) (ℝ, .) is semigroup

c) $\forall a,b,c\in\mathbb{R},\ a(b+c)=a.b+a.c.$

Definition:-

A ring $(R,+,\times)$ is commutative ring if $(R,\times)$ is a commutative semigroup. That means $a\times b=b\times a$ for all $a,b\in R$.

Definition:- A ring $(R,+,\times)$ is said to be with identity if $(R,\times)$ is a semigroup with identity. That mean there exists $e\in R$ such that $a.e=e.a=a$.

Example:-$(\mathbb{Z}_e,+,.)$ a ring without identity but is it is a commutative ring.

Example:- :-$(\mathbb{Z}_e,+,.)$ is a ring with identity and commutative ring. Note that $\mathbb{Z}_e=\{\dots,-4,-2,0,2,4,\dots\}$.

Example:-$(M_{2\times2},+,\ .)$: - is anon commutative ring with identity

Example: $(M_{2\times2},+,.)$ where $M_{2\times2}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$ is a non commutative ring without identity.

Definition (field):- A commutative ring with identity whose non zero element has an inverse under multiplication is called field.

Remark: We say $(F,+,.)$ is called a field if it is satisfy the following conditions:

1- $(F,+)$ is a commutative group;

2- $(F^*,.)$ is a commutative group where $F^*=F-\{0\}$

Example: (ℝ,+, .) is a field .

Salahaddin University-Erbil

Foundations of Mathematics II

Course Book

2024 - 2025

First stage- Second semester

College: Education

Department: Mathematics

Academic year: 2024-2025

Academic staff: Dr Hogir Mohammed Yaseen

Email: hogr.yaseen@su.edu.krd

Course Description

Module: Foundations of Mathematics II	**Language : English**
7 ECTS	**Course code : EdM0106**
Academic Year : 2024-2025	**Semester: Fall**
Contact : **e-mail :**hogr.yaseen@su.edu.krd **Tel: (optional)07504154982**	**Keywords: Function, construction of Numbers, Group , ring , Field.**
Teacher's academic profile **1. B.Sc. in Mathematics, 2007, Salahaddin University-Erbil.** **2. M.Sc. in Algebra, 2010, Salahaddin University-Erbil.** **3. PhD, in representation of Lie algebras, University of Leicester 2018.**	
Course Content:	
In this semester, first we study functions and their properties. We use them in the construction of numbers. Next, we explore different types of functions, their properties, and operations such as composition. Following that, we delve into Cardinality and Equivalence of sets. Additionally, we examine finite sets, infinite sets, denumerable sets, countable sets, Cantor sets, and uncountable sets. Afterward, we focus on the construction of numbers. We begin with a historical background of numbers, followed by a step-by-step explanation of numbers through axioms until students grasp the concept of numbers (natural numbers, integers, rational numbers, irrational numbers, real and complex numbers) and understand how they are constructed. Furthermore, we prove some properties related to them. Finally, we study an introduction about group, ring and field.	
Course Objective	
Foundations of mathematics is the study of the basic mathematical concepts (Mathematical logic, set theory, Relation, function, Construction of numbers(Natural Numbers, Integers, Rational Numbers, Irrational Numbers, Real Number, Complex Number), Group, Ring, Field, Cardinality) and how they form hierarchies of more complex structures and concepts, especially the fundamentally important structures that form the language of mathematics. Foundations of mathematics involve studying basic mathematical concepts such as mathematical logic, set theory, relations, functions, and various number systems (natural numbers, integers, rational numbers, etc.). These concepts form hierarchies of more complex structures fundamental to the language of mathematics. The study aims to deepen understanding of these fundamental structures, enhance logical reasoning skills	

through formal logic and proofs, and explore foundational mathematical structures and their properties.

Learning Outcomes

A Foundations of Mathematics I+II course is designed to give students the basic skills and ideas they need for more advanced math. It teaches students how to think logically and learn different types of proof methods, like direct proof, proof by contradiction, and mathematical induction. These skills are important for understanding and creating clear mathematical arguments. Students also learn about set theory, including operations, Venn diagrams, and set identities. These concepts are used in areas such as counting, probability, and logical thinking. The course includes lessons on functions and relations, looking at their properties like injectivity, surjectivity, and bijectivity, and how to represent them in graphs. These topics help students understand how to model real-world situations. Algebra skills are also practiced through working with expressions, solving equations, and learning about basic algebraic structures.

In addition, students improve their ability to read and write mathematical proofs, which helps them think more clearly and make better arguments. This well-rounded approach prepares students to look at problems carefully, build mathematical models, and use these ideas in different areas, helping them develop analytical thinking and problem-solving skills in real-life situations.

By the end of a Foundations of Mathematics I+II course, students should be able to confidently solve various mathematical problems using logical reasoning and proof techniques. They should also be able to read, understand, and create their own mathematical proofs, strengthening their ability to think critically and communicate their ideas clearly.

Students will also be equipped with the ability to apply mathematical concepts in different fields, such as science, engineering, and physics. This course helps build a strong mathematical foundation, preparing students for future studies and real-world applications where precise and logical thinking is important.

References: *

[1] H Behnke, F Bachmann, and Fladt. Fundamentals of mathematics, 1974.
[2] Alan G Hamilton. Numbers, sets and axioms: the apparatus of mathematics. Cambridge University Press, 1982.
[3] Elliott Mendelson. Number systems and the foundations of analysis. Technical report, 1973.
[4] Ian Stewart and David Tall. The foundations of mathematics. OUP Oxford, 2015.
[5] Raymond L Wilder et al. Introduction to the Foundations of Mathematics. Courier Corporation, 2012 [6] اسس الرياضيات جزء الاول والثاني

Type of Teaching: * 2 hours discussion+4 hours theoretical

Different forms of teaching will be used to reach the objectives of these courses to the students: power point presentation for the course outline, head titles, definition, discussion and conclusions. Also, we shall use the blackboard for solving and explaining the examples.

Requirements For Credit Points: * **Modules Course Requirements:**

1. Students have an obligation to arrive on time and remain in the classroom for the duration of scheduled classes and activities.
2. Students have an obligation to write, homework's, tests and final examinations at the times scheduled by the teacher or the College. Students have an obligation to inform themselves of, and respect, College examination procedures.
3. Students have an obligation to show respectful behavior with teacher and their class mates.
4. Electronic/communication devices (including cell phones, mp3 players, etc.) have the effect of disturbing the teacher and other students. All these devices must be turned off and put away. Students who do not observe these rules will be asked to leave the classroom.
5. Midterm exam, report, quiz, H.W and assignments and discussion in class are required.

Grade Distribution: *

The assessment is divided up as follows: 1) Discussion 5 Marks
Report and seminar 5 Marks
Quiz 6 Marks (2 quizzes and each of them is 3 marks)
Assignment and participation 4 Marks
Total is equal to 20 Marks and Midterm tests 20 Marks
2- Final Examination 60 Marks

Weekly Plan

Detail	
Week	**Detail**
1	Introduction to foundations of Mathematics II and Function
2	Some definitions and properties of functions especially domain, codomain, range, injective, surjective, Bijective • Type of functions (Inclusion function, Characteristic function, Polynomial

	function, …), Composition of functions, Inverse of functions
3	Cardinality, Equivalent sets and Finite sets
4	Infinite sets and denumerable sets and some properties of them
5	countable sets, cantor sets and uncountable sets
6	Construction of natural numbers
7	Some properties of natural number
8	Construction of integer numbers
9	Some properties of integer number
10	Review **and Mid-term exam**
11	Construction of rational numbers
12	Construction of irrational numbers
13	Construction of real and complex numbers
14	Basic defines about Group , Ring and Field

Workload

Module* : Foundations of Mathematics II			
This Prerequisite module.			
Detail: 189 /27= 7 ECTS			
Type	**Number**	**Time Factor**	**Total**
Attendance	14	6	84
Report	1	11	11
Mid Term Exam	1	20	20
Seminar	14	1	14
Class work	14	1	14
Discussion	10	1	10
Quiz	4	4	16
Site visit	0	0	0
Final exam	1	20	20
			189