Chapter 2

The Real Number System

2.1 Introduction

The study of the main concepts of real analysis, namely, convergence, continuity, differentiability, integrability, etc., has its basis on an accurately defined number-concept—more specifically, on the concept of the real number system. Our approach, in the present text, is not to give a formal method of construction of real numbers. Instead, we shall exhibit a list of fundamental properties which will characterise the system of real numbers and use these properties in learning the tools of real analysis.

We assume that our student-readers have the initial acquaintance of the primitive systems like the set $\mathbb{N}$ of natural numbers, the set $\mathbb{Z}$ of all integers and the set $\mathbb{Q}$ of all rational numbers (i.e., numbers of the form $\frac{p}{q}$, where p and q are integers, $q \neq 0$). Addition and multiplication of the elements of these sets will be supposed to be known.

Our approach in introducing real number system is, what we call, *axiomatic*: we assume that:

> **There exists an ordered field $\mathbb{R}$ which is complete (i.e., which has the least-upper-bound property). Further, $\mathbb{R}$ contains $\mathbb{Q}$ as subfield. The members of $\mathbb{R}$ are called *real numbers*.**

We shall discuss the existence-statement in considerable details in the following sections.

Richard Dedekind (1831–1916), however, made a completely different approach: He introduced the concept of cut (*Dedekind cut*) of **rational numbers** and thereby generated not only *real rational numbers* but also new type of numbers called *real irrational numbers*. Finally he showed that the section of real numbers does not lead to any further generalisation (**Dedekind's theorem**). (See Appendix at the end of this chapter 2).

Elementary Approx: Natural Numbers—Integers and Rational Numbers

First Approach: We begin with Peano's Axioms: Well ordering Prime. Principle of Mathematical Induction. Introduce Z, the set of all integers and then finally define a rational number as the ratio of two integers where the denominator in different from zero. The totality of all rational numbers form the system Q of rational numbers.

Another Approach: Define a Field—an ordered field. Define Archimedian Property, Density property, Countability Property and *then Q is defined as an ordered field obeying Density property, Archimedian property and Countability property*. Every rational number is then made to correspond to a unique point on a directed line (*Geometrical Representation of Rational Numbers*). What is most important to remember in these two approaches of introducing Rational numbers is that Q *is not order complete* this notion will be explained in due course.

Section I: Natural Numbers, Integers and Rational Numbers

2.2 The Set N of Natural Numbers: Peano's Axioms

We assume familiarity with the set of natural numbers $N = \{1, 2, 3, 4, 5, 6, \cdots\}$, along with the usual arithmetic operations of *addition* and *multiplication* of two natural numbers and with the meaning of one natural number being less than another (*order relation*).

In the following discussions we shall include three important notions:

I. **Peano's axioms** (All the known properties of natural numbers can be shown to be consequences of these axioms).

II. **Well ordering property** of the system N of natural numbers.

III. **Principle of mathematical induction** which is a part of Peano's axioms.

I. **Peano's axioms**: Let N be a set whose members we shall call natural numbers. We take the statements P_1 to P_5 as our axioms (called *Peano's axioms* or *Peano's postulates*):

P1. $1 \in N$; that is, N is a non-empty set and contains an element which we designate as 1.

P2. For each element $n \in N$, there exists a unique element $n' \in N$, called the *successor of n*.

P3. For each element $n \in N$, $n' \neq 1$; that is, 1 is not the successor of any element in N.

P4. For each pair $n, m \in N$, with $n \neq m$, $n' \neq m'$; that is, distinct elements in N have distinct successors.

P5. If (a) $M \subseteq N$; (b) $1 \in M$ and (c) $n \in M \Longrightarrow n' \in M$, then $M = N$.

The last axiom **P5** is known as the **Principle of mathematical induction.** This principle is an important tool in many mathematical proofs. It often appears in the following alternative form:

Alternative form of the principle of mathematical induction:

If $P(n)$ is a *statement*[1] about $n \in N$, then $P(n)$ may be true for some values of n and not true for some other values of n, e.g., let $P(n)$ be the statement '$n^2 = n$'. Then for $n = 1$, $P(1)$ is true, while $P(n)$ is not true for any $n > 1$, $n \in N$.

With above background in mind, we can formulate the principle of mathematical induction in the following language:

For each $n \in N$, let $P(n)$ be some statement about n. Suppose that

1. *$P(1)$ is true.*
2. *For every $k \in N$, if $P(k)$ is true, then $P(k+1)$ is also true.*

Then $P(n)$ is true for all $n \in N$.

Take $M = \{n : n \in N \text{ and } P(n) \text{ is true}\}$. Then $M \subseteq N$. Then the conditions (b) and (c) of **P5** correspond exactly to the conditions (1) and (2) stated above. The conclusion $M = N$ in **P5** corresponds to the conclusion '$P(n)$ is true for all $n \in N$.'

Observation: In (2) the assumption "if $P(k)$ is true" is called the *induction hypothesis*. In establishing (2) *we assume* $P(k)$ to be true and then establish $P(k+1)$ is true. In fact, $P(k)$ may not be true. For example, let $P(k) : k = k + 3$, then (2) is logically correct because we can simply add 1 to both sides of $P(k)$ to obtain $P(k+1)$. However, $P(1)$ is not true (since $1 = 4$ is false). Therefore, we cannot use the principle of mathematical induction to conclude that $n = n + 3$, for all $n \in N$. [See Page 51. Q.4]

A second version of the principle of mathematical induction:

It may happen that the statement $P(n)$ are false for certain natural numbers, but they are true for all $n \geq$ some particular natural number m. The principle of mathematical induction can be suitably modified in such a case. m is the basis in this case.

Statement: *Second version of the principle of mathematical induction:*

Let m be a fixed natural number.

Let $P(n)$ be a statement for each natural number $n \geq m$.

Suppose that

1. *The statement $P(m)$ is true.*

[1] A statement means an expression which has a truth value, i.e., either it is true or false.

2. *For all $k \geq m$, the truth of $P(k)$ implies the truth of $P(k+1)$.*

Then $P(n)$ is true for all $n \geq m$.

We have also another useful form of the principle of mathematical induction known as the *Second Principle of Induction* [see Example 2.3.7, Page 48].

II. Well ordering principle on $\mathbb{N}$: A fundamental property of the system $\mathbb{N}$ of natural numbers is what we call *well-ordering property of* $\mathbb{N}$. It states:

Every non-empty subset of $\mathbb{N}$ has a least element.

This means: If S is a subset of $\mathbb{N}$ and if $S \neq \phi$, then there exists an element $m \in S$ such that $m \leq k$, for all $k \in S$; m is then called the least element of S.

Explanation: 1 is the least element of $\mathbb{N} \subseteq \mathbb{N}$. 2 is the least of $\mathbb{N} - \{1\} \subset \mathbb{N}$ and $1 < 2, 3$ is the least element of $\mathbb{N} - \{1, 2\}$ and $1 < 2 < 3$ etc.

Important Deductions

A. *If we assume the truth of well-ordering principle, the principle of mathematical induction follows:*

The Principle of Mathematical Induction states:

Let M be a subset of the system $\mathbb{N}$ of natural numbers with two conditions:

1. $1 \in M$ and
2. For any $n \in \mathbb{N}$, if $n \in M$, then $(n+1) \in M$.

Then the principle states: $M = \mathbb{N}$.

Proof. Subject to the conditions (1) and (2) we shall prove that $M = N$. Suppose to the contrary that $M \neq \mathbb{N}$. Then the set $F = \mathbb{N} - M$ is not empty. So, by the well-ordering principle F has a least element m (say) (note that $m \in F$ and so $m \notin M$). Now, by hypothesis (1), $1 \in M$, so $m > 1$ (no integer in $\mathbb{N}$ can be < 1). But this implies that $(m-1)$ is a natural number and $m - 1 < m$. Since m is the least natural number such that $m \notin M$, we conclude $(m-1) \in M$.

We now apply condition (2) to the element $m - 1 \in M$. We thus obtain

$$(m-1) + 1 \in M, \quad \text{i.e.,} \quad m \in M.$$

But this statement contradicts the fact that $m \notin M$. This m was obtained on the assumption that F is not empty and by well-ordering principle $m \in F$. The contradiction proves that we cannot accept the assumption. Therefore, we must have F is empty so that $M = \mathbb{N}$

B. We shall now deduce well-ordering principle using the principle of mathematical induction.

Well-ordering Principle States: Every non-empty subset $S \subseteq \mathbb{N}$ has a least element.

Proof. Assume that S is a non-empty subset of $\mathbb{N}$ and suppose that S has no least element. We shall prove that this supposition leads to a contradiction and we can then infer that S has a least element proving the well-ordering principle.

We construct $M \subseteq \mathbb{N}$ such that

$$M = \{x \in \mathbb{N} : x < a \text{ for each } a \in S\}.$$

By the laws of trichotomy, $M \cap S = \phi$. Now, $1 \notin S$; otherwise 1 would be the least element of S. Hence for each $a \in S$, $a > 1$ and so $1 \in M$.

Now assume $p \in M$; then $p < a$ for each $a \in S$. If $p + 1 \in S$, then $p + 1$, which is the first natural number larger than p would be the least element of S, in contradiction to our assumption that S has no least element.

Thus $p + 1 \notin S$ and so $p + 1 < a$ for each $a \in S$.

Hence, $p + 1 \in M$. Thus we get two conditions: $1 \in M$ and $p \in M$ implies $p + 1 \in M$. Hence, by the principle of mathematical induction $M = \mathbb{N}$. But $M \cap S = \phi$ and so $S = \phi$, which is a contradiction. Therefore, S must have a least element.

Conclusion from the two deductions A and B:

Well-ordering principle for the system $\mathbb{N}$ is logically equivalent to the principle of mathematical induction in the sense that any one of them can be deduced, if we assume the other.

2.3 Solved Examples:
(Problems on Principle of Mathematical Induction)

Example 2.3.1. *Prove the formula: For each $n \in \mathbb{N}$, the sum of the first n natural numbers is given by $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.*

Solution: Let S be the set of all $n \in \mathbb{N}$ for which the formula is true. If $n = 1$, then we have $1 = \frac{1 \cdot (1+1)}{2}$ so that $1 \in S$.

Next, we assume that $k \in S$, i.e., we assume that

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

Add $(k+1)$ to both sides; we then obtain

$$(1 + 2 + 3 + \cdots + k) + (k+1) = \frac{k(k+1)}{2} + (k+1)$$
$$= \frac{(k+1)(k+2)}{2} \quad \text{(This is the formula for } n = k+1\text{)}.$$

Thus, if $k \in S$, we have verified $(k+1) \in S$.

Thus $S \subseteq \mathbb{N}$ having two properties: (1) $1 \in S$ and (ii) $k \in S \Longrightarrow (k+1) \in S$.

Consequently, by the principle of mathematical induction we infer that $S = \mathbb{N}$ and hence the formula holds for all $n \in \mathbb{N}$.

Example 2.3.2. *For each $n \in \mathbb{N}$, prove the inequality*

$$1 + \tfrac{1}{4} + \tfrac{1}{9} + \cdots + \tfrac{1}{n^2} \le 2 - \tfrac{1}{n}.$$

[CH 1985]

Solution: Let S be the set of all $n \in \mathbb{N}$ for which the inequality

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \le 2 - \frac{1}{n} \text{ holds.}$$

If $n = 1$, then $\frac{1}{1^2} \le 2 - \frac{1}{1}$ is true so that we write $1 \in S$.

Next we assume that $k \in S$ and we wish to infer from this assumption that $k+1 \in S$.

Thus $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2} \le 2 - \frac{1}{k}$ **(assumed)**

Adding $\frac{1}{(k+1)^2}$, we obtain

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \le 2 - \frac{1}{k} + \frac{1}{(k+1)^2}.$$

Now,

$$\begin{aligned}
2 - \frac{1}{k} + \frac{1}{(k+1)^2} &= 2 - \frac{1}{k+1} + \frac{1}{k+1} - \frac{1}{k} + \frac{1}{(k+1)^2} \\
&= 2 - \frac{1}{k+1} + \frac{k^2 + k - k^2 - 2k - 1 + k}{k(k+1)^2} \\
&= 2 - \frac{1}{k+1} - \frac{1}{k(k+1)^2} \\
&< 2 - \frac{1}{k+1}.
\end{aligned}$$

$$\therefore \quad 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}.$$

Thus, if $k \in S$, then $(k+1) \in S$. We also have $1 \in S$.

$\therefore$ by the principle of mathematical induction $S = \mathbb{N}$, i.e., the inequality holds for all $n \in \mathbb{N}$.

Example 2.3.3. *For each $n \in \mathbb{N}$, the sum of the squares of the first n natural numbers is given by the formula*

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution: To establish this formula, we see that it is true for $n = 1$, since

$$1^2 = \frac{1 \cdot (1+1)(2.1+1)}{6}.$$

If we assume that it is true for $n = k$, then

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Then adding $(k+1)^2$ to both sides, we obtain

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{1}{6}(k+1)\,[k(2k+1) + 6(k+1)] \\
&= \frac{1}{6}(k+1)\,(2k^2 + 7k + 6) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3),
\end{aligned}$$

i.e., the formula is valid for $n = k+1$, if we assume it to be true for $n = k$ and we have already proved that the formula is valid for $n = 1$.

Consequently, the formula is valid for all $n \in \mathbb{N}$ (by the principle of mathematical induction).

Example 2.3.4. *Prove, by induction for each $n \ge 2$, $(n+1)! > 2^n$.*

Solution: The inequality holds for $n = 2$, since $(2+1)! > 2^2$.

We assume that the inequality holds for some natural number $k \ge 2$. Then

$$(k+1)! > 2^k. \tag{1}$$

Now,

$$\begin{aligned}
(k+2)! &= (k+2)\,\{(k+1)!\} > (k+2)2^k, \quad \text{by (1)} \\
&> 2 \cdot 2^k \quad (\because\ k+2 > 2),
\end{aligned}$$

i.e., $(k+2)! > 2^{k+1}$, i.e., $(\overline{k+1}+1)! > 2^{k+1}$

$\therefore$ the inequality holds for $n = k+1$, if we assume it to be true for $n = k$ $(k \ge 2)$.

$\therefore$ by the principle of induction, the inequality holds for all natural numbers $n \ge 2$.

Note: The inequality is not true for $n = 1$. So we start with the basis $n = 2$.

Example 2.3.5. *The inequality $2^n > 2n + 1$ is not true for $n = 1, 2$, but it is true for $n = 3$. We take the basis $n = 3$. We can easily prove that $2^n > 2n + 1$, for all $n \in \mathbb{N}$, where $n \ge 3$.*

Example 2.3.6. *Given two positive real numbers x and y : prove by induction that $x-y$ is a factor of $x^n - y^n$ for all natural numbers n.*

Solution: The statement is true for $n = 1$. If we now assume that $x - y$ is a factor of $x^k - y^k (k \geq 1)$, then

$$x^{k+1} - y^{k+1} = x^{k+1} - xy^k + xy^k - y^{k+1}$$
$$= x\left(x^k - y^k\right) + y^k(x-y).$$

By our assumption, $x - y$ is a factor of $(x^k - y^k)$ and clearly $x - y$ is a factor of $y^k(x-y)$.

$\therefore$ $x-y$ is a factor of $x^{k+1} - y^{k+1}$ (whenever $x - y$ is a factor of $x^k - y^k$).

$\therefore$ it follows from the principle of mathematical induction that $x - y$ is a factor of

$$x^n - y^n \text{ for all } n \in \mathbb{N}.$$

As a particular case, see that $11^n - 4^n$ is divisible by $11 - 4 = 7$ for all $n \in \mathbb{N}$.

Example 2.3.7. ***Principle of strong induction (also known as second principle of mathematical induction).***

Let S be a subset of $\mathbb{N}$ such that

(a) $1 \in S$ *and*

(b) *If for every $k \in \mathbb{N}$,*

$\{1, 2, 3, \cdots, k\} \subset S$, *then* $k + 1 \in S$.

Then $S = \mathbb{N}$.

Proof. Let $F = \mathbb{N} - S$. To prove $F = \phi$.

If $F \neq \phi$, then by well-ordering principle, F will have a least element m (say).

Since $1 \in S$, $1 \notin F$.

As m is the least element of F and $1 \notin F$, $m > 1$.

All natural numbers $1, 2, \cdots, m-1$ (less than m) belong to S.

Then, by hypothesis (b), $m \in S$ which implies $m \notin F$. This is a contradiction. Hence we infer $F = \phi$, i.e., $S = \mathbb{N}$. This proves the second principle of mathematical induction.

Use this principle to prove that for all $n \in \mathbb{N}$, $\left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$ is an even integer.

Proof. The statement is clearly true for $n = 1$.

$$\left(\because (3+\sqrt{5})^1 + (3-\sqrt{5})^1 = 6 = \text{an even integer}\right)$$

Let us assume that the statement is true for $n = 1, 2, 3, \cdots, k$.

Then

$$\left(3+\sqrt{5}\right)^{k+1} + \left(3-\sqrt{5}\right)^{k+1} = a^{k+1} + b^{k+1} \ \left(\text{where } a = 3+\sqrt{5} \text{ and } b = 3-\sqrt{5}\right)$$
$$= \left(a^k + b^k\right)(a+b) - a^k b - b^k a$$
$$= \left(a^k + b^k\right)(a+b) - ab\left(a^{k-1} + b^{k-1}\right)$$
$$= 6\left(a^k + b^k\right) - 4\left(a^{k-1} + b^{k-1}\right) \ (\because a + b = 6, ab = 4).$$

This is an even integer because $a^k + b^k$ and $a^{k-1} + b^{k-1}$ are even integers (by assumption). Hence the statement for $n = k + 1$ is true whenever it is true for $n = 1, 2, 3, \cdots, k$.

$\therefore$ by the second principle of induction, the statement is true for all $n \in \mathbb{N}$.

On Principle of Mathematical Induction
Exercises for Self-Practice

Q1. Use the principle of mathematical induction to prove that for every natural number n,

(i) $2^n < n!$ for all $n \in \mathbb{N}$, $n \geq 4$. **[CH 1995]**

(ii) $10^{n+1} + 10^n + 1$ is divisible by 3.

(iii) $2^{n+1} < 1 + (n+1)2^n$ for all natural numbers $n \geq 1$.

(iv) $n^2 < n!$ for all natural numbers $n \geq 4$.

(v) $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n+1}n^2 = (-1)^{n+1}\dfrac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

(vi) $\dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{3}} + \cdots + \dfrac{1}{\sqrt{n}} > \sqrt{n}$ for all $n \in \mathbb{N}$.

$\left[\textit{Hints}: \sqrt{k} + \dfrac{1}{\sqrt{k+1}} = \dfrac{\sqrt{k}\sqrt{k+1}+1}{\sqrt{k+1}} > \dfrac{k+1}{\sqrt{k+1}}, \text{ i.e., } > \sqrt{k+1}.\right]$

(vii) $n^3 + 5n$ is divisible by 6 for all $n \in \mathbb{N}$.

[*Hints:* $(k+1)^3 + 5(k+1) = (k^3 + 5k) + 3k(k+1) + 6$ and $k(k+1)$ is always even.]

(viii) $\dfrac{1}{2} + \dfrac{1}{2^2} + \cdots + \dfrac{1}{2^n} = 1 - \dfrac{1}{2^n}$, for all $n \in \mathbb{N}$.

(ix) Suggest a formula for the sum of first n odd natural numbers

$$1 + 3 + 5 + \cdots + (2n-1)$$

and establish your conjecture by using mathematical induction.

2.5 Rational Numbers and their Main Properties

A number of the form $\frac{p}{q}$, when p, q are integers and $q \neq 0$ is called a rational number. The totality of all rational numbers forms a system called the system $\mathbb{Q}$ of rational numbers. In general, we shall take q to be a positive integer, i.e., $q \in \mathbb{N}$. With this understanding, $\frac{p}{q}$ is a positive rational number, if p is a positive integer, and $\frac{p}{q}$ is a negative rational number, if p is a negative integer. However, if $p = 0$, then the rational number $\frac{0}{q} = 0$ (zero of the rational number system). Taking $q = 1$, it can be easily seen that the set $\mathbb{Z}$ of all integers is a proper subset of $\mathbb{Q}$, i.e., $\mathbb{Z} \subset \mathbb{Q}$.

The system $\mathbb{Q}$: based on its Fundamental properties

We list below the main properties of the system $\mathbb{Q}$ of rational numbers:

I. The system $\mathbb{Q}$ forms an **ordered field.** (i.e., $\mathbb{Q}$ forms a field in which an order relation is defined).

II. The system $\mathbb{Q}$ is *dense* as well as *Archimedean.*

III. Any member of $\mathbb{Q}$ can be expressed as a *decimal* which is either terminating (e.g., $\frac{11}{4} = 2.75$) or recurring (e.g., $\frac{1}{3} = 0.\dot{3} = 0.333\cdots$).

IV. The system $\mathbb{Q}$ is *countably infinite*, i.e., $\mathbb{Q}$ can be put in one-one correspondence with the infinite set $\mathbb{N}$ of natural numbers. A set which is either finite or countably infinite is called a countable set. Therefore, Q is a *countable set.*

V. Every rational number r can be made to correspond to a point on a *directed line* but the converse is not true, i.e., every point on a directed line may not correspond to a rational number. This indicates that there are gaps between rational numbers (these gaps give rise to the existence of irrational numbers).

VI. $\mathbb{Q}$ is *unbounded,* both above and below.

VII. Lastly, the system $\mathbb{Q}$ is *not order-complete* (In other words, $\mathbb{Q}$ does no obey LUB-property)

We have, in the aforesaid list of properties of rational numbers, used certain terms which require clarification.

We begin with the first property:

Property I of Rational Numbers: The system $\mathbb{Q}$ of all rational numbers forms an ordered field.

1. What is a field?

A field is a non-empty set F in which two operators, called *addition* (+) and *multiplication* ($\cdot$), are defined and they satisfy the following axioms, known as *field axioms.*

A. Field axioms for addition:

A1. Closure property: If $x \in F$, $y \in F$, then their sum $x + y \in F$.

A2. Associative property: $(x + y) + z = x + (y + z)$, for all $x, y, z \in F$.

A3. Commutative property: $x + y = y + x$, for all $x, y \in F$.

A4. Existence of additive identity: $\exists$ a unique element 0 (zero), called *additive identity,* such that $0 + x = x + 0 = x$, for every $x \in F$.

A5. Existence of additive inverse: To every $x \in F$ corresponds an element $-x \in F$ (called *additive inverse* of x **or** *negative of* x) such that: $x + (-x) = (-x) + x = 0$.

In short, **under addition F is an Abelian group.**

M. Field axioms for multiplication:

M1. Closure property: If $x \in F$ and $y \in F$, then their product $x \cdot y \in F$ (in place of $x \cdot y$ we may write xy).

M2. Associative property: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, or all $x, y, z \in F$.

M3. Commutative property: $x \cdot y = y \cdot x$, for all $x, y \in F$.

M4. Existence of multiplicative identity: $\exists$ a unique element $1 \neq 0$ such that $1 \cdot x = x \cdot 1 = x$, for all $x \in F$.

M5. Existence of multiplicative inverse for a non-zero element of F: For every $x \in F$, $x \neq 0$, $\exists$ an element x^{-1} (or $\frac{1}{x}$) $\in$ **F** such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

(Note that multiplicative inverse exists for **any non-zero element** of F but additive inverse exists **for every element** of F.)

D. The distributive property: If x, y, z be three elements of F, then

$x \cdot (y + z) = x \cdot y + x \cdot z$ **(Left Distributive Law)**

$(y + z) \cdot x = y \cdot x + z \cdot x$ **(Right Distributive Law).**

(Because of commutative property, any one can be taken as an axiom—the other clearly follows).

2. What is an ordered field?

In order to understand the meaning of 'ordered field' we first define an **ordered set.**

Order: Let S be a set. An **order** on S is a **relation** (denoted by '<', read as 'less than') with the following two properties:

(i) **Trichotomy:** For any two elements $x, y \in S$, either $x < y$ or $x = y$ or $y < x$.

(ii) **Transitivity:** For any three elements $x, y, z \in S$, $x < y$ and $y < z \Longrightarrow x < z$.

[$x < y$ may be read as 'x is less than y' or 'x precedes y'. We shall write $y > x$ to mean $x < y$ (read: $y > x$ as 'y is greater than x'). The notation $x \leq y \Longrightarrow x < y$ or $x = y$]

Ordered Set: An ordered set is a set S in which an order is defined.

Ordered Field: A field F is called an *ordered field*, if:

(i) F obeys all the field axioms: $A_1 - A_5$, $M_1 - M_5$ and D. (We often say that F has an **algebraic structure.**)

(ii) F is an ordered set (an order relation '$<$' is defined on F obeying **Trichotomy** and **Transitivity** and the two compatibility conditions namely

(iii) If $x, y, z \in F$ and $y < z$, then $x + y < x + z$ **(Addition composition)**

(iv) If $x, y \in F$ with $x < y$ and $z > 0$, then $xz < yz$ **(Multiplication composition)**

Property I of Rational Numbers:

The set $\mathbb{Q}$ of all rational numbers forms an ordered field.

We define **addition** and **multiplication** of two rational numbers $\frac{p}{q}$ and $\frac{r}{s}$ in the following way:

Addition: $\dfrac{p}{q} + \dfrac{r}{s} = \dfrac{ps + qr}{qs}$ $\quad (qs \neq 0$ as $q \neq 0$ and $s \neq 0)$

Multiplication: $\dfrac{p}{q} \cdot \dfrac{r}{s} = \dfrac{p \cdot r}{q \cdot s}$ $\left(\text{or we write } \dfrac{pr}{qs}\right)$.

With these definitions we can verify that all the field axioms for addition and multiplication along with the distributive properties are satisfied. Hence $\mathbb{Q}$ is a field.

[**As a sample,** we prove the **associative property for addition:** We take three rational numbers $\frac{p}{q}$, $\frac{r}{s}$ and $\frac{t}{u}$.

$$\frac{p}{q} + \left(\frac{r}{s} + \frac{t}{u}\right) = \frac{p}{q} + \left(\frac{ru + st}{su}\right) = \frac{psu + qru + qst}{qsu}$$

$(qsu \neq 0$ as $q \neq 0, s \neq 0$ and $u \neq 0)$

Again,
$$\left(\frac{p}{q} + \frac{r}{s}\right) + \frac{t}{u} = \frac{ps + qr}{qs} + \frac{t}{u} = \frac{psu + qru + qst}{qsu}$$

$$\therefore \quad \frac{p}{q} + \left(\frac{r}{s} + \frac{t}{u}\right) = \left(\frac{p}{q} + \frac{r}{s}\right) + \frac{t}{u}.]$$

Now **we define an order on** $\mathbb{Q}$: If $a, b \in \mathbb{Q}$, then $a < b$, if $b - a$ is a positive rational number. Now we observe that Law of Trichotomy and Law of Transitivity both hold.

[We verify law of transitivity: $a < b \Longrightarrow b - a$ is a positive rational number

$b < c \Longrightarrow c - b$ is a positive rational number.

$\therefore$ **the sum $(b - a) + (c - b)$ must be a positive rational number, i.e., $c - a$ is a positive** rational number, i.e., $a < c$.]

Remember: If a is a positive rational number, then we write $a > 0$ and if a is a negative rational number, then we write $a < 0$.

Now check the two compatibility conditions:

$a < b \Longrightarrow a + c < b + c$, $\quad$ for all $a, b, c \in \mathbb{Q}$

$a < b$ and $c > 0 \Longrightarrow ac < bc$, $\quad$ for all $a, b \in \mathbb{Q}$ and $c > 0$.

Thus we have established that:

> The system of rational numbers $\mathbb{Q}$ is a field and this field is an ordered field (order being defined as $r < s$, if $s - r$ is a positive rational number).

Property II of Rational numbers:

The system $\mathbb{Q}$ of rational number is dense as well as Archimedean.

A. $\mathbb{Q}$ is a dense set: By this we mean that between any two unequal rational numbers a and b $(a \neq b)$, there exist infinitely many rational numbers.

Since $a \neq b$, by the law of trichotomy **either** $a < b$ or $b < a$.

Let us take the case $a < b$. Then $\exists$ a **rational number** $c = \frac{a+b}{2}$.

We prove: $a < c < b$.

For, $a < b \Longrightarrow a + b < b + b$ $\quad$ **(by compatibility condition)**

$\Longrightarrow \frac{a+b}{2} < b$, i.e., $c < b$.

Again, $a < b \Longrightarrow a + a < b + a$ $\quad$ **(by compatibility condition)**

$\Longrightarrow a < \frac{b+a}{2}$ or $a < c$.

$\therefore$ it follows $a < c < b$.

Now we see that *existence of one rational number c between a and b*

$\Longrightarrow$ *existence of infinite number of rational numbers between them.*

[$c = \frac{a+b}{2}$ lies between a and b; also $d = \frac{a+c}{2}$ lies between a and c and $e = \frac{c+b}{2}$ lies between c and b and so on. Thus we may obtain infinitely many rational numbers between a and b]

Thus we have established that $\mathbb{Q}$ is a dense set.

B. $\mathbb{Q}$ is Archimedean: *Statement:* If $a, b \in \mathbb{Q}$ and $a > 0$, then there exists a natural number n such that $na > b$. **[CH 1985]**

Proof. When $(b < 0)$ or $(b > 0$ and $a > b)$, the results holds for $n = 1$. Now, we consider $b > 0$ and $a < b$. Let $a = \frac{p}{q}$ and $b = \frac{r}{s}$, where $p, q, r, s \in \mathbb{N}$ (a **and** b **are given** to be two positive rational numbers).

We assert that the natural number $n = qr + 1$ will serve our purpose; because

$$na = (qr+1)\frac{p}{q} = pr + \frac{p}{q} > pr \geq r \geq \frac{r}{s} = b.$$

So we find some n, namely $n = qr + 1$ such that $na > b$.

The existence of n is assured by these arguments.

An alternative proof (A proof by contradiction): Suppose, on the contrary, Q is non-Archimedean, i.e., if a and b are positive rational numbers and $a < b$, then there **exists no natural number** n such that $na > b$.

This implies that for all $n \in \mathbb{N}$, $na \leq b$.

Now, $na \leq b \Longrightarrow na \cdot b^{-1} \leq b \cdot b^{-1}$ (b^{-1} is the multiplicative inverse of b)

$\Longrightarrow (na) \cdot b^{-1} \leq 1 < m$, where m is any natural number other than 1

Thus the assumption $na \leq b$ implies $(na) \cdot b^{-1} < m \Longrightarrow \frac{n}{m} < \frac{b}{a}$.

But $\frac{b}{a}$ is a fixed rational number and $\frac{n}{m}$ is any arbitrary positive rational number. Thus we have arrived at the following conclusion:

> **Any arbitrary positive rational number < a fixed rational number,** which is clearly **not true.** Thus we arrive at a contradiction. Hence we cannot assume that Q is non-Archimedean.

In other words, Q **must possess the Archimedean property.**

Property III of Rational numbers: *Decimal representation of a rational number.*

Any member of Q is either a *Terminating Decimal* or a *Recurring Decimal* (also called a *Periodic Decimal*).

The rational fraction $\frac{a}{b}$ can be expressed as a decimal by *long division.* If the denominator b contains no prime factors other than 2 or 5, the decimal for $\frac{a}{b}$ will *terminate*. Otherwise, the decimal will be *recurring* or *periodic*, i.e., eventually a group of digits will repeat without end.

This is clear from the process of long division of a by b; for after the digits in a have been exhausted and zeros are carried down, only the $b-1$ remainders of b can appear. After at most $b-1$ divisions, a remainder r will appear for a second time and thereafter all remainders will repeat infinitely in the same order.

If there are $n(< b)$ different remainders $r_1, r_2, \cdots, r_n$ and

$$10r_i = ba_i + r_i + 1 \quad (i = 1, 2, 3, \cdots, n), \quad r_{n+1} = r_1,$$

then the period of $\frac{a}{b}$ will consist of the digits $a_1, a_2, \cdots, a_n$.

For example, $\frac{1}{3} = 0.3333\cdots = 0 \cdot \dot{3}$, $\frac{1}{5} = 0 \cdot 2\dot{0}$, $\frac{1}{7} = 0 \cdot \dot{1}4285\dot{7}\cdots$ the dots above marking the period (the digit 0 is the period of terminating decimal).

Conversely, a periodic decimal is an infinite geometric series whose sum to infinity is a rational fraction of the form $\frac{a}{b}$, e.g.,

$$0 \cdot \dot{1}\dot{8} = \frac{18}{100} + \frac{18}{10000} + \cdots = \frac{0.18}{1 - 0.01} = \frac{0.18}{0.99} = \frac{2}{11}.$$

Property IV. The system Q of all rational numbers is countably infinite.

Definition 1. Countable and Uncountable sets

A set S is called *countably infinite* (or *denumerable* or *enumerable*) set if there exists a one-to-one function f which maps $\mathbb{N}$ **onto** S. We then write

$$S \sim \{1, 2, 3, \ldots, n, \ldots\}$$

(S is *equinumerous* or *equivalent* to the set $\mathbb{N}$ of natural numbers)

In this case $\exists$ *a function* f *which establishes a one-to-one correspondence between natural number and the elements of the set* S*. Hence* S *can be displayed thus:*

$$S = \{f(1), f(2), f(3), \ldots\}$$

$$\text{or} \quad S = \{a_1, a_2, a_3, \ldots\}$$

where $f(k)$ is denoted by a_k.

A countably infinite set is said to have a **Cardinal number** $\mathcal{N}_0$ (read: *aleph nought*)

Definition 2. A set S is said to be countable (or *at most countable*), if it is either a finite set or it is a countably infinite set.

A set which is not countable is called *uncountable*. The terms *denumerable* (or *enumerable*) and *nondenumerable* (or *non-enumerable*) are used in place of *countable* and *uncountable respectively*.

Summary

1. A set S is said to be *denumerable* or *countably infinite* if there exists a one-to-one function f which maps $\mathbb{N}$ onto S, i.e., if $S \sim \mathbb{N}$.
2. A set S is said to be *countable* (or *at most countable*) if it is either *finite* or *countably infinite*.

   Thus S is countable if there exists a one-to-one function f from $\mathbb{N}$ onto S. The elements of S are then the images of $\{1, 2, 3, \cdots\}$ which we can write as

   $$S = \{f(1), f(2), f(3), \cdots\} \quad \text{or,} \quad \{a_1, a_2, a_3, \cdots\}.$$

3. S is said to be *uncountable if it is not countable.*

Examples on Countability

Example 2.5.1. *Let E be the set of all possible even positive integers. Then E is countably infinite and hence countable. The function $f : \mathbb{N} \longrightarrow E$ defined by* $\boldsymbol{f(n) = 2n}$ *for each $n \in \mathbb{N}$ gives the one-to-one correspondence. Hence, $E \sim \mathbb{N}$ and therefore, E is countably infinite. See the pictorial representation given below:*

$$\begin{array}{cccccccc} \mathbb{N} & 1 & 2 & 3 & 4 & \cdots & n & \cdots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ E & 2 & 4 & 6 & 8 & \cdots & 2n & \cdots \end{array}$$

Example 2.5.2. *The set $\mathbb{Z}$ of all integers is countable. The required one-to-one correspondence $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is*

$$f(n) = \frac{n-1}{2} \quad (n = 1, 3, 5, \cdots)$$
$$= -\frac{n}{2} \quad (n = 2, 4, 6, \cdots).$$

Pictorial representation is the following:

$$\begin{array}{cccccccccc} \mathbb{N} & 1 & 2 & 3 & 4 & \cdots & 2n & , & 2n+1 & \cdots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & & \updownarrow & \\ \mathbb{Z} & 0 & -1 & 1 & -2 & \cdots & -n & , & n & \cdots \end{array}$$

Important results on countable sets because of its special importance have been given separately in Chapter 3A. Three such results are given below:

I. Every infinite set has a denumerable subset.

II. Let $A_1, A_2, A_3, \ldots$ be a sequence of countable sets then their union $\bigcup_{n=1}^{\infty} A_n$ is countable.

With these results in mind one can prove **Property IV of rational numbers mentioned earlier:**

Property IV of Rational Numbers: The set $\mathbb{Q}$ of all rational numbers is countably infinite and hence $\mathbb{Q}$ is a countable set. **[C.H. 2006]**

Proof. Let E_n be the set of all rational numbers which can be written with denominator n. Then the set $\mathbb{Q}$ of all rational numbers is $\bigcap_{n=1}^{\infty} E_n$. Now consider

$$E_n = \left\{\frac{0}{n}, -\frac{1}{n}, +\frac{1}{n}, -\frac{2}{n}, +\frac{2}{n}, -\frac{3}{n}, +\frac{3}{n}, \cdots\right\}$$
$$= \left\{\frac{0}{n} = 0\right\} \cup \left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots\right\} \cup \left\{-\frac{1}{n}, -\frac{2}{n}, -\frac{3}{n}, \cdots\right\}$$

i.e., E_n is the union of three countable sets and hence their union is countable. E_n being a countable set for each n, by the same theorem, $\bigcup_{n=1}^{\infty} E_n$ is countable, i.e., $\mathbb{Q}$ itself is countable.

III. Suppose A and B are two infinite sets such that $B \subseteq A$ (or $A \supseteq B$).

(a) An infinite subset B of a countable set A is countable;

(b) If B is an uncountable set, then A is also an uncountable set.

Proof. Let $A = \{a_1, a_2, a_3, \cdots\}$ be a countable set and let B be an infinite subset of A. We have to prove that B is countable. From the hypothesis, each element of B is some a_j.

Let n_1 be smallest subscript for which $a_{n_1} \in B$.

Let n_2 be the least positive integer such that $n_2 > n_1$ and $a_{n_2} \in B$, and so on.

Then $B = \{a_{n_1}, a_{n_2}, \cdots\}$.

Since the set $\{n_1, n_2, n_3, \cdots\}$ is countable, $\{a_{n_1}, a_{n_2}, \cdots\}$ is countable, i.e., B is countable.

As a corollary see that **the set of all rational numbers in $[0, 1]$ is countable** (because the set of rational numbers in $[0, 1]$ is an **infinite subset** of the countable set of all rational numbers).

Property IV of Rational Numbers, namely set $\mathbb{Q}$ of all rational numbers is countable, can also be proved if we proceed in the following way:

First step. We prove that the Cartesian product $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. We have $\mathbb{N} \times \mathbb{N} = \{(a, b)/a, b \in \mathbb{N}\}$.

First consider all the ordered pairs (a, b) such that $a + b = 2$. There is only one such pair, namely $(1, 1)$.

Next consider all the ordered pairs with $a + b = 3$.

In this case we have $(1, 2)$ and $(2, 1)$.

All the ordered pairs (a, b) with sum $a + b = 4$ are $(3, 1), (2, 2), (1, 3)$.

Proceeding in this manner, all the elements of $\mathbb{N} \times \mathbb{N}$ are written as $(1, 1)$, $(1, 2)$, $(2, 1)$, $(3, 1)$, $(2, 2)$, $(1, 3)$, $\cdots$

This set contains every ordered pair belonging to $\mathbb{N} \times \mathbb{N}$.

Starting from $(1, 1)$, we can enumerate them as $1, 2, 3, 4, \cdots$. Hence, $\mathbb{N} \times \mathbb{N}$ is co... able.

Second step. Let $\mathbb{Q}^+$ be the set of all positive rational numbers and $\mathbb{Q}^-$ be the s... of all negative rational numbers.

Then, $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$ is the set of all rational numbers.

Let $\frac{p}{q} \in \mathbb{Q}^+$. Define $f : \mathbb{Q}^+ \longrightarrow \mathbb{N} \times \mathbb{N}$ by the rule $f(\frac{p}{q}) = (p, q)$.

It is easy to see that f is one-to-one and $\mathbb{Q}^+$ is equivalent to a subset of $\mathbb{N} \times \mathbb{N}$.

Since $\mathbb{N} \times \mathbb{N}$ is countable, $\mathbb{Q}^+$ being an infinite subset of $\mathbb{N} \times \mathbb{N}$ is countable. In similar manner $\mathbb{Q}^-$ is countable. Hence $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$ is countable.

Note: One may prove that the set $\mathbb{Z}$ of all integers is countable, thus:

If $\mathbb{N}$ is the set of all natural numbers, then let $(-\mathbb{N}) = \{-1, -2, -3, -4, \cdots\}$. Hence we have

$$\mathbb{Z} = (-\mathbb{N}) \cup \{0\} \cup \mathbb{N}.$$

Since $-\mathbb{N}$ is countable, $\mathbb{Z}$ is the union of countable sets. Hence, $\mathbb{Z}$ is countable.

Property V of Rational Numbers (Geometric representation of rational numbers)

This property asserts that *to every rational number there corresponds a unique point on a directed line.* Is the converse true? Does every point on the line represents a rational number? The answer is no. We shall show that there are points on the line which do not represent rational numbers. But before that we explain how a given rational number corresponds to a unique point on a directed line.

We take a directed line—a line in which a direction (positive or negative) is indicated. The positive sense is indicated by an arrow (Fig 2.5.1). Points 0 and 1 are chosen arbitrarily on this line.

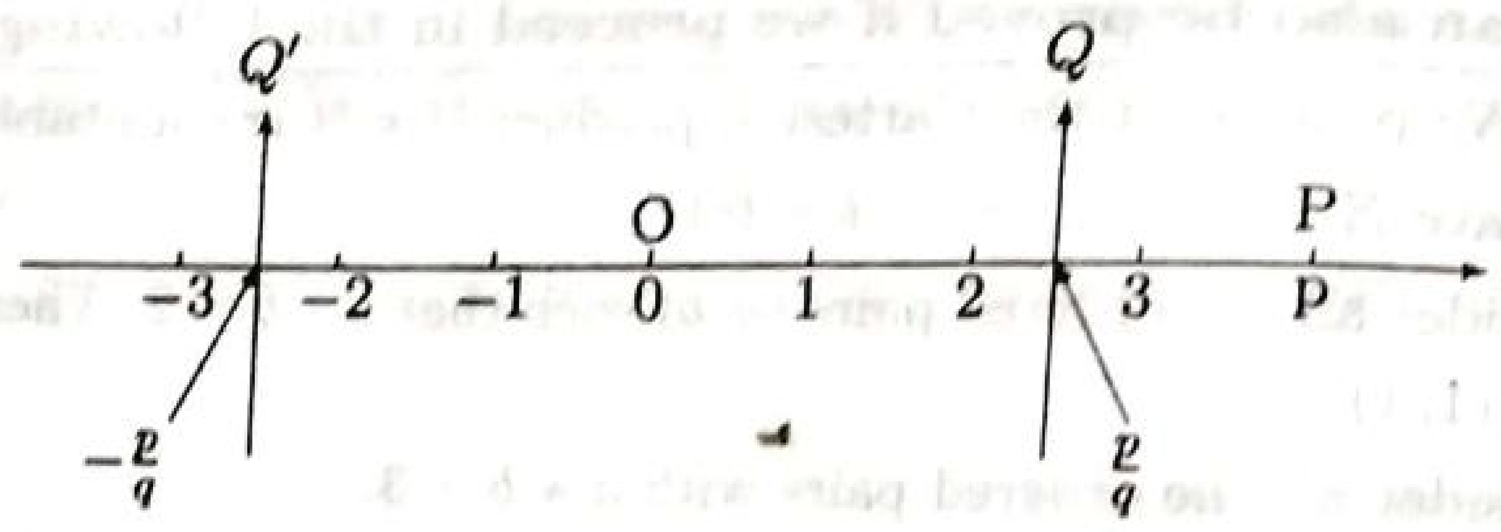

Fig 2.5.1

Then integers $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ are represented by an endless set of equidistant points.

To represent a positive rational number $\frac{p}{q}$ (p and q are both positive integers), we first represent the positive integer p by the point P on the line on the right side of O (length of $OP = p$ times the length from 0 to 1).

Next divide the length OP into q equal parts. The portion OQ representing the first of these q equal parts (or the point Q) represents the rational number $\frac{p}{q}$. A symmetric point Q' on the left of O represents the negative rational number $-\frac{p}{q}$ (p is also a positive integer and q is also a positive integer). Thus for each rational number $\frac{p}{q}$ we obtain a unique point on the line.

Examples showing the existence of numbers other than rational numbers

Example 2.5.3. *We define $\sqrt{2}$ as that number x whose square $x^2 = 2$. Prove that $\sqrt{2}$ is not a rational number.*

Proof. (by contradiction) Assume that there exists a rational number x such that $x^2 = 2$. Then x is of the form $\frac{p}{q}$, where p, q are integers, $q \neq 0$ and let p, q are in their lowest terms, i.e., there is no common factor other than 1 between p and q. This assumption can be made without any loss of generality.

Then $x^2 = 2 \Longrightarrow (\frac{p}{q})^2 = 2$ or, $p^2 = 2q^2$ which implies that p^2 is an even integer and hence p is an even integer (since the square of an odd integer is always odd).

Let $p = 2m$. Then $p^2 = 2q^2$ gives $(2m)^2 = 2q^2$ or $q^2 = 2m^2$.

$\therefore$ q^2 is an even integer and hence q is even.

Thus the assumption that x is rational of the form $\frac{p}{q}$ leads to the conclusion that p and q have a common factor 2, which is contrary to our hypothesis that p and q have no common factor other than 1. The contradiction proves that x must not be a rational number, i.e., there exists no rational number which satisfies $x^2 = 2$.

A more general problem is the following:

Example 2.5.4. *Show that no positive integer m other than a square number* (like 4, 9, 16, 25, 49, *etc.*) *has a square root within the system $\mathbb{Q}$ of rational numbers.*

[CH 1984, 1989]

Solution: To prove that $\exists$ no rational number x such that $x^2 = m$ where m is a non-square positive integer. Suppose to the contrary $\exists$ a rational number x satisfying $x^2 = m$. Then such an x can be written as $\frac{p}{q}$, where p and q are both integers, $q \neq 0$ and let p, q are in their lowest terms.

Then $x^2 = m \Longrightarrow (\frac{p}{q})^2 = m$, i.e., $p^2 = mq^2$.

Corresponding to the positive integer m we can find a positive integer n ...

$$
\begin{aligned}
n^2 &< m &&< (n+1)^2 \\
\text{or, } n^2 &< \left(\frac{p}{q}\right)^2 &&< (n+1)^2 \\
\text{or, } n^2q^2 &< p^2 &&< \{(n+1)q\}^2 \\
\text{or, } nq &< p &&< (n+1)q \\
\text{or, } 0 &< p - nq < q.
\end{aligned}
$$

We next consider

$$
\begin{aligned}
(mq - np)^2 &= m^2q^2 - 2mnpq + n^2p^2 \\
&= m\left(mq^2\right) - 2mnpq + n^2\left(mq^2\right) \\
&= mp^2 - 2mnpq + m\left(n^2q^2\right) \\
&= m\left(p^2 - 2npq + n^2q^2\right) \\
&= m(p - nq)^2
\end{aligned}
$$

$$\text{i.e., } \left(\frac{mq - np}{p - nq}\right)^2 = m.$$

This shows that m is the square of a fraction $\frac{mq-np}{p-nq}$, whose denominator $p - nq$ less than q, i.e., $\frac{p}{q}$ is not in its lowest terms, which is a contradiction to our hypothes...

The contradiction proves that $\sqrt{m}$ cannot be a rational number.

Alt. Solution: Let m be a positive integer and is not a perfect square, so we c... find positive integer n such that $n^2 < m < (n+1)^2$, i.e., $n < \sqrt{m} < n + 1$

$\therefore$ $\sqrt{m}$ cannot be an integer.

If possible, let $\sqrt{m} = \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} - \{1\}$ and gcd $(p, q) = 1$.

$\therefore$ $m = \frac{p^2}{q^2}$, i.e., $mq = \frac{p^2}{q}$, which is not possible as LHS is an integer whereas RH... is not an integer as gcd $(p^2, q) = 1$ and $q > 1$. $\therefore$ $\sqrt{m} \neq \frac{p}{q} \in \mathbb{Q}$.

Example 2.5.5. *Show that $\sqrt{23}$ is not a rational number.*

Solution: We have $4^2 < 23 < 5^2$ $\therefore$ $4 < \sqrt{23} < 5$ $\therefore$ $\sqrt{23}$ is not an integer.

Let $\sqrt{23} = \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} - \{1\}$ and gcd $(p, q) = 1$.

$\therefore$ $23q = \frac{p^2}{q}$, which is not possible as LHS is an integer but RHS is not an integer, for gcd $(p^2, q) = 1$ and $q > 1$. $\therefore$ $\sqrt{23} \neq \frac{p}{q}$, i.e., $\sqrt{23}$ is not rational.

Note: One can try this method to prove that $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$, $\sqrt{11}$, $\sqrt{13}$, $\sqrt{19}$, etc. are not rational numbers.

[CH 1989]

Example 2.5.6. ***(Gauss' theorem on the nature of the roots of a polynomial equation).*** *Any rational root of the equation $x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$ whose coefficients $a_1, a_2, \cdots, a_n$ are all integers (n is a positive integer), must be an integer which divides a_n exactly.*

Solution: Let $x = \frac{p}{q}$ be a root of the equation where p and q are integers, $q \neq 0$, and p, q are in their lowest terms (no common factor except 1). Then putting $x = \frac{p}{q}$ in the equation and multiplying through by q^{n-1}, we obtain

$$-\frac{p^n}{q} = a_1p^{n-1} + a_2p^{n-2}q + \cdots + a_{n-1}pq^{n-2} + a_nq^{n-1}.$$

Here LHS $-\frac{p^n}{q}$ is a fraction in its lowest term and RHS is a sum of several integers and, therefore, RHS itself is an integer. This is not possible unless $q = 1$ and $x = p$ simultaneously.

$\therefore$ $x = p$, an integer, is a root. So $p^n + a_1p^{n-1} + a_2p^{n-2} + \cdots + a_{n-1}p + a_n = 0$, i.e., $-p\left(p^{n-1} + a_1p^{n-2} + a_2p^{n-3} + \cdots + a_{n-1}\right) = a_n$,

p is a divisor of a_n. This proves the theorem.

Note: If m is an integer which is not a perfect square, then $x^2 - m = 0$ can have no rational root. That is, $\sqrt{m}$ is not rational. (e.g., $\sqrt{2}, \sqrt{3}, \sqrt{5}$, etc. are not rational). [See **Example 2.5.4** given above]

> The notions of boundedness and the completeness properties of real numbers will be discussed under the heading: **The Real Number System $\mathbb{R}$** (Art. 2.7): Axiomatic Approach.

EXERCISES ON CHAPTER 2: IIA
(On Rational Numbers)

1. Give the value, if any, of the following expressions:

   (a) $\dfrac{x^2 + 8x}{x}$, when $x = 0$; (b) $\sin\dfrac{1}{x}$, when $x = 0$.

   [*Ans.* (a) and (b) Undefine...

2. For what values of x are the following expressions undefined?

   (a) $\dfrac{x^2 + a^2}{x^2 - a^2}$; (b) $\tan x$;

   (c) $\dfrac{3x + 5}{(x-5)(x+3)}$; (d) $\dfrac{x^2}{(x+1)(x+2)(x+3)}$.

Note: The twelve properties **A1–A4, M1–M4, D1** and **01, 02, 03** make the system $\mathbb{R}$ of real numbers **an ordered field.**

Note: We shall often use the following notations:

1. $a \geq b$ means $a > b$ or $a = b$.
2. $a \leq b$ means $a < b$ or $a = b$.

It is easy to deduce: $a \geq b$ and $b \geq a \Longleftrightarrow a = b$.

Note: The following result is often used in proofs in analysis:

Given two real numbers x and y satisfying $x \leq y + \epsilon$, for every $\epsilon > 0$. Then $x \leq y$.

Justifications: If $x > y$, then $x \leq y + \epsilon$ is violated for $\epsilon = \frac{x-y}{2}$, because

$$y + \epsilon = y + \frac{x-y}{2} = \frac{x+y}{2} < \frac{x+x}{2} = x.$$

Hence, by the law of trichotomy, we must have $x \leq y$.

III. On completeness Axiom of $\mathbb{R}$:

We have discussed in considerable details the two axioms of real number system—namely, *field axioms* and *order axioms*. These axioms also hold for the system $\mathbb{Q}$ of rational numbers. But there is an additional property to characterise the real number system—this additional property is known as the *completeness property* (or *Supremum property*). It is an essential property of $\mathbb{R}$ (not true for the system $\mathbb{Q}$) and thus we shall arrive at the statement:

$\mathbb{R}$ is a complete ordered field.

There are several different ways to describe the completeness property: The following results are equivalent to each other and any one can be used as a *completeness property*:

1. **Dedekind property:** Let $\mathbb{R}$ be decomposed into non-empty disjoint sets A and B such that $a \in A$ and $b \in B \Longrightarrow a < b$.
   Then either A has the last element or greatest element or B has the first element or least element.
2. **Least upper bound property:** Every non-empty subset of $\mathbb{R}$ which is bounded above has the **least upper bound** or **supremum** in $\mathbb{R}$.
3. **Greatest lower bound property:** Every non-empty subset of $\mathbb{R}$ which is bounded below has the **greatest lower bound** or **infimum** in $\mathbb{R}$.
4. **Cauchy's criterion:** Every Cauchy sequence is convergent.
5. **Principle of monotone convergence:** Every bounded monotone sequence is convergent.

6. **Nested spheres property:** A nest of non-empty closed bounded spheres has a non-empty intersection.
7. **Bolzano-Weierstrass property:** Every infinite bounded set has a limit point.
8. **Heine-Borel property:** Every open covering of a closed and bounded set has a finite subcovering.

- *Ref: Introduction to Real Variable Theory: Saxena and Shah.*

Note: Properties **4** and **7** are always implied by any one of the remaining properties. Assuming the Archimedean property, all the properties mentioned above are equivalent to each other. The readers will find the discussions of these properties at various places of the present text. A *curious reader* after reading the whole text will find it interesting to establish the equivalence of these statements.

Remember: In the present text we shall describe the completeness property of $\mathbb{R}$ by assuming that each non-empty bounded above subset of $\mathbb{R}$ has a supremum in $\mathbb{R}$. It is also known as the LUB-property of $\mathbb{R}$ (No. 2 in the list given above).

We first introduce the notions of **upper bound** and **lower bound** of a set of real numbers.

Definition 2.7.1. *Let S be a non-empty subset of $\mathbb{R}$.*

(a) *The set S is said to be bounded above if $\exists$ a number $b \in \mathbb{R}$ such that for all $x \in S$, $x \leq b$. Each such number b is called an upper bound of S.*

(b) *The set S is said to be bounded below if $\exists$ a number $c \in \mathbb{R}$ such that for all $x \in S$, $x \geq c$. Each such number c is called a lower bound of S.*

(c) *A set S is said to be bounded if it is both bounded above and bounded below.*

(d) *A set S is said to be unbounded if it is not bounded.*

An upper bound b of a set S may or may not belong to S. If it does belong to S, then b is the **largest element** of S. But a set S may or may not have a *largest element,* even when S is bounded above.

Example 2.7.1. *Let $S = \{x : x \in \mathbb{R}$ and $x < 5\}$. Then S is bounded above and 5 is an upper bound of S. The set has no lower bound and hence it is not bounded below. S is unbounded below (even though it is bounded above).*

If a set S has one upper bound b, then it has infinitely many upper bounds—any number greater than b is an upper bound. Similar observations can be made for lower bounds. In the set of upper bounds of S and the set of lower bounds of S we look to the *least element* and *greatest element* respectively. They define *supremum* and *infimum* respectively of S. We call them *least upper bound* (lub) M and *greatest lower bound* (glb) m of the set S. We give these definitions more precisely:

Definition 2.7.2. *Let S be a non-empty subset of* $\mathbb{R}$.

(a) *If S is bounded above, then a number M is called a supremum [or a least upper bound (lub)] of S if it satisfies the following two conditions:*

1. *M is an upper bound of S, i.e., for all $x \in S$, $x \leq M$.*
2. *No number $M' < M$ is an upper bound of S, i.e., for each $\epsilon > 0$, $\exists$ a member $y \in S$ such that $y > M - \epsilon$.*

[It is easy to show that there can be only one supremum of a given subset S of $\mathbb{R}$. *So when a supremum exists we refer it to* **the** *supremum instead of* **a** *supremum.]*

When a supremum M of a set S exists, we write $M = \sup S$.

(b) *If S is bounded below, then a number m is called an infimum [or a greatest lower bound (glb)] of S if it satisfies the following two conditions:*

1. *m is a lower bound of S, i.e., for all $x \in S$, $x \geq m$.*
2. *No number $m' > m$ is a lower bound of S, i.e., for every $\epsilon > 0$, $\exists$ a member $y \in S$ such that $y < m + \epsilon$.*

[Here also an infimum, when exists, is unique and we write $m = \inf S$.]

Note: If M' is an arbitrary upper bound of a non-empty set S, then $\sup S \leq M'$, i.e., $\sup S$ is the least of all the upper bounds of S.

If m' is an arbitrary lower bound of a non-empty set S, then $\inf S \geq m'$, i.e., $\inf S$ is the greatest of all the lower bounds of S.

It is important to remember that the supremum of a set S may or may not belong to S. If it does belong to S, then it is the greatest element of S. Similar observations are noted for the infimum of S.

III. The completeness property of $\mathbb{R}$ (LUB-axiom of $\mathbb{R}$) **[CH 2006]**

STATEMENT

1. Every non-empty subset S of real numbers, which is bounded above, has a supremum (or a least upper bound) in $\mathbb{R}$.

   This property is called the **completeness axiom** or **LUB-property** or **supremum property** of $\mathbb{R}$. An analogous property can be deduced in the language of infimum.
2. Every non-empty subset S of real numbers, which is bounded below, has an infimum (or a greatest lower bound) in $\mathbb{R}$.

   This property is called the GLB-property or infimum property.

Theorem 2.7.1. GLB-*property follows if* LUB-*property is assumed.*

Given: A set S of real numbers, which is bounded below.

To prove: S has the infimum (or GLB) *in* $\mathbb{R}$.

Proof. We construct a set S' of those real numbers x such that $-x \in S$, i.e.,

$$S' = \{x : x \in \mathbb{R} \text{ and } -x \in S\}.$$

Since S is bounded below, S has a lower bound k, (say $k \in \mathbb{R}$).

Now, if x be any member of S', then $-x \in S$ and $-x \geq k$.

$\therefore$ $x \leq -k$ for all $x \in S'$.

This proves that $-k$ is an upper bound of S', i.e., S' is bounded above.

Hence we can use LUB-property on S', i.e., $\exists$ a supremum M of S' in $\mathbb{R}$.

By definition of supremum, we obtain for every $x \in S'$, $x \leq M$ and hence $-x \geq -M$,

$$\text{i.e., each member of } S \geq -M. \tag{2.7.1}$$

Also $\exists$ at least one member $y \in S'$ such that $y > M - \epsilon$ (ϵ is any positive number, no matter how small).

This means that $\exists -y \in S$ such that

$$-y < -M + \epsilon. \tag{2.7.2}$$

(1) and (2) together establish that $-M$ is the infimum or GLB of S.

Note: The axioms **I, II** and **III** lead to the assertion: **$\mathbb{R}$ is a complete ordered field.**

$\mathbb{Q}$ is an important subset of $\mathbb{R}$. We have already shown that $\mathbb{Q}$ is an **ordered field.** That $\mathbb{Q}$ is not **complete** can be shown by the theorem given below:

Theorem 2.7.2. *The set $\mathbb{Q}$ of rational numbers is not order complete.* **[CH 2006]**

The statement of the theorem is true if we can give an example of a non-empty set S which is a subset of $\mathbb{Q}$ and which is bounded above (i.e., $\exists$ an upper bound) but does not have the supremum in $\mathbb{Q}$, i.e., no member of $\mathbb{Q}$ is the supremum of S.

Such an example is the set S where $S = \{x : x \in \mathbb{Q}, x > 0 \text{ and } x^2 < 2\}$, i.e., S contains those positive rational numbers whose square is less than 2.

Clearly, $S \subseteq \mathbb{Q}$, $S \neq \phi$ ($\because$ $1 \in S$) and S has an upper bound 2. Thus S is a non-empty subset of $\mathbb{Q}$ which is bounded above.

We now assert that no rational number can become supremum of S. If possible, let k be a **rational number** which is the supremum of S. Then $k > 0$ and $k \in \mathbb{Q}$. **By the** law of trichotomy, exactly one of the following holds: either $k^2 < 2$ or $k^2 = 2$ or $k^2 > 2$.

(i) If $k^2 < 2$, then let us take a rational number
$$y = \frac{4+3k}{3+2k}.$$

Then $y > 0$;
$$k - y = k - \frac{4+3k}{3+2k} = \frac{2(k^2-2)}{3+2k} < 0 \quad (\because\ k^2 < 2).$$

Thus we get
$$0 < k < y. \tag{2.7.3}$$

Also
$$2 - y^2 = 2 - \left(\frac{4+3k}{3+2k}\right)^2 = \frac{2-k^2}{(3+2k)^2} > 0.$$

Therefore, we have
$$y > 0 \quad \text{and} \quad y^2 < 2. \tag{2.7.4}$$

(2.7.4) Show that $y \in S$ and (2.7.3) implies $k <$ one element y of S. Therefore, k is not the supremum of S—a contradiction to our assumption. Therefore, $k^2 \nless 2$.

(ii) If $k^2 = 2$, then k is not rational ($\because\ \sqrt{2}$ is not rational). This contradicts our assumption that k is a rational number. Therefore, $k^2 \neq 2$.

(iii) If $k^2 > 2$, let us again take a rational number y, where
$$y = \frac{4+3k}{3+2k}.$$

Then $y > 0$;
$$k - y = \frac{2(k^2-2)}{3+2k} > 0 \quad (\because\ k^2 > 2)$$
$$\text{i.e., } \quad 0 < y < k. \tag{2.7.5}$$

Also
$$2 - y^2 = \frac{2-k^2}{(3+2k)^2} < 0, \quad \text{i.e.,} \quad y^2 > 2. \tag{2.7.6}$$

(2.7.6) shows that y is an upper bound of S and (2.7.5) shows that k is not the supremum of S.

This is a contradiction to our assumption that $k = \sup S$. Therefore, $k^2 \ngtr 2$.

None of three possibilities: $k^2 > 2$, $k^2 = 2$, $k^2 < 2$ can hold. Hence our assumption that $\sup S$ is a rational number is not correct. Therefore, no rational number can become supremum of S.

2.8 Some Important Properties of the Real Field

1. Archimedean Property: If $x, y \in \mathbb{R}$ and $x > 0$, then there exists a positive integer n such that $nx > y$. **[CH 2000]**

Trivial Cases: If $y < 0$ or if $0 \le y < x$, there is nothing to prove: because, then obviously $x > y$, i.e., Archimedean property holds for $n = 1$.

We, therefore, prove Archimedean property in the form: If $x, y \in \mathbb{R}$, $x, y > 0$ and $x < y$, then there exists a positive integer n such that $nx > y$.

Proof. Let $A = \{nx : n = 1, 2, 3, \cdots\}$.

If the Archimedean Property were not TRUE, i.e., if for all $n \in \mathbb{N}$, $nx \le y$, then y would become an upper bound of the set A, i.e., A is a non-empty set (because $y \in A$), bounded above. Therefore, by lub-axiom, sup A exists $= M$ (say) and $M \in \mathbb{R}$.

Since $x > 0$, $M - x < M$ and $M - x$ is not an upper bound of A ($\because$ M is the lub of A), i.e., $M - x < mx$, for some positive integer m, i.e., $M < (m+1)x$; but $(m+1)x \in A$.

This means that M is not the sup A, a contradiction. Hence our assumption that the Archimedean property is NOT TRUE is not correct. So $\exists$ some n for which $nx > y$, i.e., the Archimedean property is TRUE in $\mathbb{R}$.

Alternative proof: Archimedean Property can also be deduced in the following manner:

Step 1. The set $\mathbb{N}$ of all natural numbers is unbounded above.
Otherwise, if $\mathbb{N}$ were bounded above, then by lub-axiom there would exist a supremum of $\mathbb{N} = a$ (say). Choose any positive number ϵ such that $0 < \epsilon < 1$. Then by the property of supremum there would exist a natural number n such that $n > a - \epsilon$, i.e., $n + 1 > a + (1 - \epsilon)$ and so the natural number $n + 1 > a$ ($\because$ $1 - \epsilon$ is positive). Now $n + 1 \in \mathbb{N}$, i.e., $\exists$ a member $n + 1$ of $\mathbb{N}$ which is greater than the supremum of $\mathbb{N}$. This would then contradict the fact that $a = \sup \mathbb{N}$.
$\therefore$ $\mathbb{N}$ cannot be bounded above. In other words, $\mathbb{N}$ is unbounded above.

Step 2. Given a positive real number x, $\exists$ a positive integer n such that $n > x$. If this were not true, then some x would be an upper bound of $\mathbb{N}$, contradicting the result '$\mathbb{N}$ is unbounded above' derived in step 1.

Step 3. If x, y are two positive real numbers such that $x < y$, then $\exists$ a positive integer n such that $nx > y$ (Archimedean property).
Use step 2 for the real number $\frac{y}{x}$. Then $\exists$ a positive integer n such that $n > \frac{y}{x}$ or $nx > y$.

As an immediate consequence of Archimedean property we prove the following interesting result:

Theorem 2.8.1. *For any positive real number x there exists a unique positive integer n such that $n - 1 \leq x < n$.* [CH 19..]

Proof. Given $x > 0$, by the Archimedean property there exists a positive integer k such that $k > x$. (Consider two positive real numbers 1 and x, and by Archimedean property $\exists$ a natural number k such that $k \cdot 1 > x$, i.e., $x < k$.)

We construct a set S of all those natural numbers p for which $p > x$, i.e.,

$$S = \{p : p \in \mathbf{N} \text{ and } p > x\}.$$

Then $S \neq \phi$ ($\because k \in S$).

$\therefore$ by well-ordering property of the set $\mathbf{N}$ of natural number, S has a least member n (i.e., $n \in S$ and $n \leq$ any member of S).

Since $n \in S$, $n > x$ (by construction).

Since n is the least member of S, $(n-1) \notin S$.

So $n - 1 \leq x$ (negation of $n - 1 > x$).

$\therefore$ we finally obtain that for a positive real number x, $\exists$ a unique positive integer n such that $n - 1 \leq x < n$ (unique because n is the least member of S).

Note:

1. The result of this theorem can be stated as: If x is any positive real number, then $\exists$ a non-negative integer denoted by $[x]$ such that $[x] \leq x < [x] + 1$ (here $[x] = n - 1$).
2. If $x \in \mathbb{R}$ and $x > 0$, then $\exists$ a natural number n such that $0 < \frac{1}{n} < x$.
   [In the result of Archimedean property (namely $nx > y$), put $y = 1$. So, $\exists$ a natural number, n such that $nx > 1$ or $\frac{1}{n} < x$. Since n is a natural number, $n >$ 0 and hence $\frac{1}{n} > 0$. $\therefore$ $0 < \frac{1}{n} < x$.]

Note: When ϵ is any arbitrary positive number $0 < \frac{1}{n} < \epsilon \Longrightarrow \lim_{n \to \infty} \frac{1}{n} = 0$.

II. Density property of real numbers

A. If x and y are two real numbers with $x < y$, then there exists a rational number r such that $x < r < y$. [CH 19..]

Observation: Existence of one rational number between x and y implies the existence of infinitely many rational numbers between x and y. This proves that $\mathbb{R}$ is dense with rational numbers.

Proof of A. Suppose $x > 0$ and the given condition states that $x < y$, i.e., $y - x > 0$. Therefore (see Note 2 above), $\exists$ a natural number n such that

$$0 < \frac{1}{n} < y - x.$$

Therefore, we have

$$nx + 1 < ny.$$

Now, see that $nx > 0$ and hence by Theorem 2.8.1, we obtain $m \in \mathbf{N}$ with

$$m - 1 \leq nx < m.$$

Therefore, $m \leq nx + 1 < ny$,
whence, $nx < m < nx + 1 < ny$
or $nx < m < ny$
or $x < \frac{m}{n} < y$.

Thus the rational number $r = \frac{m}{n}$ lies between x and y.

i.e., $\exists$ a rational number in the open interval (x, y), where $0 < x < y$.

Observation: We have taken $x > 0$ and $x < y$. Even when $x < 0$, we can find a rational number between x and y:

1. Suppose $x \leq 0 < y$, then by the Archimedean property, $\exists$ a positive integer n with $\frac{1}{n} < y$. Clearly, $\frac{1}{n}$, a rational number, lies in the open interval (x, y).
2. Suppose $x < y \leq 0$. Then we can write $0 \leq -y < -x$ (i.e., $-y$ and $-x$ are positive). So by the previous cases, $\exists$ a rational number $r \in (-y, -x)$ and so the rational number $-r \in (x, y)$.

What we observe is that in proving **A** there is no loss of generality to assume that $x > 0$ and $x < y$.

Remember: *Every open interval (x, y) contains a rational number.*

B. If x, y are real numbers with $x < y$, then there exists an irrational number z such that $x < z < y$. Here also we can add the following: [CH 1990]

Observation: Existence of one irrational number between x and y implies the existence of infinitely many irrational numbers between them. Hence this result proves that $\mathbb{R}$ is dense with irrational numbers.

Note that the results **A** and **B** together with the observations stated lead to the conclusion:

> Real numbers are dense with rational and irrational numbers, i.e., between two real numbers x and y, $\exists$ infinitely many real numbers. This is known as the density property of the system $\mathbb{R}$.

Proof of B. If we apply the density property **A** to real numbers $\frac{x}{\sqrt{2}}$ and $\frac{y}{\sqrt{2}}$, then we obtain a rational number $r (\neq 0)$ such that $\frac{x}{\sqrt{2}} < r < \frac{y}{\sqrt{2}}$.

Then $z = r\sqrt{2}$ is irrational and satisfies $x < z < y$.