Chapter (1)
Real and rational numbers

Definition:

A **field** is a non-empty set F with the operation of addition and multiplication. i.e $(F,+,\cdot)$ is a field if it satisfies the following axioms:

The axiom of real numbers: $\forall\, a,b,c \in F$

1) $a+b \in F$ (Additive closure)
2) $a+b=b+a$ (Commutative property)
3) $(a+b)+c=a+(b+c)$ (Associative property)
4) $\exists$ an element $0 \in F$ s.t $a+0=0+a=a \quad \forall\, a \in F$
5) $a \in F$ $\exists$ an element $-a \in F$ s. t $a+(-a)=-a+a=0.$
6) $a.b \in F$ (Multiply closure)
7) $a \cdot b=b \cdot a$ (Commutative property)
8) $(a \cdot b) \cdot c=a \cdot (b \cdot c)$ (Associative property)
9) $\exists$ an element $1 \in F$ s.t $a \cdot 1=1.a=a \quad \forall\, a \in F$
10) For each $a \in F$ and $a \neq 0$, $\exists$ an element $a^{-1} \in F$ s. t $a+(a^{-1})= a^{-1}.a=1$.
11) $a \cdot (b+c)=a \cdot b+a \cdot c \qquad (a+b).c=a \cdot c+b \cdot c$ (Distributive law)

Examples:

- The set of real numbers is a field.
- The set of rational numbers is a field.

Ordered Field:

A field $(F,+,\cdot)$ is called **ordered field** iff there is a relation "$<$" on F s.t $\forall\ a,b,c \in F$ satisfy the following conditions:

1) Either $a = \text{b}$ or $a < b$ or $a > b$
2) If $a < b$ and $b < c$, then $a < c$ (transitive)
3) If $a < b$, then $a + c < b + c$
4) If $a < b$ and $c > 0$, then $a \cdot c < b \cdot c$.

Complete Ordered Field:

When an ordered field is bound above and bound below, then it has a supremum and infimum is called **complete ordered field**.

Supremum of a set:

A set S of real numbers is **bounded above** if there is a real number b such that $x \leq b$ for each $x \in S$. In this case, b is an upper bound of S. If b is an **upper bound** of S, then so is any larger number, because of property (2)

If b' is an upper bound of S, but no number less than b', then b' is a **supremum** of S , and we write $b' = \sup(S)$.

Example:

If S is the set of negative numbers, then any non-negative number is an upper bound of S, and $\sup(S) = 0$.

If S_1 is the set of negative integers, then any number a such that $a \geq -1$ is an upper bound of S, and $\sup(S_1) = -1$

The example shows that a supremum of a set may or may not be in the set since S_1 contains it's supremum but S dose not

Infimum of a set:

A set S of real numbers is **bounded below** if there is a real number a such that, $x \geq a$ for each $x \in S$. In this case a is a **lower bound** of S so is any smaller number because of property (2). If a' is a lower bound of S but no number greater than a', then a' is an **infimum** of S, and we write $a' = \inf(S)$.

Remark:

If S is a non-empty set of real numbers, we write $\sup(S) = \infty$ to indicate that S is unbounded above and $\inf(S) = -\infty$ to indicate that S is unbounded below.

Example:

Let, $S = \{x : x < 2\}$, then $\sup(S) = 2$ and $\inf(S) = -\infty$

Example:

Let, $S = \{x : x \geq 2\}$, then $\sup(S) = \infty$ and $\inf(S) = -2$.

If S is the set of all integers, then $\sup(S) = \infty$ and $\inf(S) = -\infty$

H.W: Find $\sup(S)$ and $\inf(S)$, state whether they are in S.

1- $S = \{x : x^2 \leq 5\}$

2- $S = \{x : x^2 > 9\}$

3- $S = \{x : |2x + 1| < 7\}$.

Rational Numbers:

The relation between the field of rational numbers and real number

Proposition (1-1):

Every ordered field contains a subfield similar to field of rational numbers.

Proof:- Let $(F, +, \cdot)$ be an ordered field $1 \in F$ ($0 \in F$, the identity of $+$)

$1 + 1 + 1 + \cdots + 1 = n \cdot 1 = n \in F, \quad n \in Z^+$

Claim (1) $n \cdot 1 = 0 \quad iff \quad n = 0$

Proof $\Rightarrow$) Suppose the result is not true i.e there exists a positive integer $k \geq 1$ and $k \cdot 1 = 0$

It's clear that $k > 1 \Rightarrow k - 1 > 0$ and $(k-1) \cdot 1 > 0$

$0 < (k-1) \cdot 1 < k = k \cdot 1 = 0$ **C**! (since $0 < 0$)

Thus the result is not true.

$\Leftarrow$)Trivial.

Claim (2) $n \cdot 1 = m \cdot 1 \quad iff \quad n = m$

Proof :$\Leftarrow$) If $n = m$ clearly $n \cdot 1 = m \cdot 1$.

$\Rightarrow$) If $n \cdot 1 = m \cdot 1 \Rightarrow n \cdot 1 + (-m \cdot 1) = 0 \Rightarrow (n + (-m) \cdot 1) = 0$. Then **by (1)** $n - m = 0 \Rightarrow n = m$. Thus $\mathrm{N} \subset \mathrm{F}$ (F Contains a copy of Z).

$\forall\, \mathrm{n} \in \mathrm{F}$ **(F is a group)**, $\exists -n \in F$ such that $n + (-n) = 0$, hence $\mathrm{Z} \subset \mathrm{F}$ (F Contains a copy of Z)

$\forall\, \mathrm{n} \neq 0, \mathrm{n} \in \mathrm{F}$ **(F is a field)**, $\exists\ \frac{1}{n} \in F$ such that $\left(\frac{1}{n}\right) \cdot n = 1$.

$\forall\, \mathrm{m} \in \mathrm{F}$, $\left(\frac{1}{n}\right) \cdot m = \frac{m}{n} \in \mathrm{F}$ (Multiply closure).

$\mathrm{Q} \subset \mathrm{F}$ (F Contains a copy of Q).

Corollary (1-2):

$\mathrm{Q} \subseteq \mathrm{R}$

$(R, +, \cdot, \leq)$ orderd field, $1 + 1 + 1 + \cdots + 1 = n \cdot 1 = n \in R$.

Q/ Is $Q = R$.

To answer this question, we beginning by this proposition:

Proposition (1-3):
The equation $x^2 = 2$ has no solution in Q.

Proof: Suppose the result is not true i.e the equation $x^2 = 2$ has a root in Q say $\frac{a}{b}$, $b \neq 0$, $a, b \in \mathrm{Z}$ and the greatest common divisor $(a, b) = 1$, $\frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2$.

- If a and b are odd, then $a^2(odd) = 2b^2(even)$ C! .
- If a is odd and b is even, $(i.e\ b = 2m,\ m \in Z\ )$, then $a^2(odd) = 2(2m)^2 = 8m^2 = 2(4m^2)(even)$ C! .
- If a is even and b is odd, $(i.e\ a = 2n,\ n \in Z\ )$ (, then $(2n)^2 = 2b^2 \Rightarrow 4n^2 = 2b^2 \Rightarrow 2n^2(even) = b^2(odd)$ C!.
- If a and b are even, $(i.e\ a = 2n,\ n \in Z\ ,\ b = 2m,\ m \in Z\ )$ (,then $4n^2 = 8m^2 \Rightarrow n^2(even)\ or\ (odd) = 2m^2(even)$ C!..

So that there is no rational number satisfy this equation.

H.W:
The equation $x^2 = 3$ has no solution in Q.

Proposition (1-4):
The equation $x^2 = 2$ has only one real positive root.

Proof: Let $S = \{x \in Q : x > 0\ ,\ x^2 < 2\} \neq \emptyset$. $1 \in S$ and S is bounded above. Since R is complete ordered field, then S has a least upper bound say y.
$\sup(S) = y$

Claim: $y^2 = 2$

If not, then either $y^2 > 2$ or $y^2 < 2$.

1. If $y^2 < 2$ choose $0 < h < 1$,

$(y + h)^2 = y^2 + 2hy + h^2 < y^2 + 2hy + h$

$(y + h)^2 < y^2 + h(2y + 1)$

Suppose $h < \frac{2-y^2}{2y+1}$

$\Rightarrow\ y^2 + h(2y + 1) < 2 \ \Rightarrow\ (y + h)^2 < 2$

Hence $y + h \in S$ $C!$ Since $\sup(S) = y$

2. If $y^2 > 2$ choose $0 < k < 1$

$(y - k)^2 = y^2 - 2ky + k^2 > y^2 - 2ky + k$

$(y - k)^2 > y^2 - k(2y + 1)$

Suppose $k < \frac{y^2-2}{2y+1}$

$\Rightarrow\ y^2 - k(2y + 1) > 2 \ \Rightarrow\ (y - k)^2 > 2$

Hence $y - k \in S$ $C!$ Since $\sup(S) = y$, and $y - k < y$

Uniqueness:

Let $\exists\, z \in R$ s. t $z^2 = 2$ and $z \neq y$, so either $z < y \Rightarrow z^2 < y^2$ $(2 < 2)$ $C!$ or $z > y \Rightarrow z^2 > y^2$ $(2 > 2)$ $C!$. Thus $z = y$.

Corollary (1-5):

$Q \subsetneq R$. (The field of rational numbers Q is proper subfield of the field of real numbers R).

Proof: $\sqrt{2} \in R$, from (1.4).

$\sqrt{2} \notin Q$, from (1.3).

Corollary (1-6):

Q is not complete orderd field.

Proof: Let $S = \{x \in Q: x > 0\,,\ x^2 < 2\} \subset Q$. S is non-empty in Q and bounded above. But does not have least appear boned in Q since $Sup(S) = \sqrt{2} \notin Q$

Thus Q is not complete orderd field.

Remark (1-7):

$Q' = R - Q$, Q'denote the set of irrational numbers, $R = Q \cup Q'$. Q' is complete ordered field. Not that $(\sqrt{2} \in Q') \Rightarrow (Q \neq Q')$.

Now, we study the set Q' and how we distribute the elements of Q and the element of Q' in R. We start by the following theorem:

Theorem (1-8) : (Archimedean property)

For each real numbers a and b, $a > 0$ there exists a positive integer n such that $n.a > b$

Proof: Let $S = \{ka: \quad k \in Z^+\} \neq \emptyset$, S is bounded above.

Suppose the result is not true i.e. $\forall\, n \in Z^+ ,\ n.a \leq b$

i.e b is upper bounded for S, by completeness of real numbers S has a least upper bound say y i.e $y = Sup(S)$

Since $a > 0$, then $y - a < y$

$\Rightarrow \exists\ m \in Z^+$ and $m.a \in S$ such that $m.a > y - a$

$\Rightarrow m.a + a > y$

$\Rightarrow (m+1).a > y$. but $(m+1).a \in S$ $C!$ since $y = Sup(S)$.

Corollary (1.9):

$\forall \epsilon > 0$, there exists a positive integer n such that $\frac{1}{n} < \epsilon$.

Proof: Take $b = 1$, $a = \epsilon$. By (1.8) $\exists\ n \in Z^+$ s. t. $(n.\epsilon > 1) \div n$,
Hence $\frac{1}{n} < \epsilon$.

Theorem (1.10): (The density of rational numbers)

For each real numbers a and b with $a < b$, there exists at least one rational number r between a and b $(a < r < b)$

Proof: (1) Suppose $0 < a < b$ and $b - a > 1$ $\cdots (1)$

Let $S = \{n \in N: n = n \cdot 1 > a\} \neq \emptyset$, (By Archimedean) and let $k \in S$

Choose k be the smallest positive integer satisfies $k \cdot 1 = k > a$

$k - 1 \leq a < k$ $\cdots (2)$

From (1) and (2) we get $a < k < b$

$\therefore k$ is the rational number between a and b.

If $0 < b - a \leq 1$

$\exists\, n \in Z^+$ s. t. $n(b-a) = nb - na > 1$, (By Archimedean)

$\Rightarrow$ From (1) $\exists\, k \in Z^+$ such that $[na < k < nb\,] \div n$

$\Rightarrow a < \frac{k}{n} < b$

$\therefore \frac{k}{n}$ is the rational number between a and b.

(2) If $a < 0 < b$

$\therefore 0$ is the rational number between a and b.

(3) $a < b < 0$

$\Rightarrow 0 < -b < -a$

By (1) $\exists\, r \in Q$ s.t $-b < r < -a$

$\Rightarrow a < -r < b$

$\therefore r$ is the rational number

Corollary (1-11):

For each real numbers a and b there exists an infinite countable set of rational numbers between a and b

Proof: $a < b$, by **(1.10)** $\exists\, r_1 \in Q$ $s.t$ $a < r_1 < b$.

$a < r_1$, by (1.10) $\exists\, r_2 \in Q$ $s.t$ $a < r_2 < b$

And $\exists\, r_2' \in Q$ $s.t$ $r_1 < r_2' < b$

Generally $\exists\, r_n \in Q$ between a and r_{n-1} and r_n' between r_{n-1} and b.

Thus we have infinite countable set between a and b

Theorem (1.12): (The density of irrational number)

For each real numbers a and b with $a < b$, there exists an irrational number s between a and b.

Proof: Suppose the result is not true i.e between a and b there is only rational number by **(1.10)**, $\exists\, r_1 \in Q$ s.t $(a < r < b)$

$\sqrt{2} \notin Q$, $\sqrt{2} \in Q'$ $\Rightarrow$ $a + \sqrt{2} < b + \sqrt{2}$ $\Rightarrow a + \sqrt{2} < r + \sqrt{2} < b + \sqrt{2}$

$r + \sqrt{2} \in Q'$, If $(r \in Q\ ,\ s \in Q', then\ r + s \in Q')$, hence a contradiction

Corollary (1.13):

For any real numbers a and b there exists an infinite countable set of irrational numbers between a and b.

Proof : $a < b$, by (1.12) $\exists$ $s_1 \in Q'$ $s.t$ $a < s_1 < b$.

$a < s_1$, by (1.12) $\exists$ $s_2 \in Q'$ $s.t$ $a < s_2 < b$

And $\exists$ $s_2' \in Q'$ $s.t$ $s_1 < s_2' < b$

Generally $\exists$ $s_n \in Q'$ between a and s_{n-1} and s_n' between s_{n-1} and b.

we have infinite countable set $\{s_1 , s_2, s_2', \cdots\}$ between a and b

Example: $.1.25 < 1.50$

$1.50 - 1.25 = 0.25$, by Arch., then $\exists\, n \in Z^+$ $s.t$ $n(0.25) > 1$

$10(1.25) < k < 10(1.50)$ $(choose\ n = 10) \Rightarrow$ $12.5 < k < 15$ $\Rightarrow$
$k = 13$. The number is $\frac{13}{10}$