0.0.1. In calculus.

1. Extreme Value Theorem: Every continuous function $f : [a, b] \to \mathrm{R}$ admit both max and min value $\Rightarrow$ Compact set
2. Intermediate value Theorem: Given continous function $f : [a, b] \to \mathrm{R}$ for all $f(a) \leq \lambda \leq f(b) \exists c \in [a, b] \ni f(c) = \lambda \Rightarrow$ connected set

How to prove a statement: HP,then Q, $P \Rightarrow Q$

$$\begin{cases} \begin{cases} \text{Direct Proof} \\ \text{Indirect Proof} \begin{cases} \text{contrapositive } \sim Q \Rightarrow \sim P \\ \text{by contradiction} \end{cases} \end{cases} \\ Mathematical Induction \end{cases}$$

1. Some preliminary

1.1. Set Theory. We will assume that you are familiar with some basic set theory e.g. union, intersection, difference

1.2. The Number System.

$\mathbb{N} = \{ 1, 2, 3, \cdots \}$ the set of all positive integers n natural numbers
$\mathbb{Z} = \{ \cdots, -2, -1, 0, -1, -2, \cdots \}$ the set of all integers called the ring of intepus
$\mathbb{Q} = \left\{ \frac{m}{n} \ : \ n, m \in \mathbb{Z}, n \neq 0 \right\}$ the set of all rational numbers
$\mathbb{R}$ the set all of real numbers on the real number field on real line
$\mathbb{C} = \{ z = a + ib \mid a, b \in \mathbb{R} \}$ the set of all complex numbers or the complex number filed on complex plane, where $i = \sqrt{-1}$

Remark.

1. $x + 2 = 0$ *no root in* $\mathbb{N}$
   $3x - 5 = 0$ *no root in* $\mathbb{Z}$
   $x^2 + 1 = 0$ *no root in* $\mathbb{R}$
2. *One can construct* $\mathbb{Q}$ *from* $\mathbb{Z}$ *in algebraic way, called the fraction field of* $\mathbb{Z}$
3. *One can construct* $\mathbb{R}$ *from* $\mathbb{Q}$ *in two ways:*
   - *Using Dedekind cut which is given in the appendix of Rudin p17-21*
   - *Using completion of matrix space*
4. *One can construct* $\mathbb{C}$ *from in complex analysis*

Example.

1. *Between any two rational numbers, there is another one*

   Proof. Let $r, s \in \mathbb{Q}$ with $r < s$, then $\dfrac{r+s}{2} \in \mathbb{Q}$ and $r < \dfrac{r+s}{2} < s$

   $$r = \frac{m_1}{n_1}, s = \frac{m_2}{n_2}, \frac{r+s}{2} = \frac{\frac{m_1}{n_1} + \frac{m_2}{n_2}}{2} = \frac{m_1 n_2 + n_1 m_2}{2 n_1 m_1} \in Q$$
   $$s = \frac{s+s}{2} > \frac{r+s}{2} > \frac{r+r}{2} = r$$

   ∎

2. $x^2 = \dfrac{4}{9}$ *has exactly two rational solutions, namely,* $\pm\dfrac{2}{3}$

3. $x^2 = 2$ *has exactly two real root, namely,* $\pm\sqrt{2}$

4. *Is there any rational roots of* $x^2 = 2$*? i.e., is* $\sqrt{2}$ *rational?*

   Suppose $r = \dfrac{m}{n} \in \mathrm{Q}$*, is a root of* $x^2 = 2$*, where* $(m, n) = 1$
   Then $\dfrac{m^2}{n^2} = 2 \implies m^2 = 2n^2 \implies 2 \mid m^2 \implies 2 \mid m \implies 4 \mid m^2 \implies 4 \mid 2n^2$
   $\implies 2 \mid n^2 \implies 2 \mid n \implies (n, m) \neq 1$

5. *Let* $A = \left\{ r \in \mathrm{Q} \mid r > 0 \ \& \ r^2 < 2 \right\}, B = \left\{ r \in \mathrm{Q} \mid r > 0 \ \& \ r^2 > 2 \right\}$

   Then A contains no largest numbers, i.e. max element & B contains no smallest numbers, i.e. min element

   Proof. A contains no largest numbers $\Leftrightarrow$ given $r \in A$, $\exists s \in A \ni s > r$
   Now, given $r \in A$, Let $s = r - \dfrac{r^2 - 2}{r + 2} = \dfrac{2r + 2}{r + 2}$ $(\star_1)$
   $\implies s^2 - 2 = \dfrac{2(r^2 - 2)}{(r + 2)^2}$ $(\star_2)$
   Now, $r \in A, r^2 < 2 \implies r^2 - 2 < 0 \therefore$
   $(\star_1) \& (\star_2) \implies s > r \ \& \ s^2 < 2 \implies s \in A$ ∎

6. *As you know, in calculus, the sequence* $\{1, 1.4, 1.41, 1.414, 1.4142, \cdots\}$ *does not converge in* Q*, but it converges to* $\sqrt{2}$ *in* R

1.3. Order Sets.

Definition (Relation).
Let X be a nonempty set A, relation on X is a subset R *of* $X \times X = \{ (x,y) \mid x,y \in X \}$
Let R *be a relation on X, if $(x,y) \in \mathrm{R}$, then we say that x is retaliated to y, and is written as $xRy(x \sim y)$*

Definition (Order Set). *An ordered set on S, is a relation denoted by " $<$ " on S, satisfy:*

(i) The low of trichonomy

Given $x, y \in S$, one and only one of the following holds: $x < y, x = y, y < x$

(ii) Transitivity: if $x < y \& y < z$, than $x < z$

Notation

(1) $x < y$ means "x is less than y" or "x is smaller than y"

(2) $y > x$ means $x < y$

(3) $x \leq y$ means $x < y$ or $x = y$, i.e. the negative of $x > y$

Definition (bdd). *Let S is an ordered set & $E \subseteq S(E \neq \emptyset)$*

- *E is bounded above if $\exists\ \alpha \in S \implies x \leq \alpha\ \forall\ x \in E$*

  such α is called an upper bound of E

- *E is bounded below if $\exists\ \beta \in S \ni \beta \leq x, \forall\ x \in E$, such β is called a lower bdd of E*

- *E is bdd is E is both bdd above and below.*

Definition (least upper bound). *Let S be an ordered set and $E \subseteq S(E \neq \emptyset)$ bdd above. An element $\alpha \in S$ is called the last upper bound or supremum of E if*

(i) α is an upper bound of E

(ii) α is the smallest such one.

Equivalently,

(i') $x \leq \alpha, \forall x \in E$

(ii') if $\beta < \alpha$, then β is not an upper bdd of E, i.e. $\exists\ x \in E \ni x > \beta$

Such α(if exists) is denoted by

$$\alpha = sup(E)$$

similarly, one can defined the greatest lower bdd of infimum of E

Remark. *if* $\sup(E)$ *exists then it is unique*
suppose $\alpha \neq \alpha'$ both lub of E
$\because$ *by trichotomy ,$\alpha > \alpha'$ or $\alpha = \alpha'$ or $\alpha < \alpha'(\rightarrow\leftarrow)$*

<u>Definition</u> (least upper bdd property)**.** *A ordered set S is said to have the least upper bdd property if $E \subseteq S,\ E \neq \emptyset$ and E is bdd above, then* $\sup(E)$ *exists in S*

Example.

1. *In* Q *with the normal ordining*

   $A = \left\{\, r \in \mathrm{Q} \mid r > 0,\ r^2 < 2 \,\right\} \& B = \left\{\, r \in \mathrm{Q} \mid r > 0,\ r^2 > 2 \,\right\}$

   Then A is bdd above, in fact, bdd by every element in B, but $\sup(A)$ *does not exist in* Q*($\because$ by Ex1.5)*

2. *B is bdd below by every element of A and* $\inf B$ *does not exists*

3. *Note that* $\sup(E) \& \inf(E)$ *may not in E even if exist*

Remark.

1. *By the Example above,* Q *with the usual ordering has no l.u.b property*

2. *In* 1.5 *we will explain that* R *with usual ordering has the l.u.b. property. However, we usually adopt the follwing*

The Axiom of Completence or Least upper bdd property:
Every nonempty subset E of R which is bdd above has l.u.b

Theorem (l.u.b.p. $\rightarrow$ g.l.b.p.)**.** *Let S is an ordered set if S has the l.u.b. property, then S has the g.l.b. property, i.e. if $\emptyset \neq B \subseteq S$ is bdd below, then* $\inf(B)$ *exists in S*

Proof. $(\star)$
Given $B(\neq \emptyset) \subseteq S$ which is bdd below
Let $L = \{ a \in S \mid a \text{ is a lower bdd of } B \}$

- $L \neq \emptyset (\because B$ is bdd below)
- L is bdd above (in fact, every element in B is on upper bound of L)

  $\implies \forall a \in L \implies a \leq x,\ \forall x \in B \implies x$ is an upper bound of L
- $\sup(L) = \alpha$ exists by assumption

Claim $\alpha = \inf B$

(i) α is a lower bdd of B, i.e. $\alpha \leq x,\ \forall x \in B$

By $\alpha = \sup L$, if $r < \alpha$, them r is not an upper bdd of $L(\because \alpha$ is the smallest one).Hence,$r \notin B(\because$ every element of B is an upper bdd of L), so $\alpha \leq x, \forall x \in B$

We have proved $(r < \alpha \implies r \notin B) \implies (r \in B \implies r \geq \alpha)$

(ii) α is the greated one

if $\alpha < \beta$ and β is a lower bdd of B, then $\beta \notin L$, i.e. β is not a lower bdd of B, so α is the greatest one. Therefore, $\alpha = \inf(B)$

■

Remark. *Let* $E(\neq \emptyset) \subseteq \mathrm{R}$ *be bdd below, then* $\inf(E)$ *exists and* $\inf(E) = -\sup(-E)$*, where* $-E = \{ -x \mid x \in E \}$

1.4. Field.

Recall the addition & multiplication in R
$+ : \mathrm{R} \times \mathrm{R} \to \mathrm{R}((a, b) \mapsto a + b)$
$\times : \mathrm{R} \times \mathrm{R} \to \mathrm{R}((a, b) \mapsto a \cdot b = ab)$

Definition. *Let* X *is a nonempty set A, binary operation on* X *is a function,* $o : X \times X \to X$

Definition. *Let* F *be a nonempty set, we say that* F *is a field* ($(F, +, \cdot)$ *is a field) if there are two binary operator called addition* "$+$" *and multiplication* "$\cdot$" *on* F *property*

Axioms for $" + "$

(A1) Commutative: $\forall x, y \in \mathrm{F},\ x+y=y+x$

(A2) Associative: $\forall x, y, z \in F, (x+y)+z = x+(y+z)$

(A3) Additive identity or zero element: $\exists\ 0 \in F \implies x+0=0+x=x,\ \forall x \in \mathrm{F}$

(A4) Additive inverse on negative: For each $x \in X,\ \exists\ -x \in F \implies x+(-x) = (-x)+x = 0$

i.e. $(\mathrm{F},+)$ *is an abelian group* ***Axioms for multiplication***

(M1) Commutative: $\forall x, y \in \mathrm{F},\ xy = yx$

(M2) Associative: $\forall x, y, z \in \mathrm{F},\ (xy)z = x(yz)$

(M3) Muti identity: $\exists 1 \neq 0$ *in* $\mathrm{F} \ni x1 = 1x = x$

(M4) Multiplicative inverse: For each $x \neq 0, \exists x^{-1} \in \mathrm{F} \implies xx^{-1} = x^{-1}x = 1$

i.e. $(F = F \cdot \{0\}, \cdot)$ *is an abelian group*
Distributive Law

(D1) $\forall x, y, z \in \mathrm{F},\ (x,y)z = xz+yz\ \&\ x(y+z) = xy+xz$

Induction from Axioms
let $(\mathrm{F},+,\cdot)$ be a field, we list a series of basic identity as you learn in high school in the real number system

(a) Cancellation law for $" + "$: $x+y=x+z \implies y=z$

$\because x+y=x+z \implies (-x)+(x+y) = (-x)+(x+z) \implies ((-x)+x)+y = ((-x)+x)+z$ $\implies 0+y=0+z \implies y=z$

(b) 0 is "1"

suppose $0' \in \mathrm{F}$ is another element satisfy A_3, then $0 = 0+0' = 0'$

(c) $x+y=x \implies y=0$ by (a) $\because x+y=x+0 \implies y=0$

(d) negative $-x$ of x is "1"

if $x' \in F$, is another negative of x, them $x+x' = x'+x = 0$

From $x+x'=0 \implies (-x)+(x+x') = -x+0 = -x$

(e) $x+y=0 \implies y=-x$

$x+y=0 \implies (-x)+(x+y)=(-x)+0 \implies ((-x)+x)+y=-x$

$\implies 0+y=-x \implies y=-x$

(f) $-(-x)=x$

$-(-x)+(-x)=0$, By (d) $x=-(x)$

(a') cancellation law

if $x\neq 0$, then $xy=xz \implies y=z, \quad \because (x^{-1})(xy)=(x^{-1})(xz)$

$\implies (x^{-1})(xy)=(x^{-1}x)z \implies 1y=1z \implies y=z$

(b') 1 is "1"

if $1'$ is another identity, then $1=11'=1'$

(c') $x\neq 0$ & $xy=x \implies y=1$

$xy=x1 \implies y=1$

(d') For $x\neq 0$ in F, x^{-1} is "1"

if x is another one, i.e. $x'x=xx'=1 \implies (x^{-1})(xx')=(x^{-1})1=x^{-1}$

(f') $x\neq 0 \implies (x^{-1})^{-1}=x$

$(x^{-1})^{-1}(x^{-1})=1 \implies x=(x^{-1})^{-1}$

(g') $0x=x0=0$

$(0+0)x=0x+0x \implies 0x=0$

(h') $x\neq 0$ & $y\neq 0 \implies xy\neq 0$, equivalently $xy=0 \implies x=0$ or $y=0$

$\because xy=0$ then $(x^{-1})(xy)=((x^{-1})x)y=1y=y(\rightarrow\leftarrow)$

(i') $(-x)y=-(xy)=x(-y)$

$\because [(-x)+x]y=0y=0=(-x)y=-(xy) \implies (-x)y=-(xy)$

(j') $(-x)(-y)=xy$

$\because (-x)(-y)=-(x(-y))$ by (i)

$=-(-(xy))=xy$

(k) $-x=(-1)x$

$\because (1-1)x=0x=0=1x+(-1)x=x+(-1)x \implies (-1)x=-x$

Definition (Order Field). *Let* F *is a field, we say that* F *is an order field if there is an ordering* $" < "$ *satisfying*

(1) if $x < y$, then $x + z < y + z$, $\forall z \in F$

(2) if $x > y$ and $y > 0$, then $xy > 0$

Example. Q *and* R *are order field under the usual ordering*
Some basic properties of ordered field, let F *be an ordered field with ordering* $" < "$

(a) $x > 0 \implies -x < 0$

$\because x > 0 \implies x + (-x) > 0 + (-x) \implies 0 > -x$

(b) $x > y \Leftrightarrow x - y > 0$

$\because x > y \implies x + (-y) > y = (-y) \implies x - y > 0$

$x - y > 0 \implies x - y + y > y \implies x + 0 > y \implies x > y$

(c) $x > 0$ and $y < z \implies xy < xz$

$\because x > 0$ and $y < z \implies x > 0$ and $z - y < 0 \implies x(z - y) > 0 \implies xz + x(-y) > 0$
$\implies xz - xy > 0 \implies xz > xy$

(d) $x < 0$ and $y < z \implies xy > xz$

$\because x < 0$ and $y < z \implies -x > 0$ and $z-y > 0 \implies (-x)(z-y) > 0 \implies -xz+xy > 0$
$\implies xy > xz$

(e) $\forall x \neq 0$ in $\mathrm{F}, x^2 > 0$

$\because x > 0 \implies x \cdot x > x0$ by (c) or

$x < 0 \implies -x > 0$ by (a) $\implies -x > 0$ by (a) $\implies (-x)^2 > 0 \implies x^2 > 0$

(f) $1 > 0, \ -1 < 0$

$\because 1 \neq 0 \implies 1^2 > 0$ by (e) $\implies 1 > 0$

(g) $0 < x < y \implies 0 < \frac{1}{y} < \frac{1}{x}$

$\because$ Note that $\forall u \in \mathrm{F}, \ u > 0 \implies \frac{1}{u} = u^{-1} > 0$

$\because$ if $\frac{1}{u} < 0$, then $u \cdot \frac{1}{u} < 0$ by (e) $\implies 1 < 0 (\rightarrow\leftarrow) \ \therefore \ \frac{1}{u} > 0$

Now, $\frac{1}{x}, \frac{1}{y} > 0$ from $x < y$ we get $(\frac{1}{x} \cdot \frac{1}{y})x < (\frac{1}{x} \cdot \frac{1}{y})y \implies 0 < \frac{1}{y} < \frac{1}{x}$

Remark. *By (e)(f), we conclude that* $\mathbb{C}$ *is not an ordered field*
$\because \mathbb{C}$ *were an ordered field, then by (e),* $i^2 > 0 \implies -1 > 0 (\rightarrow\leftarrow)$
$\therefore \mathbb{C}$ *is not an order field*

1.5. The Real Number Field $\mathbb{R}$.

Theorem. *There exists an ordered field* $\mathbb{R}$ *containing* $\mathbb{Q}$ *which has the l.u.b. property. Moreover, such* $\mathbb{R}$ *is unique up to order-isomorphism*
i.e. if " $<$ " *and* " $<'$ " *are two orders on* $\mathbb{R}$*, them* $\exists f_i(\mathbb{R}, <) \to (\mathbb{R}, <') \implies$

(i) f *is a field isomorphism,*

   i.e. $\forall a, b \in \mathbb{R},\ f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b),\ f(1) = 1$

(ii) f *preserves ordering,* $a < b \implies f(a) < f(b)$

Such $\mathbb{R}$ *is called the real number field or real number system or real line*

Theorem.

(a) *The Archimedean property of* $\mathbb{R}$: *Given* $x, y \in \mathbb{R}$ *with* $x > 0,\ \exists\ n \in \mathbb{N} \implies nx > y$

(b) $\mathbb{Q}$ *is dense in* $\mathbb{R}$: $\forall x, y \in \mathbb{R}$ *with* $x \leq y,\ \exists\ r \in \mathbb{Q} \implies x < r < y$

Proof.

(a) Let $A = \{\, nx \mid n \in \mathbb{N} \,\} \subseteq \mathbb{R}$

   if (a) were false, them A is bdd above by y, since $\mathbb{R}$ has the l.u.b property

   $\alpha = \sup A$ exists in $\mathbb{R}$, since $x > 0,\ \alpha - x < \alpha \implies \alpha - x$ is not an upper bdd of A

   $\implies \exists m \in \mathbb{N} \ni mx > \alpha - x \implies (m+1)x > \alpha (\rightarrow\leftarrow)$

(b) Since $x < y,\ y - x > 0$, by (a),$\exists n \in \mathbb{N} \implies n(y-x) > 1$

   By (a) again, $\exists m_1, m_2 \in \mathbb{N} \implies m_1 = m_1 1 > n_x\ \&\ m_2 = m_2 \cdot 1 > -nx$

   we have $-m_2 < nx < m_1$, choose $m \in \mathbb{Z} \implies -m_2 \leq m \leq m_1\ \&\ m - 1 \leq nx < m$

   (in fact, $m = [nx] + 1$,where $[z]$ in the greatest integer of z)

   we have $nx < m < 1 + nx < ny (\because n(y-x) > 1) \implies x < \dfrac{m}{n} < y$

   Let $r = \dfrac{m}{n} \in \mathbb{Q}$, then $x < r < y$

$\blacksquare$

An application of the density property of Q in R :
Given $x \in \mathrm{R} - \mathrm{Q}$ i.e. x is an irrational numbers, i.e. $\forall\ \epsilon > 0, \exists r \in \mathrm{Q} \implies |x - r| < \epsilon$
equivalently, $\exists$ a sequence $\{ r_n \}$ in Q $\implies r_n \to x$
In fact, one may choose $\{ r_n \}$ to $\uparrow$ or $\downarrow$
$\because \forall n \geq 1,\ \exists\ r_n \in \mathrm{Q} \implies x < r_n < \dfrac{1}{n} + x$ by Thm.1.3(b) By squeezing lemma, $r_n \to x$ on $n \to \infty$

Theorem (existence of nth root)**.** *Given* $x \in \mathrm{T}, x > 0\ \&\ n \in \mathrm{N}, \exists$ "1"$y > 0 \implies y^n = x$
Such y *is called the* nth *root of* x & *denoted by* $y = \sqrt[n]{x} = x^{\frac{1}{n}}$

Proof. **not important**
"1". Suppose $y_1, y_2 > 0 \implies y_1^n = x\ \&\ y_2^n = x$
Bt trichotomy, we have

(i) $0 < y_1 < y_2 \implies y_1^n < y_2^n (\rightarrow\leftarrow)$

(ii) $0 < y_2 < y_1 \implies y_2^n < y_1^n (\rightarrow\leftarrow)$

(iii) $y_1 = y_2$

"$\exists$". Let $E = \{ t \in \mathrm{R} \mid t^n < x \}$
Claim:

- $E \neq \emptyset$, Let $t = \dfrac{x}{1+x}$, then $0 < t < 1$, hence $t^n < t < x$, $\therefore t \in E\ \&\ E \neq \emptyset$
- E is bdd above, in fact E is bdd above by $1 + x$ if $t > 1 + x > 1$, then $t^n > t > x$, so E is bdd above by $1 + 1$

  Therefore $y = \sup E$ exists & is finite
- Claim $y > 0\ \&\ y^n = x$, clearly, $y > 0 (\because \dfrac{x}{1+x} \in E\ \&\ \dfrac{x}{1+x} > 0)$

  by trichotomy, we have $y^n < x,\ y^n > x,\ y^n = x$

Now, to show that (i) & (ii) are impossible, do (iii) holds $y^n = x$
By the identity, $b^n - a^n = (b - a)(b^{n-1} + b^{n-2}a + \cdots + a^{n-1})$
(i)$y^n < x$ choose $0 < h < 1 = \alpha\ \&\ 0 < \dfrac{x - y^n}{n(y+1)^{n-1}}$, $0 < h < \min \{ \alpha, \beta \}$
put $a = y,\ b = y + h$ in $(\star)$, we obtain

$$(y + h)^n - y^n < hn(y - h)^{n-1} < hn(y + 1)^{n-1} < x - y^n$$

$\implies (y + h)^n < x \implies y + h \in E\ \&y + h > y (\rightarrow\leftarrow) \therefore$ (i) fails

(ii) $y^n > x$, Let $k = \dfrac{y^n - x}{ny^{n-1}}$, Then $0 < k < y,\ k = \dfrac{y^n - x}{ny^{n-1}} < \dfrac{y^n}{ny^{n-1}} = \dfrac{y}{n} < y$

if $t > y - k > 0$, then $y^n - t^n \leq y^n - (y-k)^n < kny^{n-1}$ by $(\star) = y^n - x$

$\implies t^n > x \implies t \in E \implies E$ is bdd above by $y - k \implies \sup E \leq y - k (\rightarrow\leftarrow)$

$\therefore$ (ii) fails ■

Corollary. *Let* $a, b \in \mathbb{R}$ *with* $a, b > 0,\ n \in \mathbb{N}$ *Then*$(ab)^{\frac{1}{n}} = a^{\frac{1}{n}} b^{\frac{1}{n}}$

$\because a^{\frac{1}{n}}, b^{\frac{1}{n}} > 0$ & $(a^{\frac{1}{n}} \cdot b^{\frac{1}{n}}) = ab$, *By (1) in Thm 1.4* $(a,b)^{\frac{1}{n}} = a^{\frac{1}{n}} b^{\frac{1}{n}}$

infinite in $\mathbb{R}$

After discuss the real number $\mathbb{R}$, sometimes, we have to work with the extended real number system $\mathbb{R}^* = [-\infty, \infty] = \mathbb{R} \cup \{+\infty, -\infty\}$ with observe, $x \in \mathbb{R}$

$$\lim_{n\to\infty} (-n) = -\infty,\quad \lim_{n\to\infty} n = \infty,\quad \lim_{n\to\infty} (\frac{1}{n} + n) = \infty,\quad \lim_{n\to\infty} (n^2 - n) = \infty$$

$$x \pm \infty = \pm\infty,\ 0 \cdot (\pm\infty) = 0,\ \infty - \infty \text{ is not define}$$

Element in $\mathbb{R} \subseteq \mathbb{R}^*$ are called finite. Now, given any nonempty subset $E \subseteq \mathbb{R}$,

$$\sup E = \begin{cases} +\infty \text{ if } E \text{ is not bdd above} \\ \text{finite if } E \text{ is bdd above} \end{cases} \quad \& \ \inf E = \begin{cases} -\infty \text{ if } E \text{ is not bdd below} \\ \text{finite if } E \text{ is bdd below} \end{cases}$$

Note that if $A \subseteq B$, then $\sup A \leq \sup$ & $\inf A \geq \inf B$

$\therefore \emptyset \subseteq B,\ \forall B \subseteq \mathbb{R}$, One may define $\sup \emptyset = -\infty, \inf \emptyset = +\infty$

1.6. The Complex Number Field $\mathbb{C}$.

Consider the contention product $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{\, (a, b) \mid a, b \in \mathbb{R} \,\}$
Note that $(a, b) = (c, d) \Leftrightarrow a = c \;\&\; b = d$, From now, we can write $\mathbb{C} = \mathbb{R}^2$

Operation on $\mathbb{C}$ Given $(a, b), (c, d) \in \mathbb{C}$

1. $(a, b) + (c, d) = (a + c, b + d)$
2. $(a, b)(c, d) = (ac - bd, ad + bc)$

It is easy to see that, with these operations, $\mathbb{C}$ is a field.

Note that

- the zero element is $(0, 0)$
- the negative of (a, b) is $-(a, b) = (-a, -b)$
- the identity is $(1, 0)$
- if $(a, b) \neq (0, 0)$, then $(a, b)^{-1} = \left(\dfrac{1}{a^2 + b^2}, \dfrac{-b}{a^2 + b^2} \right)$

R is a subset of C (not vary important)
consider that map

$$f : \mathbb{R} \to \mathbb{C} \text{ define by } f(a) = (a, 0),\; a \in \mathbb{R}$$

we have $(1)f$ is injective $(2)f(1) = (1, 0)$ $\because \forall\, a, b \in \mathbb{R}$
$f(a + b) = (a + b, 0) = (a, 0) + (b, 0) = f(a) + f(b),\; f(a \cdot b) = (ab, 0) = (a, 0) \cdot (b, 0)$
f is a field homomorphism
$\therefore f : \mathbb{R} \to \mathbb{C}$ is an injective and isomorphism
Therefore, we identify $\mathbb{R}$ with $f(\mathbb{R})$ through the injective f
i.e. $a \in \mathbb{R}$ is identified with $f(a, 0)$ in $\mathbb{C}$
$ab = (a, 0) \cdot (b, 0),\; a + b = (a, 0) + (b, 0) \;\forall\, a, b \in \mathbb{R}$

Change (a,b) to $a+bi$

Now, we can transform an element $(a,b) \in \mathbb{C}$ into the normal form:

$$(a,b) = (a,0) + (0,b) = (a,0)(1,0) + (b,0)(0,1) = a1 + bi = a + ib, \text{ where } i = (0,1)$$

Therefore, from new on, we write $\mathbb{C} = \{\, a + ib \mid a, b \in \mathbb{C} \,\}$
An element $z = a + ib \in \mathbb{C}$ is called a complex number
Hence, under this notification, $z = a + ib, w = c + id \in \mathbb{C}$

1. $z + w = (a + c) + i(b + d)$

2. $zw = (ac - bd) + i(ad + bc)$

and the a is called the real part of z, $a = \mathrm{Re}(z)$, b is called imaginary part of z, $b = \mathrm{Im}z$

Some basic properties of complex numbers whose proofs are easy
$\forall z, w \in \mathbb{C}$

- $\overline{z+w} = \overline{z} + \overline{w}$
- $\overline{zw} = \overline{z} \cdot \overline{w}$
- $\mathrm{Re}z = \dfrac{z + \overline{z}}{2}$
- $\mathrm{Im}z = \dfrac{z - \overline{z}}{2i}$
- $|z| = 0 \Leftrightarrow z = 0$
- Triangle inequality $|z + w| \leq |z| + |w|$
- $||z| - |w|| \leq |z - w|$
- $\mathbb{C}$ is not an ordered field
- $|z|^2 = z\overline{z}$
- $|\overline{z}| = |z|$
- $|\mathrm{Re}z| \leq |z|, |\mathrm{Im}z| \leq |z|$
- $|zw| = |z||w|$

Proof. $|z + w| \leq |z| + |w|$
$|z + w|^2 = (z + w)(\overline{z + w}) = (z + w)(\overline{z} + \overline{w}) = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w}$
$= |z|^2 + 2\mathrm{Re}(z\overline{w}) + |w|^2 \leq |z|^2 + 2|z\overline{w}| + |w|^2 = |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2$
$\therefore |z + w| \leq |z| + |w|$ ∎

Theorem (basic algebraic theorem)**.**
(a) $x^2 + 1$ has no root in $\mathbb{R}$
(b) $x^2 + 1$ has two distinct roots in $\mathbb{C}$

Proof.

(a) $1 > 0,\ x^2 > 0,\ \forall x \in \mathbb{R} - \{\,0\,\} \implies x^2 + 1 > 0\ \forall x \neq 0$

$0^2 + 1 = 1 > 0, \quad \therefore x^2 + 1 > 0,\ \forall\ x \in \mathbb{R}.$ Hence, $x^2 + 1 = 0$ has no root in $\mathbb{R}$

(b) $i^2 = (0,1)(0,1) = (0-1,0) = (-1,0) = -1$

$(-i)^2 = (-(0,1))^2 = (0,-1)^2 = (0,-1)(0,-1) = -1,\ \therefore \pm i$ are root of $\mathbb{C}$

■

Conclusion: Every non const polynomial $f(x) \in \mathbb{R}[x]$ has n roots where $n = \deg f(x)$

The complex root is even

no important proof

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x],\ a_n \neq 0,\ n \geq 1$

if $\alpha = a + ib \in \mathbb{C}$ is a root of $f(x)$,then

$0 = f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$

$0 = f(\overline{\alpha}) = a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \cdots + a_1\overline{\alpha} + a_0$

$\therefore (x-\alpha)|f(x),\ (x-\overline{\alpha})|f(x) \implies (x-\alpha)(x-\overline{\alpha})|f(x) \implies (x^2-(\alpha-\overline{\alpha})x+|\overline{\alpha}|^2) \mid f(x)$

$\implies (x^2 - 2ax + (a^2 + b^2)) \mid f(x)$

$\therefore$ quadratic function must have two roots in $\mathbb{C}$

The fundamental Theorem of Algebra

Every non zero polynomial $f(x) \in \mathbb{C}[x]$ has at least one root in $\mathbb{C}$

Therefore, if $\deg f(x) = n$, then $f(x)$ has n roots in $\mathbb{C}(C, M)$

$\because f(x) = (x-\lambda_1)^{e_1}\cdots(x-\lambda_t)^{e_t}(a_1x^2+b_1+c_1)^{l_1}\cdots(a_sx^2+b_sx+c_s)^{ls}$, where $\lambda_1, \cdots, \lambda_t \in \mathbb{R},\ a_i, b_i, c_i \in \mathbb{R} \& e_1 + \cdots + e_t + 2l_1 + \cdots + 2l_s = \deg f(x)$ which shows that all roots of $f(x)$ are in $\mathbb{C}$

In fact, we have the famous theorem: The fundamental theorem of algebra

Every non zero polynomial $f(x) \in \mathbb{C}[x]$ has at least one root in $\mathbb{C}$

$\therefore$ if $\deg f(x) = n$, then $f(x)$ has n roots in $\mathbb{C}(C, M)$

Theorem (Cauchy-Scheming Inequal). *Given $z_1 \cdots, z_n, w_1, \cdots, w_n \in \mathbb{C}$, we have*

$$\left|\sum_{j=1}^{n} z_j \overline{w}_j\right| \le \left(\sum_{j=1}^{n} |z_j|^2\right)^{\frac{1}{2}} \left(\sum_{j=1}^{n} |w_j|^2\right)^{\frac{1}{2}}$$

and $" = "$ *holds* $\Leftrightarrow \exists\ \lambda \in \mathbb{C} \ni\ w_j = \lambda z_j,\ 1 \le j \le n,$
In patricial, if $x_1, \cdots, x_n, y_1, \cdots, y_n \in \mathbb{R}$, *then*

$$\left|\sum_{j=1}^{n} x_j y_j\right| \le \left(\sum_{j=1}^{n} x_j^2\right)^{\frac{1}{2}} \left(\sum_{j=1}^{n} y_j^2\right)^{\frac{1}{2}}$$

and $" = "$ *holds* $\Leftrightarrow \exists\ t \in \mathbb{R} \ni\ y_j = t x_j,\ 1 \le j \le n$

The proof is too long, I am lazy

1.7. Euclidean Spaces $\mathbb{R}^n$.

Definition. *the n-dimensional Euclidean space* $\mathbb{R}^n$

$$= \{\, x = (x_1, \cdots, x_n) \mid x_i \in \mathbb{R}, 1 \le i \le n \,\} = \mathbb{R} \times \cdots \times \mathbb{R}$$

Note that

$$(x_1, \cdots, x_n) = (y_1, \cdots, y_n) \Leftrightarrow x_i = y_i\ \forall\ 1 \le i \le n$$

We are going to introduce the structure of $\mathbb{R}^n$

- vector space
- inner product space
- normed linear space
- matrix space

Definition. *Two operation on* $\mathbb{R}^n$ *as follows:*

- *Addition* $+ : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n,\ (x, y) \mapsto x + y = (x_1 + y_1, \cdots, x_n + y + n)$
- *Scalar multiplication* $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n,\ (a, x) \mapsto ax = (ax_1, \cdots, ax_n)$

we skip space example here.

1.8. Countability of Sets.

Given two nonempty set A, B and a function $f : A \to B, f(A) = \{ f(a) \mid a \in A \}$ is called the image of A under f

Some basic things

$E \subseteq A,\ f(E) = \{ f(a) \mid a \in E \}$ the image of E under f
f is infective(one-to-one) $x_1 \neq x_2 \implies f(x_1) \neq f(x_2) \Leftrightarrow f(x_1) = f(x_2) \Leftrightarrow x_1 = x_2$
f is surjective(onto) if $f(A) = B,\ f$ is bijective if f is one-to-one and onto

Given $F \subseteq B,\ f^{-1}(F) = \{ x \in X \mid f(x) \in \text{F} \}$ called the inverse image of f under F

Example

$f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2,\ x \in \mathbb{R}$
$f^{-1}([0,1]) = \{ x \in \mathbb{R} \mid f(x) \in [0,1] \} = \left\{ x \in \mathbb{R} \mid x^2 \in [0,1] \right\} = [-1,1]$
$f^{-1}([-1,1]) = [-1,1]$

Properties of inverse image

- $F_1 \subseteq F_2 \subseteq B \implies f^{-1}(F_1) \subseteq f^{-1}(F_2)$
- Inverse image presences set operation

  $\forall F_\alpha \subseteq B,\ \alpha \in I,\ F \subseteq B$

  (i) $f^{-1}(\cup_{\alpha \in I} F_\alpha) = \cup_{\alpha \in I} f^{-1}(F_\alpha)$
  (ii) $f^{-1}(\cap_{\alpha \in I} F_\alpha) = \cap_{\alpha \in I} f^{-1}(F_\alpha)$
  (iii) $f^{-1}(B - F) = f^{-1}(B) - f^{-1}(F)$
- Given $S \subseteq A,\ f'(f'(S)) \supseteq S,$" = " $\Leftrightarrow$ one-to-one, **example:**

  $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2,\ S = [0,1],\ f(S) = [0,1],\ f^{-1}(f(S)) = f^{-1}([0,1]) = [-1,1]$
- Given $F \subseteq B,\ f(f^{-1}(F)) \subseteq F,$" = " $\Leftrightarrow$ "onto", **example**

  $f(x) = x^2,\ x \in \mathbb{R},\ F = [-1,1],\ f(f^{-1}([-1,1])) = f([-1,1]) = [0,1]$
- For $y \in B,\ f^{-1}(\{ y \}) = f^{-1}(y) = \{ x \in A \mid f(x) = y \}$ the inverse image of y, **example**

  $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2,\ f^{-1}(1) = \{ 1, -1 \},\ f^{-1}(2) = \emptyset$

Definition (cardinality)**.** *Let A, B are two set ew say that A and B have the same cardinality if $\exists$ a bijective map $f : A \to B$, which is denoted by $A \sim B$*
From now on, we write $|A|$ as the cardinality of A

Claim " $\sim$ " is an $\equiv$ relation among all sets

(i) Reflexion: $\forall$ set A, $A \sim^{1A} A$, which 1_A is identity mapping

(ii) Symmetry: $A \sim^f B \implies B \sim^{f^{-1}} A$

(iii) Transitive: $A \sim^f B$ & $B \sim^g C \implies A \sim^{gof} C$

So we gave some property:

- Any two " $\equiv$ " are either disjoint or identical
- $\underline{\overline{X}}$ is a disjoint union of " $\equiv$ " classes
  $[A] = \{ B \in \underline{\overline{X}} \mid B \sim A \}$ the " $\equiv$ " class set by A

Ant two element in an " $\equiv$ " class have the same cardinality
Notation For $n \in \mathbb{N}$, $\mathbb{N}_m = \{ 1, 2, \cdots, n \}$

Definition. *Let A be a set*

(a) A is a finite set if $A = \emptyset$ or $A \sim \mathbb{N}_n$ for some $n \in \mathbb{N}$

(b) A is a infinite set if A is not a finite set

(c) A is countable if $A \sim \mathbb{N}$

(d) A is uncountable if A is not countable.

(e) A is at most countable if A is finite or countable

Remark.

1. *when A, B are finite sets, $A \sim B \Leftrightarrow |A| = |B|$, i.e. A, B have same number.*
2. *where A, B are infinite and $A \sim B$, i.e. $|A| = |B|$, the concept is abstract.*
3. $\{ a, b, c \} \cup \mathbb{N} \sim \mathbb{N}$, $f : \mathbb{N} \to \{ a, b, c \} \cup \mathbb{N}$, $f(1) = a$, $f(2) = b$, $f(3) = c, \cdots$
4. *Any finite set can not equivalent to a proper subset, i.e. A is finite, $B \subsetneq A$*
   Then $A \nsim B$, In fact $|B| < |A|$, but infinite different
5. *Any finite set A can be listed an $A = \{ a_1, \cdots, a_n \}$ where $n = |A|$*

Now, we consider the case of countable set

Recall, in calculus, a real sequence $\{ a_n \}$, e.g.

$$a_n = \frac{1}{n} \left\{ \frac{1}{n} \right\},\ a_n = 1 - \frac{1}{n}\ \left\{ 1 - \frac{1}{n} \right\},\ a_n = \begin{cases} 0 \text{ if } n \text{ is odd} \\ 1 \text{ if } n \text{ is even} \end{cases}$$

Definition. *Let X be a nonempty set, a sequence in X is a function $a : \mathbb{N} \to X$*
Given a sequence $=^a$ in X, a is "1" determine by $a(n),\ \ \in \mathbb{N}$
We write

$$a = \{ a(1), a(2), \cdots, a(n), \cdots \} = \{ a_1, a_2, \cdots, a_n, \cdots \} = \{ a_n \} = \{ a_n \}_{n=1}^{\infty}$$

Remark.

1. *For a sequence $\{ a_n \}$ in X, a_n may not be distinct.*

   If all a_n are distinct, then we say that $\{ a_n \}$ is a distinct sequence in X.

2. *We usually use $\{ a_n \}, \{ b_n \}$ to denote sequence*

3. *A sequence $\{ a_n \}$ in X in fact is a function from $\mathbb{N} \to X$, So $\{ a_n \mid n \in \mathbb{N} \}$ is the image of the sequence.*

4. *$\{ a_n \}$ is a sequence, a_n is called the n^{th} term of the sequence.*

5. *A sequence in X may begin at 0, i.e. $\{ a_n \}_{n=0}$*

   By a changing index, we can make it from $\{ b_n \}_{n=1}^{\infty}$, $b_n = a_{n+1},\ n = 1, 2, \cdots$

Definition (increasing)**.**
A function $a : \mathbb{N} \to \mathbb{N}$ is increasing, a is $\uparrow$, if $a(n) \leq a(n+1)\ \forall\ n \geq 1$
a is strictly increasing, a is st. $\uparrow$, if $a(n) < a(n+1)\ \forall\ n \geq 1$

Now, given a st. $\uparrow$ function $n : \mathbb{N} \to \mathbb{N}$, i.e. $n(k) < n(k+1),\ k \geq 1$
i.e. $n_k < n_{k+1},\ k \geq 1$, i.e. $n_1 < n_2 < \cdots < n_k < \cdots$, i.e. $\{ n_k \}_{k=1}^{\infty}$ is a st. sequence in $\mathbb{N}$

<u>Definition</u>. *Let* $\{ a_n \}$ *be a sequence in* X *and* $\{ n_k \}$ *be a st.* $\uparrow$ *sequence in* $\mathbb{N}$, *then the sequence* $\{ a_{n_k} \}$ *is called a subsequence of* $\{ a_n \}$
In fact

$$\mathbb{N} \rightarrow^{n}_{st.} \mathbb{N} \rightarrow^{a}_{seq} X \Rightarrow a \circ n : \mathbb{N} \rightarrow X \text{ is a function,}$$

hence, it also a sequence in X

$$a \circ n = \{ a \circ n(k) \} = \{ a(n(k)) \} = \left\{ a_{n(k)} \right\} = \{ a_{n_k} \}$$

Remark. *if* $\{ a_{n_k} \}$ *is st.* $\uparrow$ *in* $\mathbb{N}$, *then* $k \leq n_k \ \forall \ k \geq 1$
$\because$ *By mathematical Induction*

- $1 \leq n_1$
- *Assume it's true for* $k \geq 2$, *i.e.* $k \leq n_k$
- *Consider* $k+1$, $\ k+1 \leq n_k + 1 \leq n_{k+1}$

Example
Let $\{ a_n \}$ *be a sequence in* X, *then* $\{ a_{2k} \}$ *and* $\{ a_{2k-1} \}$ *are subsequence of* $\{ a_n \}$

Finally, we will assume that you are familiar with the following property of the countability of sets:

1. Every subset of a countable set is at most countable. The proof needs the well ordering of $\mathbb{N}$: Every nonempty subset of $\mathbb{N}$ has the smallest element
2. Countable union of countable sets is countable
3. If $A_1, A_2, \cdots, A_n$ are countable, then so is $A_1 \times \cdots \times A_n$
4. If A is countable, then so is $A^n \equiv A \times \cdots \times A \ \forall n \geq 1$
5. $\mathbb{N}, \ \mathbb{Z}, \ \mathbb{Q}, \ \mathbb{Q}^n, \ \forall n \geq 1$ are countable
6. The set $\{ a_n \mid a_n = 0 \text{ or } 1 \}$ is uncountable

   This can be proved by Canton diagonal process

   $\because$ if it is countable, then we can list it,$a_0 A = \left\{ a_1^{(1)}, a_2^{(2)}, \cdots \right\}$ where

   $a^{(1)} = \{ a_n^{(1)} \} = a_1^{(1)}, a_2^{(1)}, \cdots \ ; \ a^{(2)} = \{ a_n^{(2)} \} = a_1^{(2)}, a_2^{(2)}, \cdots$

   Now, construct a sequence $\{ a_n \}$ in $A \ni \{ a_n \} \neq a^{(k)} \ \forall \ k \geq 1 (\rightarrow\leftarrow)$

Recall, intervals in $\mathbb{R}$, $-\infty < a \leq b < \infty$, following are finite bdd interval

$(a,b) = \{ x \in \mathbb{R} \mid a < x < b \}$ open interval
$[a,b] = \{ x \in \mathbb{R} \mid a \leq x \leq b \}$ closed interval
$(a,b] = \{ x \in \mathbb{R} \mid a < x \leq b \}$ open-closed
$[a,b) = \{ x \in \mathbb{R} \mid a \leq x < b \}$ closed-open

An interval I in $\mathbb{R}$ is said to be non-degenerate if the endpoint of I are distinct i.e. length > 0. Otherwise, it is degenerate.

Note.

$(0,1)$ is uncountable, $\because (0,1) = \left\{ \sum_{n=1}^{\infty} \frac{a_n}{2^n} \mid a_n = 0 \text{ or } 1, n \in \mathbb{N} \right\}$
$x \in (0,1)$ has a unique binary representation, so $(0,1) \sim A$,
where A is $\{ \{ a_n \} \mid a_n = 0 \text{ or } 1 \}$ which is uncountable

All non-degenerate intervals in $\mathbb{R}$ are uncountable.
$\because$ It sufficient to consider bdd non-degenerate interval in $\mathbb{R}$, given $\infty < a < b < \infty$
(a,b) is uncountable$(\because (0,1) \sim (a,b))$
Note that $(0,1) \sim \mathbb{R}(\because (0,1) \to (\frac{\pi}{-2}, \frac{\pi}{2}) \to \mathbb{R})$