CHAPTER 1

SETS, REAL AND COMPLEX NUMBER SYSTEMS

1 Prelimnaries

Definition 1.1: Prelimnary definitions

1. (Cartesian Product): if A and B are non empty sets, the *Cartesian Product* $A \times B$ is defined as the set of ordered pairs a, b wherein $a \in A, b \in B$. i.e, $A \times B := \{(a, b) : a \in A, b \in B\}$
2. (Function): A function from A to B is a set $f \subseteq A \times B$ such that, $a, b \in f$ and $a, c \in f \implies b = c$. A is called the **Domain of** f. $Range(f) := f(A)$ (see next definition)
3. (Direct Image): Direct image $f(A) := \{y \in B : \exists x \in A \text{ such that } f(x) = y\}$
4. (Inverse Image):$f^{-1}(S \subseteq B) := \{x \in A : f(x) \in S\}$
5. (Relation): Any subset $R \subseteq A \times B$ is a relation from A to B.
   We say $x \in X$ is "related to" $y \in Y$ under the relation R, or simply xRy or $R(x) = y$ if $(x, y) \in R \subseteq X \times Y$.
6. (Injection): $f : A \to B$ is injective if $\forall x_1, x_2 \in A, (x_1, b) \in f$ and $(x_2, b) \in f \iff x_1 = x_2$
7. (Surjection): $f : A \to B$ is surjective if $\forall b \in B, \exists a \in A$ such that $f(a) = b$
8. (Bijection): $f : A \to B$ is bijective if its both surjective and injective.
9. (Identity function on a set): $I_A : A \to A$ defined by $\forall x \in A, I_A(x) = x$
10. (Permutation): Simply a bijection from A to itself is called a permutation.

Definition 1.2: (Left Inverse)

We say $f : A \to B$ has a left inverse if there is a function $g : B \to A$ such that $g \circ f = I_A$

Theorem 1.3

$f : A \to B$ has a left inverse if and only if it is injective.

Proof for Theorem.

$\implies$) If f has a left inverse g, Consider $x, y \in A$ such that $f(x) = f(y) = p$.
We have $g \circ f(x) = g(p) = x = g \circ f(y) = y$. Hence, $x = y$, Injective.
$\impliedby$) Given that $f : A \to B$ is injective, define $g : B \to A$ as:

$$g(z \in B) = \begin{cases} a, \text{ where } f(a) = z, \text{ if } z \in f(A) \\ \text{whatever, if } z \notin f(A) \end{cases}$$

consider $g \circ f(x \in A) = g \circ (f(x))$.
Obviously, $f(x) \in f(A)$, therefore, $g(f(x)) =$ that a such that $f(a) = f(x)$.
That a is x. Hence, $g(f(x)) = x$ ∎

Definition 1.4: (Right Inverse)

$f : A \to B$ is said to have a right inverse if there is a function $g : B \to A$ such that $f \circ g = I_B$

Theorem 1.5

$f : A \to B$ has a right inverse if and only if f is Surjective.

Proof for Theorem.

$\implies$) If f has a right inverse g, such that $f \circ g = I_B : B \to B$, then it is evident that the range of f is B, for if not, range of $f \circ g$ wouldn't be B either.
$\impliedby$) If f is surjective, then for all $b \in B$, there exists atleast one $a \in A$ such that $f(a) = b$ define g as:

$$g(x \in B) = \text{one of those a} \in A \text{ such that} f(a) = b$$

Consider $f \circ g(x \in B) = f($ one of the a such that $f(a) = b) = b, \forall b \in B$
Hence, $f \circ g = I_B$ ∎

Theorem 1.6

If f has left inverse g_1 and right inverse g_2, then $g_1 = g_2$. *(True for anything that is Associative, and function composition is associative.)*

Proof for Theorem.

> $g_1 \circ f = I_A$ and $f \circ g_2 = I_B$
> $g_1 \circ (f \circ g_2) = g_1 \circ I_B = g_1$
> $= (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2$
> Hence $g_1 = g_2$

Corollary 1.7

f is invertible (i.e, both left and right inverse exist) if and only if it is bijective.

Proof for Corollary.

> Obvious

1.1 Operations on Relations

If R and S are binary relations over $X \times Y$:

1. $R \bigcup U := \{(x, y) | xRy \text{ or } xSy\}$
2. $R \bigcap S := \{(x, y) | xRy \text{ and } xSy\}$
3. Given $S : Y \to Z$ and $R : X \to Y$, $S \circ R := \{(x, z) | \exists y \text{ such that } ySz \ \& \ xRy\}$
4. If R is binary over $X \times Y$, $\bar{R} := \{(x, y) | \neg(xRy)\}$

1.2 Homogeneous Relations

If R is a binary relation over $X \times X$, it is Homogeneous.

Definition 1.8: Definitions Regarding Relations

1. (Reflexive): $\forall x \in X, xRx$
2. (Symmetric): $\forall x, y \in X, xRy \implies yRx$
3. (Transitive): $\forall x, y, z \in X,$ if xRy & $yRz \implies xRz$
4. (Dense): $\forall x, y \in X,$ if $xRy,$ then there is some $z \in X$ such that xRz & zRy
5. (**Equivalence Relation**): R is an equivalence relation if it is Reflexive, Symmetric and Transitive.
6. (Equivalence class of $a \in A$(where there is an equivalence relation defined)): Set of all $b \in A$ such that bRa.
7. (Partition of A): Any collection of sets $\{A_i : i \in I\}$ (where I is some indexing set) such that:

$$A = \bigcup_{i \in I} A_i$$

$$A_i \cap A_j = \phi \text{ if } \forall i, j \in I, i \neq j$$

Theorem 1.9

Let A be a non-empty set. If R defines an equivalence Relation on A, then the set of all equivalence classes of R form a partition of A

Proof for Theorem.

Define our collection $\{A_\alpha\}$ as the set of all equivalence classes of A. Clearly, $\bigcup_{\alpha \in I} A_\alpha = A$. If A only has one element, obviously, that singleton set makes up the partition. Let A_α and $A_{\alpha'}$ be equivalence classes of two elements a and a' in A. If aRa', then $A_\alpha = A_{\alpha'}$ since every element in the equivalence class of a will, from the transitive property, be in the equivalence class of a' . Suppose $\neg(aRa')$. If, then, $\exists x \in A_\alpha$ such that $x \in A_{\alpha'}$, this means that $xR\alpha$ and $xR\alpha'$, but from transitive property, this means $\alpha R\alpha'$, which is a contradiction. Therefore, the pairwise intersection is disjoint. ∎

Theorem 1.10

If $\{A_i : i \in I\}$ is a partition of A, then there exists an equivalence relation R on A whose equivalence classes are $\{A_i : i \in I\}$.

Proof for Theorem.

Define $R(x, y)$ if and only if $\exists$ unique $m \in I$ such that $x \in A_m$ and $y \in A_m$.

$R(x, x)$ is obvious if non empty, hence R is reflexive.

Suppose $R(x,y)$ and $R(y,z)$. Then, there exists a unique $m \in I$ such that x, y are in A_m. Similarly, there exists a unique $n \in I$ such that y, z are in A_n . Obviously, if $n \neq m$, intersection of A_n and A_m would be non empty, hence, $n = m$. Hence, R is transitive.

Consider $R(x,y)$, which means $\exists$ unique $n \in I$ such that $x, y \in A_n \implies R(y,x)$. Hence, R is an equivalence relation. ∎

2 Induction, Naturals, Rationals and the Axiom of Choice

Axiom 2.1: Peano Axioms, characterisation of $\mathbb{N}$

1. $1 \in \mathbb{N}$
2. every $n \in \mathbb{N}$ has a predecessor $n-1 \in \mathbb{N}$ except 1
3. if $n \in \mathbb{N} \implies n+1 \in \mathbb{N}$

Definition 2.2: (Sequence of something)

A sequence of some object is simply a collection of objects $\{O_l : l \in \mathbb{N}\}$ which can be counted.

Axiom 2.3: Well Ordering Property of $\mathbb{N}$

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

Axiom 2.4: Weak Induction

For all subsets $S \subseteq \mathbb{N}$, $((1 \in S)\&((\forall k \in \mathbb{N})(k \in S \implies k+1 \in S)) \iff S = \mathbb{N})$

Weak Induction's Negation:(One direction)
There exists subset $S_0 \subseteq \mathbb{N}$, $((1 \in S_0)\&((\forall k \in \mathbb{N})(k \in S_0 \implies k+1 \in S_0))$ but $S_0 \neq \mathbb{N})$

Axiom 2.5: Strong Induction

For all subsets $S \subseteq \mathbb{N}$, $((1 \in S)\&((\forall k \in \mathbb{N})(1, 2, ...k \in S' \implies k+1 \in S')) \iff S = \mathbb{N})$

Strong Induction's Negation:(One direction)
There exists subset $S' \subseteq \mathbb{N}$, $((1 \in S')\&((\forall k \in \mathbb{N})(1, 2, ...k \in S' \implies k+1 \in S'))$ but $S' \neq \mathbb{N})$

Theorem 2.6

Weak Induction $\iff$ Strong Induction.

Proof for Theorem.

$\implies$) Suppose Weak induction is true, but not strong induction. Take our set to be that S' in the negation of the Strong Induction Statement. $S' \neq \mathbb{N}$ implies that, either $1 \notin S'$ or $\exists k \in \mathbb{N}$ such that $k \in S'$ but $k+1 \notin S'$. We know that $1 \in S'$, so it must be that $\exists k \in \mathbb{N}$ such that $k \in S'$ but $k+1 \notin S'$. $\{1\} \in S' \implies \{1,2\} \in S'$. Assume that for n, $\{1,2,..n\} \in S'$. This means that $\{1,2,...n+1\} \in S'$. This means that for every $n \in \mathbb{N}$, $\{1,2,...n\} \in S' \implies n \in S'$. Contradiction.
$\impliedby$)Suppose Strong Induction is true, but not weak induction. Take the set S_0 from the negation of Weak Induction. $S_0 \neq \mathbb{N}$. This means, from strong induction, either $1 \notin S_0$ or $\exists k \in \mathbb{N}$ such that $1, 2, \ldots, k \in S_0$ but $k+1 \notin S_0$. $1 \in S_0$, hence, $2 \in S_0$ and $\{1,2\} \in S_0$. assume that $\{1,2,....n\} \in S_0$. This means, $n \in S_0 \implies n+1 \in S_0$, which means that $\forall k \in \mathbb{N}, \{1,2,..k\} \in S_0 \implies k+1 \in S_0$. Therefore, S_0 is $\mathbb{N}$. ■

Theorem 2.7

Weak Induction $\iff$ Strong Induction $\iff$ Well ordering.

Proof for Theorem.

$\implies$) Suppose that, on the contrary, S_0 is a non empty subset of $\mathbb{N}$, with no least element. Does 1 exist in S_0? No, for that will be the least element. Likewise, then, 2 does not belong in S_0. Assume that $\{1,2,...n\} \notin S_0$. Does $n+1$ exist in S_0? No, for that will become the least element then. From Strong Induction, $\mathbb{N} - S_0 = \mathbb{N} \implies S_0 = \phi$. Contradiction.
$\impliedby$)Suppose $\exists S_0 \subseteq \mathbb{N}$ such that $1 \in S_0$ and $\forall k \in \mathbb{N}$, $k \in S_0 \implies k+1 \in S_0$. Suppose on the contrary, S_0 is not $\mathbb{N}$. $\mathbb{N} - S_0$ is then, non-empty. From Well Ordering, there is a least element $q \in \mathbb{N} - S_0$. $\implies, q-1 \in S_0$. But this would imply $q-1+1 \in S_0$. Contradiction. $\mathbb{N} - S_0$ is empty. ■

Definition 2.8: (Finite Sets)

A set X is said to be finite, with n elements in it, if $\exists n \in \mathbb{N}$ such that there exists a bijection $f : \{1, 2.., n\} \to X$. Set X is *infinite* if it is non-finite.

Theorem 2.9

If A and B are finite sets with m and n elements respectively, and $A \cap B = \phi$, then $A \cup B$ is finite, with $m+n$ elements.

Proof for Theorem.

$f : \mathbb{N}_m \to A$ and $g : \mathbb{N}_n \to B$.

Define $h : \mathbb{N}_{m+n} \to A \cup B$ given by:

$$h(i) = \begin{cases} f(i) \text{ if } i = 1, 2...m \\ g(i-1) \text{ if } i = m+1, m+2, ...m+n \end{cases}$$

If $i = 1, 2, ...m$,$h(i)$ covers all the elements in A through f. If $i = m+1, ...m+n$, $h(i)$ covers all the elements in B through g.

Moreover, $h(i) \neq h(j); i \in [1, m], j \in [m+1, m+n]$ since $A \cap B = \phi$ ∎

Theorem 2.10

If C is infinite, and B is finite, then $C - B$ is infinite.

Proof for Theorem.

Suppose $C - B$ is finite. We have $B \cap (C - B) = \phi$ and $B \cup (C - B) = C \cup B$

$n(C \cup B) = n(B \cup (C - B)) = n(B) + n(C - B)$ This implies $C \cup B$ is finite. Contradiction. ∎

Theorem 2.11

Theorem: Suppose T and S are sets such that $T \subseteq S$. Then:

a) If S is finite, T is finite.

b)If T is infinite, S is infinite.

Proof for Theorem.

Given that S is finite, there is a function $f : \mathbb{N}_m \to S$. Suppose that S has 1 element. Then either T is empty, or S itself, which means T is finite. Suppose that, upto n, it is true that, if S is finite with n elements, all its subsets are finite. Consider S with $n+1$ elements.

$f : \mathbb{N}_{n+1} \to S$.

If $f(n+1) \in T$, consider $T_1 := T - \{f(n+1)\}$ We have $T_1 \subseteq S - \{f(n+1)\}$, and since $S - \{f(n+1)\}$ is a finite set with $n-1$ elements, from induction hypothesis, T_1 is finite. Moreover, since $T = T \cup \{f(n+1)\}$, T is also finite with one more element than T_1.
If $f(n+1) \notin T$, then $T \subseteq S - \{f(n+1)\}$, we are done.

(b) is simply the contrapositive of (a). ∎

Definition 2.12: (Countable Sets)

A set S is said to be *countable*,or *denumerable* if, either S is finite, or $\exists f : \mathbb{N} \to S$ which is a bijection. If S is *not countable*, S is said to be *uncountable*

Theorem 2.13

The set $\mathbb{N} \times \mathbb{N}$ is countable.

Proof for Theorem.

The number of points on diagonals $1, 2, ...l$ are: $\psi(k) = 1 + 2 + ...k = \frac{k(k+1)}{2}$

The point (m, n) occurs on the $(m + n - 1$ th diagonal, on which the number $m + n$ is an invariant. The (m, n) point occurs m points down the diagonal. So, to characterise a point, it is enough to specify the diagonal it falls in, and its ordinate (the "rank" of that point on that diagonal). Count the elements till the $m + n - 2$nd diagonal, then add m, and this would be the position of the point (m, n).
Define $r : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $r(m, n) = \psi(m + n - 2) + m$ That this is a bijection is pretty clear because we are counting the position of the point (m, n). For a given point (m, m), there can only be one unique diagnonal on which it exists, and on the diagonal, its rank is unique. Moreover, for every $q \in N$, there corresponds an (m, n) such that $r(m, n) = q$, for, we simply count along each diagonal in the "zig-zag" manner until we reach that (m, n) for which the position is given by q. Therefore, r is a bijection. (There are other explicit bijections too)

Alt Proof (Slicker): Define the explicit map $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as:

$$f(m, n) = 2^m(2n - 1)$$

For every $k \in \mathbb{N}$, there exists a unique prime decomposition. Let m be the power of 2 in that, and n be so that the product of the rest of the primes (which is odd) comes to be $2n - 1$. From here, it is easy to see a bijection.

■

Theorem 2.14

The following are equivalent:

1. S is countable
2. $\exists$ a surjective function from $\mathbb{N} \to S$
3. $\exists$ an injective function from $S \to \mathbb{N}$

Proof for Theorem.

$(1 \implies 2)$ is obvious
$(2 \implies 3)$ $f : \mathbb{N} \to S$, every element of of S has atleast one preimage in $\mathbb{N}$. Define a function from $S \to \mathbb{N}$ by taking for each $s \in S$ the least such $n \in \mathbb{N}$ such that $f(n) = s$. This defines an injection.
$(3 \implies 1)$ If there is an injection from $S \to \mathbb{N}$, then there is a bijection from $S \to$ a subset of $\mathbb{N}$, which implies S is countable. ■

Corollary 2.15

The set of Rational Numbers $\mathbb{Q}$ is countable.

Proof for Corollary.

We know that a surjection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{Q}$ exists (where $f(0,0) = 0$, and $f(m,n) = \frac{m}{n}$). We know that $\mathbb{N} \times \mathbb{N}$ is bijective to $\mathbb{N}$. This means $\mathbb{N}$ is surjective to $\mathbb{Q}$. We are Done. ∎

Theorem 2.16

Every infinite subset of a countable set is countable.

Proof for Theorem.

Consider $N_s \subseteq \mathbb{N}$ which is infinite.

Define $g(1) =$ least number in N_s

Having defined $g(n)$, define $g(n+1)=$ least number in N_s which is larger than $g(n)$.

That it is an injection is obvious, for $g(m) > g(n)$ if $m > n$.

Suppose it is not a surjection, i.e, $g(\mathbb{N}) \neq N_s \implies g(\mathbb{N}) \subset N_s \implies N_s - g(\mathbb{N}) \neq \phi$ Therefore, $N_s - g(\mathbb{N})$ has a least element, k. This means that $k-1$ is in $g(\mathbb{N})$. Therefore, there exists q in $\mathbb{N}$ such that $g(q) = k-1$. But then, $g(q+1)=$ least number in N_s such that it is bigger than $g(q)$. This would, ofcourse be, k, which means $k = g(q+1)$, which puts k in $g(\mathbb{N})$. Contradicton. Hence, $g(\mathbb{N}) = N_s$, therefore, g is a bijection from $\mathbb{N} \to N_s$. Since every countable set is bijective to $\mathbb{N}$, and every infinite subset of a countable set is bijective to an infinite subset of $\mathbb{N}$, the theorem holds generally for countable sets. ∎

Theorem 2.17

$\mathbb{N} \times \mathbb{N} \cdots \mathbb{N}$ is bijective to $\mathbb{N}$

Proof for Theorem.

$\mathbb{N} \times \mathbb{N}$ is bijective to $\mathbb{N}$ obviously. Assuume that $f : \mathbb{N} \to \mathbb{N} \cdots \mathbb{N}(\text{ n times })$ is bijective.

Consider $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \cdots \mathbb{N}(n+1 \text{ times })$ given by $g(m,n) = (f(m), n)$. Clearly, this is bijective. ∎

2.1 Axiom of Choice

Axiom 2.18: Axiom of Choice (AC)

For any collection of non empty sets $C = \{A_l : l \in L\}$, there exists a function f called the "counting function" which maps each set A_l to an element in A_l.
Formally: $f : C \to \bigcup_l A_l$ such that $\forall l \in L, f(A_l) \in A_l$

Theorem 2.19

Countable union of Countable sets is countable *(This theorem is an example of a theorem that requires* Axiom of Choice*)*

Proof for Theorem.

Suppose we are given a sequence of countable sets $\{S_n : n \in \mathbb{N}\}$. Since each S_j is countable, we have for each j, at least one bijective map $f_j : \mathbb{N} \to S_j$. Define $k : \mathbb{N} \times \mathbb{N} \to \bigcup_j S_j$ given by: $k(m, n) = f_m(n)$. Suppose $x \in \bigcup_j S_j$, i.e, $x \in S_j$ for some j. This means that, $f(n) = x$ for some n. Therefore, $k(j, n) = x$. Hence, k is surjective. From theorem 2.14, we are done.

(**Remark:** Keep in mind, for each S_j, there are a myriad of functions $(f_j)_k : \mathbb{N} \to S_j$. For each S_j, which is countably infinite, we have to choose one of the many functions that biject $\mathbb{N}$ to S_j. So we have a countable collection of sets $C = \{E_j : j \in \mathbb{N}\}$, where E_j denotes the set of all functions that biject $\mathbb{N}$ into S_j. So for every element in C, we need to choose one element in each element of C. This is where the Axiom of Choice comes into play.) ∎

Theorem 2.20

If $f : A \to B$ is a surjection, then B is bijective to a subset of A

Proof for Theorem.

We are told that $f(A) = B$, i.e, for every $b \in B$, $\exists x_b$(many such x_b-s are possible) such that $f(x_b) = b$. Define a functino $g : B \to A$ as: $g(b) =$ one of those x_b such that $f(x_b) = b$. g is bijective to the set of all the chosen x_b for every b ∎

Remark.

We make use of the Axiom of Choice in the previous theorem when we choose an x_b from a set of all possible x_b-s for b. Let A_b be the set of all possible x_b-s. Then the collection $\{A_b : b \in B\}$ is a collection of non-empty sets. And we are to select "one" element from each A_b. This requires AC.

Definition 2.21: (Power Set of a set)

Power set of A, denoted by $P(A)$ is the set of all subsets of A.

Definition 2.22: Partial ordering relation on a set P

A "partial order" on a set is a relation $\leq$ defined on a set that follows:

1. $\forall x \in P, x \leq x$ (reflexive)
2. If $x, y \in P$ such that $x \leq y$ and $y \leq x$, then $x = y$ (antisymmetry)
3. forall $x, y, z \in P$, if $x \leq z$ and $z \leq y$, then $x \leq y$

Any set P that is partially ordered is called a **poset**. A set C which is totally ordered and is a subset of a poset P is called a **chain** of P.

Definition 2.23: Total Order on a set C

An ordering relation (that obeys the above conditions), added with the condition that, if $x, y \in C$, then it definitely must be that one of $x \leq y$ or $y \leq x$ is true. Then the set C is *totally* ordered.

Remark.

> For example, the order relation on R is a total ordering from the trichotomy property. Consider the ordering relation on $\mathbb{Z}$ as follows: If $a \in \mathbb{Z}$ divides $b \in \mathbb{Z}$, then $a \leq b$. This is a partial order, certainly. It is reflexive, anti symmetric and transitive. But 3 and 5 are unrelated in this definition. Whereas, consider the same ordering but in the space $1, p, p^2, \cdots$ where p is a prime, we then see that the set is totally ordered here.

Definition 2.24: Boundedness of a subset C of P, where a partial order is defined

We say set C in a poset P is bounded, or has an upper bound, if $\exists M \in P$ so that $\forall q \in C, q \leq M$.

Example :
We consider the power set of a set P, where inclusion is defined by $S \subseteq T$ if $\forall x \in S, x \in T$. This defines a partial ordering on the power set. ■

Axiom 2.25: Zorn's Lemma

Given a poset P, if for every chain C of P, there exists an upper bound M_c in P, then P has a maximal ememento with respect to $\leq$ (i.e, there exists M in P so that $x \leq M, \forall\ x \in P$)

Theorem 2.26

AC $\iff$ Zorn's Lemma

Proof for Theorem.

hmm

Some Corollaries of AC:

Theorem 2.27

Every vector space has a basis

Proof for Theorem.

Theorem 2.28

$|S| = |\text{set of all finite subsets of } S|$

Proof for Theorem.

Theorem 2.29

For an arbitrary dimensioned vector space, every linearly independent set is injective to any spanning set.

Proof for Theorem.

Theorem 2.30: Cantor's Theorem

For any set A, there *does not exist* any surjection from A onto $P(A)$

Proof for Theorem.

Suppose, on the contrary, a surjection $\psi : A \to P(A)$ exists. For every subset A_s of A, there exists an element x of A such that $\psi(x) = A_s$. Either this x exists in A_s, or it doesnt. Conider $D := \{x \in A : x \notin \psi(x)\}$. D is a subset of A, so there must be some element $y \in A$ such that $\psi(y) = D$. does y belong in D? If so, $y \notin \psi(y) = D$. Which means $y \notin D$. If, though, $y \notin D$, that implies $y \notin \psi(y) \implies y \in D$. Contradictions left and right. ∎

3 The Real and Complex Fields

Definition 3.1: (Field $(F, +, \cdot)$)

set F, along with two functions $+ : F \times F \to F$ and $\cdot : F \times F \to F$ is called a field if:

1. $\forall x, y \in F$, $x + y \in F$ (closed under addition)
2. $\forall x, y \in F$, $x + y = y + x$ (commutative under addition)
3. $\forall x, y, z \in F$, $x + (y + Z) = (x + y) + z$ (assiciative under addition)
4. $\exists 0$(additive identity) such that $\forall x \in F, x + 0 = 0 + x = x$ (Additive identity)
5. $\forall x \in F, \exists(-x)$(additive inverse) such that $x + (-x) = (-x) + x = 0$ (Additive inverse)
6. $\forall x, y \in F, x \cdot y \in F$ (Multiplication is closed)
7. $\forall x, y \in F, x \cdot y = y \cdot x$ (Multiplication is commutative)
8. $\forall x, y, z \in F, x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Multiplication is associative)
9. $\forall x \in F, x \neq 0, \exists(x^{-1})$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$ (Multiplicative inverse)
10. $\forall x \in F, 1 \cdot x = x \cdot 1 = x$ (Multiplicative identity)
11. $\forall a, b, c \in F, a \cdot (b + c) = a \cdot b + a \cdot c$ (Left Distributivity)
12. $\forall a, b, c \in F, (a + b) \cdot c = a \cdot c + b \cdot c$ (Right Distributivity)

3.1 The Reals $\mathbb{R}$

The real numbers are characterised by the following axioms:

Definition 3.2: (The Real Field)

1. F, field axioms listed above.
2. Order Axioms:There exists a subset $P \subset \mathbb{R}$ called "positive numbers" such that:
   (a) $\forall a \in \mathbb{R}$, only one of $a \in P$, $-a \in P$ or $a = 0$ are true. (Trichotomy Law)
   (b) $\forall a, b \in P, a + b \in P$ (Positive numbers are closed under addition)
   (c) $\forall x, y \in P, x \cdot y \in P$ (Positive numbers are closed under multiplication)
3. Completeness axiom*

Definition 3.3

1. (Max of a set) $M \in S \subseteq \mathbb{R}$ is said to be the maximum of S if $M \geq x \forall x \in S$
2. (Min of a set) $m \in S \subseteq \mathbb{R}$ is said to be the minimum of a set if $m \leq x \forall x \in S$
3. (Upper bound of a set) $L \in \mathbb{R}$ is said to be an upper bound of S if $L \geq x \forall x \in S$
4. (Lower bound of a set) $l \in \mathbb{R}$ is said to be a lower bound of S if $l \leq x \forall x \in S$
5. (Sup(S)) $\alpha \in \mathbb{R}$ is said to be the supremum of S if it is the minimum of the set of all Upper bounds of S.
6. (Inf(S)) $\beta \in \mathbb{R}$ is said to be the infimum of S if it is the maximum of the set of all lower bounds of S.

Axiom 3.4: Completeness Axiom for the Real Number Field

Every non empty subset of $\mathbb{R}$ that is bounded above has a supremum.

Corollary 3.5

Every non empty subset of $\mathbb{R}$ that is bounded below has an infimum.

Proof for Corollary.

$S \subseteq \mathbb{R}$ has a lower bound $\implies \exists L \in \mathbb{R}$ such that $L \leq x \forall x \in S \implies -L \geq -x \forall x \in S$
Define $S' := \{-x : x \in S\}$. Then, $-L$ is an upper bound of S'.
$\implies \exists q \in \mathbb{R}$ such that $q \geq y \forall y \in S'$ and $q \leq z \forall z$ such that $z \geq y \forall y \in S'$.
$\implies \exists q' = -q \in \mathbb{R}$ such that $q' \leq x \forall x \in S$ and $q' \geq z' = -z \forall z$ such that $z' \leq x \forall x \in S$
Cleaning up a bit: $\implies \exists q' \in \mathbb{R}$ such that $q' \leq x \forall x \in S$ and $q' \geq z' \forall z'$ such that $z' \leq x \forall x \in S$
Therefore q' is the greatest lower bound, i.e the infimum. ∎

Lemma 3.6: The Lemma

Suppose $a \in \mathbb{R}^+$ and $0 \leq a < \varepsilon \ \forall \varepsilon \in \mathbb{R}^+$ then $a = 0$

Proof for Lemma

Suppose not, i.e, $a > 0$. Choose $\varepsilon = \frac{a}{2}$. Contradiction. ∎

Proposition 3.7

Supremum of a set is unique.

Proof for Proposition.

Supremum is the "least" of the set of the upper bounds, it itself being part of the set of all the upper bounds. Since minima is unique, Supremum is unique. ■

Lemma 3.8

$U \in \mathbb{R}$ is the supremum of $S \subseteq \mathbb{R} \iff$

1. $s \leq U \forall s \in S$
2. if $v < U, \exists s_v \in S$ such that $v < s_v$

Proof for Lemma

$\implies$) Given that U is the supremum, (1) is pretty obvious since it is an upper bound. Suppose $v < U$, but for every $s \in S$, $s \leq v$. This would mean v is the supremum, and not U. Absurd. ■

Fact 3.9

Given that U is an upper bound of S, U is the supremum of $S \iff \forall \varepsilon > 0, \exists s_\epsilon \in S$ such that $U - \varepsilon < s_\epsilon$

Theorem 3.10: Archimedean Property of $\mathbb{R}$

Given $a, b \in \mathbb{R}^+, \exists n \in \mathbb{N}$ such that $an - b > 0$

Proof for Theorem.

Suppose not, i.e, $\forall n \in \mathbb{N}, an < b \implies \forall n \in \mathbb{N}, n < \frac{b}{a}$. Consider the set $S = \{an : n \in \mathbb{N}\}$. This has an upper bound b, and therefore, a supremum u. consider $u - n$. $\exists n_0$ such that $u - n < an_0 \implies u < a(n_0 + 1)$. Absurd. ■

Corollary 3.11

Alternate formulation of the previous statement: $\forall x \in \mathbb{R}, \exists n_0 \in \mathbb{N}$ such that $x < n_0$

Lemma 3.12: Useful Lemma

$\forall \varepsilon > 0, x < \varepsilon \iff \forall n \in \mathbb{N}, x < \frac{1}{n}$

Proof for Lemma

$\implies$)Contrapositive to prove would be: $\exists n_0 \in \mathbb{N}, x \geq \frac{1}{n_0} \implies \exists \varepsilon_0 > 0, x \geq \varepsilon_0$. Simply choose $\varepsilon_0 = \frac{1}{n_0}$
$\impliedby$)Contrapositive to prove would be: $\exists \varepsilon_0 > 0$ such that $x \geq \varepsilon \implies \exists n_0$ such that $x \geq \frac{1}{n_0}$. From Archimedean, $\exists n_0$ such that $n_0 \geq \frac{1}{\varepsilon_0} \implies \varepsilon_0 \geq \frac{1}{n_0} \implies x \geq \varepsilon_0 \geq \frac{1}{n_0}$ ■

Theorem 3.13: Archimedean Properties of $\mathbb{R}$

1. $inf(\{\frac{1}{n} : n \in \mathbb{N}\}) = 0$
2. If $t > 0, \exists n_0 \in \mathbb{N}$ such that, $0 < \frac{1}{t} < n$
3. If $y > 0$, $\exists n_y \in \mathbb{N}$ such that $n_y - 1 \leq y < n_y$

Proof for Theorem.

1)Obvious
2)Application of Archimedean
3) We know from archimedean that such an n_y exists such that $y < n_y$. Consider the set of all n such that $y < n$. Obviously, this is a non empty set. Therefore, from Well Ordering, this has a least element $n_0 \implies n_0 \leq y < n_0$ ∎

Theorem 3.14: Density of $\mathbb{Q}$ in $\mathbb{R}$

$\forall x, y \in \mathbb{R}, x < y \implies \exists q \in \mathbb{Q}$ such that $x < q < y$

Proof for Theorem.

$y - x > 0 \implies$ from archimedean $\exists n_0$ such that $n_0(y - x) > 1 \implies n_0 y > 1 + n_0 x$. Form Archimedean Propery, $\exists m \in \mathbb{N}$ such that $m - 1 < n_0 y \leq m$.Since $m \geq n_0 y > 1 + n_0 x \implies m - 1 > n_0 x \implies n_0 y > m - 1 \leq n_0 x \implies y > \frac{(m-1)}{n_0} > x$ ∎

Corollary 3.15

Given $x, y \in \mathbb{R}, y > x$, $\exists q \in \mathbb{R} - \mathbb{Q}$ such that $y > q > x$ (Assumed that $\sqrt{2}$ is irrational.)

Theorem 3.16: Existence of nth Roots in $\mathbb{R}^+$

let $y \in \mathbb{R}^+$ and $n \in \mathbb{N}$, then $\exists$ a unique $x \in \mathbb{R}^+$ such that $x^n = y$

Proof for Theorem.

Consider $E := \{t \in \mathbb{R} : t^n < y\}$. Is E bounded above? obviously, $1 + y$ is an upper bound. Is it non empty? Of course, consider $t = \frac{y}{1+y} < y$. Hence, E has a supremum u. Claim: $u^n = y$. Suppose not. Let $u^n < y$. We want to find an $h \in \mathbb{R}^+$ such that $(u + h)^n < y$ so that a contradiction can be raised ($u + h$ cannot be in the set). In effect we want to show that $(u+h)^n - u^n < y - u^n$. Recall the identity: $p^n - q^n = (p-q)(p^{n-1} + qp^{n-2} \cdots + q^{n-1})$. If $p > q$, we have $p^n - q^n < n(p-q)(p^{n-1})$. Therefore: $(u+h)^n - u^n \leq n(h)(u+h)^{n-1}$. We want h so that $n(h)(u + h)^{n-1} < y - u^n \implies h < \frac{y-u^n}{n(u+h)^{n-1}}$. Choose $h < 1$, which would mean $\frac{y-u^n}{n(u+1)^{n-1}} < \frac{y-u^n}{n(u+h)^{n-1}}$. Now simply choose such an h such that $h < \frac{y-u^n}{n(u+1)^{n-1}} < \frac{y-u^n}{n(u+h)^{n-1}}$ which is possible from density.
Suppose now that $u^n > y$, we need an h so that $(u - h)^n > y$ or $-(u - h)^n < -y$,

which would mean that $u-h$ is the actual supremum, contradicting the assumption. Therefore, we have to show that $u^n-(u-h)^n<u^n-y$. From the identity, we have that $u^n-(u-h)^n\leq n(h)(u)^n$. It would suffice if we find an h so that $nhu^{n-1}<u^n-y$ or $h<\frac{u^n-y}{nu^{n-1}}$. Again, from Density theorem this is possible.
Uniqueness, once existence is established, is trivial since, if $q_1>q_2,(q_1)^n>(q_2)^n$.

Fact 3.17

1. $n>0,q>0$ and $r=\frac{m}{n}=\frac{p}{q}$, then $(b^m)^{\frac{1}{n}}=(b^p)^{\frac{1}{q}}$
2. $x^{(p+q)}=x^px^q$ for $p,q\in\mathbb{Q}$

Theorem 3.18: Results regarding powers

Suppose $b>1$. If $x\in\mathbb{R}$, define $B(x):=\{b^t:t\in\mathbb{Q}:t\leq x\}$. Then $sup(B(r))=b^r$ if r is a rational number.

Proof for Theorem.

Of course, the set is bounded and non-empty, hence, has a supremum. It is clear that b^r cannot be $<sup(B(r))$ because if so, there would exist $t\in\mathbb{Q},t\leq r$ such that $b^r<b^t$. Absurd. So $b^r\geq sup(B(r))$. It also can't be strictly greater, since b^r is in the set itself, so it can't exceed its supremum. Hence,$Sup(B(r))=b^r$.

With the previous result in mind as motivation, we define the following:

Definition 3.19: (Real "raised" to Reals)

Given $b>1$, we define $b^x:=sup(B(x):=\{b^t:t\in QQ:t\leq x\in\mathbb{R}\})$

Theorem 3.20

$b^xb^y=b^{x+y}$ for all $b>1,x,y\in\mathbb{R}$

Proof for Theorem.

$$b^x:=sup(\{b^p:p\in\mathbb{Q}:p\leq x\})$$
$$b^y:=sup(\{b^q:q\in\mathbb{Q}:q\leq y\})$$
$$b^{x+y}:=sup(\{b^t:t\in\mathbb{Q}:t\leq x+y\})$$

Suppose that $b^xb^y<b^{x+y}$. Then, $\exists q\in\mathbb{Q},q<x+y$ such that $b^xb^y<b^q$. Suppose WLOG $x<y$. Choose a $t\in Q^+$ such that $q-x<t<y$. This means, $q<x+y$ as we know, but also, $q-t<x$ and $t<y$. We now have $b^xb^y\leq b^{q-t+t}=b^{q-t}b^t$ where $q-t<x$ and $t<y$. Absurd.
Now assume $b^xb^y>b^{x+y}$. This implies $b^x>\frac{b^{x+y}}{b^y}\implies\exists q<x$ such that $b^q>\frac{b^{x+y}}{b^y}\implies$

$b^y > \frac{b^{x+y}}{b^q} \implies \exists p < y$ such that $b^p > \frac{b^{x+y}}{b^q} \implies b^p b^q = b^{p+q} > b^{x+y}$ but $p < y$ and $q < x \implies p + q < x + y$. Absurd. So $b^x b^y = b^{x+y}$ ∎

Theorem 3.21: Existence of Log

Let $b > 1$, $y > 0$, then,$\exists$ a unique $x \in \mathbb{R}$ such that $b^x = y$

Proof for Theorem.

Consider $E := \{x \in \mathbb{R} : b^x \leq y\}$. The claim is that $Sup(E) = z$ exists and $b^z = y$.
Case 1-$y \geq b > 1$:
It is obvious that in this case E is non empty. Suppose that, it is unbounded. i.e, $\forall n \in \mathbb{N}, b^n \leq y$. Since $b > 1$,$b = 1 + \delta$ for some $\delta > 0$. $\implies b^n = (1 + \delta)^n = 1 + n\delta + \frac{n(n-1)}{2}\delta^2 \cdots \leq y, \forall n \in \mathbb{N}$. i.e, $1 + n\delta < y, \forall n \in \mathbb{N}$. This would be absurd, obviously. Hence, $\exists n_0 \in \mathbb{N}$ such that $b^{n_0} > y$, and obviously $\forall n \geq n_0$. Therefore, in this case, E is bounded and non empty, hence has a supremum $z = sup(E)$.
Case 2- $b > y$:
Sub Case 1: $b > y > 1$:
Boundedness is clear here. We claim that $\exists n_0 \in \mathbb{N}$ such that $y^{n_0} \geq b$ or $y \geq b^{\frac{1}{n_0}}$. Suppose not, i.e $\forall n \in \mathbb{N}, y^n < b \implies (1 + \delta)^n < b \implies 1 + n\delta < b \forall n \in \mathbb{N}$. Again, this is absurd. Hence, $\exists n_0$ such that $y > b^{\frac{1}{n_0}}$. Hence, it is bounded and non empty.
Sub Case 2: $b > 1 > y$:
Boundedness is clear here as well. Since $y < 1$, $y^{-1} > 1$, and say $z = y^{-1}$. Does $\exists r_0 \in \mathbb{Q}$ such that $b \geq z^{r_0}$? If $z \geq b > 1$, from the proof of case-1, $\exists r_0 \in \mathbb{Q}$ such that $b \geq z^{r_0} \implies b \geq y^{-r_0} \implies y \leq b^{-\frac{1}{r_0}}$. If $b > z > 1$, then that $r_0 = 1$. From here we see that $b > y^{-1} \implies b^{-1} < y$.

In all cases. Supremum exists for E. Call it s

Does $b^s = y$? suppose not, i.e, let $b^s < y$. We want to establish a number $s + z_0 > s$ such that $b^{s+z_0} < y$ which would lead to contradiction since s is supposed to be the supremum of E.
$\exists \delta \in \mathbb{R}^+$ such that $b^s + (\delta)b^s = b^s(1 + \delta) < y$ from density. We need a $q \in \mathbb{Q}^+$ such that $b^q < 1 + \delta$. We know that $b > 1$ and $1 + \delta > 1$, so either from case 1 where $1 + \delta \geq b > 1$, or from case 2 subcase 1 where $b > 1 + \delta > 1$, we can find such a q. Hence, $b^s b^q = b^{s+q} < b^s(1 + \delta) < y$. This would be absurd.
Consider the case where $b^s > y$. From density, $\exists \delta \in \mathbb{R}^+$ such that $b^s > y + \delta \implies b^s > y + \delta_0 y \implies b^s > y(1 + \delta_0$ for some δ_0. This means that $b^s \frac{1}{1+\delta_0} > y$. We need to find, again, a positive rational such that $b^q < 1 + \delta_0$. From the previous analysis, it can be done. Hence, $b^{s-q} > y$, which means that for every $z \in \mathbb{R}$ such that $z > s - q$, we have that $b^z > y$. This means that $s - q$ is an upper bound for E, which is absurd. Hence, $b^s = y$.

∎

3.2 The Complex field $\mathbb{C}$

Definition 3.22

We define $\mathbb{C}$ as the set of all ordered pairs in $\mathbb{R}^2$ with the following additional properties:

1. $x = (a_1, b_1), y = (a_2, b_2)$ with $a_1, b_1, a_2, b_2 \in \mathbb{R}$, then $x + y$ is defined as $(a_1 + a_2, b_1 + b_2)$
2. $x = (a_1, b_1), y = (a_2, b_2)$ with $a_1, b_1, a_2, b_2 \in \mathbb{R}$, we define multiplication xy as $(a_1a_2 - b_1b_2 - a_1b_2 + a_2b_1)$

This set $\mathbb{C}$ with $+$ and juxtaposition obey field axioms with $(0, 0)$ the additive identity, and $(1, 0)$ the multiplicative one.
For consistency, we define $\frac{1}{x} := (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$, where $x = (a, b)$.

Definition 3.23

1. (Conjugate) If $z = (a, b)$, the conjugate $\bar{z} =$ is defined as $\bar{z} = (a, -b)$.
2. (Mod) If $z = (a, b)$, the mod of z, $|z|$ is defined as $(z\bar{z})^{\frac{1}{2}}$

Fact 3.24

Some facts:

1. $\bar{(x + y)} = \bar{x} + \bar{y}$
2. $\bar{(zw)} = \bar{z}\bar{w}$
3. $z\bar{z} \geq 0$ and $= (a^2 + b^2, 0)$
4. We can identify $\mathbb{R}$ as a subset of $\mathbb{C}$ by setting $a \in \mathbb{R}$ to be $(a, 0)$ in $\mathbb{C}$.
5. $|zw| = |z||w|$
6. $|z + w| \leq |z| + |w|$
7. $|Re(z)| \leq |z|$

Theorem 3.25: Cauchy-Schwartz Inequality

If $a_1, a_2, \cdots a_n$ and $b_1, b_2, \cdots, b_n$ are numbers in $\mathbb{R}^+$, then

$$\big(\sum_{i=1}^{n} a_i b_i\big)^2 \leq \sum_{i=1}^{n} (a_i)^2 \sum_{j=1}^{n} (b_j)^2$$

Extending this theorem for a_j and b_j in the complex domain, we have

$$|\big(\sum_{i=1}^{n} a_i \bar{b_i}\big)|^2 \leq \sum_{i=1}^{n} |(a_i)|^2 \sum_{j=1}^{n} |(b_j)|^2$$

Proof for Theorem.

Consider $\alpha = (a_1b_1 + a_2b_2 \ldots a_nb_n)^2 = (a_1b_1 + a_2b_2 \ldots a_nb_n)(a_1b_1 + a_2b_2 \ldots a_nb_n)$ which is $((a_1b_1)^2 + (a_2b_2)^2 \ldots (a_nb_n)^2) + K$ where K is given by

$$\begin{array}{cccccc} 0 & +a_1b_1a_2b_2 & +a_1b_1a_3b_3 & \cdots & +a_1b_1a_nb_n \\ a_2b_2a_1b_1 & +0 & +a_2b_2a_3b_3 & \cdots & +a_2b_2a_nb_n \\ \vdots & & & & \\ a_nb_na_1b_1 & +a_nb_na_2n_2 & +a_nb_na_3b_3 & \cdots & +0 \end{array}$$

Consider $\beta = (a_1^2 + a_2^2 + \ldots)(b_1^2 + b_2^2 \ldots)$ This would be$(a_1b_1)^2 + (a_2b_2)^2 \cdots (a_nb_n)^2 + L$ where L is given by:

$$\begin{array}{cccccc} 0 & +a_1^2b_2^2 & +a_1^2b_3^2 & \cdots & +a_1^2b_n^2 \\ a_2^2b_1^2 & +0 & +a_2^2b_3^2 & \cdots & +a_2^2b_n^2 \\ \vdots & & & & \\ a_n^2b_1^2 & +a_n^2b_2^2 & +a_n^2b_3^2 & \cdots & +0 \end{array}$$

$$\beta - \alpha = \sum_{i=1}^{n} \sum_{j=i+1}^{n} (a_ib_j)^2 + (a_jb_i)^2 - \sum_{i=1}^{n} \sum_{j=i+1} 2a_ia_jb_ib_j = \sum_{i=1}^{n} \sum_{j=i+1} (a_ib_j - b_ia_j)^2$$

. Hence, $\beta = \alpha +$ some square term. Therefore

$$\beta - \alpha \geq 0$$

.

Theorem 3.26: Bernoulli's Inequality

Given $x > -1$, $(1 + x)^n \geq 1 + nx$

Proof for Theorem.

For $n = 1$, it's trivially true. Assume it's correct for $n = n$. Consider $(1+x)^n(1+x) \geq (1+nx)(1+x) = 1+x+nx+nx^2 = 1+x(n+1)+nx^2 \implies (1+x)^{n+1} \geq 1+(n+1)x$ ■

Theorem 3.27: AM-GM Inequality

Given $a_1, a_2, \ldots, a_n \in \mathbb{R}^+$,

$$\left(\frac{S_n}{n}\right)^n = (\frac{a_1+a_2+\cdots+a_n}{n})^n \geq (a_1a_2\cdots a_n)$$

Proof for Theorem.

For a_1, it is trivially true. Assume for $n = n$, and consider

$$\left(\frac{S_{n+1}}{n+1}\right)^{n+1} = \left(\frac{S_n + a_{n+1}}{n+1}\right)^{n+1} \rightarrow$$

$$\left(\frac{\frac{nS_n}{n} + a_{n+1}}{n+1}\right)^{n+1} \rightarrow$$

$$\left(\frac{\frac{(n+1-1)S_n}{n} + a_{n+1}}{n+1}\right)^{n+1} = \left(\frac{\frac{(n+1)S_n - S_n}{n} + a_{n+1}}{n+1}\right)^{n+1} =$$

$$\left(\frac{\frac{(n+1)S_n}{n} - \frac{S_n}{n} + a_{n+1}}{n+1}\right)^{n+1} = \left(\frac{S_n}{n} + \frac{-\frac{S_n}{n} + a_{n+1}}{n+1}\right)^{n+1} =$$

$$\left(\frac{S_n}{n}\right)^{n+1}\left(1 + \frac{-1 + \frac{na_{n+1}}{S_n}}{n+1}\right)^{n+1}$$

From Bernoulli inequality,

$$\left(\frac{S_n}{n}\right)^{n+1}\left(1+\frac{-1+\frac{na_{n+1}}{S_n}}{n+1}\right)^{n+1} \geq \left(\frac{S_n}{n}\right)^{n+1}\left(1+(n+1)\frac{-1+\frac{na_{n+1}}{S_n}}{n+1}\right) = \left(\frac{S_n}{n}\right)^{n+1}\left(\frac{na_{n+1}}{S_n}\right)$$

$$\geq \left(\frac{S_n}{n}\right)^{n}\left(a_{n+1}\right) \geq a_1a_2\cdots a_na_{n+1}$$

■

3.3 Some Inequalities

Theorem 3.28: Generalised AM-GM

If $x, y \in \mathbb{R}^+$ and $t \in (0,1)$, then

$$(1-t)x + ty \geq x^{1-t}y^t$$

Proof for Theorem.

We use the fact that a differentiable function f is convex if and only if its first derivative f' is monotone increasing. Under this criteria, e^x is certainly convex. That means $\forall x, y \in \mathbb{I}$, $t \in (0,1)$,

$$e(x) + t(e(y) - e(x)) \geq e(x + t(y - x))$$

or in other words:

$$e((1-t)x + ty) \leq (1-t)e(x) + te(y)$$

Making the substitution $x \mapsto ln(x)$ gives us

$$e((1-t)ln(x) + tln(y)) \leq (1-t)e(ln(x)) + tln(y)$$

which implies (since e is a monotone increasing function)

$$(1-t)x + ty \geq x^{1-t}y^t$$

Theorem 3.29: Concavity of $log_e : \mathbb{R}^+ \to \mathbb{R}$ (assumed knowledge of e, and existence of log.)

The function $f := log_b : \mathbb{R}^+ \to \mathbb{R}$ proven to be unique for a given $b > 1$ and any real number x, follows the following: For every $x, y \in \mathbb{R}^+$, and $t \in (0,1)$

$$f((1-t)x + ty) \geq (1-t)f(x) + tf(y)$$

Proof for Theorem.

We want to prove

$$log((1-t)x + ty) \geq (1-t)log(x) + tlog(y)$$

which amounts to showing that

$$log((1-t)x + ty) \geq log(x^{1-t}y^t)$$

Since log is an increasing function, from general AM-GM, we have $(1-t)x + t(y) \geq x^{1-t}y^t$ which gives (taking log on both sides)

$$log((1-t)x + ty) \geq log(x^{1-t}y^t)$$

which gives us the desired result.

Theorem 3.30: Young's Inequality

If a, b are non negative reals, with $p > 1, q > 1$ such that $\frac{1}{p} + \frac{1}{q} = 1$, then

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}$$

With equality holding if and only if $a^p = b^q$

Proof for Theorem.

Let $\frac{1}{p} = t < 1$ and $\frac{1}{q} = 1 - t < 1$. From generalised AM-GM, in place of $(1-t)x + ty \geq x^{1-t}y^t$, make the following transformations:

$$x \mapsto x^{\frac{1}{(1-t)}}$$

$$y \mapsto y^{\frac{1}{t}}$$

to arrive at the modified am-gm which is

$$(1-t)x^{\frac{1}{(1-t)}} + ty^{\frac{1}{t}} \geq xy$$

Plugging the values for $1 - t$ and t respectively we get

$$\frac{1}{q}x^q + \frac{1}{p}y^p \geq xy$$

Theorem 3.31: Hoelder's Inequality

Given $\{x_i\}_{i=1}^k, \{y_i\}_{i=1}^k$ in $\mathbb{R}$, we have (given positive integers p, q so that $\frac{1}{p} + \frac{1}{q} = 1$, $p, q > 1$)

$$\sum_{i=1}^{k} |x_i y_i| \leq (\sum_{i=1}^{k} |x_i|^p)^{1/p} (\sum_{i=1}^{k} |y_i|^q)^{1/q}$$

Proof for Theorem.

Consider the case when $\sum_{i=1}^k |x_i|^p = 1$ and $\sum_{i=1}^k |y_i|^q = 1$. Using Young's Inequality which is $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$, we have

$$|x_i y_i| \leq \frac{|x_i|^p}{p} + \frac{|y_i|^q}{q}$$

Taking the sum on both sides gives

$$\sum_{i=1}^{k} |x_i y_i| \leq \frac{1}{p} + \frac{1}{q} = 1$$

Now suppose $z_i = \frac{|x_i|}{(\sum_{i=1}^{k} |x_i|^p)^{1/p}}$ and $w_i = \frac{|y_i|}{(\sum_{i=1}^{k} |y_i|^q)^{1/q}}$. It is easy to see that $\sum_{i=1}^{k} |z_i|^p = \sum_{i=1}^{k} |w_i|^p = 1$. This means, from Young's inequality,

$$\sum_{i=1}^{k} |z_i w_i| \leq 1$$

which implies

$$\sum_{i=1}^{k} |x_i y_i| \leq (\sum_{i=1}^{k} |x_i|^p)^{1/p} (\sum_{i=1}^{k} |y_i|^q)^{1/q}$$

Theorem 3.32: Minkowski's Inequality

Given $\{x_i\}_{i=1}^{k}$ and $\{y_i\}_{i=1}^{k}$ in $\mathbb{R}$, and an integer $p \geq 1$, we have:

$$(\sum_{i=1^k} (|x_i + y_i|^p))^{1/p} \leq (\sum_{i=1}^{k} |x_i|^p)^{1/p} + (\sum_{i=1}^{k} |y_i|^p)^{1/p}$$

Proof for Theorem.

Consider $(\sum_{i=1}^{k} |x_i + y_i|^p) \leq (\sum_{i=1}^{k} (|x_i| + |y_i|)^p) \leq (\sum_{i=1}^{k} (|x_i| + |y_i|)(|x_i| + |y_i|)^{p-1})$ This is

$$(\sum_{i=1}^{k} (|x_i|)(|x_i| + |y_i|)^{p-1} + \sum_{i=1}^{k} (|y_i|)(|x_i| + |y_i|)^{p-1})$$

Apply Holder inequality to each summand to get:

$$(\sum_{i=1}^{k} |x_i|^p)^{1/p} (\sum_{i=1}^{k} (||x_i| + |y_i||^{p-1})^{\frac{p}{p-1}})^{\frac{p-1}{p}}$$

$$+$$

$$(\sum_{i=1}^{k} |y_i|^p)^{1/p} (\sum_{i=1}^{k} (||x_i| + |y_i||^{p-1})^{\frac{p}{p-1}})^{\frac{p-1}{p}}$$

Which simplifies down to:

$$(\sum_{i=1}^{k} |x_i|^p)^{1/p} (\sum_{i=1}^{k} (|x_i| + |y_i|)^p)^{\frac{p-1}{p}} + (\sum_{i=1}^{k} |y_i|^p)^{1/p} (\sum_{i=1}^{k} (|x_i| + |y_i|)^p)^{\frac{p-1}{p}}$$

which again simplifies to

$$\{(\sum_{i=1}^{k}|x_i|^p)^{1/p}+(\sum_{i=1}^{k}|y_i|^p)^{1/p}\}(\sum_{i=1}^{k}(|x_i|+|y_i|)^p)^{\frac{p-1}{p}}$$

This gives us the equation:

$$\sum_{i=1}^{k}(|x_i|+|y_i|)^p \leq \{(\sum_{i=1}^{k}|x_i|^p)^{1/p}+(\sum_{i=1}^{k}|y_i|^p)^{1/p}\}(\sum_{i=1}^{k}(|x_i|+|y_i|)^p)^{\frac{p-1}{p}}$$

Which immediately gives us (after multiplying both sides)

$$(\sum_{i=1}^{k}(|x_i|+|y_i|)^p)^{1/p} \leq \{(\sum_{i=1}^{k}|x_i|^p)^{1/p}+(\sum_{i=1}^{k}|y_i|^p)^{1/p}\}$$

Which is the desired result

Theorem 3.33: Minkowski for Infinite Sums

Given sequences $\{x_n\}$ and $\{y_n\}$ we have (where it is assumed/ given that each of the right side term is finite)

$$(\sum_{i=1}^{\infty}(|x_i+y_i|^p))^{1/p} \leq (\sum_{i=1}^{\infty}|x_i|^p)^{1/p}+(\sum_{i=1}^{\infty}|y_i|^p)^{1/p}$$

o

Proof for Theorem.

Given $\{x_i\}_{i=1}^{k}$ and $\{y_i\}_{i=1}^{k}$, the good old Minkowski inequality reads:

$$(\sum_{i=1}^{k}(|x_i+y_i|^p))^{1/p} \leq (\sum_{i=1}^{k}|x_i|^p)^{1/p}+(\sum_{i=1}^{k}|y_i|^p)^{1/p}$$

For any $k \in \mathbb{N}$. Since the right side is monotone increasing (and assuming it is bounded above, i.e, convergent) we can take the limit to arrive at

$$(\sum_{i=1}^{k}(|x_i+y_i|^p))^{1/p} \leq (\sum_{i=1}^{\infty}|x_i|^p)^{1/p}+(\sum_{i=1}^{\infty}|y_i|^p)^{1/p}$$

Whence we see the inequality holding again for all $k \in \mathbb{N}$. Simply take the limit again th arrive at:

$$(\sum_{i=1}^{\infty}(|x_i+y_i|^p))^{1/p} \leq (\sum_{i=1}^{\infty}|x_i|^p)^{1/p}+(\sum_{i=1}^{\infty}|y_i|^p)^{1/p}$$

Lemma 3.34: Useful lemma

if $p > 1$, with $a, b \geq 0$, then

$$(\frac{a+b}{2})^p \leq (\frac{a^p}{2} + \frac{a^p}{2})$$

Proof for Lemma

Consider the function $x \mapsto x^p$ for $p > 1$. Note that this map is convex. That means that the line is bigger than the function. We therefore have $(1-t)f(x)+tf(y) \geq f((1-t)x+ty)$. Plugging $t = 1/2$ gives us the desired result. ■

3.4 Intervals on the Real Line

Definition 3.35: Intervals

1. (Open Interval): $(a, b) \subset \mathbb{R} := \{x \in \mathbb{R} : a < x < b\}$
2. (Closed Interval): $[a, b] \subset \mathbb{R} := \{x \in \mathbb{R} : a \leq x \geq b\}$

Definition 3.36: Nested Intervals

If $I_n := [a_n, b_n] : n \in \mathbb{N}$ is a sequence of intervals such that $I_n \subseteq I_{n-1} \cdots \subseteq I_1$, then $\{I_n\}$ is said to be a sequence of nested intervals.

Theorem 3.37: Nested Interval Theorem

Given a sequence of closed and bounded, and non empty nested intervals $\{I_n : n \in \mathbb{N}\}$, $\exists \xi \in I_n \ \forall n \in \mathbb{N}$ or equivalently, $\xi \in \cap_{n=1}^{\infty} I_n$.

Proof for Theorem.

Let $I_n = [a_n, b_n]$. From the definition, it is clear that $\{a_n\}$ is an increasing sequence of reals, while $\{b_n\}$ is a decreasing sequence. Moreover, from the non empty property of each interval, we have that $a_m < b_n, \forall n \in \mathbb{N}, \forall m \in \mathbb{N}$. This implies that the set of $\{a_n\}$ has a supremum S_a, while the set $\{b_n\}$ has an infimum L_b. $a_n \leq L_b \forall n \in \mathbb{N}$ while $S_a \leq b_n \forall n \in \mathbb{N}$. $a_n \leq$. Moreover, $a_n \leq S_a \forall n \in \mathbb{N}$ while $L_b \leq b_n \forall n \in \mathbb{N}$. since a_n is a lower bound of $\{b_n\}$, $a_n \leq L_b$, and since L_b is an upper bound of $\{a_n\}$, $a_n \leq S_a \leq L_b \leq b_n : \forall n \in \mathbb{N}$. From Density, $\exists \xi \in [S_a, L_b]$ such that $\xi \in \cap_{i=1}^{\infty} I_i$ ∎

Corollary 3.38

In the previous theorem, if the size of the nested intervals converges to 0, then the intersection contains only one point.

Proof for Corollary.

We see that $len(I_n) \to 0$ which means $\forall \varepsilon > 0 \ \exists n_0$ such that $\forall n \geq n_0$

$$len(I_n) < \varepsilon$$

Say two points survive the intersection, call them x and y. They have a finite, non zero distance d between them. Let $\varepsilon < d$. This means that after n_0, the length of the intervals go below $\varepsilon < d$. So, if x is in the intersection, y, by virtue of being d distance away, wont survive the intersection. ∎

3.5 Decimal Expansions, and related results

Every $x \in \mathbb{R}$ can be written as an expansion in the following way:

Definition 3.39: Decimals

Let $z \in \mathbb{R}^+$ be given. Let n_0 be the "largest" integer such that $n_0 \leq z$. Let n_1 be the largest integer such that $n_0 + \frac{n_1}{10} \leq z$. As such, say n_k is defined for some k. Let n_{k+1} be the largest integer such that $n_0 + \frac{n_1}{10^1} + \frac{n_2}{10^2} + \cdots + \frac{n_k}{10^k} + \frac{n_{k+1}}{10^{k+1}} \leq z$. Consider the set of all such "finite sums", i.e, the set of all

$$z_k = n_0 + \frac{n_1}{10^1} + \frac{n_2}{10^2} + \cdots + \frac{n_k}{10^k} + \frac{n_{k+1}}{10^{k+1}} \leq z$$

. This set has a supremum and that is z itself. We symbolically write $z = n_0.n_1n_2\ldots$

Theorem 3.40

The set $K = \{z_n : n \in \mathbb{N}\}$ above, is bounded and non-empty, and Sup(K)=z

Proof for Theorem.

That it is non-empty and bounded is obvious. Suppose that $x = sup(K)$. Since z is an upper bound, let us assume $x < z \implies \exists \xi \in \mathbb{R}$ such that $\xi = z - x$. From Archimedean, choose a $k \in \mathbb{N}$ such that $\frac{1}{10^k} < \xi \implies -\frac{1}{10^k} > -\xi$. This means that $z - \frac{1}{10^k} > z - \xi = x$. Consider one such $z_k \in K$, we can see that $n_0 + \frac{n_1}{10^1} + \cdots + \frac{n_k}{10^k} < x < z - \frac{1}{10^k} \implies n_0 + \frac{n_1}{10^1} + \cdots + \frac{n_k+1}{10^k} < z$. But this would mean that for some $q \leq k \in \mathbb{N}$, n_k isn't the largest integer such that $z_k \leq z$.

Fact 3.41

The above definition is special in that, it ensures that decimal expansions are unique, since supremum's are unique. But the caveat is that, not all series' correspond to any real number as a decimal expansion. For example, in this definition: $0.999999\ldots \neq 1$ since the unique decimal expansion for $1 = 1.00000$. So $0.9999\ldots$ doesn't really correspond to any real number but we know obviously that it is 1.

Theorem 3.42

$x \in \mathbb{R}$ is rational $\iff$ x has either terminating, or repeating decimal expansion

Proof for Theorem.

$\Longleftarrow$)Obvious
$\Longrightarrow$) Suppose $x = \frac{p}{q}$ for p, q integers. Then $xq = p$. Let k_0 be the smallest integer such

that $10^{k_0}p \geq q$. From Euclid's algorithm, we have

$$10^{k_0}p = z_0 q + r_0 \implies \frac{p}{q} = \frac{z_0}{10^{k_0}} + \frac{\frac{r_0}{q}}{10^{k_0}}$$

with $|r_0| < q$. Also note that $z_0 < 10$ for if not, $10^{k_0}p = z_0 q + r_0 \geq q z_0 \implies 10^{k_0-1}p \geq qz_0/10 \geq q$ which is contradictory. Next, choose the smallest $k_1 \in \mathbb{N}$ such that $10^{k_1}r_0 > q$ Now consider $10^{k_1}r_0$, again we have $10^{k_1}r_0 = z_1 q + r_1$ with $|r_1| < q$. Thus $\frac{r_0}{q} = \frac{z_1}{10^{k_1}} + \frac{r_1}{10^{k_1}q}$. This implies

$$\frac{p}{q} = \frac{z_0}{10^{k_0}} + \frac{z_1}{10^{k_0+k_1}} + \frac{r_1}{q10^{k_0+k_1}}$$

. We can keep going on as such, finding k_n, and applying Euclid's algorithm so that

$$\frac{p}{q} = \frac{z_0}{10^{k_0}} + \frac{z_1}{10^{k_0+k_1}} + \frac{z_2}{10^{k_1+k_2+k_3}} \cdots + \frac{z_n}{10^{k_1+k_2\cdots+k_n}} + \frac{r_n}{q10^{k_1+k_2\ldots+k_n}}$$

Since for every $n \in \mathbb{N}, |r_n| < q$, and $q \in \mathbb{N}$, only finite amount of remainders are possible when dividing by q. Hence, at some point $p \in \mathbb{N}$, $r_n = r_p$ for a previous $n \in \mathbb{N}$. This means that, $10^{k_{p+1}}p = z_{p+1}q + r_{p+1} \implies \frac{r_p}{q} = \frac{z_{p+1}}{10^{k^{p+1}}} + \frac{r_{p+1}}{10^{k_{p+1}}q}$

$$\implies \frac{r_n}{q} = \frac{r_p}{q} \implies z_{n+1} = z_{p+1}$$

Hence, we can see that it is recurring.

We are not yet done though. We showed that one of the representations of $x \in \mathbb{R}$, i.e, the one derived from long division is recurring. We now consider two different expansions for x. First, let us decompose x into $[x]$ and $\{x\}$. We note that the integral parts must be the same, so we can wholly focus on the fractional part. Let $0.a_1a_2\cdots$ and $0.b_1b_2\cdots$ be two expansions (base p) of $\{x\}$. Suppose they are different first at $j-$th entry. We then have $\frac{1}{p^j}(a_1a_2\cdots a_j.a_{j+1}a_{j+2}\cdots) = \frac{1}{p^j}(b_1b_2\cdots b_j.b_{j+1}b_{j+2}\cdots)$ which we can relabel to give:

$$\{x\} = \frac{1}{p^j}e_1e_2\cdots e_j.a_1^{j+}a_2^{j+}a_3^{j+}\cdots = \frac{1}{p^j}e_1e_2\cdots e'_j.b_1^{j+}b_2^{j+}b_3^{j+}\cdots$$

Say $e_j \geq 1 + e'_j \implies e_j - e'_j \geq 1 \implies e_1e_2\cdots e_j - e_1e_2\cdots e'_j \geq 1$ WLOG. This means that $p^j\{x\} - e_1e_2\cdots e'_j = 0.a_1^{j+}a_2^{j+}a_3^{j+}\cdots \geq 1$. Note that, given an expansion of the kind $0.c_1c_2\cdots$ (p-base) where there exists, at index r, an integer c_r so that $c_r < p-1$ or $c_r \leq p-1-1$, then $0.c_1c_2\cdots \leq 0.(p-1)(p-1)\cdots(p-1-1(\text{r-th position}))(p-1)\cdots \leq 1 - p^{-r} < 1$ strictly. So if in an expansion (fractional), even if one of the elements is strictly smaller than $p-1$, the entire sum will be smaller than 1, strictly. This implies that, every element in the expansion of $0.a_1^{j+}a_j^{2+}\cdots$ is indeed $p-1$ so that the sum can be ≥ 1 instead of being strictly less than 1. Hence, we are done. ∎

Lemma 3.43

Given $p \geq 2$ and $a_n \leq p-1 : a_n \in \mathbb{N}$, we have

$$\sum_{n=1}^{\infty} \frac{a_n}{p^n}$$

converges to some x in $[0,1]$.

Proof for Lemma

We note that this is a monotone increasing sequence. Note that, since $a_n \leq p-1$, we have

$$\sum_{n=1}^{\infty} \frac{a_n}{p^n} \leq (p-1) \sum_{n=1}^{n} \frac{1}{p^n}$$

which is 1. Therefore, this sequence is bounded, and from monotone convergence theorem, is convergent to $x \in [0,1]$. ∎

Lemma 3.44

Conversely, if x is a number in $[0,1]$ and p is an integer ≥ 2, we have that, there exists $a_1, a_2, \cdots \in \mathbb{N}$ that are less than $p-1$ so that x can be written as the limit of

$$\sum_{n=1}^{\infty} \frac{a_n}{p^n}$$

Proof for Lemma

The construction is very similar to the decimal expansion proof. Take a_1 to be the largest integer such that $\frac{a_1}{p} < x$. Find a_2 so that $\frac{a_1}{p} + \frac{a_2}{p^2} < x$. These can be achieved by Archimedean property. Note that $a_1 \leq p-1$, as is a_2. Inductively define a_n as the largest integer $a_n \leq p-1$ such that $\sum_{i=1}^{n} \frac{a_i}{p^i} < x$. Now, the decimal expansions proof proves that x is the supremum of the set of all

$$\sum_{i=1}^{n} \frac{a_i}{p^i}$$

. An alternate approach is to see that, by asserting that a_n is the *largest such* integer following the above property, we note that:

$$\sum_{i=1}^{n} \frac{a_i}{p^i} < x \leq \sum_{i=1}^{n} \frac{a_i}{p^i} + \frac{1}{p^n}$$

Taking limit on both sides proves the result. ∎

4 Misc Results

Theorem 4.1: (A perhaps useful theorem for LimSup LimInf)

If $A + B := \{a + b : a \in A, b \in B\}$, then $\gamma = sup(A + B) = sup(A) + sup(B) = \alpha + \beta$.

Proof for Theorem.

$\alpha \geq a, \forall a \in A$ and $\beta \geq b, \forall b \in B$. We hence see that $\alpha + \beta \geq a + b \forall a \in A, b \in B$. Therefore, $\alpha + \beta \geq \gamma$.

Now consider $a + b \leq \gamma \ \forall a \in A, b \in B$. This means that $\alpha + b \leq \gamma \ \forall b \in B$. From here we see that $\alpha + \beta \leq \gamma$ whence we see that $\gamma = \alpha + \beta$

Theorem 4.2

The set of all $0, 1-$sequences (i.e, sequences containing only 1 or 2) are atleast as large as $\mathbb{R}$ (**p-adic proof**)

Proof for Theorem.

Consider a point x in $[0, 1]$. By virtue of the above decmial expansion results, we can find a sequence a_n consisting of just 0 and 1 so that $\sum_{i=1}^{\infty} \frac{a_n}{2^n}$ converges to x. For every $0, 1$ sequence, we can map a unique number in $[0, 1]$ so that that sequence becomes the $2-$adic or binary representation of that number. This is a well defined surjection from the set of all $0, 1$ sequences to $[0, 1]$.

Theorem 4.3

If $a, b > 0$ and $0 < p < 1$, then $(a + b)^p \leq a^p + b^p$

Proof for Theorem.

Let $p = 1 - q$ for $q \in (0, 1)$. $(a + b)^p = (a + b)(a + b)^{-q} = (a)(a + b)^{-q} + b(a + b)^{-q} \leq a^{1-q} + b^{1-q} = a^p + b^p$

Theorem 4.4

If $f : \mathbb{I} \to \mathbb{R}$ is continuous on $\mathbb{I}$ and differentiable on $\mathbb{I}^0$, then f is convex if and only if f' is monotone increasing.

Proof for Theorem.

$\implies$) Suppose f is convex. That means for any $a, b \in \mathbb{I}$, and for any $x \in (a, b)$ we have (line larger than function):

$$f(x) - f(a) \leq \frac{f(b) - f(a)}{b - a}(x - a)$$

and

$$-(f(b)-f(x)) \leq -\frac{f(b)-f(a)}{b-a}(b-x)$$

Which together gives us:

$$\frac{f(x)-f(a)}{x-a} \leq \frac{f(b)-f(a)}{b-a} \leq \frac{f(b)-f(x)}{b-x}$$

Taking the b limit first, and then the a limit we get finally: $f'(a) \leq f'(b)$

$\Longleftarrow$) Suppose $\exists a, b$ and x between them so that

$$f(x) \geq f(a) + \frac{f(b)-f(a)}{b-a}(x-a)$$

which gives

$$\frac{f(x)-f(a)}{x-a} \geq \frac{f(b)-f(a)}{b-a}$$

But non-convexity also implies

$$f(x) \geq f(b) + \frac{f(b)-f(a)}{b-a}(x-b)$$

which yields:

$$\frac{f(b)-f(a)}{b-a} \geq \frac{f(x)-f(b)}{x-b}$$

Together this gives:

$$\frac{f(x)-f(a)}{x-a} \geq \frac{f(b)-f(x)}{b-x}$$

which (from MVT) means:

$$f'(p) \geq f'(q)$$

for $p < q$. We. are. done. ■