

DE MATHEMATICA PURA  
On Pure Mathematics

Harry Han

February 14, 2023

# Index Capitum

<b>1</b>	<b>Notation</b>	<b>1</b>
<b>2</b>	<b>Analysis</b>	<b>2</b>
2.1	Real Number . . . . .	2
2.1.1	The Countable Sets . . . . .	2
2.2	Sequence and Series . . . . .	3
2.2.1	Sequence . . . . .	3
2.2.2	Series . . . . .	4
<b>3</b>	<b>Algebra</b>	<b>7</b>
3.1	Group . . . . .	7
<b>I</b>	<b>Latin and Abbreviations</b>	<b>10</b>
<b>II</b>	<b>Chronology of Proposed, Proved, and Disproved Hypotheses</b>	<b>11</b>

## **Abstract**

These are my notes when taking the class *Fundamentals of Pure Mathematics* at the University of Edinburgh. They are not a replicate of the lecture notes: they are my thoughts and explorations. Most importantly, all proofs presented in this document are of my own conception.

Terms like “Theorem, Proposition” are coined in Latin. As the English terms descended from Latin, most of them are self-explanatory.

# Caput 1

## Notation

- The `\mathbb{}` fonts are used to denote sets. ( $\mathbb{S}, \mathbb{Y}$ , etc.)
- $\mathbb{A} \succ \mathbb{B}$  denotes there exists a surjective function  $f : \mathbb{A} \rightarrow \mathbb{B}$ .  $\prec, \asymp$  denotes injective, bijective, respectively.
- $e$  is used to denote the identity of a group.
- When there is no ambiguity, the notation for the operation of group is omitted. (i.e.,  $a \odot b = ab$ ).  $a^{-1}$  is used to denote the inverse of  $a$ .
- Sequence and series are denoted as  $(s_n)$  and  $\sum_{k=1}^{\infty} s_k$  respectively.
- $\mathcal{L}_s(s_n), \mathcal{L}_s(s_n)$  is the limit of supremum & infimum. See definition 2.2.4.

# Caput 2

## Analysis

### 2.1 Real Number

#### 2.1.1 The Countable Sets

**Axioma 2.1.1** (The "Smallest" Infinite Set). A set  $\mathbb{S}$  is infinite iff  $\mathbb{S} \succ \mathbb{N}$ .

*Observatio 2.1.1.* Although FPM is a pure mathematic class with emphasis on rigor, no rigorous definition for the infinite set has been proposed. This definition/axiom is of my own conception.

**Definitio 2.1.1** (Countable Set). A set  $\mathbb{S}$  is countable iff  $\mathbb{N} \asymp \mathbb{S}$  (there exists a bijection  $f : \mathbb{N} \rightarrow \mathbb{S}$ ).

**Theorema 2.1.1** (At Most Countable). *Let  $\mathbb{A}$  be an infinite set.*  
 $(\mathbb{A} \prec \mathbb{N})$  iff  $(\mathbb{A} \asymp \mathbb{N})$ .

**Demonstratio.** We want to prove  $\mathbb{A} \prec \mathbb{N}$  is equivalent to  $\mathbb{A} \asymp \mathbb{N}$ .  $\mathbb{A} \asymp \mathbb{N} \rightarrow \mathbb{A} \prec \mathbb{N}$  is by definition. We only need to prove the other direction; i.e., provided  $\mathbb{A} \prec \mathbb{N}$ , find a bijective function  $h : \mathbb{A} \rightarrow \mathbb{N}$ .

Let  $f : \mathbb{A} \rightarrow \mathbb{N}$  be an injective mapping. If  $f$  is bijective, we are done. If  $f$  is injective but not bijective, let  $\mathbb{N}^-$  be the range of  $f$ . As  $\mathbb{A}$  is infinite,  $\mathbb{N}^-$  is also infinite. Let  $f' : \mathbb{A} \rightarrow \mathbb{N}^-$  such that  $f(a) = f'(a)$ .  $f'$  is an bijective mapping.

Thus we only need to show there exists a mapping  $g : \mathbb{N}^- \rightarrow \mathbb{N}$  that is bijective.

$g$  can be constructed by such: sort  $\mathbb{N}^-$  and  $\mathbb{N}$  in ascending order. Let the first element in the sorted  $\mathbb{N}^-$  maps to the first in the sorted  $\mathbb{N}$ , the second to second, etc. As  $\mathbb{N}^-$  is infinite,  $g$  must be bijective.

Indeed  $h = g \circ f' : \mathbb{A} \rightarrow \mathbb{N}$  is the bijective mapping we seek. **Q.E.D.**

**Theorema 2.1.2** (List of Countable and Uncountable Sets). *Any of the following sets are countable.*

1.  $\mathbb{Z}, \mathbb{Q}$
2. *Any infinite subset of countable sets.*
3. *Any Unions of countable and finite sets.*
4. *Any products of countable sets and finite sets. i.e., if  $\mathbb{S}, \mathbb{T}$  are countable,  $\{\mathbb{S} \times \mathbb{S}\}, \{\mathbb{S} \times \mathbb{T} \times \cdots \times \mathbb{S}\}$  are also countable.*

*Coniectura 2.1.1.* Is the product of countable number of countable sets countable? (Proposed Feb 6)

## 2.2 Sequence and Series

### 2.2.1 Sequence

**Definitio 2.2.1** (Sequence).

**Definitio 2.2.2** (Convergent and Divergent).

**Definitio 2.2.3** (Increasing and Decreasing Sequence(Monotone)).

**Definitio 2.2.4** (Limit of supremum & infimum). For a sequence  $(s_n)$ , let  $b_i$  denotes the supremum of  $\{s_n | n > i\}$ . If  $(b_n)$  converges, the value it converges to is called the limit of supremum of  $(s_n)$ , and is denoted as  $\mathcal{L}_s(s_n)$ .  $(b_n)$  is called the supremum sequence. Similarly infimum sequence and limit of infimum are defined, and the later denoted as  $\mathcal{L}_i(s_n)$ .

*Observatio 2.2.1.* Notice supremum and infimum sequences are monotone.

**Theorema 2.2.1** (Convergence and Limit of supremum & infimum). *A sequence  $(s_n)$  converges if and only if  $\mathcal{L}_s(s_n) = \mathcal{L}_i(s_n)$ . (Proposed Feb 8 2023, proved Feb 9)*

**Demonstratio.** We want to prove that  $(\mathcal{L}_i(s_n) = \mathcal{L}_s(s_n)) \iff (s_n)$  converges.

Forward direction: We shall show that  $\lim_{n \rightarrow \infty} (s_n) = \mathcal{L}_s(s_n) = \mathcal{L}_i(s_n) = \lambda$ .  $\forall \epsilon > 0$ , we know by our assumption that  $(\exists N \in \mathbb{N})(\forall n > N)$  the set  $\{s_n | n > N\}$  is bounded by  $\lambda \pm \epsilon$ . This is the definition for the convergent sequence.

We shall prove the contraposition of the backwards direction, i.e.  $(\mathcal{L}_i(s_n) \neq \mathcal{L}_s(s_n)) \rightarrow (s_n)$  diverges. The contraposition can be proved by contradiction.

Assuming  $(\lambda = \mathcal{L}_i(s_n) \neq \mathcal{L}_s(s_n))$  and  $(s_n)$  converges to  $l$ . S.D.U., let  $\lambda > l$ . Let  $\epsilon = (\lambda - l)/2$ . Since  $(s_n)$  converges to  $l$ , there exists  $N \in \mathbb{N}$  such that  $\forall n > N, |s_n - l| < \epsilon$ . However, we know that  $\mathcal{L}_i(s_n) = \lambda$ , which means that there exists  $N'$  such that  $\forall n > N'$  we have at least one element  $s_i > \lambda - \epsilon$ . Indeed  $s_i - l > \epsilon$ , contradicting with our assumption that  $(s_n)$  converges. Thus we conclude the backwards direction is also true. **Q.E.D.**

**Definitio 2.2.5** (Cauchy Sequence). [1] A sequence  $(s_n)$  is a Cauchy Sequence iff  $(\forall \epsilon > 0)(\exists N)(\forall n, m > N)(|s_n - s_m| < \epsilon)$

**Theorema 2.2.2.** A sequence converges if and only if it is a Cauchy Sequence.

*Observatio 2.2.2.* We are to outline our proof of  $(s_n)$  converges  $\iff (s_n)$  is Cauchy Sequence.

The forward direction is obvious. To prove the backwards direction, notice: 1) All Cauchy Sequences are bounded; 2) the infimum and supremum sequence converge by monotone convergence theorem; 3) They must converge to the same value; 4) By theorem 2.2.1 the sequence must converge.

*Observatio 2.2.3.* We can define a pseudo Cauchy Sequence to be sequence  $(s_n)$  such that  $(\forall \epsilon > 0)(\exists N)(\forall n > N)(|s_n - s_{n+1}| < \epsilon)$ . Indeed all convergent sequence are pseudo Cauchy Sequence, but not all pseudo Cauchy Sequence are convergent. An example is the partial sum of harmonic series, i.e,  $(\sum_{i=1}^n \frac{1}{i})$ .

## 2.2.2 Series

**Definitio 2.2.6** (Series). A series can be expressed as  $\sum_{k=1}^{\infty} a_k$ .

**Definitio 2.2.7** (Convergent and Divergent). Consider the seires :  $(s_n) = \sum_{k=1}^n a_k$ .  $(s_n)$  is called the partial sum of the series. The series  $\sum_{k=1}^{\infty} a_k$  converges if and only if its partial sum converges; otherwise it diverges.

*Exempli Gratia 2.2.1.* List of Convergent and Divergent series:

1. Harmonic Series.

**Definitio 2.2.8** (Cauchy Criterion). A series befits Cauchy Criterion if and only if its partial sum is a Cauchy Sequence.

**Definitio 2.2.9** (Absolute Convergent). A series  $\sum_{k=1}^{\infty} a_k$  converges absolutely if and only if  $\sum_{k=1}^{\infty} |a_k|$  converges. Otherwise it converges non-absolutely

**Theorema 2.2.3** (Convergence Reveries).

1. For convergent series  $\sum_{k=1}^{\infty} s_k$ ,  $\sum_{k=1}^{\infty} s'_k$ , and constant  $c$ , all of the following sequence converges:  $\sum_{k=1}^{\infty} -s_k$ ,  $\sum_{k=1}^{\infty} c \cdot s_k$ ,  $\sum_{k=1}^{\infty} s_k + s'_k$ ,  $\sum_{k=1}^{\infty} s_k \cdot s'_k$ .  
In particular,  $\sum_{k=1}^{\infty} \frac{1}{s_k}$  diverges.  
 $\sum_{k=1}^{\infty} \frac{s_k}{s'_k}$  may diverge or converge.
2. **Absolute Convergent:**  
If a series converges absolutely, it converges. The converse is not true.
3. **Comparison Test:**  
For convergent series  $\sum_{k=1}^{\infty} s_k$ , if  $|b_k| \leq s_k$  for all  $k$ ,  $\sum_{k=1}^{\infty} b_k$  converges.  
For divergent series  $\sum_{k=1}^{\infty} d_k = \infty$ , if  $e_k \geq d_k$  for all  $k$ ,  $\sum_{k=1}^{\infty} e_k$  diverges. If  $\sum_{k=1}^{\infty} a_k$  and  $\sum_{k=1}^{\infty} b_k$  converges, the followings also converge:  $\sum_{k=1}^{\infty} (a_k + b_k)$ ,  $\sum_{k=1}^{\infty} (a_k - b_k)$ ,  $\sum_{k=1}^{\infty} (a_k \cdot b_k)$
4. **Ratio Test:**  
For series  $\sum_{k=1}^{\infty} s_k$ , let  $d = \lim_{k \rightarrow \infty} \left| \frac{s_k}{s_{k-1}} \right|$ .  
If  $d < 1$ , the series converges absolutely.  
If  $d > 1$ , the series diverges.  
If  $d = 1$ , the series may converge or diverge.
5. **Root Test:**  
For series  $\sum_{k=1}^{\infty} s_k$ , let  $d = \lim_{k \rightarrow \infty} |(s_k)^{1/k}|$ .  
If  $d < 1$ , the series converges absolutely.  
If  $d > 1$ , the series diverges.  
If  $d = 1$ , the series may converge or diverge.
6. **Alternating Series Test:**  
For series in the form  $\sum_{k=1}^{\infty} (-1)^k s_k$ . If  $s_k$  is decreasing and  $\lim_{k \rightarrow \infty} s_k = 0$ , the series converge. (Copied from textbook on 14 Feb 2023, not proved.)
7. **Cauchy's Condensation Test:**  
Consider series  $\sum_{k=1}^{\infty} s_k$ . If  $s_k$  is decreasing and greater than zero, the series converge if and only if  $\sum_{k=1}^{\infty} s_{2^k} 2^k$  converges.
8. **Integral Test** For  $s_k > 0$ , the series  $\sum_{k=1}^{\infty} s_k$  converge if and only if  $\int_a^{\infty} f(k)$  converge for some constant  $a$ , provided  $\forall k \in \mathbb{N}, f(k) = s_k$ .  
(Proposed Feb 14 2023)

**Demonstratio.**



- To prove 2 of theorem 2.2.3, Consider the convergent series  $\sum_{k=1}^{\infty} |a_k|$ . Split  $\sum_{k=1}^{\infty} a_k$  into  $\sum_{k=1}^{\infty} p_k$  and  $\sum_{k=1}^{\infty} n_k$ , where  $p_k, n_k$  are positive and negative, respectively. (We can safely ignore any 0) As  $\sum_{k=1}^{\infty} p_k \leq \sum_{k=1}^{\infty} |a_k|$  and  $\sum_{k=1}^{\infty} n_k \geq -\sum_{k=1}^{\infty} |a_k|$ , both series are bounded. By Monotone convergence theorem, both series converge. Thus  $\sum_{k=1}^{\infty} a_k$ , as the sum of two convergent series, must converge.
- Entry NO. 7, Cauchy's Condensation Test, has two directions: for decreasing and positive  $s_k$ ,  $\sum_{k=1}^{\infty} s_k$  converges  $\iff \sum_{k=1}^{\infty} s_{2^k} 2^k$  converges.

To prove the forward direction, consider the convergent series:

$$2 \cdot \sum_{k=1}^{\infty} s_k = 2 \cdot s_1 + 2 \cdot (s_2 + s_3) + 2 \cdot (s_4 + s_5 + s_6 + s_7) \cdots$$

And

$$\sum_{k=1}^{\infty} s_{2^k} 2^k = s_1 + \underbrace{2 \cdot s_2}_{< 2 \cdot s_1} + \underbrace{4 \cdot s_4}_{< 2 \cdot (s_2 + s_3)} + \underbrace{8 \cdot s_8}_{< 2 \cdot (s_4 + s_5 + s_6 + s_7)} + \cdots \quad (2.1)$$

Thus by comparison test we conclude (2.1) converges.

The backwards direction directly follows the comparison test as

$$\sum_{k=1}^{\infty} s_{2^k} 2^k \geq \sum_{k=1}^{\infty} s_k.$$

***Q.E.D.***

# Caput 3

## Algebra

### 3.1 Group

**Definitio 3.1.1** (Group). Group is a set  $\mathbb{S}$  with an operation  $\odot$  that fulfills the following four properties:

1. Closure
2. Associativity:  $(a \odot b) \odot c = a \odot (b \odot c)$ ;
3. Identity
4. Inverse

**Theorema 3.1.1** (Consequence of the Definition). *There are many non-obvious properties that directly follows the definition.*

1. *General Associativity: Parenthesis does not matter, as long as the order is the same:  $a \odot b \odot c \odot d \odot e \odot f \odot g \cdots = (a \odot ((b \odot c) \odot e (\odot f \odot g) \cdots)) = \cdots$*
2. *Order of Inverse:  $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$ .*

Here are some examples of groups.

1.  $\mathbb{S} = \{e\}$
2.  $\mathbb{S} = \{e, a, b, c\}$ . With the following operation: 1. All elements are their own inverse; 2. The group is abelian. 2.  $a \odot b = c, a \odot c = b, b \odot c = a$ .

*Coniectura 3.1.1.* These are some of my hypothesis and thoughts.

1. different properties of odd finite groups and even finite groups

2. If defining the revert of the operation  $\odot$  to be  $\oslash$  as such:  $a \odot b = a \oslash b^{-1}$ . What are the sets such that it would be a group under both  $\odot$  &  $\oslash$ ?
3. Can we have a set  $\mathbb{S}$ , such that under the operation  $\odot$  we have  $\forall a, b \in \mathbb{S}, a \odot b = b \odot a$  but without associativity? (Community without associativity?)

**Definitio 3.1.2** (Order of Group and element). The order of the group  $\mathbb{S}$  is  $|\mathbb{S}|$  (How many elements it has).

The order of an element  $s \in \mathbb{S}$  is the smallest integer  $i$  such that  $s^i = e$ . (If such  $i$  exists)

**Definitio 3.1.3** (Cyclic Group). Let  $\mathbb{G}$  be a group and  $g$  one of its element. Considering the set:

$$\mathbb{S} = \{\cdots g^{-2}, g^{-1}, e, g, g^1, g^2 \cdots\}$$

If  $\mathbb{S}$  is finite, it is called a cyclic group. (It can be shown that it must be a subgroup of  $\mathbb{G}$ ).

**Theorema 3.1.2** (Properties of Cyclic Group). *Here are some properties immediately follows the definition.*

1. *Any subgroup of a cyclic group is also cyclic.*

**Theorema 3.1.3** (Lagrange Theorem). *Consider finite group  $\mathbb{G}$  and its subgroup  $\mathbb{S}$ .  $|\mathbb{S}|$  divides  $|\mathbb{G}|$ .*

*Exempli Gratia* 3.1.1. The followings demonstrate Lagrange Theorem.

1.  $\mathbb{Z}_{10}$  under addition modula 10 and its subgroup  $\mathbb{S} = \{0, 2, 4, 6, 10\}$ .  
 $|\mathbb{Z}_{10}| = 10, |\mathbb{S}| = 5$ .

**Demonstratio.**[Proof of Lagrange Theorem] Let  $\mathbb{G} = \{g_1, g_2, g_3, \cdots\}$  be a group and  $\mathbb{S} = \{s_0, s_1, s_2, \cdots\}$  (let  $s_0 = e$ ) be its subgroup. If  $\mathbb{S} = \mathbb{G}$ , we are done. If not, sine detrimento universalitatis (without loss of generality), let  $g_i \notin \mathbb{S}$ . Consider the set:  $\mathbb{D}_1 = \{g_1 s | s \in \mathbb{S}\}$ . The set  $\mathbb{D}_1$  has the following properties:

1.  $g_1 s \in \mathbb{D}_1 \rightarrow g_1 s \in \mathbb{G}$
2.  $|\mathbb{D}_1| = |\mathbb{S}|$ .
3.  $(\forall d \in \mathbb{D}_1)$  the set  $\mathbb{D}'_1 = \{ds | s \in \mathbb{S}\} = \mathbb{D}_1$
4.  $g_1 s \in \mathbb{D}_1 \rightarrow g_1 s \notin \mathbb{S}$ .

Property I is true because  $\mathbb{G}$  is a group with the property closure.

By claiming that  $g_1 s_i \neq g_1 s_j$  for  $i \neq j$  it is sufficient to show property II is true.

To prove property III, we shall prove statement 1)  $\mathbb{D}_1 \subseteq \mathbb{D}'_1$  and 2)  $\mathbb{D}'_1 \subseteq \mathbb{D}_1$ . To prove statement 1), consider  $a \in \mathbb{D}_1$ ,  $\exists s_1 \in \mathbb{S}$  such that  $g_1 s_1 = a$ . Let  $\mathbb{D}'_1$  be defined as  $\mathbb{D}'_1 = \{bs | s \in \mathbb{S}\}$ . and  $b$  can be written in the form of  $g_1 s_2$ . Indeed  $bs_2^{-1} s_1 = a \rightarrow a \in \mathbb{D}'_1 \rightarrow \mathbb{D}_1 \subseteq \mathbb{D}'_1$ . Statement 2) can be proved similarly.

Property IV can be proved by contradiction. Assuming  $\exists g_1 s \in \mathbb{D}_1$  and  $g_1 s \in \mathbb{S}$ . We have  $g_1 s s^{-1} \in \mathbb{S}$  (by Inverse and Closure property of group)  $\rightarrow g_1 \in \mathbb{S}$ , (by associativity property of group) contradicting our assumption that  $g \notin \mathbb{S}$ .

If  $\mathbb{G} = \mathbb{S} \cup \mathbb{D}_1$ , we are done, as  $|\mathbb{G}| = 2|\mathbb{S}|$ .

If  $\exists g_2 \in \mathbb{G} \setminus \mathbb{S}, \mathbb{D}_1$ . Construct the set  $\mathbb{D}_2 = \{g_2 s | s \in \mathbb{S}\}$ . All elements in  $\mathbb{D}_2$  have properties I, II of  $\mathbb{D}_1$ , and a stronger IV property:  $g_2 s \in \mathbb{D}_2 \rightarrow g_2 s \notin \mathbb{S}, \mathbb{D}_1$ .

Thus by same reasoning, if  $\mathbb{G} = \mathbb{S} \cup \mathbb{D}_1 \cup \mathbb{D}_2$ ,  $|\mathbb{G}| = 3|\mathbb{S}|$ . If not, we can construct more disjointed sets  $\mathbb{D}_3, \mathbb{D}_4, \dots, \mathbb{D}_n$  until the union of them and  $\mathbb{S}$  forms  $\mathbb{G}$ . This can always be done as  $\mathbb{G}$  is finite, and will have an order of  $(n+1) \cdot |\mathbb{S}|$ . ***Q.E.D.***

# Appendix I

## Latin and Abbreviations

De Mathematica Pura	On Pure Mathematics
Caput	Chapter
Index Capitis	Index of Chapters
Theorema, Theoremata .....	Theorem
Definitio, Definitiones	Definition
Propositio, Propositiones	Proposition
Coniectura, Coniecturae	Conjecture
Demonstratio, Demonstrationes	Proof
Q.E.D.	Quod Erat Demonstrandum
	Which was to be demonstrated, signify end of proof
Exempli gratia	For (the sake of) example
SDU(sine detrimento universalitatis)	without any loss of generosity

## Appendix II

# Chronology of Proposed, Proved, and Disproved Hypotheses

Hypothesis/Theorem	Date of Proposition	Date of Resolution	Outcome
Theorem 2.2.1	Feb 8, 2023	Feb 9	PROVED
Theorem 2.2.3.8	Feb 14, 2023		

# Bibliography

- [1] Kenneth A. Ross. *Elementary Analysis, The Theory of Calculus, Second Edition*. Springer, 2013. ISBN: 9781461462705.