DE MATHEMATICA PURA

On Pure Mathematics

Harry Han

March 15, 2023

Index Capitum

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 exits a surjective function $f : \mathbb{A} \to \mathbb{B}$. $\prec$, $\asymp$ 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 ommited. (i.e., $a \odot b = ab$). a^{-1} is used to denote the inverse of a.
- $\mathbb{H} \leq \mathbb{S}$ donotes that $\mathbb{H}$ is a subgroup of $\mathbb{S}$. If $\mathbb{H} \neq \mathbb{S}$, it is a proper subgroup and is denoted as $\mathbb{H} < \mathbb{S}$. See definition.
- 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 Axioms

Axioma 2.1.1 (Archimedean Property)**.** $\forall r \in \mathbb{R}, \exists n \in \mathbb{N}$ such that $n > a$.

Axioma 2.1.2 (The Completeness of Real Number)**.** Let $\mathbb{D} \subseteq \mathbb{R}$. If $\mathbb{D}$ is bounded, there exists $s\&i, \in \mathbb{R}$ such that they are the supremum and infimum of $\mathbb{D}$.

2.1.2 The Countable Sets

Axioma 2.1.3 (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 $f : \mathbb{N} \to \mathbb{S}$).

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

Let $f : \mathbb{A} \to \mathbb{N}$ 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 $f' : \mathbb{A} \to \mathbb{N}^-$ such that $f(a) = f'(a)$. f' is an bijective mapping.

Thus we only need to show there exists a mapping $g : \mathbb{N}^- \to \mathbb{N}$ 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 secound to secound, etc. As $\mathbb{N}^-$ is infinite, g must be bijective.

Indeed $h = g \circ f' : \mathbb{A} \to \mathbb{N}$ 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 $\lim_{n\to\infty}(s_n) = \mathcal{L}_s(s_n) = \mathcal{L}_i(s_n) = \lambda$. $\forall\epsilon > 0$, 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. $(\mathcal{L}_i(s_n) \neq \mathcal{L}_s(s_n)) \to (s_n)$ 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 monoteon 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.

Exampli 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 $d = \lim_{k\to\infty} |\frac{s_k}{s_{k-1}}|$.
   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 $d = \lim_{k\to\infty} |(s_k)^{1/k}|$.
   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 $\lim_{k\to\infty} s_k = 0$, the sereis converge. (Copied from textbook on 14 Feb 2023, not proved.)

7. ***Cauchy's Condenstation Test**:*
Consider series $\sum_{k=1}^{\infty} s_k$. If s_k is decreasing and greater than zero, the seires 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 $\int_a^{\infty} S(k)dk$ converge for some constant a, provided $\forall k \in \mathbb{N}, S(k) = s_k$. (Proposed Feb 14 2023, modified and proved 16 Feb)*

9. ***Raabe's Test** For series $\sum_{k=1}^{\infty} s_k$, let $l = n\left(1 - \dfrac{s_{n+1}}{s_n}\right)$. The series converge if $l > 1$, diverges if $l < 1$, and is inconclusive if $l = 1$.*

Coniectura 2.2.1 (Inspired from the Integral Test)*.* If the finite integral, with some constant a, $\int_a^{\infty} f(k)dk$, converges for function f, $\lim_{n\to\infty} \sum_{i=0}^{n} f(\Delta x_i i + a)$ converge for $\Delta x_i \in \mathbb{R}$, provided $\{\Delta x_i\}$ is bounded. (Proposed 15 Feb 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 serieses converge. Thus $\sum_{k=1}^{\infty} a_k$, as the sum of two convergent seires, 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

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

  Thus by comparison test we conlude (2.1) converges.

  The backwards direction directly follows the comparison test as $\sum_{k=1}^{\infty} s_{2^k} 2^k \geq \sum_{k=1}^{\infty} s_k$.

- Here we present an informal proof fo 2.2.3.8, the integral test with an extra restriction that the function is strictly decreasing. (15 Feb 2023)

  Consider the function S with the property $\int_a^\infty S(k)dk$ converges for some constant a and its correspondent series $\sum_{k=1}^\infty S(k)$. Consider the function $\sigma(x) = S(x-1)$ $\int_a^\infty \sigma(k)dk$ converges, and is greater than $\sum_{k=\lceil a \rceil}^\infty s_k$(as the function is strictly decreasing), thus by comparison test it converges, thus $\sum_{k=1}^\infty s_k$, as the sum of a convergent series and a constant also converge.

Q.E.D.

2.2.3 Interestring Sequences and Series

Sequences

Series

1. $\sum_{n=1}^\infty \frac{n}{2^n} = 1$

2.2.4 Decimal Expansion

2.3 Real Functions

2.3.1 Continuity

Definitio 2.3.1 (Continuity of a Function)**.** Function $f : \mathbb{D} \to \mathbb{R}$ (provided $\mathbb{D} \subseteq \mathbb{R}$) is continuous at a if and only if for all sequence (x_i) (provided $x_i \in \mathbb{D}$) that converges to a the sequence $(f(x_i))$ converges to $f(a)$.

If the function f is continuous for all $a \in \mathbb{A}$, we say f is continous on the interval $\mathbb{A}$.

Theorema 2.3.1 (Equivalent Defintion)**.** *The definition 2.3.1 of function $f : \mathbb{D} \to \mathbb{R}$ is continuous at $a \in \mathbb{D}$ is equivalent to $\lim_{x\to a} f(x) = f(a)$, provided $\mathbb{D}$ is a non-degenerate interval in $\mathbb{R}$; i.e. $\forall \epsilon \in \mathbb{D} \exists \delta$ such that $|x-a| < \delta \implies |f(x) - f(a)| < \epsilon$.*

Definitio 2.3.2 (Extreme Value Theorem)**.** $f : \mathbb{I} \to \mathbb{R}$ where $\mathbb{I}$ is a close interval of real number is bounded and would attain supremum and infimum on $\mathbb{I}$.

Demonstratio. We shall first show that a continuous function whose domain is a closed interval must have finite number of local maxima, and thus bounded above. Its maximum is the maximum of the set consisted of all local maxima and its value at the end points. [1]

In this proof let $f(x)$ be a continous function defined in a closed interval $[l, h]$.

A real number $r = f(a)$ is a local maximum of function f if there exists $\delta > 0$ such that for all $x \in (a - \delta, a + \delta), f(a) > f(x)$.

Moreover, we claim that for all local maxima $f(a)$ attained at a, there exists a interval (s, a) such that the function is strictly increasing in the interval (s, a), but not so for any interval (s', a) with $s' < s$. There also exists another interval (a, d) such that the function is stricting decreasing in the interval but not so for any interval $(a.d')$ with $d < d'$.

The interval (s, d) is called the charateristic interval of local maxima attained at a, and $\lambda = (d - a)$ is its charateristic length. We claim the characteristic intervals partitions $[l, h]$. Define function $\gamma : [l, h] \to \mathbb{R}$ as $\gamma(x) = \lambda$ if $x \in (a, d)$. Importantly, $\exists \beta > 0$ such that $\exists \zeta \in [x - \lambda, x + \lambda]$ and $|f(x) - f(\zeta)| > \beta$.

If $f(x)$ attains infinitely many local maxima, we claim that $\exists \alpha \in [l, h]$ such that $\lim_{x \to \alpha} \gamma(x) = 0$. Thus there exists $\beta > 0$ such that for all $\delta > 0$ there exists $0 < \lambda < \delta$ such that there exists $\zeta \in [\alpha - \lambda, \alpha + \lambda]$ and $|f(\alpha) - f(\zeta)| > \beta$, which means f is discontinuous at α, contridicting our assumption, and we can conclude that f is indeed bounded above.

So far we have proved that a function that is continuous in a closed interval must be bounded above. It is similar to prove that it is bounded below. Q.E.D.

Observatio 2.3.1. We have not restrict the domain of function f to be real number to show it is bounded, although it may be required if we need to show it would attains sup and inf.

Notice, extreme value theorem does not hold when $\mathbb{I}$ is a open interval. For example, function $f(x) = \frac{1}{x}$ is continous but unbounded in the open interval $(0, 1)$.

Corollarium 2.3.1. *Let function $f : \mathbb{D} \to \mathbb{R}$ be continuous on the inteval $I = [a, b]$. For all $\epsilon \in I$, there exists a subinterval $S \subseteq I$ and $\epsilon \in S$ such that in S the function f is either strictly increasing, decreasing, or remain constant.*

[1] Indeed a continuous function in a closed interval may have 0 local maximum or minimum: in such cases the statement still holds, though it requires more justifications.

Coniectura 2.3.1 (Valid Domain for EVT)*.* Investigate the valid domain for EVT under the definition of continuity.

Theorema 2.3.2 (Intermediate Value Theorem)**.** *Let* $f : \mathbb{D} \to \mathbb{R}$ *be continuous on the interval* $[a, b] \in \mathbb{D}$*.* $\forall c$ *such that* $f(a) < c < f(b)$ $\exists d \in [a, b]$ *such that* $f(d) = c$*.*

Demonstratio.[Proof of Intermediate Value Theorem] Construct a set $\mathbb{E} = \{e \in [a, b] | f(e) < c\}$. Since $f(a) < c$, $\mathbb{E}$ is non empty. As $\mathbb{E}$ is bounded, by the completeness of real number, there exists a supremum , which shall be denoted as $\sup \mathbb{E} = s$. As $\mathbb{E}$ is bounded by a close inteval, s is also bounded by the same intevral. Our aim is to show that $f(s) = c$.

By our assumption f is continous at s. Assuming $f(s) < c$. Since f is continous as s, there exists $\delta \in \mathbb{R}$ such that for all $s < x < \delta$, $|f(x) - f(s)| < c - f(s)$, i.e., $f(s) < f(x) < c$, contradicting our assumption that s is the supremum of $\mathbb{E}$. Thus we conlude $f(s) \geq c$. $f(s) \leq c$ can be proved similarly. Q.E.D.

Observatio 2.3.2*.* The sequence definition of continuity sets no restrains on the domains of the function. Indeed by this definition all discrete functions are continuous: contradicting our intuition about continuity.

The more important consequence of continuity relies heavily on the properties of real number, i.e, the completeness of real number.

2.3.2 Bizare Functions

Coniectura 2.3.2*.*

1. Is there a defined in close interval $[a, b]$ but is not strictly increasing nor decreasing for any interval in its domain?

2. Is there a function that is continuous everywhere but not differentiable at any point?

Non Increasing Nor Decreasing Let function $f : \mathbb{R} \to \mathbb{R}$ be defined as such:

$$f(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{otherwise} \end{cases}$$

As infinitely many number of rational numbers and irrational number are contained in any domain $[a, b]$, such funtion is not increasing nor decreasing for any intervals of real number.

Unbounded Functions Commonly, unbounded functions are defined in a open inteval, e.g., $\frac{1}{x}$ in the interval $(0, 1]$. By extreme value theorem we know that there is no continuous function in close interval that is unbounded. However, there is function that is non-continuous that shows unbounded behaviour in close inteval.

Consider the function $f : [0, 1] \to (\infty, 1]$ defined as thus:

$$f(x) = \begin{cases} 2^{n+1}, & \text{if } x = 2^{-n} \text{ for some natural number } n \\ x, & \text{otherwise} \end{cases}$$

Caput 3

Algebra

3.1 Group: Definition

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

1. Closure: $\forall a, b \in \mathbb{S}, a \odot b \in \mathbb{S}$.
2. Associtivity: $\forall a, b, c \in \mathbb{S}, (a \odot b) \odot c = a \odot (b \odot c)$;
3. Identity: $\exists e \in \mathbb{S}$ such that $a \odot e = e \odot a = a$ for all $a \in \mathbb{S}$;
4. Inverse: $\forall a \in \mathbb{S}, \exists a^{-1} \in \mathbb{S}$ such that $a \odot a^{-1} = e$.

Observatio 3.1.1*.* A quick definition for operation, $\odot$, within the set $\mathbb{S}$ is that $\odot : \mathbb{S} \times \mathbb{S} \to \mathbb{S}$; moreover, we can denote $\odot(a, b) = a \odot b$.

The definition of identity can not be simplified to $\exists e \in \mathbb{S}$ such that $a \odot e = a$ for all $a \in \mathbb{S}$. Nothing has prevented us from arbitrating that for a certain set $\mathbb{S}$ and $a, b \in \mathbb{S}$, $a \odot b = a$ while $b \odot a \neq a$.‘

In contrast, the definition of inverse needs not such emphasis. If a set $\mathbb{S}$ has the property of closure, associtivity, and identity, $\forall a \in \mathbb{S} \exists a^{-1} \in \mathbb{S}$ such that $a \odot a^{-1} = e$ would implies that $a^{-1}a = e$. Here is a quick proof.

Let $b = a^{-1}$. $ab = e \implies abb = bab = b$ (multiply both sides of e with b). We know b itself has an inverse, denoted as c; thus $abbc = babc = bc$, and by associtivity, $ab(bc) = abbc = babc = ba(bc) \implies ab = ba = e$.

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

1. *General Associtivity: 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:* $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$.

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 reverto 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 associtivity? (Community without associtivity?)

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)

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. $a \odot b = c, a \odot c = b, b \odot c = a$.

Definitio 3.1.3 (Subgroup)**.** A subgroup of a group $\mathbb{S}$ is a subset $mathbbH$ of $\mathbb{S}$ that is also a group under the same operation $\odot$. It is denoted as $\mathbb{H} \leq \mathbb{S}$. If $\mathbb{H} \neq \mathbb{G}$, we call it a proper subgroup with notation $\mathbb{H} < \mathbb{S}$.

Theorema 3.1.2 (Test For Subgroup)**.** *For group* $\mathbb{S}$ *and it subset*$\mathbb{H} \subseteq \mathbb{S}$*,* $\mathbb{H}$ *is a subgroup of* $\mathbb{S}$ *if and only if*

1. $\mathbb{H}$ *is not empty*

2. $\forall h, k \in \mathbb{H}, h \odot k^{-1} \in \mathbb{H}$.

Graphs can help us to construct/discover more examples of groups.

Definitio 3.1.4 (Graph)**.** A graph is a finite set of vertices and edges connecting the vertices; or, with abstraction of set theory, a graph consists of two sets $\mathbb{V}$ and $\mathbb{E}$, where each element of $\mathbb{E}$ is an element of $\mathbb{V} \times \mathbb{V}$.

Definitio 3.1.5 (Isomophisim)**.** Isomophisim of a graph is a bjection of vertices that preseves all edges; or, $\exists$ bijective $f : \mathbb{V} \to \mathbb{V}$, such that $\mathbb{E}' = \{(f(a), f(b)) | a, b \in \mathbb{E}\} = \mathbb{E}$.

Definitio 3.1.6 (Dihedral Group)**.** The dihedral group of order $2n$ is the group of symmetries of a regular n-gon. It is the direct product of two copies of the cyclic group of order n.

Definitio 3.1.7 (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. Most importantly, all sets of such form with inheritted operation must be a group.

Theorema 3.1.3 (Properties of Cyclic Group)**.** *Here are some properties immediately follows the definition.*

1. *All set in the form of the defintion of the cyclic group is a subgroup.*
2. *Any subgroup of a cyclic group is also cyclic.*

Demonstratio.

Q.E.D.

Exampli Gratia 3.1.1. An example of cyclic group is $\mathbb{Z}_n$. (Integer under modular n addition);

Propositio 3.1.3.1 (Number of Subgroup for $\mathbb{Z}_n$)**.** *The number of the subgroup of cyclic group $\mathbb{Z}_n$ is equal to the number of the divisor of n. (Proposed 27 Feb 2023)*

Definitio 3.1.8 (Left Coset)**.**

Theorema 3.1.4 (Lagrange Theorem)**.** *Consider finite group $\mathbb{G}$ and its subgroup $\mathbb{S}$. $|\mathbb{S}|$ divides $|\mathbb{G}|$.*

Propositio 3.1.4.1. *Lagrange theorem implies that: for a group $\mathbb{G}$ and $g \in \mathbb{G}$:*

1. *$\omega(g)$ divides $|\mathbb{G}|$;*
2. *$g^{|\mathbb{G}|} = e$;*

Exampli Gratia 3.1.2. 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. $g_1 s \in \mathbb{D}_1 \to g_1 s \in \mathbb{G}$
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. $g_1 s \in \mathbb{D}_1 \to g_1 s \notin \mathbb{S}$.

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 sufficently 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 $g_1 s_1$. 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 $bs_2^{-1} s_1 = a \to a \in \mathbb{D}_1' \to \mathbb{D}_1 \subseteq \mathbb{D}_1'$. 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) $\to g_1 \in \mathbb{S}$,(by associtivity 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 $\exists g_2 \in \mathbb{G} \vee g_2 \notin \mathbb{S}, \mathbb{D}_1$. Construct the set $\mathbb{D}_2 = \{g_w s | s \in \mathbb{S}\}$. All elements in $\mathbb{D}_2$ have properties I, II of $\mathbb{D}_1$, and a stronger IV property: $g_1 s \in \mathbb{D}_2 \to g_1 s \notin \mathbb{S}, \mathbb{D}_1$..

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 constuct more disjoined sets $\mathbb{D}_3, \mathbb{D}_4, \cdots \mathbb{D}_n$ 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.

Propositio 3.1.4.2 (Some Application of Lagrange Theorem)**.**

1. *For a group $\mathbb{G}$ with order p and $k \in \mathbb{G}$ with order q; then q divides p.*
2. *For a group $\mathbb{G}$ with prime order (i.e., $|\mathbb{G}|$ is prime), it must be a cyclic group.*

Demonstratio. 3.1.4.2.1 implies 3.1.4.2.2. To prove proposition 3.1.4.2.1, let $\mathbb{G}$ be a group and $\langle g \rangle$ be a cyclic group containing $g \in \mathbb{G}$, by langrange theorem $|\langle g \rangle|$ must divides $|\mathbb{G}|$. Q.E.D.

3.2 Between Groups

Definitio 3.2.1 (Homomorphism)**.** Group $\mathbb{G}$ & $\mathbb{P}$ are isomorphic to each other if there exists a function (shall we add the following[proposed 14 mar] defined for all $a \in \mathbb{G}$) $\phi : \mathbb{G} \to \mathbb{P}$ such that $a, b \in \mathbb{G} \implies \phi(ab) = \phi(a)\phi(b)$.

The function ϕ is denominated as a homomorphism of the group $\mathbb{G}$&$\mathbb{P}$.

Definitio 3.2.2 (Isomorphism)**.** A homomorphism $\phi\mathbb{G} \to \mathbb{P}$ that is also a bijection is a isomorphism of group $\mathbb{B}$&$\mathbb{P}$, and we denote two such isomorphic group with $\mathbb{G} \cong \mathbb{P}$.

Propositio 3.2.0.1 (Consequence of homomorphism)**.** *Let* $\phi : \mathbb{G} \to \mathbb{P}$ *denote a homomorphism.*

1. $\phi(e_{\mathbb{G}}) = e_{\mathbb{P}}$.
2. $\{\phi(c) | c \in \mathbb{G}\} \leq \mathbb{P}$.

Appendix I

On Polynomials

Coniectura I.0.1. Provided $n + 1$ points in 2 dimensional spaces,there are exactly one n degree polynomials that passes through all the points, provided that those $n + 1$ points are not passed throught by another polynomial of lower degree.

Extension: how about $n + 1$ points in d dimensional spaces? (Proposed 1 Mar 2023)

Exampli Gratia I.0.1. For points $(0, 0), (1, 1), (2, 4)$, the only 2 degree polynomials that pass throught it is $y = x^2$.

However, for points $(0, 0), (1, 1), (2, 2)$, there are no degree 2 polynomials that pass through it.

This hypothesis is definitely related to linear independence.

Demonstratio.[A Quick proof using Fundamental Theorem of Algebra]

Q.E.D.

Appendix II

Latin and Abbreviations

De Mathematica Pura	On Pure Mathematics
Caput	Chapter
Index Capitis	Index of Chapters
Theorema, Theoremae	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
Exampli gratia	For (the sake of) example
SDU(sine detrimento universalitatis)	without any loss of generosity

Appendix III

Chronology of Proposed, Proved, and Disproved Hypotheses

Hypothesis/Theorem	Date of Proposition	Date of Resolvation	Outcome
Theorem 2.2.1	Feb 8, 2023	Feb 9	PROVED
Theorem 2.2.3.8	Feb 14, 2023	Feb 17	PROVED[1]
Theorem 2.2.3.6	Feb 14, 2023		
Hypothesis 2.2.1	Feb 16, 2023		
Theorem 2.2.3.9	Feb 17, 2023		

Bibliography

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