DE MATHEMATICA PURA

On Pure Mathematics

Harry Han

February 5, 2023

Index Capitum

1 **Notation** 1

2 **Analysis** 2

3 **Algebra** 4

I **Latin and Abbreviations** 7

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. 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 $f : A \to B$. $\prec$, $\asymp$ 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.

Caput 2

Analysis

Axioma 2.0.1 (The "Smallest" Infinite Set)**.** A set $\mathbb{S}$ is infinite iff $\mathbb{S} \succ \mathbb{N}$.

Observatio 2.0.1. 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 2.0.1 (Countable Set)**.** A set $\mathbb{S}$ is countable iff $\mathbb{N} \asymp \mathbb{S}$ (there exists a bijection $f : \mathbb{N} \to \mathbb{S}$).

Corollarium 2.0.1 (At Most Countable)**.** *Let $\mathbb{A}$ be an infinite set. ($\mathbb{A} \prec \mathbb{N}$) iff ($\mathbb{A} \asymp \mathbb{N}$).*

Proof. 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 2.0.1 (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 products of countable sets. If* $\mathbb{S}$ *is countable,* $\{\mathbb{S} \times \mathbb{S}\}, \{\mathbb{S} \times \mathbb{S} \times \cdots \times \mathbb{S})\}$ *are also countable.*

Caput 3

Algebra

Definitio 3.0.1 (Group)**.** Group is a set $\mathbb{S}$ with an operation $\odot$ that fulfills the following four properties:

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

Theorema 3.0.1 (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:* $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$.

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 3.0.1*.* 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 3.0.2 (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 3.0.3 (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 3.0.2 (Properties of Cyclic Group)**.** *Here are some properties immediately follows the definition of cyclic group.*

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

Theorema 3.0.3 (Lagrange Theorem)**.** *Consider finite group* $\mathbb{G}$ *and its subgroup* $\mathbb{S}$*.* $|\mathbb{S}|$ *divides* $|\mathbb{G}|$*.*

Exampli Gratia 3.0.1. The followings demonstrate Lagrange Theorem.

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

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: $\mathbb{D}_1 = \{g_1 s | s \in \mathbb{S}\}$. All elements in $\mathbb{D}_1$ 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. $g_1 s \in \mathbb{D}_1 \to g_1 s \notin \mathbb{S}$.

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. Property III 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 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 III property: $g_1 s \in \mathbb{D}_2 \rightarrow g_1 s \notin \mathbb{S}, \mathbb{D}_1$..

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.

Appendix I

Latin and Abbreviations

Theorema	Theorem
SDU(sine detrimento universalitatis)	without any of generosity