Lu Sun, and many more.

A Notebook on Algebra

To my family, friends and communities members who have been dedicating to the presentation of this notebook, and to all students, researchers and faculty members who might find this notebook helpful.

Contents

Foreword

If software or e-books can be made completely open-source, why not a notebook?

This brings me back to the summer of 2009 when I started my third year as a high school student in Harbin No. 3 High School. In around the end of August when the results of Gaokao (National College Entrance Examination of China, annually held in July) are released, people from photocopy shops would start selling notebooks photocopies that they claim to be from the top scorers of the exam. Much curious as I was about what these notebooks look like, never have I expected myself to actually learn anything from them, mainly for the following three reasons.

First of all, some (in fact many) of these notebooks were more difficult to understand than the textbooks. I guess we cannot blame the top scorers for being so smart that they sometimes make things extremely brief or overwhelmingly complicated.

Secondly, why would I want to adapt to notebooks of others when I had my own notebooks which in my opinion should be just as good as theirs.

And lastly, as a student in the top-tier high school myself, I knew that the top scorers of the coming year would probably be a schoolmate or a classmate. Why would I want to pay that much money to a complete stranger in a photocopy shop for my friend's notebook, rather than requesting a copy from him or her directly?

However, things had changed after my becoming an undergraduate student in 2010. There were so many modules and materials to learn in a university, and as an unfortunate result, students were often distracted from digging deeply into a module (For those who were still able to do so, you have my highest respect). The situation became even worse as I started pursuing my Ph.D. in 2014. As I had to focus on specific research areas entirely, I could hardly split much time on other irrelevant but still important and interesting contents.

This motivated me to start reading and taking notebooks for selected books and articles, just to force myself to spent time learning new subjects out of my comfort zone. I used to take hand-written notebooks. My very first notebook was on *Numerical Analysis*, an entrance level module for engineering background graduate students. Till today I still have on my hand dozens of these notebooks. Eventually, one day it suddenly came to me: why not digitalize them, and make them accessible online and open-source, and let everyone read and edit it?

—

As most of the open-source software, this notebook (and it applies to the other notebooks in this series as well) does not come with any "warranty" of any kind, meaning that there is no guarantee for the statement and knowledge in this notebook to be absolutely correct as it is not peer reviewed. **Do NOT cite this notebook in your academic research paper or book!** Of course, if you find anything helpful with your research, please trace back to the origin of the citation and double confirm it yourself, then on top of that determine whether or not to use it in your research.

This notebook is suitable as:

- a quick reference guide;
- a brief introduction for beginners of the module;
- a "cheat sheet" for students to prepare for the exam (Don't bring it to the exam unless it is allowed by your lecturer!) or for lecturers to prepare the teaching materials.

This notebook is NOT suitable as:

- a direct research reference;
- a replacement to the textbook;

because as explained the notebook is NOT peer reviewed and it is meant to be simple and easy to read. It is not necessary brief, but all the tedious explanation and derivation, if any, shall be "fold into appendix" and a reader can easily skip those things without any interruption to the reading experience.

—

Although this notebook is open-source, the reference materials of this notebook, including textbooks, journal papers, conference proceedings, etc., may not be open-source. Very likely many of these reference materials are licensed or copyrighted. Please legitimately access these materials and properly use them.

Some of the figures in this notebook is drawn using Excalidraw, a very interesting tool for machine to emulate hand-writing. The Excalidraw project can be found in GitHub, *excalidraw/excalidraw*.

Preface

This notebook is on *Algebra*. The first part of the notebook is about linear algebra, one of the first few modules a science and engineering undergraduate student would take in his first semester in the collage. It is absolutely the fundamental of almost all the mathematical tools he would use in the future. The second part of the notebook is about abstract algebra, a far more advanced topic and yet still a lot of fun to learn.

The key reference of this notebook is listed below. During the development of the notebook, this list may become longer and longer.

Book *Basic Algebra Second Edition (I and II)* by Nathan Jacobson, published by DOVER [1]

List of Figures

List of Tables

-

Part I

Linear Algebra

Part II

Abstract algebra

1

Abstract Algebra Basics

CONTENTS

What does "abstract" mean in the context of abstract algebra? How is abstract algebra different from classic algebra that has been introduced in earlier chapters? In short, classic algebra solves a particular problem using algebra algorithms, whereas abstract algebra studies these algorithms.

As an example, consider the following equation

$$Ax = y$$

where x, y are vectors and A a matrix. Solving x given particular A and y falls into the classic algebra domain. It is obvious that x does not necessarily exist or being unique for different y and A. Studying the general rules when x exists and when it is unique for a set of y and A becomes an abstract algebra problem.

Consider another example where

$$\begin{aligned} a+b &= b+a \\ ab &= ba \end{aligned}$$

which are often used to demonstrate the commutative property of calculations (summation and multiplication, in this example). In classic algebra, they are considered as ground truth. In abstract algebra, however, the focus shifts to a more formal and generalized understanding of the property. We need to dig deeper into how commutative property is defined, and why it holds true for summation and multiplication, but not for some other operations such as division.

In conclusion, while classic algebra performs calculations on numbers, vector and matrices, abstract algebra studies the concepts, tools, derivations and logic we use in the calculation, and tries to explain why they work in the way they do. Abstract algebra also develops new concepts, tools and algorithms that we can use to solve more complicated algebraic problems.

1.1 A Motivating Example

One of the most famous applications of abstract algebra is to study the analytical solution to the following polynomial equation

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0 \tag{1.1}$$

where $n \geq 1$ is the order of the polynomial and $a_1, \ldots, a_n$ are any arbitrary values. The analytical solutions to (1.1) for $n = 1$ and $n = 2$ are obvious. With some effort, the analytical solutions for $n = 3$ and $n = 4$ were found in the 16th century. Since then, people have been struggling to find the analytical solution to the fifth order and beyond $n \geq 5$ polynomial equations.

In the 18th and 19th century, Euler, Lagrange and Gaussian tried to address this problem. Their conclusion was that there is no analytical solution to polynomial equations of fifth order or higher, but they could not give a very solid proof to the statement. Nevertheless, the methods they used inspired a lot of people that would work on this problem.

In the 19th century, Abel was able to prove that there is no solution in radicals to general polynomial equations of fifth degree or higher with arbitrary coefficients (see Abel–Ruffini theorem). Furthermore, he discussed a set of special cases (with non-arbitrary coefficients in the polynomial equation) that can have analytical solutions. These special cases form a set of sufficient condition for a fifth order polynomial equation to have the analytical solution.

The necessary and sufficient condition for a fifth or higher order polynomial to have an analytical solution is finally fully discovered by the genius Galois at a remarkably young age. Galois was able to create his theorem (known Galois theorem) and use it to find the ultimate answer to this problem that people have been studied for centuries. His theorem goes far beyond that. Galois theorem will find its usefulness in many areas to come, and eventually it becomes an important building block of a subject known as abstract algebra today.

1.2 General Algebraic System

An algebraic system is essentially a mathematical system consisting of a non-empty set known as the domain together with a series of operations defined on the domain. There are many algebraic systems, and abstract algebra studies the properties of different algebraic systems. As will be introduced in later parts of the notebook, depending on the properties of the algebraic system, we can categorize them as groups, rings, fields, vector spaces, etc.

1.2.1 Set and Mapping

Set is one of the most commonly used terms across different mathematical subjects. It is also one of the fundamental concepts in abstract algebra. A set usually refers to a collection of distinct objects. Given a set U and an object x, one and only one of the following two statements must be true:

- Object x is a member of set U, denoted by $x \in U$;
- Object x is not a member of set U, denoted by $x \notin U$.

However, notice that due to the Russell's paradox, it is challenging to give a rigorous mathematical definition to a set that fulfill the above features.

Mapping, or function, is used to describe the association of elements in two sets. Mapping and function are used interchangeably in the this notebook. For example, let A be a set, and $A_0 \subset A$ a subset of A. For any element $x \in A_0$, define mapping

$$i \quad : \quad A_0 \rightarrow A$$

where

$$i(x) \quad = \quad x$$

In this case, mapping i is called the **embedding mapping** from A_0 to A.

Let A, B be two sets, and $A_0 \subset A$ as subset of A. Let $f : A \rightarrow B$, and $g : A_0 \rightarrow B$. Let $x \in A_0$. If $f(x) = g(x)$, function f is known as an **extension** of function g, and function g a **restriction** of function f (on A_0). This is denoted by $g = f|_{A_0}$.

Mappings can be chained together. For example, consider two mappings

$$\begin{aligned} f_1 &: A_1 \rightarrow A_2 \\ f_2 &: A_2 \rightarrow A_3 \\ f_3 &: A_3 \rightarrow A_4 \end{aligned}$$

With the above, we can denote $f = f_3 \circ f_2 \circ f_1$ a mapping from A_1 to A_4.

Meantime, consider other mappings

$$g_1 \quad : \quad A_1 \to B$$
$$g_2 \quad : \quad B \to A_4$$

Clearly, $g = g_2 \circ g_1$ is also a mapping from A_1 to A_4. The mappings above can be illustrated intuitively using the **mapping diagram** in Fig. 1.1. Mapping

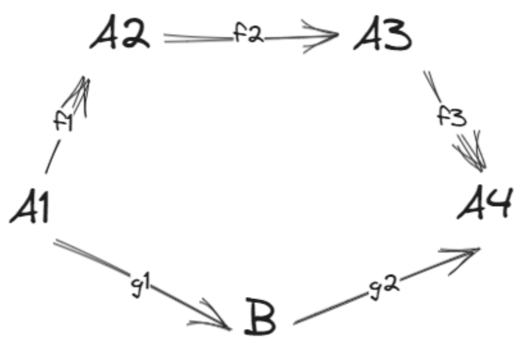

FIGURE 1.1
Mapping diagram that demonstrates f and g.

diagram can become handy with some complicated mappings.

The embedding mapping, extension function and restriction function introduced earlier can also be represented by a mapping diagram as shown in Fig. 1.2, where $A_0 \subset A$ and $i : A_0 \to A$ a embedding mapping. Function g defined on the subset A_0 is a restriction of f defined on the superset, whereas f is an extension of g, i.e., $f(x) = g(x)$ for $x \in A_0$.

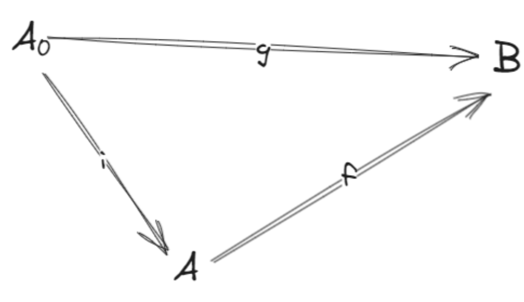

FIGURE 1.2
Mapping diagram of embedding mapping.

Multiple sets can be "combined" and "augmented" to form new sets. For example, the **Cartesian product** of two sets, A_1 and A_2, is defined as follows.

$$A_1 \times A_2 = \{(a, b)|a \in A_1, b \in A_2\}$$

where the tuple (a, b) can be interpreted as a probable ordered combination of elements in A_1 and A_2. The idea can be applied similarly to more sets.

1.2.2 Operation

Summation, multiplication, etc., are operations. In abstract algebra, we are more interested in the broad definition of operations from set perspective, instead of listing down individual operations and study how they work.

An operation essentially describes the rule of deriving or mapping from one or multiple elements to a new element, each element belongs to some non-empty set. Take binary operation as an example which maps two elements to one element. Let A, B, D be three non-empty sets. Let f be a mapping

$$f \quad : \quad A \times B \to D \tag{1.2}$$

Then f is called a algebraic operation from A, B to D. The operation can be denoted by $f(a, b)$ where $a \in A$ and $b \in B$. For convenience, binary operation is often denoted by $a \oplus b$, $a \otimes b$, or something similar from the writer preference. Notice that there are conventions to follow when using the symbols. For example, $+$, $-$, $\times$, etc., already have clear meanings.

The following is an example of operations. Let the domain of interest be $\mathbb{R}$, which is the real number set. Let v be a vector space (a set that contains a bunch of vectors) defined under $\mathbb{R}^n$. We can then define summation $+$ as a binary operation

$$+ \quad : \quad v \times v \to v$$

which indicates that the summation takes in two elements in the vector space, and generates a new vector that also belongs to the same vector space.

In the case where the domain and range of the operation come from the same set, i.e., in (1.2) $A = B = D$, the operation is said to be **closed** under this operation. In this example, the summation operation $+$ defined on v is closed, and we can simply say "$+$ is a binary operation defined on v".

Operations may have some unique properties. For example, let binary operation defined on A, denoted by $\oplus$, i.e., $\oplus : A \times A \to A$. If

$$a \oplus b \quad = \quad b \oplus a, \forall a, b \in A$$

then the operation is said to have **commutative property**. If

$$a \oplus (b \oplus c) \quad = \quad (a \oplus b) \oplus c, \forall a, b, c \in A \tag{1.3}$$

then the operation is said to have **associative property**, and (1.3) can be simply denoted by $a \oplus b \oplus c$. Let two binary operations defined on A, denoted by $\oplus$ and $\otimes$ respectively. If

$$a \oplus (b \otimes c) \quad = \quad (a \oplus b) \otimes (a \oplus c)$$

then the operation $\oplus$ is said to have the left-hand **distributive property** on operation $\otimes$. Similarly, right-hand distributive property can also be defined.

Commutative property, associative property and distributive property are commonly seen and widely discussed properties of operations. When operations have some of the three properties, simplified notation may apply. For example, if $\oplus$ operation has associative property, then

$$a^n \quad \equiv \quad \overbrace{a \oplus \cdots \oplus a}^{n}$$

can be used. If both commutative and associative properties hold, then it can be easily proved that

$$a^n b^n \quad = \quad (ab)^n$$

There are several different ways to present the result of an operation. When the cardinal number of the input sets are finite, a simple way is to list all the input-output associations in a table. An example is given in Fig. 1.3 which exhaustively lists down "and" logical operation results.

AND	0	1
0	0	0
1	0	1

FIGURE 1.3
Result of "and" logical operation.

1.2.3 Relation

Consider the relation of two elements a and b. In mathematics, relation essentially describes a property that the tuple made from the two elements, i.e. (a, b), may or may not have. Therefore, a straight forward way of defining a relation is to construct a set that contains some tuples, and if the specified tuple (a, b) is in the set, we say a, b have that relation, and equivalently (a, b) has that associated property.

For example, consider $a, b \in \mathbb{Z}$. Define relation

$$R = \{(a, b) \mid a - b = kn,\ k, n \in \mathbb{Z}, n > 1\} \tag{1.4}$$

where $\mathbb{Z}$ denotes the integer set. If a, b are such that $(a, b) \in R$, we say a, b are congruent modulo n, which is a congruence relation and can be denoted by

$$a \equiv b \ (\text{mod } n)$$

To summarize, let $a \in A$, $b \in B$. Let $R \subset A \times B$ be a subset of $A \times B$. the following statements can be considered equivalent:

- Two elements a and b have relation R;
- Tuple (a, b) has the property associated with relation R;
- Tuple $(a, b) \in R$;

and in that case we can use aRb to signify the relation. From above, we can see that each relation is associated with a subset R defined on the Cartesian product of the sets that the two elements belong to, and vise versa.

Like the case of operation where commutative, associative and distributive properties are defined, relation can also have special properties. For example, let relation R be defined on $A \times A$. If $\forall a, b, c \in A$,

$$aRa$$

then R is said to be **reflexive**. If

$$aRb \quad \Rightarrow \quad bRa$$

then R is said to be **symmetric**. If

$$aRb, bRc \quad \Rightarrow \quad aRc$$

then R is said to be **transitive**. Finally, if

$$aRb, bRa \quad \Rightarrow \quad a = b$$

then R is said to be **antisymmetric**.

From the above definitions, we can see that the commonly seen "$=$" relation defined on $\mathbb{R} \times \mathbb{R}$ is reflexive, symmetric and transitive. Similarly, "$\leq$" is reflexive, transitive and antisymmetric.

If a relation is simultaneously reflexive, symmetric and transitive, it is called an **equivalence relation**. The equal "$=$" relation and congruence relation introduced earlier are examples of equivalence relation.

We can define a **partition of a (non-empty) set** by grouping its elements into non-empty subsets in such a way that every element is included in exactly one subset, i.e.

$$A = \bigcup_{i\in I} A_i, \forall i,j \in I, i \neq j, A_i \neq \varnothing, A_i \bigcap A_j = \varnothing$$

A partition of a set can form a new set $\{A_i\}$. Furthermore, we can define a relation $R \subset A \times A$ on top of that partition as follows

$$R = \{(a,b) \mid \exists i, a, b \in A_i\}$$

and it is clear that such R is an equivalence relation. A partition of a set A can determine an equivalence relation $R \subset A \times A$ using the above method. Vise versa, an equivalence relation $R \subset A \times A$ can also determine a partition of set A as follows. For $\forall a \in A$, define

$$[a] = \{b \in A | aRb\}$$

where R is the equivalence relation, and $[a]$ the **equivalence class** of a.

With the definition of equivalence class, a partition of a set A can then derived from the equivalence relation R by

$$A/R = \{[a]|a \in A\} \text{ (remove duplication)} \tag{1.5}$$

where A/R is the partition of set A (this can be proved easily) derived from equivalence relation R. Notice that $[a]$ derived from different a yet in the same equivalence class will duplicate. When putting duplicated $[a]$ into a set, duplication should be removed, hence the note "remove duplication". It is not compulsory to add that note because it is inherently addressed by the fundamental properties of a set. The partition of set obtained using the above method is known as the **quotient set**. There is a one-to-one correspondence between an equivalent relation a partition of the set which is also known as the quotient set of that corresponding equivalent relation.

Given an equivalence relation, the following mappings can be defined.

$$\pi : A \to A/R,\ \pi(a) = [a]$$

which is known as the **canonical projection** or **quotient map**.

1.2.4 Congruent Modulo

We have introduced congruent modulo in the context of number theory as an example of equivalence relation. In that example, when two integers a and b are congruent modulo n, their equivalence relation persists even if k_1n, k_2n are added or subtracted from both of them respectively.

The concept of congruent modulo can be further generalized in the context of operation and equivalence relation as follows. Let A be an non-empty set. Let $\oplus$ be a closed binary operation defined on A, i.e., $\oplus : A \times A \to A$. Let R be an equivalence relation defined on A, i.e., $R \subset A \times A$, and A/R its corresponding quotient set. Let $a_1, a_2, b_1, b_2 \in A$. If operation $\oplus$ and equivalence relation R satisfy the following condition

$$a_1 R a_2,\ b_1 R b_2 \quad \Rightarrow \quad (a_1 \oplus b_1) R (a_2 \oplus b_2) \tag{1.6}$$

then we say that R is congruent modulo $\oplus$. This is demonstrated by Fig. 1.4 the left plot. From Fig. 1.4 the left plot, it can be intuitively interpreted that

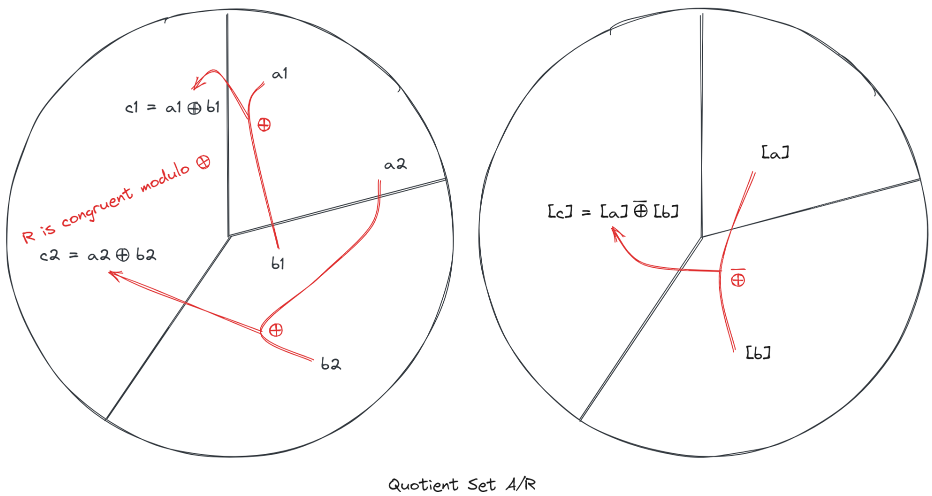

FIGURE 1.4
A relation is congruent modulo an operation.

when two elements a_1, b_1 are equivalent, their equivalence relation persists even if operation $\oplus a_2$, $\oplus b_2$ are applied to them respectively, so long as a_2, b_2 are also equivalent.

If R is congruent modulo $\oplus$ indeed, we can define an operation on the quotient set A/R as follows. Let $[\cdot]$ denote the equivalence class of an element in A. Define $\bar{\oplus}$ as an operation on A/R as follows.

$$[a]\bar{\oplus}[b] \quad = \quad [a \oplus b],\ a \in [a],\ b \in [b] \tag{1.7}$$

where a, b are arbitrarily selected elements in the equivalence class $[a]$ and $[b]$ respectively, as shown in Fig. 1.4 right plot. Notice that $[a \oplus b]$ should be well-defined regardless of the choice of a and b so long as they are selected in their associated equivalence class $[a]$ and $[b]$ respectively since R is congruent modulo $\oplus$. In this context, $\bar{\oplus}$ is known as the **included operation** or **quotient operation** of $\oplus$ on the quotient set A/R.

To conclude, in the algebraic system with non-empty set A and an operation $\oplus$ (denoted by $\{A; \oplus\}$), if there is a equivalent relation R which is congruent modulo $\oplus$, we can construct a new algebraic system $\{A/R; \bar{\oplus}\}$, where A/R is the quotient set of A on R from (1.5), and $\bar{\oplus}$ the included operation of $\oplus$ on A/R from (1.7).

1.3 Semi-Group and Group

In the previous section, general algebraic system is introduced. A general algebraic system shall contain a set of interest as well as one or more operation defined on that set. The operations can be unary (involving one operand), binary (involving two operands), ternary (involving three operands), etc. Relations within these systems are defined as sets of tuples, with each element of the tuple coming from the set of interest. Likewise, relation can also be binary, ternary, etc.

Special properties can apply to both operations and relations. Binary operations, for instance, can exhibit commutativity, associativity, and distributivity. Binary relations, on the other hand, can be reflexive, symmetric, and transitive. If a relation is simultaneously reflexive, symmetric and transitive, it is called a equivalent relation. Each equivalent relation is corresponded with a quotient set which is a partition of the original set by equivalence classes of the relation.

When a relation is congruent modulo an operation (recall (1.6) and Fig. 1.4), we can establish a new algebraic system. This system comprises the quotient set and a well-defined induced operation on that set. The new system retains structural properties from the original set, reflecting the consistency and compatibility of the congruence relation with the operation.

Moving forward, our focus will shift to specialized algebraic systems characterized by distinctive properties. This exploration will pave the way to understanding the fundamental algebraic structures such as semi-groups, groups, and rings. We will see the critical impact the operation possess over the algebraic system. Even with the same set, different operations often leads to very different features of the algebraic system.

1.3.1 Semi-Group

Let S be a non-empty set, and $\oplus : S \times S \to S$ a closed binary operation defined on S. If $\oplus$ has associative property, i.e. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$, then algebraic system $\{S; \oplus\}$ (for simplicity, S, when there is no ambiguity) is called a **semi-group**.

Examples of semi-group include $\{\mathbb{N}; +\}$, $\{\mathbb{N}; \times\}$ where $\mathbb{N}$ refers to the (positive) natural numbers $1, 2, 3, \ldots$. Let A be an non-empty set, and $\{\mathcal{M}(A); \circ\}$

is also a semi-group, where $\mathcal{M}(A)$ is the set of all the closed mappings defined on A, and $\circ$ the compound operation. Additionally, $\{\mathcal{P}(A); \bigcup\}$, $\{\mathcal{P}(A); \bigcap\}$ are also semi-groups, where $\mathcal{P}(A)$ represents the power set of A.

Is Zero Included in Natural Numbers?

The definition of natural numbers may or may not include zero "0" depending on the context. In the context of number theory and abstract algebra, natural numbers often exclude zero.

1.3.2 Monoid

Consider semi-group $\{S; \oplus\}$. If $\exists e \in S$ so that

$$e \oplus a \quad = \quad a, \ \forall a \in S$$

then e_1 is known as the **left identity**. Similarly, we can define **right identity**. Notice that a semi-group may have many distinct left and right identities.

If an element e is both left identity and right identity, it is called the **identity element**. If a semi-group has an identity element, the identity element must be unique. This can be easily illustrated using proof by contradiction as follows. Assume that e_1, e_2 are two distinct identity elements, thus

$$e_1 \oplus e_2 = e_1 \quad \text{and} \quad e_1 \oplus e_2 = e_2$$

indicating $e_1 = e_2$, which contradicts with the assumption.

A semi-group with the identity element is knows as a **monoid**. From the definition, we know that $\{\mathbb{N}; \times\}$, $\{\mathcal{M}(A); \circ\}$, $\{\mathcal{P}(A); \bigcup\}$ and $\{\mathcal{P}(A); \bigcap\}$ are all monoids, with their identity elements being 1, $f : A \to A, f(a) = a$, $\varnothing$ and A, respectively.

1.3.3 Group

Let $\{S; \oplus\}$ be a monoid with identity element e. If for $a \in S$, there is

$$a' \oplus a \quad = \quad e$$

then a' is called the left inverse of a. Likewise, right inverse can be defined. Notice that an element may have many left and right inverses.

If a' is both the left and the right inverse of a, then a' is known as the inverse of a. In this case, similar to the identity element, a' must be unique. The proof can be obtained similarly using proof by contradiction. The inverse of a is often denoted by a^{-1}.

If in a monoid $\{S; \oplus\}$, there is the inverse for all its elements, the monoid is called a group, usually denoted by $\{G; \oplus\}$, or simply G when without ambiguity.

The relationship of general algebraic system, semi-group, monoid and group are demonstrated in Fig. 1.5.

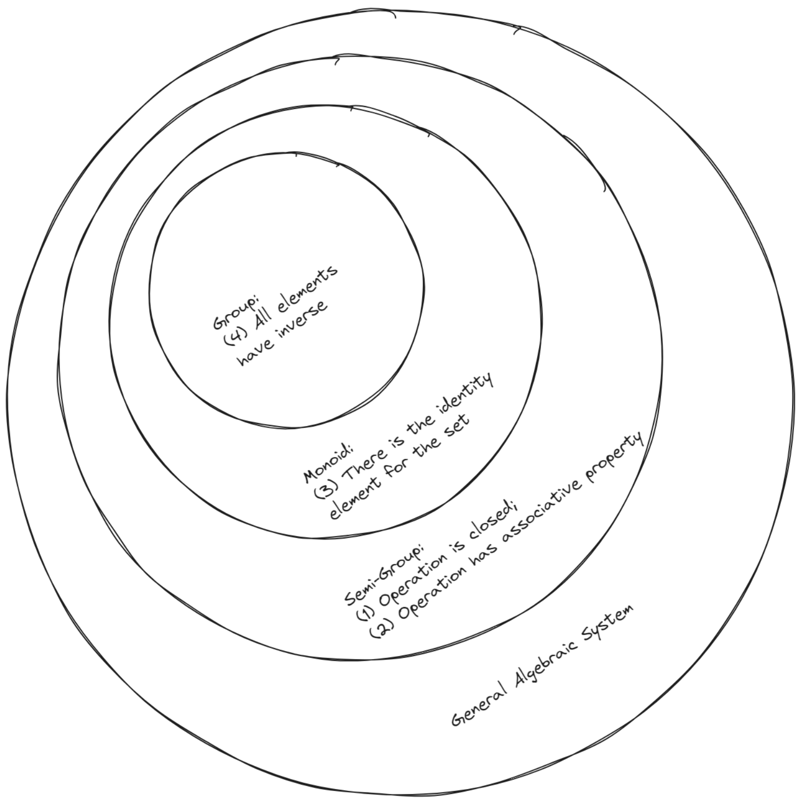

FIGURE 1.5
General Algebraic System, Semi-Group, Monoid and Group.

Notice that group does not pre-assume commutativity. If a group's operation is commutative, it is called an **abelian group** named after Niels Henrik Abel. Examples of abelian group include $\{\mathbb{Z};+\}$, $\{\mathbb{R};+\}$, $\{\mathbb{C};+\}$ where $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ represent integer set, real number set and complex number set, respectively. Additionally, $\{\mathbb{R}^*;\times\}$, $\{\mathbb{R}^*;\times\}$ are also abelian groups, where $\mathbb{R}^*$, $\mathbb{C}^*$ denotes the corresponding sets excluding zero.

We know that $\{\mathcal{M}(A);\circ\}$ introduced earlier is not a group. This is because not all mappings defined on a set A necessarily have an inverse. However, if define $\{\mathcal{S}(A);\circ\}$ where $\mathcal{S}(A)$ represents the set of all bijections (invertible mappings) on A, $\{\mathcal{S}(A);\circ\}$ becomes a group. Notice that $\mathcal{S}(A)$ is not necessarily an abelian group.

To conclude, a group must meet the following requirement:

- There is a non-empty set G;

- There is a closed binary operation $\oplus : G \times G \to G$;
- The operation $\oplus$ has associative property, i.e. $\forall a, b, c \in G, (a \oplus b) \oplus c = a \oplus (b \oplus c)$;
- There is the identity element, i.e. $\exists e \in G$, $\forall a \in G, e \oplus a = a \oplus e = a$;
- There is the inverse for all elements, i.e., $\forall a \in G$, $\exists a^{-1}$, $a \oplus a^{-1} = a^{-1} \oplus a = e$;

Furthermore, if

- Operation $\oplus$ has commutative property, i.e. $\forall a, b \in G, a \oplus b = b \oplus a$;

the group is called an abelian group.

It can be proved that if a semi-group has left identity and all its elements have left inverse, the left identity must also be its right identity and all its elements must also have left reverse, thus making the semi-group a group. The proof is given below. Let e be the left identity of semi-group $\{S; \oplus\}$, while b be the left inverse of any arbitrary element $a \in S$. Let c be the left inverse of b.

$$\begin{aligned} a \oplus b &= e \oplus a \oplus b \\ &= c \oplus (b \oplus a) \oplus b \text{ (associativity)} \\ &= c \oplus (e \oplus b) \text{ (associativity)} \\ &= c \oplus b \\ &= e \end{aligned}$$

Therefore, b is also the right inverse of a. Furthermore,

$$\begin{aligned} a \oplus e &= (a \oplus b) \oplus a \text{ (associativity)} \\ &= e \oplus a \\ &= a \end{aligned}$$

Therefore, e is also the right identity. All the above derivations also apply when a semi-group has right identity and all its elements have right inverse.

1.3.4 Properties of Semi-group and Group

Commonly used properties and notations of semi-group and group are introduced in this section.

If S is a semi-group and $a, b \in S$, then the following criteria can be used to further determine that S is a group.

- For $\forall a, b \in S$, if both $ax = b$ and $xa = b$ have solution, then S is a group.
- If $|S| < \infty$ (cardinal number of S is finite), and $\forall a, b, c \in S$, $ac = bc \Rightarrow a = b$, $ca = cb \Rightarrow a = b$, then S is a group.

If G is a group and $a, b, c \in G$, then the following properties apply.

- $ac = bc \Rightarrow a = b$;
- $ca = cb \Rightarrow a = b$;
- $ax = b$ has the unique solution $x = a^{-1}b$; $xa = b$ has the unique solution $x = ba^{-1}$;

Given group $\{G; \oplus\}$ and $a \in G$. The following notations apply.

$$a^n \equiv \overbrace{a \oplus \cdots \oplus a}^{n} \tag{1.8}$$

$$a^0 \equiv e \tag{1.9}$$

$$a^{-n} \equiv \overbrace{a^{-1} \oplus \cdots \oplus a^{-1}}^{n} \tag{1.10}$$

where n is a positive integer, e the identity element of G and a^{-1} the inverse of a. With this notation, instead of (1.8), (1.9) and (1.10), the following properties apply.

- $a^m a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$

When studying abelian groups, "+" is most commonly used to represent the operation, and the following notations apply.

$$\begin{aligned} na &\equiv \overbrace{a + \cdots + a}^{n} \\ 0a &\equiv e \\ (-n)a &\equiv \overbrace{(-a) + \cdots + (-a)}^{n} \end{aligned} \tag{1.11}$$

where $-a$ is used to denote the inverse of a. In this case, the identity element e in (1.11) is often denoted by "0". It might be confusing since it is visually the same with the numerical number zero, but what it really represents is the identity element of that group, not necessarily numerical zero. When the group G is $\mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$, and the operation is indeed summation, the identity element is indeed numerical zero.

The idea of group goes beyond number theory and mathematics. Generally speaking, any system that can move from states to states with movements revertible can be described by a group or something similar. When a system shows symmetry, it can probably be described by a group.

1.3.5 Order of Elements in a Group

Let G be a group, e its identity element, and $a \in G$. If there exists a smallest positive integer n so that $a^n = e$, we say that the **order** of a is n. If no such n exists, the order of a is infinity. The identity element e is the only element that has an order of 1. For an element with order n, its inverse also has the order of n.

Let G be a group, e its identity element, and $a \in G$. Consider the sequence of a^n as follows.

$$\dots \quad a^{-3} \quad a^{-2} \quad a^{-1} \quad a^0(e) \quad a^1 \quad a^2 \quad a^3 \quad \dots$$

If a has the order of infinity, then $a^m \neq a^n$ for any integers $m \neq n$, and vise versa. This can be easily proved with proof by contradiction. If an element has the order of d, then $a^m = a^n$ repeats if and only if $m - n = kd, k \in \mathbb{Z}$.

If $a \in G$ has order d, then $a^k, k \neq 0$ has order $d/(d, |k|)$, where $(d, |k|)$ is the greatest common divisor of d and $|k|$. This implies that a^k has order no more than d, and it has order d if and only if $(d, |k|) = 1$.

If $a, b \in G$ has order m and n respectively, and $ab = ba$, then ab and ba have the order of $[m, n]$, where $[m, n]$ stands for the least common multiple of m and n.

1.4 Subgroup and Quotient Set

Subgroup and quotient set are both fundamental concepts in group theory. They not only form an important part of abstract algebra by themselves, but also help with better understanding group and its properties.

1.4.1 Subgroup

Let $\{G; \oplus\}$ be a group, and $H \subset G, H \neq \varnothing$ is a non-empty subset of the group. If $\{H; \oplus\}$ forms a group under the same operation $\oplus$, then H is called a **subgroup** of G, denoted by $H \leq G$. Notice that if $H \neq G$, H is called a **proper subgroup** of G and can be denoted by $H < G$. That implies that

- The operation $\oplus$ which is close in G is also close in H;
- The identity element of G, denoted by e, is in H;
- For every element $a \in H$, its inverse a^{-1} is also in H.

Here is an example of a subgroup. Consider group $\{\mathbb{R}^*; \cdot\}$ where $\mathbb{R}^*$ denotes real number set excluding zero, and $\cdot$ the multiplication operation. Then group $\{\mathbb{R}^+; \cdot\}$ where $\mathbb{R}^+$ denoting positive real number set is a subgroup of $\{\mathbb{R}^*; \cdot\}$.

The following criteria can be used to determine whether a subset is a subgroup under the operation. Let $\{G; \oplus\}$ be a group, and $H \subset G$ a non-empty subset. The following three statements are equivalent.

(i) $H \leq G$;

(ii) $\forall a, b \in H,\ a \oplus b \in H,\ a^{-1} \in H$;

(iii) $\forall a, b \in H,\ a \oplus b^{-1} \in H$.

Furthermore, if $|H| < \infty$, the following two statements are equivalent.

(i) $H \leq G$;

(ii) $\forall a, b \in H,\ a \oplus b \in H$.

The proof is neglected in this notebook.

Subgroup has the following properties.

- If $H_1 < G$, $H_2 < G$, $H_1 \bigcap H_2 \neq \varnothing$, then $H_1 \bigcap H_2 < G$;
- If $H_1 < G$, $H_2 < G$, then $H_1 \bigcup H_2$ is not necessarily a subgroup of G.

1.4.2 Coset

Let $\{G; \oplus\}$ be a group, $H < G$ a subgroup, and $a \in G$. Define **left coset** of H about a, aH, as follows.

$$aH = \{a \oplus h | h \in H\}$$

Similarly, the **right coset** Ha can be defined.

Let $\{G; \oplus\}$ be a group, $a, b \in G$ and $H < G$. Define the following relation

$$aRb = \left\{(a, b) \middle| a^{-1} \oplus b \in H\right\} \tag{1.12}$$

It can be proved that the above relation is a equivalence relation. The equivalence class of a is nothing but aH. This theorem associate a subgroup H with a equivalence relation (1.12).

Part III

Number Theory

Bibliography

[1] Nathan Jacobson. *Basic algebra I and II*. Courier Corporation, 2012.