1. The Alphabet

1.1 Sets

1.1.1 The Third Mathematical Crisis

Before communicating freely in any language, we first need to understand the words of that language. Even before this, we need to know the building blocks of words, the alphabet. For the mathematical language, we will first understand what the concept of *alphabet* means. For different purposes in math, we define different alphabets, hence different mathematical structures arise from these alphabets. The basic concept of alphabet is called **sets**.

> **Definition 1.1.1 — Sets.** A **set** is a collection of objects. We call an object x *"an element of a set S"* if x is contained in S, denoted $x \in S$.

■ **Example 1.1 — Examples of Sets.** ■

- $S = \{1,2,3\}$ is a **finite** set since S only has finite number (3) items.
- $S = \{\dots,-2,-1,0,1,2,\dots\}$ is an **infinite** set (often denoted as $\mathbb{Z}$, the integers).
- $S = \{$MAT157, MAT240, CSC148, CSC165$\}$ is a set of courses a typical student wishing to study math and CS would take at U of T.
- $S = \{a,b,c,d,\dots,z\}$ is a set of letters used in English, which is exactly the alphabet of English.

R Here, objects do not necessarily refer to mathematical objects, in fact it can be *anything*. A *set* is also an object itself.

> **Definition 1.1.2** The number of elements in a set S is called its **cardinality**, denoted $\#S$ or $|S|$.

■ **Example 1.2 — Cardinality.** ■

The examples in example 1.1 has cardinality $3, \infty, 4, 26$ respectively. We call a set S **finite** if $\$S$ is finite, and otherwise we call S to be **infinite**.

The above definition of sets gives rise to the following question: is the collection of all sets a set or not a set? Both answers will lead to a contradiction. This is known as the *Russel's paradox* and *the third mathematical crisis*. To address this problem, various set theories were proposed, the most famous one being what is known as the *"axiom of choice"*. However, we will now go into further details about these philosophical analysis on mathematics. We will focus more on the understanding of the math language.

1.1.2 Subsets

In fact, the mathematical language is much more general than any language we speak, for example English. One of the main reason is that we can extend or narrow our alphabet used while still having meaningful conversations, which is not possible for English (imagine using only a, b, c for daily lives). Narrowing down a set gives rise to the definition of subsets and intersection of sets. Extending a set gives rise to the definition of union of sets.

Definition 1.1.3 The sub-collection of objects (let us denote it C) in a set S is called a **subset** of S, denoted $C \subset S$.

Example 1.3 — Examples of subsets.

- $C = \{1\}$, $D = \{2,3\}$ are both subsets of $S = \{1,2,3\}$.
- We denote the empty collection of objects $\emptyset$. This is a subset of any set S.
- A proper subset C of a given set S is a subset $C \subset S$ with extra constraint that C and S are not the same collection. This can be emphasized using notation $C \subsetneq S$.

Definition 1.1.4 Given two sets A and B, we call the intersection of A and B another set $C : \{x : x \in A \text{ and } x \in B\}$, denoted $C = A \cap B$.

Example 1.4 — Set intersection.

- Let $S = \{1,2,3\}$, $T = \{1,3,5\}$, then $S \cap T = \{1,3\}$.
- Let $S = \{1,2,3\}$, $T = \{4\}$, then $S \cap T = \emptyset$. If two sets have empty intersection, we call them **disjoint** sets.
- From the definition of subsets, we can see that if $A \subset B$, $A \cap B = A$.

On the contrary of narrowing down to common elements of two sets which is the intersection described above, we have another operation on sets called the union of sets, which extends two sets to a set containing all appearing elements in them.

Definition 1.1.5 Given sets A, B, we define the union of A and B to be the set $C = \{x : x \in A \text{ or } x \in B\}$. We denote $C = A \cup B$.

Example 1.5 — Set union.

- Let $S = \{1,2,3\}$, $T = \{1,3,5\}$, then $S \cup T = \{1,2,3,5\}$.
- From the definition of subsets, we can see that if $A \subset B$, $A \cup B = B$.

There is sometimes another operation on sets that we care about, which involves dealing with what elements are not in a particular subset.

Definition 1.1.6 Given set A and set $S \subset A$, the complement of S in A, denoted S^c or $A \setminus S$ is the set $T = \{x : x \in A \text{ and } x \notin S\}$.

With the concept of subsets, intersection, union and complements defined, we can prove interesting properties on sets. In fact, there is an area of mathematics called *set theory*, and an introductory course to this is MAT409.
Different mathematical structures you will encounter often uses different alphabets, discussing relationships between these alphabets also allows us to discuss relationships between these mathematical structures.

1.1.3 Operations and Closedness

Beauty of mathematics begins to appear when we discuss how to combine letters in the alphabet to produce "words". The ways of combining letters to get words is known as **operations**.
An important difference between the mathematical language and natural language is that in some mathematical structures, combining letters in the alphabet using a defined operation can only give rise to other letters in the alphabet and *nothing outside* of this alphabet. In this case, this mathematical structure is said to be "closed" under the defined operation. We now will define *closedness* formally. This allows us to understand the mathematical language we would like to use in analysis later on. We will begin by defining the concept of operation.

Definition 1.1.7 An **operation** on a set S is an assignment of a unique element $s \in S$ to a fixed number of elements in S.

■ Example 1.6 — Operations. ■

- By definition, the addition "+" and multiplication "·" defined on $\mathbb{R}$ is an operation that assigns a unique number $x \in \mathbb{R}$ given 2 elements $a, b \in \mathbb{R}$, denoted $x = a + b$ or $x = a \cdot b$, respectively.
- It is also an operation to assign any unique element $x \in S$ given the whole set of elements in S.

Definition 1.1.8 Given an operation $\cdot$ defined on a set S, a subset $A \subset S$ is said to be **closed** under this operation if for all $x, y \in A$, $x \cdot y \in A$.

R By definition of closedness and operation, we know that given an operation $\cdot$ defined on S, S is automatically closed under this operation.

■ Example 1.7 — Operation and Closedness. ■

- Using the normal definition of addition as the operation, integers $\mathbb{Z}$, rationals $\mathbb{Q}$ and real numbers $\mathbb{R}$ are all closed under this operation.
- With the normal definition of multiplication as the operation, integers $\mathbb{Z}$, rationals $\mathbb{Q}$ and real numbers $\mathbb{R}$ are also closed under this operation.
- With the normal definition of division, rationals $\mathbb{Q}$ and real numbers $\mathbb{R}$ are still closed under this operation. However, $\mathbb{Z}$ is not closed under division since $\frac{1}{2} \notin \mathbb{Z}$.

R In the above example, "normal" just mean that addition and multiplication are defined as what we always know, $1 + 2 = 3, 3 \cdot 2 = 6$ and so on.

1.2 Mathematical Structures

Most mathematical structures that we are ever interested in are sets closed under one or more kind of operations. Additional properties give rise to various mathematical structures we care about. The concept of mathematical structures lies in the area of *abstract algebra*, and the details will be covered in MAT347Y1.
As of now, it is important to understand the very basics of these structures as our primary interest, the real numbers $\mathbb{R}$, is assumed to be a member of an important type of mathematical structure.

1.2.1 Groups

Definition 1.2.1 A **magma** (binar, groupoid) $(M,\star)$ is a set M that is closed under operation $\star$ with no additional property assumptions.

■ Example 1.8 — Magma. ■

Since $\mathbb{R}$ is closed under addition and multiplication, we can define the operation $x\star y$ to be any combination of adding and multiplying x or y together and conclude that $\mathbb{R}$, together with the operation $\star$ is a magma, for example $x\star y = x^6y + x^3y^3$, then $(\mathbb{R},\star)$ in this case is a magma.

Definition 1.2.2 A **semigroup** $(M,\star)$ is a magma M that satisfies associative law: $a\star(b\star c) = (a\star b)\star c$, for all $a,b,c\in M$.

■ Example 1.9 — Semigroup. ■

The set $\{0,1\}$ can be equipped with operation "AND", "OR" and result in two semigroups. We define a AND $b = 1$ only when $a = b = 1$, and a AND $b = 0$ otherwise. We define a OR $b = 1$ when either a or b is 1, and a OR $b = 0$ otherwise, for all $a,b\in\{0,1\}$. An exercise is to try to verify that this is associative.

Definition 1.2.3 A **monoid** $(M,\star)$ is a semigroup M with an identity $e\in M$ such that for all $a\in M$, $a\star e = e\star a = a$.

■ Example 1.10 — Monoid. ■

The first example is a "flip-flop" monoid, which is the set $\{a,b,c\}$ where a represents operation "SET", b represents operation "RESET" and c represents operation "DO NOTHING". We know that $a\star b = c$, $a\star c = a$, $b\star c = b$, thus the identity element is c. An exercise is to try to verify that the "flip-flop" monoid is associative.

With grounds layed, we can talk about one of the most important algebraic structures - groups.

Definition 1.2.4 A **group** $(M,\star)$ is a monoid M with an additional operation *inv* on M, where we denote $inv(g) = g^{-1}\in M$ for all $g\in M$. This operation satisfies that $g\star g^{-1} = g^{-1}\star g = e$. If for all $a,b\in M$, we also have $a\star b = b\star a$, we call the group to be **abelian**.

■ Example 1.11 — groups. ■

- We call the Hamiltonian Quarternions $\mathbb{H} = \{\pm 1,\pm i,\pm j,\pm k\}$ to be the set of 8 elements with operation $\cdot$, where $1^2 = 1 = (-1)^2$, $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$ and

$ik = j = -ki$. You can check that it is indeed a group (it satisfies associative laws, has identity and inversion operation).
- We call Klein four group $\mathbb{K} = \{1, a, b, c\}$ to be the set of 4 elements with operation $\cdot$, where 1 is the identity and $a \cdot b = c = b \cdot a$, $b \cdot c = a = c \cdot b$, $a \cdot c = b = c \cdot a$. This is an example of an *abelian group*.

R It is easy to see once the inverse of an element $m \in M$ exists, then it is unique. Suppose m has two inverses m_1, m_2, then we know that $m \star m_1 = m \star m_2 = e$, hence $(m_1 \star m) \star m_1 = (m_1 \star m) \star m_2$, and we conclude $m_1 = m_2$. Therefore, the inverse is **unique** if it exists.

1.2.2 Fields and $\mathbb{R}$

Definition 1.2.5 A **ring** is an abelian group $(M, \star)$ equipped with another operation $\cdot$ different from $\star$, such that M is closed under $\cdot$ and associativity holds for $\cdot$. A ring is **commutative** if M is commutative under $\cdot$, i.e., for all $a, b \in M$, $a \cdot b = b \cdot a$.

R Note that the identity for $\cdot$ may be different from the identity for $\star$. Notation wise, we often define the inverse of $a \in M$ under $\star$ to be $-a$ and inverse of a under $\cdot$ to be a^{-1}.

■ **Example 1.12 — Rings.** ■

The integers $\mathbb{Z}$ is a classic example of a ring. It is easy to check that $(\mathbb{Z}, +)$ is an abelian group, and $(\mathbb{Z}, \cdot)$ is associative.

In fact the reason why $\mathbb{Z}$ is a ring is purely by definition (assumption). This assumption comes from a broader assumption about $\mathbb{R}$. Before we go into this assumption about the "words" which is also our alphabet for the rest of the notes, we need to understand the concept of *fields*.

Definition 1.2.6 A **field** is a commutative ring $(M, \star, \cdot)$ with an inversion operation defined on $\mathbb{F} \setminus \{e\}$ for $\cdot$, where e is the identity for operation $\star$.

It is important to note that up to this point, we know that field $\mathbb{F}$ with operations $\star, \cdot$ and identities e, e' respectively has the following properties. For all $a, b, c \in \mathbb{F}$, $a \neq e$:
- **Associative Law for $\star$:** $a \star (b \star c) = (a \star b) \star c$.
- **Existence of identity for $\star$:** $a \star e = e \star a = a$.
- **Existence of inverse for $\star$:** $a \star (-a) = e = (-a) \star a$.
- **Commutativity for $\star$:** $a \star b = b \star a$.
- **Associative Law for $\cdot$:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- **Existence of identity for $\cdot$:** $a \cdot e' = e' \cdot a = a$.
- **Existence of inverse for $\cdot$:** $a \cdot a^{-1} = e' = a^{-1} \cdot a$.
- **Commutativity for $\cdot$:** $a \cdot b = b \cdot a$.

R We sometimes denote e by 0, and e' by 1.

The above 8 properties are also called **field axioms**. Now, we are finally able to understand the "words" of our mathematical language which is the real numbers $\mathbb{R}$. We begin by making assumptions on our words $\mathbb{R}$ as follows:

Theorem 1.2.1 $\mathbb{R}$ with operations addition $(+)$ and multiplication $(\cdot)$ is a field.

This is the end of this chapter, but the starting point of everything that follows. We assumed that our alphabet is also our words $\mathbb{R}$ and we equipped lots of interesting field axioms on $\mathbb{R}$. Just as the English words, we have nouns, verbs and different type of nouns, etc.. We will talk about different types of words in $\mathbb{R}$, including $\mathbb{Q}, \mathbb{Z}$, and $\mathbb{N}$ in the next chapter. We will also talk about logics and proofs that somewhat defines the "grammar" of the math language.