§0.1 Sets and Relations

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

Prelude; I look at Algebra as the mathematical formalism. The traditional thinking that Algebra without geometric motivation may not be worth doing, may have to be reevaluated. Over last half a century, things have changed. In my view, without formalism it would be tough to create any good mathematics (in particular Geometry). The core of the main stream mathematics research frontier, of the current time, cannot be reached without formalism. My motto: Do Algebra without Apology.

Abstract: We talk about axiomatic of set theory. Then we define Relations.

1 Sets

§1.The premitive mathematical concept

1. In mathematics, the most premitive objects that we work with are **sets**. In fact, any object that we work with is a set.

2. Given a set S, each of its element x is also a set.

3. The familiar objects that we work with are sets. For example,

   (a) Each number is a set.

   (b) The integer 0 is a set. It is the empty set ϕ.
   Likewise, "1" is the set $\{\phi\}$.

   (c) The integer 8 is a set. Like wise, any integer is a set. Any rational number $\frac{m}{n}$ or $\frac{171}{233}$ is a set.

   (d) The real number π is a set. Like wise, each real number x is a set.

   (e) Then, of course, the collection of all integers $\mathbb{Z}$ is a set. The collection of all rational numbers $\mathbb{Q}$ is a set. The collection of all real numbers $\mathbb{R}$ is a set. The collection of all complex numbers $\mathbb{C}$ is a set.

   (f) A function f is also a set.

Russell's Paradox

Various attempts to define sets, and work with them without any apparent restrictions, led to various paradoxes. Most well known among them is Russell's Paradox.

Russell's Paradox (1901): Let S be the collection of all objects that are not members of themselves. So,

$$S = \{x : x \notin x\}. \qquad \textit{Question:} \quad S \in S \textit{ or not?}$$

So, the question is whether S is a member of itself? Now,

1. If $S \in S$ then, by definition of S we have $S \notin S$.
2. Conversely, if $S \notin S$ then again by definition of S, we have $S \in S$.
3. In summary,
$$S \in S \qquad \Longleftrightarrow \qquad S \notin S.$$

§3 Axiomatic Set Theory

Because of such Paradoxes, mathematical community concluded that it is not possible to define sets. They concluded that it is best to work under a set of axioms, which we do not question.

Among several axiomatic set up, **Zermelo-Fraenkel set theory** is accepted as standard framework. Again, there are many equivalent formulation of the Zermelo-Fraenkel set theory. Many provides nine axioms. (Search internet for more). Out of those, our textbook lists a few axioms, which will suffice for this course.

§4 Four axioms from the textbook

1. A set is made up of elements, which are also sets. If a is an element of S then we write $a \in S$.
2. (**Empty Set**:) There is exactly one set with no element. It is called the **empty set** or the **null set**. It is denoted by ϕ.
3. (**Specification**:) Suppose S is a set. Let $P(x)$ is a characteristic of the elements $x \in S$. Then
$$T = \{x \in S | P(x) \ is \ true\} \quad is \ a \quad set.$$
For example, for interger $x \in \mathbb{Z}$, let $P(x)$ be the statement that "x is an even integer". The
$$E = \{x \in \mathbb{Z} | P(x) \ is \ true\} \quad is \ a \quad set.$$
describes the the "set" of even integers. Assuming that $\mathbb{Z}$ is a set (*which we did not establish*), it follows from this axiom that E is a set.

4. (**Well definedness**): Suppose S is a set and a is an object (set), then

$$\textit{either} \quad a \in S \quad \textit{or} \quad a \notin S \quad \textit{not both.}$$

Remark. We will not get lost in set theory. We take a lot of things for granted, that we always did. For exmple, we will not prove all the stements we made at the beginning. We will not prove, each integer is a set, or π is a set or $\mathbb{Z}, \mathbb{R}$ are sets. We will take them for granted.

Other than that, we will need to define every object we work with. We will need to provide proofs of any statement that proclaims something, which will be called lemmas and theorems etc.

What is a Definition? A definition describes a class of objects fully and precisely. It is an if and only if type of statement.

1.1 Subsets, union etc.

Definition 1.1 *A set B is said to be a* **subset of a set** *A, written as $B \subseteq A$, if every element of B is also an element of A. Notationally,*

$$B \subseteq A \Longleftrightarrow [x \in B \Longrightarrow x \in A].$$

We say that B is a **proper subset of** *A, if $B \subseteq A$ and $B \neq A$.*

Exercise. Let A be a set. Give two trivial examples of subsets of A.

Definition 1.2 *Suppose A, B are two sets. The* **Cartesian product** *of $A \times B$ is defined as*

$$A \times B = \{(x, y) : x \in A, y \in B\}.$$

Exercise. Describe $A \times \phi$.

Question. Is $A \times B = B \times A$?

Example. Geometric realization of the Cartesian product $\mathbb{R} \times \mathbb{R}$ is the Euclidean plane.

Notations. As usual $\mathbb{Z}$ will denote the set of all integers. $\mathbb{Q}$ will denote the set of all rational numbers. $\mathbb{R}$ will denote the set of all real numbers. $\mathbb{C}$ will denote the set of all complex numbers. Clearly,

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Before we proceed, we define intersection, union etc.

Definition 1.3 Let X_i be a collection of sets, indexed by a set $i \in I$. Also let X, Y be two sets.

1. Define union
$$\bigcup_{i \in I} X_i = \{x : x \in X_i \quad for \ some \quad i \in I\}.$$
So,
$$X \cup Y = \{x : x \in X \quad OR \quad x \in Y\}.$$

2. Define intersection
$$\bigcap_{i \in I} X_i = \{x : x \in X_i \quad \forall \quad i \in I\}.$$
So,
$$X \cap Y = \{x : x \in X \quad and \quad x \in Y\}.$$

3. We say that X_i are pairwise disjoint if no two have any common element. That means, if
$$X_i \cap X_j = \phi \qquad \forall \quad i, j \in I \quad and \quad i \neq j.$$
So, X, Y are mutually disjoint if $X \cap Y = \phi$.

2 Relations

Definition 2.1 A **relation** between the sets A and B is a subset $\mathcal{R}$ of $A \times B$. So,

$$\mathcal{R} \subseteq A \times B.$$

If $(x, y) \in \mathcal{R}$ we say x **is related to** y and write $x\mathcal{R}y$. When $\mathcal{R}$ is clear from the context, we also write $x \sim y$ to mean $x\mathcal{R}y$.

A relation between X and itself, will be called a **realtion on** X.

Example. Suppose A is a set. Then the equality " = " is a relation between A with itself. This is given by the subset

$$\Delta = \{(x, x) : x \in A\} \subseteq A \times A.$$

Example. Given any function f, its graph is a relation. For example, the graph of $f(x) = \sqrt{x}$ is given by the subset

$$\mathcal{G}(f) = \{(x, \sqrt{x}) : x \geq 0\} \subseteq \mathbb{R} \times \mathbb{R}.$$

So, the graph $\mathcal{G}(f)$ is a relation between $\mathbb{R}$ with itself.

2.1 §1 Functions

We redefine functions in the set theoretic context.

Definition 2.2 Let X and Y be two sets. By a function f from X to Y, we mean a relations f between X and Y (i.e. $f \subseteq X \times Y$) such that

$$\forall\ x \quad \textit{there is exactly one} \quad (x, y) \in f.$$

1. If f is such a function, we write "$f : X \longrightarrow Y$ is a function from X to Y".

2. We also write $y = f(x)$ to mean $(x, y) \in f$.

3. A function f is also called a **map** or **mapping**.

4. We say X is the **domain** of f and Y is the **codomain**. The range is define as $f(X) = \{f(x) : x \in X\}$.

Remark. *Note that the definition of a function $f : X \longrightarrow Y$ comes with its domain and codomain. In calculus courses, you ask the students to compute the domain. That would be the "baby way".*

Question. Consider the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 2^x$. Also consider the function $g : \mathbb{R} \longrightarrow \mathbb{R}^+$ defined by $g(x) = 2^x$ where $R^+ = [0, \infty)$. **Are these two functions same?**

Definition 2.3 Let $f : X \longrightarrow Y$ be a function. Then,

1. We say f is **one to one** (or **injective**), if

$$f(x_1) = f(x_2) \qquad \Longrightarrow \qquad x_1 = x_2.$$

2. We say f is **onto** (or **surjective**), if range $f(X) = Y$. That means,

$$\forall\, y \in Y \quad \exists\, x \in X \quad \ni \quad f(x) = y.$$

3. We say that f is **bijective**, if f is both injective and surjective.

Theorem 2.4 Suppose $f : X \longrightarrow Y$ is a function. Then, f is bijective if and only if there is a function $g : Y \longrightarrow X$ such that $gof = ID_X$ and $fog = ID_Y$. Such a g is unique. This function g is called the **inverse of** f and it is denoted by $g = f^{-1}$.

Proof. Suppose f is bijective. Define $g : Y \longrightarrow X$ as follows

$$\forall\, y \in Y, \quad define \quad g(y) = x \quad if \quad f(x) = y.$$

We can easily check, g is well defined and $gof = ID_X$ and $fog = ID_Y$.. As a subset of $Y \times X$, g is given by

$$g = \{(y, x) \in Y \times X : (x, y) \in X \times Y\}.$$

Conversely, suppose such a g exists. Then

$$f(x_1) = f(x_2) \Longrightarrow gof(x_1) = gof(x_2) \Longrightarrow x_1 = x_2.$$

So, f is one to one. Also, for $y \in Y$, we have $y = f(g(y))$. So, f is onto. ■

Notations 2.5 Let $f : X \longrightarrow Y$ be a function.

1. For a subset $A \subseteq X$ denote $f(A) = \{f(x) : x \in A\}$. So, $f(A) \subseteq Y$.

2. For a subset $B \subseteq Y$ denote $f^{-1}(B) = \{x : f(x) \in B\}$. So, $f^{-1}(B) \subseteq X$.

2.2 §2 Cardinality

The **cardinality** of a set X measures the size of X. It is denoted by $|X|$. When, X has only finitely many elements, $|X|$ is the number of elements in X.

Definition 2.6 Two sets X and Y are said to have **same cardinality**, if there is a bijection f from X to Y.

1. The cardinality of $\mathbb{Z}$ is denoted by $\aleph_0$ (read as "aleph-null"). Notationally, $|\mathbb{Z}| = \aleph_0$.

2. In fact, if X is countably infinite then $|X| = \aleph_0$.

3. It is easy to see that $|\mathbb{Z}^+| = \aleph_0$ and $|\mathbb{Q}| = \aleph_0$

4. A standard proof is given in the analysis classes that $\aleph_0 < |\mathbb{R}|$. This fact is stated as that "$\mathbb{R}$ is not countable".

3 Partitions and Equivalence Relations

Definition 3.1 A **partition** of a set S is a collection of nonempty subsets X_i of S such that every element is in exactly one of them. This means, if X_i are pairwise disjoint and $S = \bigcup X_i$. Each X_i is called a **cell**.

Example. $\mathbb{R}$ can be partitioned in to rationals $\mathbb{Q}$ and irrationals $\mathcal{I}$.

$\mathbb{R}$ can also be partitioned in to intervals $(n, n+1]$ with $n \in \mathbb{Z}$.

Definition 3.2 An **equivalence relation** $\mathcal{R}$ on a set S is a relation on S that satisfies the following three properties.

1. (Reflexive) $\forall\ x \in S \quad x\mathcal{R}x$.
2. (Symmetric) $\forall\ x, y \in S \quad (x\mathcal{R}y \implies y\mathcal{R}x)$.
3. (Transitive) $\forall\ x, y, z \in S \quad (x\mathcal{R}y \quad and \quad y\mathcal{R}z) \quad \implies x\mathcal{R}z$.

Examples

1. S be any nonempty set. The equality is an equivalence relation.
2. $\leq$ would not define an equivalence realtion on $\mathbb{R}$. Because it is not symmetric : $2 \leq 2.5$, but $2.5 \not\leq 2$.
3. (**Congruence Modulo** n**:**) Let n be a fixed positive integer. Define a relation $\equiv_n$ on $\mathbb{Z}$ as follows

$$\forall\ x, y \in \mathbb{Z} \quad define \quad x \equiv_n y \quad if \quad n|x - y.$$

This is an equivalence relation. It is called the **Congruence Modulo** n. (**Proof.** Exercise).

Theorem 3.3 Let S be a nonempty set and $\sim$ be an equivalence relation. For $a \in S$ define the **equivalence class of** a as

$$\bar{a} = \{x \in S : x \sim a\}.$$

Then,

1. $\forall\ a \in S \quad a \in \bar{a}$

2. For $a, b \in S$ we have

$$\bar{a} = \bar{b} \quad \Longleftrightarrow \quad a \sim b.$$

3. The equivelance classes $\{\bar{a} : a \in S\}$ gives rise to a partition of S.

Proof. By reflexive property $a \sim a$ and so $a \in \bar{a}$. So, (1) is proved.

To prove (2), first assume $\bar{a} = \bar{b}$. Since $a \in \bar{a}$ we have $a \in \bar{b}$. So, $b \sim a$. By symmetry $a \sim b$. So, $\Longrightarrow$ is established. To prove $\Longleftarrow$, assume $a \sim b$. Let $x \in \bar{a}$. So, $x \sim a$. By trasitivity, $x \sim b$. So, $x \in \bar{b}$. Therfore, $\bar{a} \subseteq \bar{b}$. Similarly, $\bar{b} \subseteq \bar{a}$. So, $\bar{a} = \bar{b}$. So, both implications of (2) are established.

Now (3) follows from (1) and (2). For $a \in S$ we have $a \in \bar{a}$. So, $S = \cup\{\bar{a} | a \in A\}$. By (2), the equivalence classes are pairwise disjoint. So, they form a partition of S. The proof is complete. ■

The converse of this theorem is also true, as follows.

Theorem 3.4 Let X be a set and $\{X_i : i \in I\}$ be a partition of X. Define a relation on X as follows:

$$\forall\ x, y \in X \quad define \quad x \sim y \quad if \quad \exists\ i \in I \quad \ni \quad x, y \in X_i.$$

Then, $\sim$ is an equivalence realtion on X. Also for $a \in X_i$ the equivalence class $\bar{a} = X_i$.

Proof. Obviosly, for any $x \in X$ we have $x \sim x$, because $x_i \in X_i$ for some $i \in I$. So, it is reflexive.

Now suppose $x \sim y$. Then there is an $i \in I$ such that $x, y \in X_i$. So, $y \sim x$. Reflexibilty is established.

For transitivity, let $x \sim y$ and $y \sim z$. Then, $x, y \in X_i$ and $y, z \in X_j$ for some $i, j \in I$. Since $y \in X_i \cap X_j$, it follows $i = j$. So, $x, z \in X_i$. So, the transitivity is established. So, $\sim$ is an equivalence relation.

It is also obvious, for $a \in X_i$ the equivalence class $\bar{a} = X_i$. The proof is complete. ■.

Summary: These two theorems say that giving an equivalence relation $\sim$ on X is same as giving a partition of X.

3.1 Example.

(**Congruence Modulo** n**:**) As before, let n be a fixed positive integer. Define a relation $\equiv_n$ on $\mathbb{Z}$ as follows

$$\forall\ x, y \in \mathbb{Z} \quad define \quad x \equiv_n y \quad if \quad n | x - y.$$

Then, $\equiv_n$ is an equivalence relation. This partitions $\mathbb{Z}$ into equivalence classes $\overline{a}$, where $a \in \mathbb{Z}$.

1. In fact, there are exactly n equivalence classes:

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}.$$

   Proof. Use division algorithm ■

2. Clearly

$$\overline{0} = \overline{n} = \overline{2n} = \overline{rn} \quad \forall\ r \in \mathbb{Z}.$$

   Similarly,

$$\overline{1} = \overline{1+n} = \overline{1+2n} = \overline{1+rn} \quad \forall\ r \in \mathbb{Z}.$$

   For any integer $0 \le k \le n-1$ we have

$$\overline{k} = \overline{k+n} = \overline{k+2n} = \overline{k+rn} \quad \forall\ r \in \mathbb{Z}.$$

3. The set of all $\equiv_n$ −equivalence classes is denoted by $\frac{\mathbb{Z}}{n\mathbb{Z}}$. So,

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

The textbook defines

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}.$$

There is a bijection

$$\mathbb{Z}_n \xrightarrow{\sim} \frac{\mathbb{Z}}{n\mathbb{Z}} \quad \textit{sending} \quad r \mapsto \overline{r}.$$

I will identify these two sets via this bijection.

Exercise. On $\mathbb{Z}_n$ define addition and multiplication

$$\overline{a} + \overline{b} := \overline{a+b}$$

and

$$\overline{a} * \overline{b} := \overline{ab}$$

Prove that this addition and multiplication are well defined. Also prove that they satisfy "all" the properties of addition and multiplication. Research, which properties may not be satisfied, if any.

4 Partially Ordered Sets and Zorns Lemma

Definition 4.1 *Let S be a set and "$\leq$" be a relation. We say $(S, \leq)$ (or simply S) is a* **Partially Ordered set***,* if for all $a, b, c \in S$ the following holds:

1. (**Reflexive**): We have
$$a \leq a.$$
2. (**Anti-Symmetric**):
$$(a \leq b \quad and \quad b \leq a) \qquad \Longrightarrow \qquad a = b.$$
3. (**Trnasitive**):
$$(a \leq b \quad and \quad b \leq c) \qquad \Longrightarrow \qquad a \leq c.$$

In addition to the four axioms of set theory, the following is another axiom of set theorey (although it is called a "Lemma").

Definition 4.2 (Zorn's Lemma) *Suppose $(S, \leq)$ is a partially ordered set. Suppose that every chain in S has an upper bound in S. Then S has a maximal element $m \in S$.*

This means $\forall a \in S$ either $a \leq m$ or a is not related to m.

Remark. Zorn's lemma is called a "lemma" because it is equivalent to "Axiom of choice".

5 Categories

Definition 5.1 A **Category** $\mathcal{C}$ consisists of the following

1. It has a class of objects $\mathcal{C}$ of objectes.

2. For each pair of objects X, Y there is a sets $Hom(X, Y)$. We assume that these sets $Hom(X, Y)$ are disjoint. Elemnets $f \in Hom(X, Y)$ are called **morphisms** from X to Y, written as $X \longrightarrow Y$.

3. Given objects X, Y, Z, there is a function

$$Hom(X, Y) \times Hom(X, Y) \longrightarrow Hom(X, Z)) \qquad (g, f) \mapsto gof$$

   gof is called the **composition**. The composition satisfy the follwoing:

   (a) (**Associativity**) If $f : X \longrightarrow Y, g : Y \longrightarrow Z, h : X \longrightarrow W$ are morphisms then

$$ho(gof) = (hog)of.$$

   (b) (**Identity**): For each object X there exists a morphisms $1_X : X \longrightarrow X$ such that

$$\forall f : A \longrightarrow X,\ g : X \longrightarrow B \quad 1_B of = f, \quad go1_B = g.$$

Example 5.2 *1. The class $\mathcal{S}$ of all sets and the set maps is a category.*

2. The class $\mathcal{V}(\mathbb{R})$ of all vector spaces over $\mathbb{R}$ and linear transformations.

3. The class $\mathcal{G}$ of all groups and group homomorphisms.

4. The class $\mathcal{T}$ of all topological spaces and continuous maps.

5. The class $\mathcal{U}$ of all subsets of Euclidean spaces $\mathbb{R}^n$ and continuous maps.

Definition 5.3 Let $\mathcal{C}, \mathcal{D}$ be two categories. A **contravarient functor** T from $\mathcal{C}$ to $\mathcal{D}$ (denoted by $T : \mathcal{C} \longrightarrow \mathcal{D}$) consists of the follwoing:

1. To each object A of $\mathcal{C}$ it associtates an object $T(A)$ in $\mathcal{D}$. We write $A \mapsto T(A)$.

2. To each mosphism $f : A \longrightarrow B$ of $\mathcal{C}$ it associtates an morphisms $T(f) : T(A) \longrightarrow T(B)$ in $\mathcal{D}$. such that

   (a) $T(1_A) = 1_{T(A)}$ for all objects A of $\mathcal{C}$.

   (b) $T(gof) = T(g)oT(f)$ whenever the composition gof is defined for two morphisms f, g of $\mathcal{C}$.