0 Sets and Relations

The plan for this course is that I will be teaching for the first 5 weeks and your main instructor will take over on week 6. Each day we will see one or two sections of the textbook (Fraleigh, 7th Edition).

This introductory course has many definitions. We need these definitions to be able to communicate with each other efficiently. Obviously there is not enough class time to cover every definition in the book. Furthermore, the definitions are already there. Therefore, you need to read your textbook.

A note on definitions: It is customary to write a definition by using the conditional "if." However, every definition is an equivalence statement, saying something is equivalent to something else. That is, every definition is really an "if and only if" statement, which we may denote by the symbol $\iff$.

There are concepts that we do not define and accept them as being understood universally. One such item is the idea of a set as a collection of objects. Each set has elements, except for the empty set that has no element.

It is customary to use uppercase letters for sets. We may denote a set by listing its elements between curly braces.

Example 1. *$S = \{0, 1, 7\}$ and $A = \{x \mid x = 2k, k \in \mathbb{Z}\}$. Here, the set A is defined using a characteristic of its elements. The vertical line $\mid$ is read as "such that." The symbol $\in$ means "in" or "is a member of." The set $\mathbb{Z}$ is one of special sets with its own name, the set of integers:*

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

There are other special sets that have their own names, such as:

$$\begin{aligned} \mathbb{Z}^+ &= \{1, 2, 3, \ldots\} \\ \mathbb{R} &= \textit{set of real numbers} \\ \mathbb{Q} &= \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\} \\ \mathbb{C} &= \{a + bi \mid a, b \in \mathbb{R}\} \end{aligned}$$

The letter i is reserved for the imaginary unit. Mathematicians invented this number to have a solution for the equation $x^2 = -1$. Thus $i^2 = -1$. The set $\mathbb{C}$ is the set of complex numbers.

We say a set B is a **subset** of a set A if every element of B is also an element of A and we write $B \subseteq A$. If there are elements in A that are not in B, then we write $B \subset A$.

The **Cartesian product** of sets A and B is a set:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

We define a **relation** from a set A to a set B as a subset of $A \times B$. If (a, b) is in the relation $\mathcal{R}$, then we write $a\mathcal{R}b$.

A function is a special relation from a set called domain to a set called codomain such that each element of domain is related to only one element of codomain. A function is also called a mapping or a map, and we say a function maps the elements of domain to the elements of the range, where range is a subset of codomain.

Example 2. *Let $A = \{1, 2, 3\}$ and $B = \{2, 4, 6\}$. For each relation between A and B below, decide whether it is a function mapping A into B. If it is a function, decide whether it is 1-1 and whether it is onto B.*

a) $\{(1, 4), (2, 6), (3, 4)\}$

b) $\{(1, 6), (1, 2), (1, 4)\}$

c) $\{(2, 2), (1, 6), (3, 4)\}$

The number of elements in a set is called the **cardinality** of that set. The cardinality of infinite sets is more complicated than the cardinality of finite sets.

The cardinality of countable infinite sets is denoted by the symbol $\aleph_0$. The notation for cardinality is the same as the notation for absolute value. Thus:

$$|\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{Z}^+|$$

because we may have a one-to-one (1-1) correspondence between elmeents of one set and the elements of the other set. In other words, we may math each element from one set to an element from the other set. We may prove that $\mathbb{R}$ is uncountable, that is, $|\mathbb{R}| > |\mathbb{Z}|$. We denote $|\mathbb{R}| = \mathfrak{c}$.

When a relation $\mathcal{R}$ is from a set S to the same set S, we say $\mathcal{R}$ is a relation *on* S.

An **equivalence relation** $\mathcal{R}$ on a set S has three properties; for all $x, y, z \in S$:

1. $x \mathcal{R} x$ (reflexive)
2. $x \mathcal{R} y \Rightarrow y \mathcal{R} x$ (symmetric)
3. $x \mathcal{R} y$ and $y \mathcal{R} z \Longrightarrow x \mathcal{R} z$ (transitive)

A **partition** of a set S is a collection of nonempty subsets of S such that every elemlent of S is in exactly one of the subsets. Thus the union of all partition subsets is S and the subsets are pairwise disjoint. An equivalence relation on S partitions S.

Theorem (Equivalence Relations and Partitions)**.** *Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\sim$ partitions S, where*

$$\bar{a} = \{x \in S \mid x \sim a\}$$

is the equivalence class of the element a for each a. Also, each partition of S gives an equivalence relation $\sim$ on S where $a \sim b$ if and only if a and b are in the same equivalence class of the partition.

Often times we want to prove two sets A and B are equal. To do so, a prevalent technique is to show that $A \subseteq B$ and $B \subseteq A$. Then it must be that $A = B$. This is similar to show that two numbers a and b are equal: show that $a \leq b$ and $b \leq a$. Then it must be the case that $a = b$. We use the above technique to prove part of the Equivalence Relations and Partitions Theorem.

Proof. We want to show (abbreviated as WTS) that different equivalence classes $\bar{a}$ for $a \in S$ give a partition of S, so that every element of S is in some equivalence class, and if $a \in \bar{b}$, then $\bar{a} = \bar{b}$.

Let a be an arbitrary element of S. By reflexive property of equivalence relations, $a \in \bar{a}$. So a is in at least one equivalence class.

Now suppose $a \in \bar{b}$. WTS $\bar{a} = \bar{b}$.

$\bar{a} \subseteq \bar{b}$:

Let x be an arbitrary element of $\bar{a}$. WTS $x \in \bar{b}$.

$x \in \bar{a}$, therefore $x \sim a$. $a \in \bar{b}$, so $a \sim b$. By transitive property of equivalence relations, $x \sim b$, that is, $x \in \bar{b}$. Thus $\bar{a} \subseteq \bar{b}$.

$\bar{b} \subseteq \bar{a}$:

Let y be an arbitrary element of $\bar{b}$. WTS $y \in \bar{a}$.

$y \in \bar{b}$, therefore $y \sim b$. Since $a \in \bar{b}$, $a \sim b$ and by symmetry property, $b \sim a$. Since $y \sim b$ and $b \sim a$, by transitive property, $y \sim a$. Thus $y \in \bar{a}$. Therefore $\bar{b} \subseteq \bar{a}$.

$\bar{a} \subseteq \bar{b}$ and $\bar{b} \subseteq \bar{a}$ implies $\bar{a} = \bar{b}$. □

Example 3. *Suppose $n\mathcal{R}m$ in $\mathbb{Z}^+$ if n and m have the same final digit in the usual base ten notation. Is this relation an equivalence relation? If so, describe the partition arising from it.*

Example 4. ***Congruence modulo*** *n, where $n \in \mathbb{Z}^+$, is an equivalence relation on $\mathbb{Z}^+$, where each whole number belongs to a partition with the remainder after division by n. For example, 6 and 1 both belong to the same "bin" modulo 5. We write* $6 \equiv 1 \pmod 5$ *(read "6 is congruent to 1, modulo 5").*

1 Introduction and Examples

In abstract algebra, we are interested in *structural properties*. Sometimes two different sets with different binary operations turn out to have the same algebraic structure. To demonstrate this idea, consider the complex numbers.

We have seen how the points on a number line correspond to real numbers. Similarly, points on a plane correspond to complex numbers, with the vertical axis used for the imaginary axis, with points such as $i, 2i, -i$, and so on. Thus we may write a complex number in Cartesian form as $z = a + bi$, where $a, b \in \mathbb{R}$ and $i^2 = -1$. Equivalently, we may write a complex number in polar form, as $z = |z|e^{i\theta}$, where $|z| = \sqrt{a^2 + b^2}$ and $\tan\theta = \frac{b}{a}$. This is because of Euler's Formula:

$$e^{i\theta} = \cos\theta + i\sin\theta$$

While addition of complex numbers is easier in Cartesian form:

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2),$$

multiplication is easier in polar form:

$$|z_1|e^{i\theta_1} \cdot |z_2|e^{i\theta_2} = |z_1||z_2|e^{i(\theta_1+\theta_2)}$$

Example 5. *Calculate* $(8 + 2i)(3 - i)$.

Example 6. *Find all solutions of* $z^3 = -8$ *in* $\mathbb{C}$.

Now consider the unit circle: the circle with radius 1 (unit) centered at origin. All complex numbers on the circumference of the circle have magnitude 1. Thus their product results in another complex number with magnitude 1, that is, the unit circle is *closed* under multiplication. On unit circle, *multiplication* of complex numbers is equivalent to *addition* of their angles. We have a 1-1 correspondence, called an *isomorphism*:

$$(z_1 \leftrightarrow \theta_1 \text{ and } z_2 \leftrightarrow \theta_2) \Longrightarrow z_1 \cdot z_2 \leftrightarrow \theta_1 + \theta_2$$

Example 7 (Roots of Unity)**.** *The elements of* $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ *are called the* n^{th} *roots of unity:*

$$\zeta^k = \cos\left(\frac{2\pi}{n}k\right) + i\sin\left(\frac{2\pi}{n}k\right), \quad k = 0, 1, 2, \ldots, n-1$$

U_n is isomorphic to $\mathbb{Z}_n$.

For example, with $n = 8$, $\zeta^4 \cdot \zeta^6 = \zeta^{10} = \zeta^2$. This is the same structure in modular arithmetic with $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Addition modulo 8 is closed on $\mathbb{Z}_8$ and multiplication is closed on U_8.

Example 8. *Find all solutions $x \in \mathbb{Z}_7$ of*

$$x +_7 x +_7 x = 5$$