0 Logical Background

0.1 Sets

In this course we will use the term *set* to simply mean a collection of things which have a common property such as the totality of positive integers or the collection of points on a plane curve where the slope does not make sense. In truth the concept of the mathematical term *set* is a subtle one, and unless some care is exercised paradoxes will result. However, no pathology will occur in our (very) concrete situation, allowing us to be not precise about the definition of a set. Those students who are interested in learning more about these wonderful artifacts of human imagination can take Ma6c or consult the book, *Axiomatic Set theory* by Suppes.

We will often use the following symbolic abbreviations: $\exists$ for *There exists*, $\forall$ for *for all* (or *for every*), $=$ for *equals*, $\neq$ for *not equal to*, $\Rightarrow$ for *if*, $\Leftarrow$ for *only if*, $\Leftrightarrow$ or *iff* for *if and only if*, s.t. for *such that*, i.e., for *that is*, qed for *quod erat demonstrandum* (*end of proof*), $\in$ for *belongs to*, and $\notin$ for *does not belong to*.

The *members* of a set will also be called *elements*. If a set X consists of the elements $a, b, c, \ldots$, then we will write

$$X = \{a, b, c, \ldots\}.$$

Two sets will be equal *if and only if* they have the *same* elements. The empty set is denoted by the symbol $\emptyset$.

A *subset* of a set X is a subcollection Y consisting of a portion of the elements of X. We will write $Y \subset X$, or $X \supset Y$, to indicate that Y is a subset of X. Typically, Y will be given as the set of elements of X satisfying some property P, in which case we will write

$$Y = \{x \in X \,|\, x \quad \text{has} \quad \text{property} \quad P\}.$$

Clearly, the empty set is a subset of every set. We will say that Y is a *proper subset* of X if it is a subset *and* if $Y \neq X$.

If Y is a subset of X, then the *complement* of Y (in X) is the set

$$Y^c = \{x \in X \,|\, x \notin Y\}.$$

It is sometimes denoted $X - Y$.

If X, Y are two sets, their *union*, resp. *intersection*, is defined to be

$$X \cup Y \;=\; \{z \,|\, z \in X \quad or \quad z \in Y\},$$

resp.

$$X \cap Y \;=\; \{w \,|\, w \in X \quad and \quad w \in Y\}.$$

The following Theorem is a fundamental law, called the *de Morgan Law*:

Theorem *Let A, B be subsets of a set X. Then we have*

$$(A \cup B)^c \;=\; A^c \cap B^c$$

and

$$(A \cap B)^c \;=\; A^c \cup B^c.$$

When A, B have no intersection, we will call $A \cup B$ a *disjoint union*.

0.2 Functions

A *function*, or a *mapping*, from a set X to another, say Y, is a rule (or an assignment) f which associates, to each element x in X, a *unique* element y, denoted $f(x)$, of Y. The symbolic way of describing the function is the following:

$$f : X \;\rightarrow\; Y.$$

It is important that $y = f(x)$ be assigned uniquely to each x, but it might happen that for a fixed y, there may be many x in X with $f(x) = y$.

The *image* of such a mapping f is defined to be

$$\mathrm{Im}(f) \;=\; \{y \in Y \,|\, \exists\, x \in X \quad \text{s.t.} \quad y = f(x)\}.$$

Here s.t. is an abbreviation for *such that*. For any y in the image, its *pre-image*, sometimes called its *fiber*, is the set

$$f^{-1}(y) \;=\; \{x \in X \,|\, f(x) = y\}.$$

When $f^{-1}(y)$ is a singleton for each y in $\mathrm{Im}(f)$, we will say that the function f is *one-to-one* or *injective*. When the image of f is all of Y, we will say that f is *onto* or *surjective*.

If f is both one-to-one and onto, we will say that f is a *one-to-one correspondence* or that it is *bijective*.

When f is a function from a set X to itself, i.e., when $X = Y$, one calls f a *self-mapping*. Any bijective self-mapping of X is called a *permutation*. Show, as a simple exercise, that the number of distinct permutations of a set X with exactly n elements is $n!$

0.3 Cardinality

The *cardinality*, or the *order*, of a set X, denoted $|X|$, is the number of elements in it. This intuitive definition is easy enough to grasp when X is finite, i.e., when it has only a finite number of elements. But when X is *infinite*, i.e., not finite, there are various types of infinities, and we will be crude and settle on having only two types of such infinities, namely of the countable type and the uncountable type.

To be precise, let us denote by $\mathbb{N}$ the set of all counting numbers $\{1, 2, 3, 4, 5, \ldots\}$. See section 1.1 for a discussion of these numbers and their properties. We will call a set X *countable* if it is either finite or if there is a one-to-one correspondence between X and $\mathbb{N}$; a countable infinite set will be said to be *countably infinite*. If X is *not* countable, we will call it *uncountable*. It will turn out that the set of all real numbers is uncountable.

Clearly, two sets have the same cardinality if there is a bijective mapping between them.

Example: *The subset* $\mathbb{N}_{\text{even}}$ *of* $\mathbb{N}$ *consisting of even counting numbers has the same cardinality as* $\mathbb{N}$*; so they are both countably infinite.* To prove it, observe that the natural mapping $f : \mathbb{N} \to \mathbb{N}_{\text{even}}$ defined by $n \to 2n$ is one-to-one and onto.

Note however, that if Y is a proper subset of a *finite* set X, we will always have $|Y| < |X|$.

A basic result on cardinality is the following

Proposition *Let* X, Y *be arbitrary finite sets. Then we have*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

The proof is left as an exercise.

0.4 Equivalence Relations

Sometimes it is important to partition sets into blocks, where each block consists of elements which are equivalent in some sense. For example, we can split $\mathbb{N}$ into two blocks $\mathbb{N}_{\text{even}}$ and $\mathbb{N}_{\text{odd}}$, the former consisting of *even numbers*, and the latter consisting of *odd numbers*. The equivalence would be $a \sim b$ iff a and b have the same *parity*, i.e., iff $a - b$ is divisible by 2.

In general one has to make sure that a *relation* $\sim$ on a set X has certain natural properties in order to be called an *equivalence relation*. The properties one needs are

$$a \sim a \qquad (\textbf{reflexivity})$$

$$a \sim b \Leftrightarrow b \sim a \qquad (\textbf{symmetry})$$

$$a \sim b, b \sim c \Longrightarrow a \sim c \qquad (\textbf{transitivity})$$

Check that the relation defined above on $\mathbb{N}$ by using parity satisfies these three conditions.

Now let X be any set with an equivalence relation $\sim$. For any element x, we can put together all the elements of X which are equivalent to it, and call it the *equivalence class* of x (or represented by x). Check that the properties above preclude any element from belonging to two different equivalence classes. (Such a way of writing a set as a disjoint union of subsets is called a *partition*.)

This allows us to form a new set, often denoted $X/\sim$, whose elements are equivalence classes in X. Again, when $X = \mathbb{N}$ and $\sim$ is the relation given by parity, $X/\sim$ consist of two classes, namely $\mathbb{N}_{\text{even}}$ and $\mathbb{N}_{\text{odd}}$.

Sometimes one finds the notion of a set of equivalence classes a bit abstract and opts to do the following: Choose, for each class C, a fixed element $x(C)$ representing it in X, and view $X/\sim$ as the *set of* such *representatives* $\{x(C)\}$. In the example we have been considering, we may choose 0, resp. 1, to represent the class of even, resp. odd numbers, and identify $\{0, 1\}$ with the set of equivalence classes. (When we say that two sets can be identified, we mean that there is a one-to-one correspondence between them.)

There is no reason to feel intimidated by taking equivalence classes. One does it often in real life without thinking about it explicitly. For example everyone is used to dealing with fractions, which are really equivalence classes, because we identify $\frac{md}{nd}$ with $\frac{m}{n}$ for any non-zero integer d. More on this in section 2.1.