Chapter 4

Thursday, July 14, 2011

This past week, we have seen that concepts as rudimentary as set theory and number systems have far-reaching importance in many fields of Mathematics. Today's application section will focus on some of the major implications of these ideas in pure Mathematics. Specifically, the notion of size or *cardinality* will be defined below and give us a context to discuss which infinities are larger. Furthermore, we will discover why complex numbers are, in many ways, much more powerful than real or rational numbers.

4.1 Counting Infinities and the Continuum Hypothesis

The goal of this section is to expand the concept of the *cardinality* of a set to infinite sets. In studying the cardinalities of infinite sets, we will notice that certain infinite sets are bigger than other infinite sets; we will try to make sense of how this can be true by giving a formal definition of size and cardinality.

4.1.1 The Cardinality of a Set

To make sense of cardinalities of a general set, we will recall the concept of a bijection. Given two sets S and T, a ***function*** f is a map

$$f : S \to T$$

that assigns to every element $s \in S$ an element $f(s) \in T$. A set function $f : S \to T$ is ***one-to-one*** or ***injective*** if whenever $f(s_1) = f(s_2)$, then $s_1 = s_2$. In other words, for every $t \in T$, there is at most one $s \in S$ that maps to t. It could be possible that $t \in T$ has no pre-images (i.e., elements of S that map to t); so, a one-to-one map is one in which every element of $t \in T$ has *at most* one pre-image. We say that a map $f : S \to T$ is ***onto*** or ***surjective*** if every $t \in T$ has at least one pre-image; that is, for every $t \in T$, there exists some $s \in S$ such that $f(s) = t$. Another way of saying this is that f is onto/surjective if the image of f is all of T. Finally, we say that a function $f : S \to T$ is a ***bijection*** if f is both *one-to-one* and *onto*.

If we have two sets S and T such that there exists some bijection $f : S \to T$, then we say that the sets S and T have the same *cardinality* or *cardinal numbers*. In this case, we write

$$|S| = |T|$$

and believe that these sets are of the same size.

4.1.2 Cardinalities of Finite Sets

We must make sure that our new notion of cardinality agrees with our previously established notion of the *size of a set*. Let's consider a set with n elements given by

$$S = \{x_1, x_2, x_3, \ldots, x_n\}.$$

Intuitively, we know that S will have size n; to verify that this is consistent with our new definition, we will show that our set S bijects (i.e., has a bijection) onto the set

$$T_n = \{1, 2, 3, \ldots, n\}.$$

Indeed, consider the set map

$$f : S \to T_n$$
$$f(x_i) = i.$$

Our map is *onto* because every $i \in \{1, 2, \ldots, n\}$ has a pre-image x_i. It is also *one-to-one* because each i only has the one pre-image x_i. Thus, we can say that out set $S = \{x_1, x_2, \ldots, x_n\}$ has cardinality n because it bijects onto the set $T_n = \{1, 2, \ldots, n\}$.

Further, we can say that a set S is *finite* if it bijects onto some finite set $T_n = \{1, 2, \ldots, n\}$. If there does not exist such a bijection, we say our set is *infinite*.

4.1.3 Cardinalities of Infinite Sets

Now that we understand finite sets, we want to comprehend what kinds of bijections we can have between infinite sets; that is, we want to understand what kinds of infinite sets can biject. The most basic examples of infinite sets come from our number systems.

Consider the most basic set of infinite numbers: the integers

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

By definition, any set S that bijects onto the integers $\mathbb{Z}$ has the same cardinality as $\mathbb{Z}$; let's call this cardinality $\aleph_0$ (aleph-naught).

Now, consider the set of natural numbers

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

At first glance, this set $\mathbb{N}$ seems to be smaller than $\mathbb{Z}$ since it is a *proper* subset of $\mathbb{Z}$. However, we will construct a bijection $f : \mathbb{N} \to \mathbb{Z}$. Consider the map

$$f(n) = \begin{cases} k & \text{if } n = 2k \\ -k & \text{if } n = 2k - 1 \end{cases}$$

Thus, it sends the k-th even number to k and the k-th odd entry to $-k$. One can easily check that this is both one-to-one and onto. Thus, $\mathbb{N}$ also has cardinality $\aleph_0$.

4.1.4 The Cardinality of the Rationals

One of the most surprising outcomes of studying cardinal numbers is that the rationals $\mathbb{Q}$ (the set of all fractions) have cardinality $\aleph_0$. By the definition of $\aleph_0$, this means that there is a bijection

$$f : \mathbb{Q} \to \mathbb{Z}.$$

Intuitively, this is surprising since the rationals seem to be so much larger than the integers. In fact, inside of any tiny interval there are infinitely many rationals. The argument for this uses a standard graph of ordered pairs to give the bijection.

4.1.5 Countable Sets

Above we saw that many sets that are at first glance very different are actually bijective. In other words, sets like $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ have bijections between them and thus all have the same cardinality $\aleph_0$. Since the natural numbers $\mathbb{N}$ are also known as *counting numbers*, we see that the above sets have the property that one can essentially list them off. The above sets (and any sets in bijection with them) and finite sets all have this property, called ***countability***. Formally, we say that a set S is ***countable*** if there exists an *injection* (i.e. one-to-one function)

$$f : S \to \mathbb{N}.$$

Clearly, any set that is bijective with $\mathbb{N}$ (like $\mathbb{Z}$ or $\mathbb{Q}$) is countable since, by definition, there exists a bijection with $\mathbb{N}$ (which is stronger than an injection). However, countability also includes finite sets. Intuitively, these sets are the ones that we can list off or count. Many surprising facts are true about countable sets.

Theorem. A countable union of countable sets is countable.

This theorem is somewhat surprising because it says that if we take a countable number of sets that are themselves countable, then the entire union is countable.

Even more surprising is the following theorem about direct products of countable sets.

Theorem. The direct product of two countable sets is countable.

This theorem is more unexpected than the previous one since, intuitively, in taking a union the number of elements is bounded above by the sum of the sizes of each set, whereas the size of a direct product is the product of the individual sets. Of course, "sum" and "product" don't mean much when dealing with infinity, but this certainly clues us into how large we should intuit these sets to be.

4.1.6 The Reals are Not Countable

Now for an example of an infinite set that is larger than the countable sets we have been dealing with. Consider the real numbers (intuitively, you can think of these as infinite decimal sets). There are two ways of doing this. The first one uses the *completeness* property of the reals and the second uses *Cantor's Diagonal Argument*.

Theorem. The real numbers $\mathbb{R}$ are not countable.

Any set with the cardinality of the real numbers is said to have the cardinality of the ***continuum***. This is also denoted by saying that

$$|\mathbb{R}| = \aleph_1.$$

The above notion also makes sense since it can be shown that the power set of the integers bijects with the reals. Thus, on the level of cardinal numbers, we have that

$$|\mathcal{P}(\mathbb{Z})| = |\mathbb{R}|.$$

4.1.7 The Continuum Hypothesis

The continuum hypothesis was the focus of much study for the past several decades. Essentially, it says that there is no cardinal number between $\aleph_0$ and $\aleph_1$. Put another way, there exists no set A such that

$$\aleph_0 < |A| < \aleph_1.$$

Georg Cantor, one of the fathers of set theory, tried for many years to prove it in vain. It then became a key problem in David Hilbert's list of important open questions in Mathematics.

In 1940, Kurt Gödel showed that the Continuum Hypothesis cannot be disproved using the axioms for set theory (known as the Zermelo-Fraenkel Axioms). Later, Paul Cohen demonstrated in 1963 that the Continuum Hypothesis also cannot be proved using the Zermelo-Fraenkel Axioms. Thus, this establishes that the Continuum Hypothesis is independent of the Zermelo-Fraenkel Axioms. Of course, this is not horribly surprising given that Gödel's Incompleteness Theorem states that any sufficiently complicated axiom system will have true statements which can not be proven using said axioms.

4.2 Factoring Polynomials and the Fundamental Theorem of Algebra

4.2.1 Factoring Polynomials

The question of deciding whether a given polynomial can be written as a product of two smaller polynomials has spurred a great deal of important Mathematics. Recall that any polynomial can be written as

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0.$$

One of the defining characteristics of a polynomial is the degree (in this case, the largest number n such that the coefficient a_n is non-zero) and where the coefficients live. For example, a polynomial with coefficients in $\mathbb{Z}$ are those in which the a_i are all integers. We say that a polynomial $P(x)$ is ***reducible*** over S if it can be written as $P(x) = Q(x) \cdot R(x)$ where $Q(x)$ and $R(x)$ are polynomials with coefficients in S of degree greater than 0. If it cannot be written in this way, we say that $P(x)$ is ***irreducible*** over S.

For example, consider the polynomial $P(x) = x^2 + 1$; this is a polynomial with coefficients in $\mathbb{Z}$ (or also can be considered as one with coefficients in $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$). We have shown that $P(x)$ is irreducible over $\mathbb{R}$. However, we may write $P(x)$ as $P(x) = (x - i)(x + i)$, and thus $P(x)$ is reducible over $\mathbb{C}$.

The obstruction to factoring the above polynomial $P(x) = x^2+1$ over the reals comes from the lack of real root for $P(x)$. In the complex numbers, however, $P(x)$ does have two roots: i and $-i$. In general, any time that a polynomial $P(x)$ has a root r in $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$, then it can be factored as

$$P(x) = (x - r)Q(x)$$

where $Q(x)$ is a polynomial with coefficients in $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$, respectively. Of course, this begs the question of it *very* polynomial can be factored over $\mathbb{C}$. The Fundamental Theorem of Algebra answers this questions affirmatively.

4.2.2 The Fundamental Theorem of Algebra

One of the most surprising and exciting features of $\mathbb{C}$ is that it is *algebraically closed*; that is, any complex polynomial with complex coefficients has all its roots in $\mathbb{C}$. In other words, any polynomial of degree greater than 1 is reducible over $\mathbb{C}$.

Fundamental Theorem of Algebra. Any degree $n \geq 1$ polynomial $P(x)$ with coefficients in $\mathbb{C}$ has n complex roots (counting multiplicities). Thus, we can write

$$P(x) = \alpha(x - r_1)(x - r_2) \cdots (x - r_n)$$

where the r_i are the roots of $P(x)$ and $\alpha \in \mathbb{C}$ is some complex constant.

Note that this is particularly helpful even if one doesn't work with complex numbers. Consider a polynomial with coefficients in $\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{Z}$). It is, of course also a polynomial with coefficients in $\mathbb{C}$ (since all of these are subsets of $\mathbb{C}$). This will tell us that even if we can't find roots in $\mathbb{R}$, all of its roots will be at most in $\mathbb{C}$.

Another way of stating this theorem is that any polynomial with coefficients in $\mathbb{C}$ which are irreducible over $\mathbb{C}$ are those of degree at most 1; note that degree 1 polynomials are always irreducible by definition.