Math 310
October 26, 2020 Lecture

Steven G. Krantz

October 11, 2020

Figure: This is your instructor.

Proposition *The collection $\mathcal{P}$ of all polynomials $p(x)$ with integer coefficients is countable.*

Proof: Let $\mathcal{P}_k$ be the set of polynomials of degree k with integer coefficients. A polynomial p of degree k having integer coefficients has the form

$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_k x^k \, ,$$

where the p_j are integer constants. The identification

$$p(x) \longleftrightarrow (p_0, p_1, \ldots, p_k)$$

identifies the elements of $\mathcal{P}_k$ with the $(k+1)$-tuples of integers. By an earlier corollary, it follows that $\mathcal{P}_k$ is countable. But then the next corollary implies that

$$\mathcal{P} = \bigcup_{j=0}^{\infty} \mathcal{P}_j$$

is countable. □

Definition Let x be a real number. We say that x is *algebraic* if there is a polynomial p with integer coefficients such that $p(x) = 0$.

Example The number $\sqrt{2}$ is algebraic because it satisfies the polynomial equation $x^2 - 2 = 0$. The number $\sqrt{3} + \sqrt{2}$ is also algebraic. This assertion is less obvious, but in fact the number satisfies the polynomial equation $x^4 - x^2 + 1 = 0$. The numbers π and e are *not* algebraic, but this assertion is extremely difficult to prove. We say that π and e are *transcendental*. In the next proposition, we give an elegant method for showing that most real numbers are transcendental without actually saying what any of them are.

Georg Cantor's remarkable discovery is that *not all infinite sets are countable*. We next give an example of this phenomenon.

In what follows, a *sequence* on a set S is a function from $\mathbb{N}$ to S. We usually write such a sequence as $s(1), s(2), s(3), \ldots$ or as $s_1, s_2, s_3, \ldots$.

Example There exists an infinite set which is not countable (we call such a set *uncountable)*. Our example will be the set S of all sequences on the set $\{0, 1\}$. In other words, S is the set of all infinite sequences of 0's and 1's.

To see that S is uncountable, assume the contrary—that is, we assume that S is countable. Then there is a first sequence

$$\mathcal{S}^1 = \{s_j^1\}_{j=1}^{\infty},$$

a second sequence

$$\mathcal{S}^2 = \{s_j^2\}_{j=1}^{\infty},$$

and so forth. This will be a complete enumeration of all the members of S. But now consider the sequence $\mathcal{T} = \{t_j\}_{j=1}^{\infty}$, which we construct as follows:

- If $s_1^1 = 0$ then set $t_1 = 1$; if $s_1^1 = 1$ then set $t_1 = 0$;
- If $s_2^2 = 0$ then set $t_2 = 1$; if $s_2^2 = 1$ then set $t_2 = 0$;
- If $s_3^3 = 0$ then set $t_3 = 1$; if $s_3^3 = 1$ then set $t_3 = 0$;

$$\dots$$

- If $s_j^j = 0$ then set $t_j = 1$; if $s_j^j = 1$ then set $t_j = 0$;

etc.

Now the sequence $\mathcal{T} = \{t_j\}$ differs from the first sequence $\mathcal{S}^1$ in the first element: $t_1 \neq s_1^1$.

The sequence $\mathcal{T}$ differs from the second sequence $\mathcal{S}^2$ in the second element: $t_2 \neq s_2^2$.

And so on: the sequence $\mathcal{T}$ differs from the j^{th} sequence $\mathcal{S}^j$ in the j^{th} element: $t_j \neq s_j^j$. So the sequence $\mathcal{T}$ is not in the set S. But $\mathcal{T}$ is *supposed* to be in the set S because it is a sequence of 0's and 1's and all of these are supposed to have been enumerated in our enumeration of S.

This contradicts our assumption, so S must be uncountable.

Example Consider the set of all decimal representations of numbers strictly between 0 and 1—both terminating and nonterminating. Here a terminating decimal is one of the form

$$0.43926$$

while a nonterminating decimal is one of the form

$$0.14159265\ldots.$$

In the case of the nonterminating decimal, no repetition is implied; the decimal simply continues without cease.

Now the set of all those decimals containing only the digits 0 and 1 can be identified in a natural way with the set of sequences containing only 0 and 1 (just put commas between the digits). And we just saw that the set of such sequences is uncountable.

Since the set of all decimal numbers is an even bigger set, it must be uncountable also. [Put a different way, if the set of all decimal numbers *were* countable, then any of its infinite subsets would be countable—that is one of our earlier results. Thus the collection of decimal numbers containing only the digits 0 and 1 would be countable, and that is a contradiction.]

As you may know, the set of all decimals identifies with the set of all real numbers. [Many real numbers have two decimal representations—one terminating and one not. Think for a moment about which numbers these are, and why this observation does not invalidate the present discussion.] We find then that the set $\mathbb{R}$ of all real numbers is uncountable. (Contrast this with the situation for the rationals.) In a later lecture we will learn more about how the real number system is constructed using just elementary set theory.

Now we have the promised very dramatic result of Georg Cantor about the transcendental numbers.

Proposition *The set of all algebraic real numbers is countable. The set of all transcendental numbers is uncountable.*

Proof: Let $\mathcal{P}$ be the collection of all polynomials with integer coefficients. We have already noted that $\mathcal{P}$ is a countable set. If $p \in \mathcal{P}$ then let s_p denote the set of real roots of p. Of course s_p is finite, and the number of elements in s_p does not exceed the degree of p. Then the set A of algebraic real numbers may be written as

$$A = \cup_{p \in \mathcal{P}} s_p \, .$$

This is the countable union of finite sets, so of course it is countable.

Now that we know that the set A of algebraic numbers is countable, we can see that the set T of transcendental numbers must be uncountable. For $\mathbb{R} = A \cup T$. If T were countable then, since A is countable, it would follow that $\mathbb{R}$ is countable. But that is not so. $\square$

Our last result in this section is a counterpoint to Proposition 4.5.13 and the discussion leading up to it.

Proposition *Let S be any infinite set. Then S has a subset T that is countable.*

Proof: Let $t_1 \in S$ be any element. Now let $t_2 \in S$ be any element that is distinct from t_1. Continue this procedure. It will not terminate, because that would imply that S is finite. And it will produce a countable set T that is a subset of S. $\square$

To repeat the main point of this section, the natural numbers have a cardinality that we call *countable*, and the real numbers have a cardinality that we call *uncountable*. These cardinalities are distinct. In fact the real numbers form a larger set because there is an injective mapping of the natural numbers into the reals but not the other way around. We refer to the cardinality of the natural numbers as "countable" and to that of the real numbers as "the cardinality of the continuum."

It is natural to ask whether there is a set with cardinality strictly between countable and the continuum. Georg Cantor posed this question one hundred years ago, and his failed attempts to resolve the question tormented his final years. We shall discuss the resolution of this "continuum hypothesis" in a later lecture.

It is an important result of set theory (due to Cantor) that, given any set S, the set of all subsets of S (called the *power set* of S) has strictly greater cardinality than the set S itself. As a simple example, let $S = \{a, b, c\}$. Then the set of all subsets of S is

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

The set of all subsets has eight elements while the original set has three.

We stress that this result is true not just for finite sets but also for infinite sets: if S is an infinite set then the set of all its subsets (the power set) has greater cardinality than S itself. Thus there are infinite sets of arbitrarily large cardinality. In other words, there is no “greatest” cardinal. This fact is so important that we now formulate it as a theorem.

Theorem [Cantor] *Let S be any set. Then the power set $\mathcal{P}(S)$, consisting of all subsets of S, has cardinality greater than the cardinality of S. In other words,*

$$\mathit{card}(S) < \mathit{card}(\mathcal{P}(S)) .$$

Proof: First observe that the function

$$\begin{array}{rcl} f : S & \longrightarrow & \mathcal{P}(X) \\ s & \longmapsto & \{s\} \end{array}$$

is one-to-one. Thus we see that $\mathrm{card}(S) \leq \mathrm{card}(\mathcal{P}(S))$. We need to show that there is no function from S *onto* $\mathcal{P}(S)$. Let $g : S \to \mathcal{P}(S)$. We will produce an element of $\mathcal{P}(S)$ that cannot be in the image of this mapping.

Define $T = \{s \in S : s \notin g(s)\}$. Assume, seeking a contradiction, that $T = g(z)$ for some $z \in S$. By definition of T, the element $z \in T$ if and only if $z \notin g(z)$; thus $z \in T$ if and only if $z \notin T$. That is a contradiction. We see that g cannot map S onto $\mathcal{P}(S)$, therefore $\text{card}(S) < \text{card}(\mathcal{P}(S))$. $\square$

In some of the examples in this section, we constructed a bijection between a given set (such as $\mathbb{Z}$) and a proper subset of that set (such as $\mathcal{E}$, the even integers). It follows from the definitions that this is possible only when the sets involved are infinite. In fact any infinite set can be placed in a set-theoretic isomorphism with a proper subset of itself. We explore this assertion in the exercises.

Put in other words, we have come upon an intrinsic characterization of infinite sets. We state it (without proof) as a proposition:

Proposition *Let S be a set. The set S is infinite if and only if it can be put in one-to-one correspondence with a proper subset of itself.*

Exercise 4.41 outlines a proof of this proposition.