Bonus Facts

Math 347

January 14, 2022

This is a collection of bonus facts and ideas for your reading pleasure throughout the term. Nothing in here is required knowledge for the course; this is mainly to satisfy your curiosity. Please let me know if you find typos or mistakes!

1 Set Sizes

Fact 1. $\overline{\mathbb{Q}}$ *is countable*

Proof. The idea behind this proof of this fact came from Chris Wurst.

We're going to try to construct a function $f : \mathbb{Q} \to \overline{\mathbb{Q}}$. The goal is to take an rational number x and use it to "code" a particular algebraic number. Note that to code an algebraic number, you need only know two things: a polynomial (with integer coefficients) it is a root of and which root it is.

Here's a big assumption we're going to start with. Let's assume that given a polynomial with integer coefficients, we've ordered its roots (i.e. every polynomial has a "first" root and a "second" root, and so on; additionally, let's start our index at 1 so that there is no "zero"th root). This is actually kind of a big assumption because it requires something called the Axiom of Choice, which is kind of controversial in mathematics (okay, this assumption only requires the axiom of countable choice, but that's getting a little too far into the weeds).

We're also going to use the following fact: every rational number (except 0) has a prime factorization. Now, you're probably used to factoring integers into primes, but what does it mean to factor rationals into primes? The trick is to allow yourself negative exponents. Given any nonzero rational number $\frac{a}{b}$ (in lowest terms, so that a and b have no common factors), you can factor a and b into primes, then write $\frac{a}{b}$ in prime powers where the prime has a positive exponent if a is a multiple of that prime, a negative exponent if b is a multiple of that prime, and an exponent of 0 if neither a nor b is a multiple of that prime. For instance: the rational number $\frac{6}{125} = 2^1 \cdot 3^1 \cdot 5^{-3} \cdot 7^0 \cdot 11^0 \cdots$. Also, $1 = 2^0 \cdot 3^0 \cdot 5^0 \cdots$. It's helpful to think about the zero exponents for the function we're about to construct.

Now we can define our function on rational numbers $\frac{a}{b}$. Rather than overwhelm you with notation, I'll describe the process of how you start with a rational number and get an algebraic number. If $\frac{a}{b} = 0$, then define $f(\frac{a}{b}) = 0$. If $\frac{a}{b} \neq 0$, then check if the following condition is true:

> Factor $\frac{a}{b}$ into primes, say $\frac{a}{b} = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot 7^{a_7} \cdots$. Note that there is a largest p for which $a_p \neq 0$ (think about this). Suppose that p is the nth prime. The condition we want to check is the following: is $a_2 > 0$ and is $a_2 < n - 1$?

If the answer to the previous question is "no," define $f(\frac{a}{b}) = 1$. Otherwise, define $f(\frac{a}{b})$ to be the a_2th root of the polynomial $a_3 + a_5 X + a_7 X^2 + a_{11} x^3 + \cdots$.

At this point, it's probably not super clear what f does or why we've defined these conditions, so let's look at some examples. The main idea of the function is that you want the rational number $2^3 \cdot 3^1 \cdot 5^0 \cdot 7^{-2} \cdot 11^1$

to map to the third root of the polynomial $1 + 0X - 2X^2 + X^3$. So the power of 2 codes "which root am I looking at?" where the powers on the later primes code "which polynomial am I looking at?"

The reason for the checking of "is $a_2 > 0$ and is $a_2 < n - 1$?" is to answer the question of "where should we map $2^{-1} \cdot 3^1 \cdot 5^0 \cdot 7^{-2} \cdot 11^1$?" (because there is no -1st root of any polynomial) and "where should we map $2^7 \cdot 3^1 \cdot 5^0 \cdot 7^{-2} \cdot 11^1$?" (because the corresponding polynomial doesn't have 7 roots, so you can't talk about a seventh root).

Okay, great, so now we have a function. But we didn't involve $\mathbb{N}$ anywhere in the creation of our function, so how does this help show that $\overline{\mathbb{Q}}$ is countable? Note first that f is surjective (onto). If I take any element in $\overline{Q}$, it is some root of some polynomial with integer coefficients and I can use the ordering of the roots and the coefficients of the polynomial to come up with an appropriate $2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdots$ which maps to my favorite element of $\overline{\mathbb{Q}}$. f is not injective, however (why?), but this isn't important. By coming up with a surjective function $f : \mathbb{Q} \to \overline{\mathbb{Q}}$, we've shown that $\overline{\mathbb{Q}}$ is "no bigger than" $\mathbb{Q}$. Hence, $\overline{\mathbb{Q}}$ is no bigger than a countable set, so $\overline{\mathbb{Q}}$ is countable.

One last note about this: the typical proof of the fact that $\overline{\mathbb{Q}}$ is countable passes through the following fact: the countable union of countable sets is countable. So you first show that the set of polynomials with integer coefficients is countable, then you note that the set of algebraic numbers is the union of the sets of roots of the individual polynomials with integer coefficients. □

Question 1.1. *(Andrea) Can a power set be well-ordered?*

This question has a lot of depth to it!

Every finite set can be well-ordered: if your set looks like $S = \{a_1, a_2, \ldots, a_n\}$ then you can impose the ordering $a_1 < a_2 < \cdots < a_n$ and see that any subset of S has a least element.

Hence, the power set of a finite set can be well-ordered (since the power set will also be finite). The ordering won't seem natural, but it can be done. For example, if $S = \{1, 2\}$, then and we can impose a well-ordering on $\mathcal{P}(S) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$ by defining

$$\varnothing < \{2\} < \{1, 2\} < \{1\}$$

Of course, there are other ways of well ordering $\mathcal{P}(S)$ (if you like counting things, try to find out how many well-orderings there are!)

Finite sets aren't the only interesting ones. We have countably infinite sets too. These can also be well-ordered since they can always be written as a sequence $a_0, a_1, a_2, \ldots$ and you can well-order any sequence by defining

$$a_0 < a_1 < a_2 < \cdots$$

Again, this order might not be the ordering you want, but it can be done. For instance, since $\mathbb{Q}$ is countable, you can well-order it. But you can't use the usual ordering on since $\{x \in \mathbb{Q} \mid x > 0\}$ doesn't have a least element under the usual ordering.

And then there are uncountably infinite sets. These are not merely trickier, but trickier to the point that we need an axiom if we want to do this. The Well-Ordering Axiom states that every set can be well-ordered. It turns out that the well-ordering axiom is equivalent to the axiom of choice (which is the most philosophically controversial of the standard set theory axioms). Since we often take the axiom of choice to be an axiom (and since the well-ordering axiom follows from the axiom of choice), it's more common to call the well-ordering axiom the "well-ordering theorem." You can read more about it here: `https://en.wikipedia.org/wiki/Well-ordering_theorem`

2 Induction

We have a couple of different principles/axioms that relate to induction. Here they are:

Axiom 1. *(Well-Ordering) If $S \subseteq \mathbb{N}$ and $S \neq \varnothing$, then S has a least element.*

Axiom 2. *(Weak induction) Suppose that $S \subseteq \mathbb{N}$, $0 \in S$, and for every $k \in \mathbb{N}$, if $k \in S$, then $k+1 \in S$. Then $S = \mathbb{N}$*

Axiom 3. *(Strong induction) Suppose that $S \subseteq \mathbb{N}$, $0 \in S$, and for every $k \in \mathbb{N}$, if $0, 1, \ldots, k \in S$, then $k+1 \in S$. Then $S = \mathbb{N}$*

Recall that in class, we showed that strong induction implies the well-ordering principle and we also showed that the well-ordering principle implies weak induction (we didn't call it weak induction in class, we just called it induction—here, we'll call it weak induction to distinguish it from strong induction). To complete the equivalence of all three of these things, we need to show the following fact:

Fact 2. *Weak induction implies strong induction.*

Proof. Suppose that weak induction is true. We need to show that strong induction also holds.

Let $T \subseteq \mathbb{N}$, suppose that $0 \in T$ and suppose that for any integer k, if $0, 1, 2, \ldots, k \in T$, then $k+1 \in T$.

If we want to show that $T = \mathbb{N}$ using weak induction, we need to show the following three things:

1. $T \subseteq \mathbb{N}$
2. $0 \in T$
3. For all k, if $k \in T$, then $k+1 \in T$

Note that the first two are trivial because we supposed that $T \subseteq \mathbb{N}$ and $0 \in T$. However, the third point is *not* trivial (even though it might seem like it, on the face of it). While we've supposed that "if $0, 1, 2, \ldots, k \in T$, then $k+1 \in T$" we have not supposed "if $k \in T$, then $k+1 \in T$." In fact, the third claim is hard enough to prove, that we're not going to try. We need to take a different approach to solving this problem.

Instead we'll consider $R := \{x \in \mathbb{N} : \text{for all } y \in \mathbb{N} \text{ with } y < x, y \in T\}$. Note that $0 \in R$ (after all, the claim "for all $y \in \mathbb{N}$ with $y < 0$, $y \in T$" is vacuously true since there are no $y \in \mathbb{N}$ with $y < 0$).

Next, we claim that if $k \in R$, then $k+1 \in R$. Suppose that $k \in R$. Then for all $y \in \mathbb{N}$ with $y < k$, $y \in T$. Now we apply what we know about T: since $0, 1, \ldots, k-1 \in T$, we know that $k \in T$. Now, since $0, 1, \ldots, k \in T$, we can conclude that $k+1$ has the defining property of R, so $k+1 \in R$.

We've now shown that $0 \in R$ and if $k \in R$, then $k+1 \in R$. By weak induction, $R = \mathbb{N}$.

Now we're going to show that $T = \mathbb{N}$ directly. Pick $n \in \mathbb{N}$. Since $n+1 \in R$, it is true that for every $y < n+1$, $y \in T$. Since $n < n+1$, we conclude that $n \in T$. We've now shown that $\mathbb{N} \subseteq T$ and since $T \subseteq \mathbb{N}$, we have $T = \mathbb{N}$. This is the conclusion of strong induction and hence, strong induction holds. □