COUNTABILITY OF RATIONALS

We have proved several propositions about denumerable sets. These propositions will allow us to prove the following fact.

Theorem. The set $\mathbb{Q}$ of rational numbers is denumerable.

Before starting the proof, let me recall a property of natural numbers known as the Fundamental Theorem of Arithmetic.

The Fundamental Theorem of Arithmetic. Every positive integer can be decomposed into a product of (powers of) primes in an essentially unique way.

I will not give a proof here. The proof of this fact is given in an introductory Number Theory class; this proof is analyzed and generalized in an introductory Abstract Algebra class.

Proof. It suffices to find an injection of $\mathbb{Q}$ into a denumerable set. Indeed, every injection is an isomorphism onto its image, and this image, being a subset of a denumerable set, must be denumerable.

We will find an injection

$$\mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{N}^*,$$

where $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, the set of positive integers.

In order to present this injection, I recall that, by definition, rational numbers are elements of the set $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$. A rational number is thus an equivalence class $[(a, b)]_{\sim}$ with some integers $a$ and $b \neq 0$. We need to map this class to a pair of integers, the second one in the pair being positive. We will do that with the help of the following proposition.

Proposition. In every equivalence class $[(a, b)]_{\sim} \in \mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$, there is a unique element

$$(m, n) \in [(a, b)]_{\sim}$$

such that $n > 0$ and the greatest common divisor of $m$ and $n$ is 1.

EXERCISE Explain to yourself why this proposition is nothing but reduction of a fraction to lowest terms, and try to prove it making use of the Fundamental Theorem of Arithmetic.

We now associate the element whose existence and uniqueness is guaranteed by the above proposition to every equivalence class. In this way, we produce a map $\mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{N}^*$.

EXERCISE Prove that this map is not surjective.

EXERCISE Prove that this map is injective. This completes the proof of the theorem.

In the above proof, we proved the existence of an isomorphism between $\mathbb{N}$ and $\mathbb{Q}$. In other words, we have proved that there exists a bijection

$$\mathbb{Q} \rightarrow \mathbb{N}. $$
EXERCISE Prove that if two sets, $S$ and $T$ are denumerable, then there exist infinitely many different bijections $S \rightarrow T$.

However, this proof provides no clue about any specific map $\mathbb{Q} \rightarrow \mathbb{N}$. Let me now give another proof of this theorem which presents a more specific map instead.

Proof. I begin in the same way as in the above proof, and use the reduction to lowest terms proposition which I have used there. I now want to construct an isomorphism

$$f : \{(m,n) | m \in \mathbb{Z}, n \in \mathbb{N}^*, \text{gcd}(m,n) = 1\} \rightarrow \mathbb{Z}$$

That would suffice since $\mathbb{Z}$ is countable. It is natural to think take a pair $(m,n)$ simply as the fraction $m/n$, and I will do that now. Let me make use of the Fundamental Theorem of Arithmetic, and decompose both integers into products of powers of primes.

$$m = p_1^{i_1} p_2^{i_2} \cdots p_M^{i_M},$$

$$n = q_1^{j_1} q_2^{j_2} \cdots q_N^{j_N}$$

Here all primes $p_1, p_2, \ldots, p_M, q_1, q_2, \ldots, q_N$ are distinct primes. If $m = 0$, there is no decomposition, and I simply set $f(0) = 0$. Now, for $m \neq 0$, set

$$f(m/n) = \frac{m^{3/2} q_1 q_2 \cdots q_N}{|m|}$$

In order to prove that $f$ is indeed an isomorphism, we analyze the above formula. Note that

$$p_1^{i_1} p_2^{i_2} \cdots p_M^{i_M} = \frac{m}{|m|} p_1^{2i_1} p_2^{2i_2} \cdots p_M^{2i_M} q_1^{2j_1+1} q_2^{2j_2+1} \cdots q_N^{2j_N+1}.$$ 

The fraction $\text{sign}(m) = m/|m|$ simply takes care about the sign: $f$ takes positive rationals to positive integers, and negative rationals to negative integers.

We now construct an inverse $g : \mathbb{Z} \rightarrow \mathbb{Q}$. We set $g(0) = 0$. For an integer $x \in \mathbb{Z}$, we have that $x = \pm t$ with $t \in \mathbb{N}$. We now make use of the Fundamental theorem of Arithmetic, and decompose $t$ into a product of powers of distinct primes:

$$t = l_1^{k_1} l_2^{k_2} \cdots l_K^{k_K}.$$ 

All $l_1, l_2, \ldots, l_K$ are distinct primes. Some of the positive powers $k_1, k_2, \ldots, k_K$ are even, while others are odd. We set for $i = 1, \ldots, K$,

$$s_i = \begin{cases} k_i/2 & \text{if } k_i \text{ is even} \\ -(k_i - 1)/2 & \text{if } k_i \text{ is odd} \end{cases}$$

and produce

$$g(x) = \text{sign}(x) l_1^{s_1} l_2^{s_2} \cdots l_K^{s_K}.$$ 

Exercise Prove that $g$ is the inverse of $f$. □

The fact that $\mathbb{Q}$ is countable does not check well with our intuition of "number line". Let me illustrate that. Let

$$f : \mathbb{Q} \rightarrow \mathbb{N}$$

be an isomorphism. For every rational number $r \in \mathbb{Q}$, let us cover this number, considered as a dot on the number line, with an interval centered in $r$ of length $1/2f(r)$. It looks like the whole line is covered, because rational numbers are dense in the line, there is another rational number as close to any one as one wants, and
every one is covered by a whole interval. Moreover, these intervals have a huge intersection. However, if we try to calculate the total length of these intervals, we find it as

$$\sum_{r \in \mathbb{Q}} \frac{1}{2^{l(r)}} = \sum_{m=0}^{\infty} \frac{1}{2^m} = 2,$$

and that is obviously too small to cover the whole line!