MATH 2080, Lecture 5 § 0.4 continued.

Last day we defined equivalent sets, meaning there's a 1-1 onto (bijective) function between them. Today we consider a special case:

Example: Let $E \subset \mathbb{N}$ denote the set of even, positive integers. Define a map

$$f : E \longrightarrow \mathbb{N}, \quad f(2n) = n.$$

by dividing by two. Then it is easy to check that $f$ is 1-1 and onto, since

$$f(2m) = f(2n) \Rightarrow m = n \quad (\text{so } 1\text{-}1)$$

and given $n \in \mathbb{N}$, $f(2n) = n$. (so onto).

Thus $E \sim \mathbb{N}$.

Remark: This might seem strange – a set being equivalent to one of its proper subsets – but such is the nature of infinite sets.

Example: Define a function $f : \mathbb{N} \longrightarrow \mathbb{Z}$ by

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is } \cancel{\text{odd}} \text{ even} \\[2ex] \dfrac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Diagrammatically; $f$ is going to have $\mathbb{Z}$ as its image with

$\{k \in \mathbb{Z} \mid k \le 0\}$ = image of odds

$\{k \in \mathbb{Z} \mid k > 0\}$ = image of evens, and $f$ is 1-1 and onto.

Let's prove this claim.

First, we check $f$ is onto. Suppose $k \in \mathbb{Z}$ is positive, then $2k \in \mathbb{N}$ and $f(2k) = k$. On the other hand
even

if $k \le 0$, then $1-2k \ge 1$ and $1-2k$ is odd, so we compute
$$f(1-2k) = \frac{1-(1-2k)}{2} = k.$$
So $f$ is onto.

To show $f$ is 1-1, suppose $f(n) = f(m)$.

If $f(n) = f(m) > 0$, then $n$ and $m$ must be even (because only evens map to positive numbers). Then we can calculate:
$$f(n) = f(m) \Rightarrow \frac{n}{2} = \frac{m}{2} \Rightarrow n = m.$$
On the other hand if $f(n) = f(m) \le 0$, then $n$ and $m$ are both odd (since only odds map to numbers $\le 0$). Then
$$f(n) = f(m) \Rightarrow \frac{1-n}{2} = \frac{1-m}{2} \Rightarrow n = m$$
Therefore $f$ is 1-1.

Thus $\mathbb{N} \sim \mathbb{Z}$.

Sets equivalent to $\mathbb{N}$ get a special name.

**Definitions:** A set is *countably infinite* iff it is equivalent to $\mathbb{N}$. A set is *finite* if and only if it is empty or equivalente to $\{1, 2, \dots, n\}$ for some $n$. A set is *countable* if it is either finite or countably infinite. A set is *infinite* if it is not finite, and *uncountable* if it is not countable.

---

*Question*: which sets are countable? Is $\mathbb{Q}$ countable? Is $\mathbb{R}$ countable? We will answer these, eventually.

*Theorem*: Any subset of $\mathbb{N}$ is countable.

*Proof*: If $S \subset \mathbb{N}$ is finite, it's countable. Suppose $S \subset \mathbb{N}$ is infinite. Then it's nonempty, by the well-ordering principle it has a smallest element, call it $f(1)$. Now after defining $f(1), f(2), \dots, f(k)$, define $f(k+1)$ to be the smallest element of $S \setminus \{f(1), f(2), \dots, f(k)\}$. This defines a function $f: \mathbb{N} \longrightarrow S$. The function is 1-1 because of its construction. It is onto because for any $m \in S$, the set

$$\{x \in S \mid x < m\}$$

is finite, say it has $k$ elements. Then $\{f(1), f(2), \dots, f(k)\} = \{x \in S \mid x < m\}$ and $f(k+1) = m$. Therefore $S \sim \mathbb{N}$.

<u>Corollary</u>: Any subset of a countable set is countable.

Note that in order to prove countability of a set $S$, we no longer need to give a function $f: S \longrightarrow \mathbb{N}$ that is 1-1 and onto, it's enough to give $f: S \longrightarrow \mathbb{N}$ that's 1-1.

<u>Theorem</u>: If $A$ and $B$ are countable, so is $A \times B$.

<u>Proof</u>: If $A$ and $B$ are countable, there are 1-1 functions $f: A \to \mathbb{N}$ and $g: B \to \mathbb{N}$. Define $h: A \times B \longrightarrow \mathbb{N}$ by $h(a,b) = \cancel{f(a)g(b)}\, 2^{f(a)} 3^{g(b)}$.

Then
$$h(a,b) = h(x,y)$$
$$\Rightarrow 2^{f(a)} 3^{g(b)} = 2^{f(x)} 3^{g(y)}$$
$\Rightarrow f(a) = f(x)$ and $g(b) = g(y)$ by unique factorization

$\Rightarrow a = x$ and $b = y$, so $(a,b) = (x,y)$ and $h$ is 1-1.

<u>Example</u>: $\mathbb{Q}$ is countable.

Every element of $\mathbb{Q}$ can be written $\frac{p}{q}$ where $p, q$ have no common divisors and $q > 0$, moreover this representation is unique.

So define $f: \mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{N}$ by

$$f\left(\frac{p}{q}\right) = (p, q).$$

This function is 1-1 since the representation of each rational number is unique. The set $\mathbb{Z} \times \mathbb{N}$ is countable, therefore so is the image $f(\mathbb{Q})$, so $\mathbb{Q}$ is countable.

We need one more method of making new countable sets from old. This will be used when we study continuity.

Theorem: Let $S \subseteq \mathbb{N}$ be a nonempty subset. Let $\{A_s\}_{s \in S}$ be a family of countable sets. Then $\bigcup_{s \in S} A_s$ is countable. ("A countable union of countable sets is countable").

Proof: For each $s \in S$, there's a 1-1 function $f_s: A_s \longrightarrow \mathbb{N}$. We need to build a 1-1 function $f: \bigcup_{s \in S} A_s \longrightarrow \mathbb{N} \times \mathbb{N}$, and we do it as follows:

Let $x \in \bigcup_{s \in S} A_s$, and let $m_x \in S$ be the smallest integer such that $x \in A_{m_x}$, this exists by the well-ordering principle. Define

$$f(x) = (m_x, f_{m_x}(x)).$$

We need to argue that $f$ is 1-1. So suppose

$f(x) = f(y) = (m,n)$ for some $x, y \in \bigcup_{s \in S} A_s$.

Then $x$ and $y$ are both in $A_m$, because $m$ is the smallest index such that $x \in A_m$ and $y \in A_m$. Applying the 1-1 function $f_m : A_m \longrightarrow \mathbb{N}$ to both $x$ and $y$ gives $f_m(x) = f_m(y) = n$, since $f_m$ is 1-1 we get $x = y$. Thus $f$ is 1-1. Therefore $\bigcup_{s \in S} A_s$ is countable.

Not all sets are countable. Two famous examples:

- $P(\mathbb{N})$, the set of all subsets of $\mathbb{N}$ is not countable (Exercise 37 proves this, to appear on Assl 2)
- $\mathbb{R}$ is not countable, to be proved in class in mid October.

To study $\mathbb{R}$, it's actually enough to study $(0,1)$, since:

Example: $\mathbb{R} \sim (0,1)$.

Proof: Define $f : (0,1) \longrightarrow \mathbb{R}$ by $f(x) = \tan\left(\pi x - \frac{\pi}{2}\right)$.

This is 1-1 and onto.

Challenge: Find a 1-1 onto function $f : (0,1) \longrightarrow \mathbb{R}$ without using trig.

Example of an uncountable set:

Let $X = \{\text{all functions } f: \mathbb{N} \longrightarrow \mathbb{N}\}$. Suppose $\phi: \mathbb{N} \longrightarrow X$ is any function, we'll show that $\phi$ cannot be surjective. Let $f_n: \mathbb{N} \longrightarrow \mathbb{N}$ denote the function $\phi(n)$. Build a new function

$$g: \mathbb{N} \longrightarrow \mathbb{N}$$

by defining $g(n) = f_n(n) + 1$ for all $n \in \mathbb{N}$.

Then $g \in X$, but $g$ is not in the image of $\phi$. It's not in the image of $\phi$ because:

Suppose it is. Then $g = f_k$ for some $k$. But when we plug $k$ into both sides, we get

$$g(k) = f_k(k)$$

which is false since we set $g(k) = f_k(k) + 1$. So $g \notin \operatorname{im} \phi$ and $X$ is uncountable.

MATH 2080

## §0.5 Real numbers

It is possible to start with nothing but the natural numbers $\mathbb{N}$, and from them describe $\mathbb{Z}$, then $\mathbb{Q}$, and finally $\mathbb{R}$. This approach to studying the real numbers is extremely difficutt (but interesting!) and is not how we shall approach the problem.

Instead, we will assume that there is a set denoted by $\mathbb{R}$, and functions

$$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \qquad \cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(x, y) \longmapsto x+y \qquad (x, y) \longmapsto x \cdot y$$

and a relation $< \subset \mathbb{R} \times \mathbb{R}$ that together obey twelve rules: (called axioms).

1. $(x+y)+z = x+(y+z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. $x+y = y+x$ and $x \cdot y = y \cdot x$
3. $x \cdot (y+z) = x \cdot y + x \cdot z$
4. There is exactly one element $0 \in \mathbb{R}$ such that $0 + x = x$ for all $x \in \mathbb{R}$
5. For every $x \in \mathbb{R}$ there is exactly one $y \in \mathbb{R}$ such that $x+y=0$, we write $-x$ for such an element

6. There is exactly one element $1 \in \mathbb{R}$ such that $x \cdot 1 = x$ for all $x \in \mathbb{R}$.

7. For each $x \in \mathbb{R}$ with $x \neq 0$ there exists a unique $y \in \mathbb{R}$ such that $x \cdot y = 1$, we denote such a $y$ by $1/x$. (or $x^{-1}$)

8. $x < y$ implies $x + z < y + z$

9. $x < y$ and $y < z$ implies $x < z$

10. For all $(x, y) \in \mathbb{R} \times \mathbb{R}$ exactly one of $x < y$, $y < x$ or $x = y$ is true

11. $x < y$ and $z > 0 \Rightarrow xz < yz$.

These 11 properties make $\mathbb{R}$ what is called an <u>ordered field</u>. But we want $\mathbb{R}$ to be special in some way, so we add a $12^{th}$ rule.

<u>Definition</u>: A set $S \subseteq \mathbb{R}$ is bounded from above (or below) if there is a number $M \in \mathbb{R}$ such that $x \leq M$ for all $x \in S$ (or $x \geq M$ for all $x \in S$).
The number $M$ is called an <u>upper bound</u> (or <u>lower bound</u>) in this case. If $S$ has an upper and lower bound, it's called a <u>bounded set</u>

Example: Any finite set $S \subseteq \mathbb{R}$ is bounded, because it has a biggest and smallest element, which we denote by $\max S$ and $\min S$.

Example: The set $(1, \infty)$ is not bounded, but it is bounded below. All of the elements of $(-\infty, 1]$ are lower bounds. Obviously $1$ is the "best" lower bound in some sense, though.

---

We introduce the idea of least upper bound and greatest lower bound to capture the idea of "best" upper and lower bounds.

Definition: Let $S \subseteq \mathbb{R}$. Then $a \in \mathbb{R}$ is a least upper bound for $S$ if it is an upper bound for $S$ and if $b$ is also an upper bound for $S$, then $a \leq b$. Similarly $a \in \mathbb{R}$ is a greatest lower bound for $S$ if it is a lower bound and if $b$ is also a lower bound for $S$ then $b \leq a$.

We abbreviate these terms as

$$a = \text{l.u.b.}\, S \quad \text{or} \quad a = \sup S \quad \text{(supremum)}$$

and

$$a = \text{g.l.b.}\, S \quad \text{or} \quad a = \inf S \quad \text{(infemum)}$$

respectively.

The $12^{th}$ property of $\mathbb{R}$ is then:

12. Every nonempty subset of $\mathbb{R}$ that is bounded above has a least upper bound.

This $12^{th}$ property distinguishes $\mathbb{R}$ from other "ordered fields". For example, properties 1 – 11 are true in $\mathbb{Q}$, but 12 is <u>not</u>. Let's prove this.

<u>Example</u>: The set

$$X = \{x \in \mathbb{Q} \mid x^2 < 2\} \subset \mathbb{Q}$$

has no least upper bound in $\mathbb{Q}$.

<u>Proof</u>: The proof in full detail is very long (e.g. a full class at least) but the idea/sketch is this:

First note $X$ is nonempty since $0 \in X$. Now suppose $\alpha \in \mathbb{Q}$ is a least upper bound for $X$. It is possible to show that we must have $\alpha^2 = 2$. The idea of the proof is to prove that $\alpha^2 > 2$ forces $\alpha$ to be too large (it's not a <u>least</u> upper bound any more) and $\alpha^2 < 2$ forces $\alpha$ to not be an upper bound. So $\alpha^2 = 2$.

But now we ask: Is there $\alpha \in \mathbb{Q}$ with $\alpha^2 = 2$? No, here is the proof:

Suppose we choose $p, q > 0$ with no common divisors and $2 = \left(\frac{p}{q}\right)^2$.

Then $2q^2 = p^2$, so $p^2$ is even and therefore $p$ is even (since $p$ odd implies $p^2$ odd). So write $p = 2r$ for some integer $r$. Then

$$2q^2 = (2r)^2 = 4r^2$$
$$\Rightarrow q^2 = 2r^2,$$

so $q$ is even, too. But we assumed $p$ and $q$ had no common divisors, a contradiction.

---

So property 12 distinguishes $\mathbb{R}$ from $\mathbb{Q}$, indeed it distinguishes $\mathbb{R}$ from <u>all other</u> ordered fields (making $\mathbb{R}$ unique).

Now from these 12 properties we can prove all properties of $\mathbb{R}$ that you're familiar with.

<u>Theorem</u>: Let $x, y, z \in \mathbb{R}$. Then:

(i) If $x < y$, then $-y < -x$.

(ii) $0 < 1$

(iii) If $0 < x < y$ then $0 < \frac{1}{y} < \frac{1}{x}$

(iv) If $x < y$ and $z < 0$ then $zx > zy$

(v) $x^2 \geq 0$ (for all $x \in \mathbb{R}$).