Lecture 11

Uniqueness

Definition: $\exists!$ means "There exists a unique".

Note: To prove uniqueness, we can do one of the following:

(i) Assume $\exists x, y \in S$ such that $P(x) \wedge P(y)$ is true and show $x = y$.

(ii) Argue by assuming that $\exists x, y \in S$ are distinct such that $P(x) \wedge P(y)$, then derive a contradiction.

To prove uniqueness and existence, we also need to show that $\exists x \in S$ such that $P(x)$ is true.

Example: Suppose $x \in \mathbb{R} - \mathbb{Z}$ and $m \in \mathbb{Z}$ such that $x < m < x + 1$. Show that m is unique.

Proof: Assume that $\exists m, n \in \mathbb{Z}$ such that

$$x < m < x + 1 \qquad \text{and} \qquad x < n < x + 1$$

Look at the value $m - n$. This value is largest when m is largest and n is smallest. Since $m < x + 1$ and $n > x$, we see that $m - n < 1$. Further, for this to be minimal, we could flip the roles of m and n above to see that $-1 < m - n$. Thus $-1 < m - n < 1$ and $m - n \in \mathbb{Z}$. Hence $m - n = 0$, that is $m = n$.

Handout or Document Camera or Class Exercise

Let $f(x)$ be the function defined by

$$\begin{aligned} f : (0, \infty) &\to (0, \infty) \\ x &\mapsto x^2. \end{aligned}$$

Prove for all $y \in (0, \infty)$ there exists a unique $x \in (0, \infty)$ such that $f(x) = y$

Instructor's Comments: Some things to note: This is the first time students will realize that in order to properly define a function, a function has a domain and codomain that are given. Note that the range is the set of all values the domain maps into. The codomain might actually be larger than the range. They have not seen this notation before so you'll be wise to explain to them that this is the same as $f(x) = x^2$.

Proof: Existence. For each $y \in (0, \infty)$, let $x = \sqrt{y}$. Then

$$f(x) = f(\sqrt{y}) = (\sqrt{y})^2 = y$$

Uniqueness. Suppose that there exists $a, b \in (0, \infty)$ such that

$$\begin{aligned} f(a) &= f(b) \\ a^2 &= b^2 \\ |a| &= |b| \end{aligned}$$

and since $a, b > 0$, we have that $a = b$. ∎

Instructor's Comments: Use this as a lead in to Injections and Surjections. This is the 15 minute mark.

Injections and Surjections

Definition: Let S and T be sets. A function $f : S \to T$ is said to be

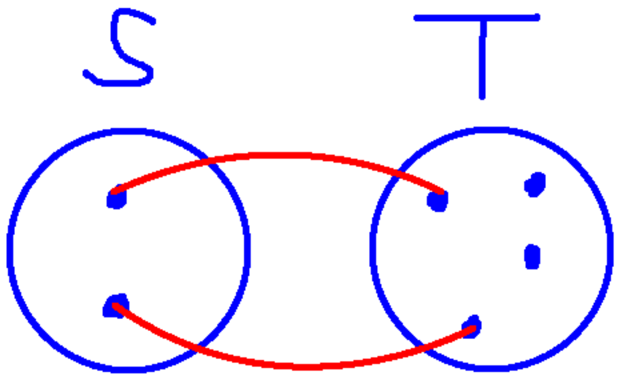
(i) Injective (or one to one or $1:1$) if and only if

$$\forall x, y \in S, f(x) = f(y) \Rightarrow x = y.$$

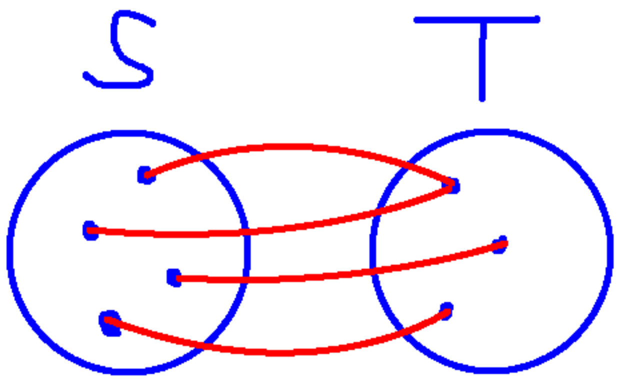
(ii) Surjective (or onto) if and only if

$$\forall y \in T \; \exists x \in S \text{ such that } f(x) = y$$

Example: A function that is one to one but not onto:



Example: A function that is onto but not one to one:



Example: Prove

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

is not injective.

Proof: Notice that

$$f(-1) = (-1)^2 = 1 = (1)^2 = f(1)$$

but $-1 \neq 1$. ■

Instructor's Comments: Emphasize that this is the negation of the definition above. Disproving a for all means finding a counter example.

Example: Prove

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto 2x^3 + 1 \end{aligned}$$

is one to one.

Proof: Let $x, y \in \mathbb{R}$ such that $f(x) = f(y)$. Then

$$\begin{aligned} 2x^3 + 1 &= 2y^3 + 1 \\ x^3 &= y^3 \\ \sqrt[3]{x^3} &= \sqrt[3]{y^3} \\ x &= y \end{aligned}$$

Thus f is injective. ■

Example: Prove

$$\begin{aligned} f : \mathbb{R} &\to (-\infty, 1) \\ x &\mapsto 1 - e^{-x} \end{aligned}$$

is onto.

Proof: We need to show that every $y \in (-\infty, 1)$ has some $x \in \mathbb{R}$ with $f(x) = y$.

Discovery:

$$\begin{aligned} 1 - e^{-x} &= y \\ e^{-x} &= 1 - y \\ -x &= \ln(1 - y) \\ x &= -\ln(1 - y) \end{aligned}$$

Formal proof: Take $x = -\ln(1 - y)$ for any $y \in (-\infty, 1)$. Notice that this is well defined since $\ln(1 - y)$ is defined on $(-\infty, 1)$. Then

$$\begin{aligned} f(x) &= 1 - e^{-x} \\ &= 1 - e^{-(-\ln(1-y))} \\ &= 1 - e^{\ln(1-y)} \\ &= 1 - (1 - y) \\ &= y \end{aligned}$$

Therefore, f is an onto function. ■

Instructor's Comments: This is the 35-40 minute mark.

Division Algorithm

This is just like grade school division. For example, $51/7$ can be written as:

$$51 = 7(7) + 2$$

where $a = 51$, $b = 7$, $q = 7$ and $r = 2$. Similarly, $-35/6$ can be written as

$$-35 = 6(-6) + 1$$

where $a = -35$, $b = 6$, $q = -6$, and $r = 1$.

Handout or Document Camera or Class Exercise

Theorem: (Division Algorithm) Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then $\exists! q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b$.

Proof: Existence: Use the Well Ordering Principle on the set

$$S = \{a - bq : a - bq \geq 0 \wedge q \in \mathbb{Z}\}$$

Uniqueness:

Suppose that $a = q_1 b + r_1$ with $0 \leq r_1 < b$. Also, suppose that $a = q_2 b + r_2$ with $0 \leq r_2 < b$ and $r_1 \neq r_2$. Without loss of generality, we can assume $r_1 < r_2$.

Instructor's Comments: Introduce the acronym WLOG. Explain that if two integers are not equal, then one must be bigger than the other and the proof is symmetric depending if $r_1 < r_2$ or $r_2 < r_1$

Then $0 < r_2 - r_1 < b$ and $(q_1 - q_2)b = r_2 - r_1$.

Instructor's Comments: Take the difference of the two a values. Given that $0 \leq r_1, r_2 < b$, the biggest value of $r_2 - r_1$ is b.

Hence $b \mid (r_2 - r_1)$. By Bounds By Divisibility, $b \leq r_2 - r_1$ which contradicts the fact that $r_2 - r_1 < b$.

Instructor's Comments: This is a contradiction. Notice that we don't need $|b|$ as in (BBD) since $b \in \mathbb{N}$.

Therefore, the assumption that $r_1 \neq r_2$ is false and in fact $r_1 = r_2$. But then $(q_1 - q_2)b = r_2 - r_1$ implies $q_1 = q_2$.

Instructor's Comments: This is the 50 minute mark. Note you could leave the division algorithm for extra reading if you'd like and replace it by an example with a negative number. If you have time, I'd recommend digesting the Division algorithm proof carefully. If you're really ahead try the following: Define a line to be the set of points (x, y) satisfying $y = mx + b$ for some $m, b \in \mathbb{R}$. Show that if two lines have distinct slopes (m values) and that they intersect, then this solution is unique.