Lecture 13: Bijections

Sunday, November 13, 2016 8:03 PM

In the previous lecture we proved:

Theorem. Suppose $f: X \to Y$ is a function. Then

(1) f has a left-inverse $\iff$ f is injective.

(2) f has a right-inverse $\iff$ f is surjective.

We also showed

Lemma. If g is a left inverse of $f: X \to Y$ and h is a right inverse of f, then $g = h$.

Theorem. Suppose $f: X \to Y$ is a function. Then

f is bijective $\iff$ there exists $g: Y \to X$ such that

$g \circ f = I_X$ (a left-inverse) and

$f \circ g = I_Y$ (a right-inverse).

Moreover, there is a unique function g which is both a left-inverse and a right-inverse of f. (Such a function $g: Y \to X$ is called the inverse of f, and it is denoted by $f^{(-1)}$.)

(A function that has an inverse is called an invertible function.)

Proof. ($\Rightarrow$) We have to prove two things ① existence of such a function

Lecture 13: Bijections

Sunday, November 13, 2016 10:43 PM

② uniqueness of such a function.

① Existence. f: bijective $\Rightarrow$ f: injective $\overset{\text{by the previous theorem}}{\Rightarrow}$ f has a left-inverse g.

f: bijective $\Rightarrow$ f: surjective $\overset{\text{by the previous theorem}}{\Rightarrow}$ f has a right-inverse h.

Hence by the previous lemma, $g=h$. Hence $g\circ f=I_X$ and $f\circ g=I_Y$.

② Uniqueness. Suppose both $g_1, g_2: Y\to X$ satisfy the above conditions. So g_1 is a left inverse of f and g_2 is a right inverse of f. Hence, by the above lemma, $g_1=g_2$, which shows the uniqueness of such function. ■

Theorem (a) If f is invertible, then $f^{(-1)}$ is invertible and $(f^{(-1)})^{(-1)}=f$.

(b) If $X\xrightarrow{f}Y$ and $Y\xrightarrow{g}Z$ are invertible, then $g\circ f$ is invertible; moreover $(g\circ f)^{(-1)}=f^{(-1)}\circ g^{(-1)}$.

Proof. (a) By the definition of the inverse function $f^{(-1)}$, we have $f^{(-1)}\circ f=I_X$ and $f\circ f^{(-1)}=I_Y$. Hence f is the inverse of $f^{(-1)}$, which means $(f^{(-1)})^{(-1)}=f$.

(b) We show that $(g\circ f)\circ(f^{(-1)}\circ g^{(-1)})=I_Z$

and $(f^{(-1)}\circ g^{(-1)})\circ(g\circ f)=I_X$.

This implies that $g\circ f$ has an inverse and

$$(g\circ f)^{(-1)}=f^{(-1)}\circ g^{(-1)}.$$

Lecture 13: Bijection

Sunday, November 13, 2016 10:44 PM

$$(g\circ f)\circ(f^{(-1)}\circ g^{(-1)}) = g\circ I_Y\circ g^{(-1)} = g\circ g^{(-1)} = I_Z$$

$$(f^{(-1)}\circ g^{(-1)})\circ(g\circ f) = f^{(-1)}\circ I_Y\circ f = f^{(-1)}\circ f = I_X. \blacksquare$$

. Notice that f is invertible $\iff$ f is bijective.

Definition Two sets A and B are called **equipotent sets**, and we write $A\sim B$ if there is a bijection $f: A\to B$.

Lemma. For every non-empty sets A, B, and C, we have

1. $A\sim A$. (reflexive)
2. $A\sim B \Rightarrow B\sim A$. (symmetric)
3. $A\sim B$, $B\sim C \Rightarrow A\sim C$. (transitive)

(1, 2, 3: equivalent)

Proof 1. $I_A: A\to A$ is a bijection.

2. If $A \xrightarrow{f} B$ is a bijection, then $B \xrightarrow{f^{(-1)}} A$ is a bijection.

3. If $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ are bijections, then $A \xrightarrow{g\circ f} C$ is a bijection. $\blacksquare$

Based on our intuition of cardinality of finite sets we have:

Theorem. Suppose A and B are two non-empty finite sets.

Then $A\sim B \iff |A| = |B|$.

In fact a bit stronger result is true:

Lecture 13: Pigeonhole principle

Sunday, November 13, 2016 10:55 PM

Theorem. Suppose X and Y are non-empty finite sets and $X \xrightarrow{f} Y$ is a function. Then

$$f \text{ is injective} \implies |X| \leq |Y|.$$

The contra-positive of the above theorem is called the pigeonhole principle.

$$|X| > |Y| \implies \exists\, x_1, x_2 \in X,\ x_1 \neq x_2 \wedge f(x_1) = f(x_2).$$

Alternatively: If there are n pigeons, m pigeonholes and $n > m$, then at least two pigeons share a pigeonhole.

The pigeonhole principle has many unexpected applications. Here are two examples that I encourage you to think about.

Exercise. Suppose $n \in \mathbb{Z}^+$. Prove that there exists a multiple of n whose decimal digits are either 0 or 1.

(**Hint**. Consider the remainders of $1, 11, 111, \ldots, \underbrace{11\cdots1}_{n+1}$ divided by n, use the pigeonhole principle to deduce that two of these remainders are the same. Look at their difference.)

Lecture 13: Enumerable and countable

Sunday, November 13, 2016 11:13 PM

Exercise. Suppose P_1, P_2, P_3, P_4, and P_5 are five points in a unit square. Prove that there exist $i \neq j$ such that $P_i P_j \geq \frac{1}{\sqrt{2}}$.

(Hint. Divide the unit square into four equal subsquares  . Use the pigeonhole principle and deduce that at least two points are in the same smaller square.)

Using the pigeonhole principle, one can see that there is no surjective function from a proper subset A of a finite set B to B.

Q What if B is NOT finite?

Ex. (Hilbert's hotel) $\mathbb{Z}^+ \sim \mathbb{Z}^{\geq 0}$.

(In Hilbert's hotel, we have room 1, room 2, ... (infinitely many rooms). All of them are occupied. Let's say guest number i is in the i^{th} room. A new guest arrives; let's call her guest number 0. Can we make a room available for her?)

Proof. We have to construct a bijection $f: \mathbb{Z}^+ \to \mathbb{Z}^{\geq 0}$.

Let $f(k) = k-1$ for every $k \in \mathbb{Z}^+$. Let $g: \mathbb{Z}^{\geq 0} \to \mathbb{Z}^+$, $g(k) = k+1$ for every $k \in \mathbb{Z}^{\geq 0}$. Then one can check that $f \circ g = I_{\mathbb{Z}^{\geq 0}}$ and $g \circ f = I_{\mathbb{Z}^+}$.

Lecture 13: Enumerable and countable

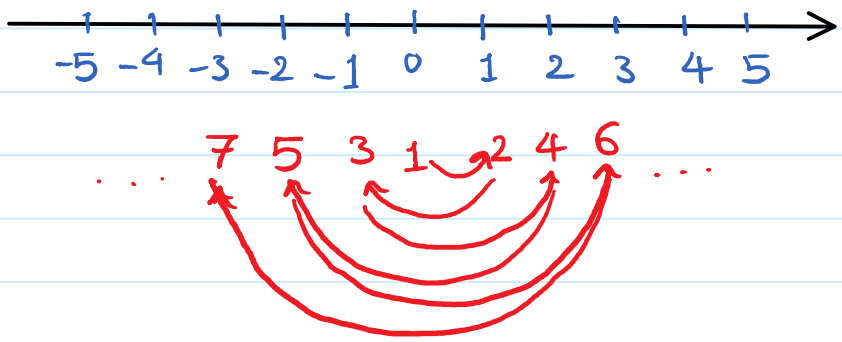
Sunday, November 13, 2016 11:46 PM

Definition. A set X is called **enumerable** if $\mathbb{Z}^+ \sim X$.

A set X is called **countable** if X is either finite or it is enumerable.

Ex. $\mathbb{Z}$ is enumerable.

Proof. "We have to enumerate elements of $\mathbb{Z}$."



This picture suggests the following functions:

$$f: \mathbb{Z}^+ \to \mathbb{Z}, \quad f(n) = \begin{cases} -k & \text{if } n = 2k+1, \\ k & \text{if } n = 2k. \end{cases}$$

and

$$g: \mathbb{Z} \to \mathbb{Z}^+, \quad g(n) = \begin{cases} 2n & n > 0, \\ -2n+1 & n \le 0. \end{cases}$$

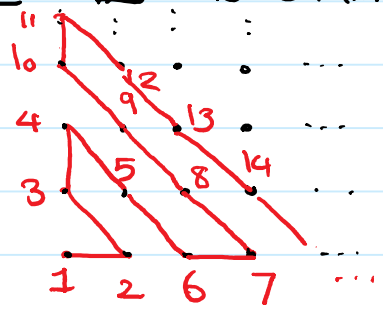
Check that f is well-defined and f is an inverse of g. ∎

Though writing the details of the above proof might be a bit tricky, the whole idea is in the mentioned "labeling" or "enumerating" of elements of $\mathbb{Z}$:

To show a set A is enumerable it is enough to present a method of labelling A's elements by numbers $1, 2, 3, \dots$ in a way that for sure all the elements of A get labelled at some point. (and only once).

Ex. $\mathbb{Z}^+ \times \mathbb{Z}^+$ is enumerable.

Proof.



Clearly this red path passes through all the points of $\mathbb{Z}^+ \times \mathbb{Z}^+$ once and exactly once. So we get a bijection between $\mathbb{Z}^+ \times \mathbb{Z}^+$ and $\mathbb{Z}^+$. ■

Lemma. $(A_1 \sim A_2 \text{ and } B_1 \sim B_2) \Rightarrow A_1 \times B_1 \sim A_2 \times B_2$ for every non-empty sets A_1, A_2, B_1, and B_2.

Lecture 13: Enumerable and countable sets

Monday, November 14, 2016 10:53 PM

Proof. $A_1 \sim A_2 \Rightarrow \exists\ A_1 \xrightarrow{f} A_2$ which is bijective, and

$B_1 \sim B_2 \Rightarrow \exists\ B_1 \xrightarrow{g} B_2$ which is bijective.

Let $A_1 \times B_1 \xrightarrow{h} A_2 \times B_2$, $h(a_1, b_1) = (f(a_1), g(b_1))$. Since f and g are bijective, they have inverses $f^{(-1)}$ and $g^{(-1)}$. Now let $A_2 \times B_2 \xrightarrow{h'} A_1 \times B_1$. $h'(a_2, b_2) = (f^{(-1)}(a_2), g^{(-1)}(b_2))$.

Then $(h \circ h')(a_2, b_2) = h(f^{(-1)}(a_2), g^{(-1)}(b_2))$

$= (f(f^{(-1)}(a_2)), g(g^{(-1)}(b_2)))$

$= (a_2, b_2)$,

and similarly you can see $(h' \circ h)(a_1, b_1) = (a_1, b_1)$. So h' is an inverse of h. Hence h is a bijection, which implies

$$A_1 \times B_1 \sim A_2 \times B_2. \quad \blacksquare$$

Corollary If A and B are enumerable, then $A \times B$ is enumerable.

Proof A and B are enumerable $\Rightarrow \left\{ \begin{array}{l} A \sim \mathbb{Z}^+ \\ B \sim \mathbb{Z}^+ \end{array} \right\} \Rightarrow A \times B \sim \mathbb{Z}^+ \times \mathbb{Z}^+$ (by Lemma).

$\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. So $A \times B \sim \mathbb{Z}^+$, and so $A \times B$ is enumerable. $\blacksquare$

Lecture 13: The concept of cardinality

Friday, November 18, 2016 3:31 PM

Definition. Cardinality of A, denoted by $|A|$, is a concept such that $|A| = |B|$ exactly when $A \sim B$.

• The same way that you got positive integers as an abstraction of enumerating objects: getting an abstract concept 3 instead of 3 apples, 3 books, etc.

Def. Cardinality of $\mathbb{Z}^+$ is denoted by the hebrew letter $\aleph_0$ (aleph). So we write $\mathbb{Z}^+ = \aleph_0$.

So A is enumerable $\iff |A| = \aleph_0$, and A is countable $\iff$ either $|A| < \infty$ or $|A| = \aleph_0$.

We have seen that $|\mathbb{Z}^+ \times \mathbb{Z}^+| = |\mathbb{Z}| = \aleph_0$, and

if $|A| = |B| = \aleph_0$, then $|A \times B| = \aleph_0$.

Q Is there any uncountable set?

The following result due to Cantor gives us an affirmative answer to this question.

Lecture 13: Cantor's theorem

Monday, November 14, 2016 11:07 PM

Theorem. For every non-empty set X, there is NO surjection $f: X \to \mathcal{P}(X)$, where $\mathcal{P}(X)$ is the power set of X.

Corollary. $\mathcal{P}(\mathbb{Z}^+)$ is uncountable.

Proof of corollary. For every $n \in \mathbb{Z}^+$, $\{n\} \in \mathcal{P}(\mathbb{Z}^+)$. So $\mathcal{P}(\mathbb{Z}^+)$ is not finite. By Cantor's theorem there is no bijection from $\mathbb{Z}^+$ to $\mathcal{P}(\mathbb{Z}^+)$. So $\mathcal{P}(\mathbb{Z}^+)$ is NOT enumerable.

Therefore $\mathcal{P}(\mathbb{Z}^+)$ is NOT enumerable. ■

Proof of Theorem. Suppose to the contrary that there is a surjection $f: X \to \mathcal{P}(X)$. Let

$$A = \{ x \in X \mid x \notin f(x) \}$$

Since f is surjective, $\exists x_0 \in X$, $f(x_0) = A$.

Case 1. $x_0 \in A$. Then $x_0 \notin f(x_0) = A$ which is a contradiction.

Case 2. $x_0 \notin A$. Then $x_0 \in f(x_0) = A$ which is a contradiction. ■

Remark. The idea of the proof is similar to Russel's paradox.

Lecture 13: Continuum hypothesis

Friday, November 18, 2016 3:59 PM

Q Is there a set A such that $|\mathbb{Z}^+| < |A| < |P(\mathbb{Z}^+)|$?

This means A is uncountable, there is an injective function $f: A \to P(\mathbb{Z}^+)$, but there is bijection from A to $P(\mathbb{Z}^+)$.

P. Cohen proved that it is undecidable, which means both this statement and its negation are compatible with the axioms of set theory. Continuum hypothesis asserts that such set does NOT exist.

Next we show that the set $\mathbb{R}$ of real numbers is uncountable.

In fact, we show that there is no surjective function

$$f: \mathbb{Z}^+ \to \mathbb{R}.$$

We use an argument that is known as Cantor's diagonal argument.

Lecture 13: Cantor's diagonal argument

Tuesday, November 15, 2016 12:15 AM

This proof is based on the following property of real numbers that we accept without proof:

Lemma Every real number x has a unique representation of the form: $x = n + 0.d_1 d_2 \cdots$ where $n, d_i \in \mathbb{Z}$, $0 \le d_i \le 9$, and d_i's are NOT exentually all 9's.

Remark. The last condition is necessary in order to get uniqueness: $0.99\cdots = 1$.

Theorem. There is no surjection $\mathbb{Z}^+ \xrightarrow{f} \mathbb{R}$.

Proof. Let $f: \mathbb{Z}^+ \to \mathbb{R}$ be a function. We will find a real number which is not in the image of f. To get such number, we use the representations of $f(n)$'s as described in the above lemma:

$f(1) = m_1 + 0.a_{11}\, a_{12}\, a_{13}\cdots$

$f(2) = m_2 + 0.a_{21}\, a_{22}\, a_{23}\cdots$

$f(3) = m_3 + 0.a_{31}\, a_{32}\, a_{33}\cdots$

$\vdots \quad \vdots \quad \vdots$

To get a real number which is not in the image of f, we have to give a real number which is different from all

of these numbers $f(1), f(2), \cdots$. It is enough to write the decimal representation of a number which is different from each of the above ones at least in one digit.

Cantor's idea is to look at the diagonal digits and change them.

Let $d_i = \begin{cases} 0 & \text{if } a_{ii} \neq 0 \\ 1 & \text{if } a_{ii} = 0 \end{cases}$. In particular, $d_i \neq a_{ii}$ (and $d_i \neq 9$.)

Claim The real number $0.d_1 d_2 \cdots$ is NOT in the image of f.

Proof of claim. Suppose to the contrary that

$$f(n) = 0.d_1 d_2 \cdots$$

So $m_n + 0.a_{n1} a_{n2} \cdots = 0.d_1 d_2 \cdots$; in particular we should have $a_{nn} = d_n$ which is a contradiction.

Hence $\mathrm{Im}(f) \neq \mathbb{R}$, which means f is NOT surjective. ■