Lecture 3: Equivalent forms of an implication

Wednesday, September 28, 2016 9:15 AM

Most of statements in mathematics are of form of conditional propositions also known as implications.

P implies Q.

If P, then Q.

P is sufficient for Q.

Q is necessary for P.

They are denoted by

$P \Rightarrow Q$

We have seen its truth table

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

<u>Ex.</u> $P \Rightarrow Q \equiv (\neg P) \vee Q$

either (the hypothesis does NOT hold)

or (the conclusion should hold.)

<u>Proof.</u>

P	Q	$P \Rightarrow Q$	$\neg P$	$(\neg P) \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

are the same.

<u>Ex.</u> (Contra-positive) $P \Rightarrow Q \equiv (\neg Q) \Rightarrow (\neg P)$

Lecture 3: Implications and proof by contradiction

Wednesday, September 28, 2016 9:32 AM

Proof. You can use truth table to show this, but I prefer this method:

$$P \Rightarrow Q \equiv (\neg P) \vee Q \quad \text{(because of previous example)}$$

$$\equiv Q \vee (\neg P)$$

$$\equiv (\neg Q) \Rightarrow (\neg P) \quad \text{(again because of previous example)} \blacksquare$$

Ex. (Proof by contradiction)

$$P \Rightarrow Q \equiv (P \wedge (\neg Q)) \Rightarrow \perp$$

(you assume hypothesis holds, but the conclusion does NOT, and reach to a conclusion.)

Proof. Again you can use truth table to check this, but I prefer this:

As we have seen in the previous lecture for any proposition R, we have $R \equiv (\neg R) \Rightarrow \perp$. So

$$P \Rightarrow Q \equiv (\neg (P \Rightarrow Q)) \Rightarrow \perp$$

$$\equiv (\neg (\neg P \vee Q)) \Rightarrow \perp \quad \text{(by the 1}^{\text{st}}\text{ example)}$$

$$\equiv ((\neg (\neg P)) \wedge (\neg Q)) \Rightarrow \perp \quad \text{(by de Morgan's law)}$$

$$\equiv (P \wedge (\neg Q)) \Rightarrow \perp . \blacksquare$$

Lecture 3: Divisibility

Wednesday, September 28, 2016 9:42 AM

<u>Definition</u>. Suppose m and n are two integers. We say <u>m divides n</u> if, for some integer k,

$$n = mk.$$

In this case we also say <u>n is a multiple of m</u>. And it is denoted by $m \mid n$.

<u>Basic Properties of divisibility</u>.

- For any integer n, $1 \mid n$.

  <u>Proof</u>. Since $n = 1 \times n$ and n is an integer, n is a multiple of 1. ■

- For any integer n, $n \mid 0$.

  <u>Proof</u>. Since $0 = n \times 0$ and 0 is an integer, 0 is a multiple of n. ■

<u>Lemma</u>. Suppose a and b are integers.

$$(b \neq 0 \wedge a \mid b) \Longrightarrow |a| \leq |b|.$$

<u>Proof</u>. Since $a \mid b$, for some integer k we have $b = ak$.

Lecture 3: Divisibility and backward argument

Wednesday, September 28, 2016 10:43 PM

Claim $k \neq 0$.

Proof of claim. Suppose to the contrary that $k = 0$.

Then $b = ak = a \times 0 = 0$, which contradics our assumption that $b \neq 0$. ■

Since $k \neq 0$, $|k| > 0$. Since k is integer, we have $|k| \geq 1$. Hence $|k|\,|a| \geq |a|$.

Therefore $|a| \leq |k|\,|a| = |ka| = |b|$. ■

How did we know that we need to show $k \neq 0$?

Whenever you want to prove an implication, it is useful to write down what your hypothesis is and what your goal is. Then start moving forward in the hypothesis side and backward in the goal side.

Lecture 3: Backward argument

Wednesday, September 28, 2016 10:53 PM

Hypothesis

$b \neq 0 \wedge a \mid b$

$\Downarrow$

$b \neq 0 \wedge b = ak$

for some integer k

forward.

?

Goal

$|a| \leq |b|$

$\Uparrow$

$|a| \leq |ak|$

$\Uparrow$

$|a| \leq |a||k|$

$\Uparrow$

$1 \leq |k|$

$\Uparrow$

$k \neq 0 \wedge k \in \mathbb{Z}$

the other direction is NOT correct.

backward.