Discrete Math

Lecture 19

Proofs by Contradiction

Proof by Contradiction Outline

Proposition. $P \Rightarrow Q$

Proof. (By Contradiction)

(First Step) Suppose the entire proposition is false
In other words, assume $\neg(P \Rightarrow Q) = P \wedge \neg Q$

(Intermediate Steps) Use facts and definitions about both P and $\neg Q$ to find a contradiction – *any* contradiction.

⋮

(Last Step) End the proof once a contradiction is established. $\Rightarrow\Leftarrow$

We never know which contradiction we're looking for!

Proposition $\sqrt{2} \notin \mathbb{Q}$

note: this claim "feels" difficult
$\forall\, a,b \in \mathbb{Z}\ (b \neq 0),\ \sqrt{2} \neq \frac{a}{b}$

2nd note: there are direct proofs, but they require more ideas/concepts (e.g. continued fractions)

Proposition If $x^2 = 2$, then $x \notin \mathbb{Q}$.

Proof (by contradiction) Suppose $x^2 = 2$ and $x \in \mathbb{Q}$.

This means $x = a/b$ where $a, b \in \mathbb{Z}$ and $b \neq 0$.

It follows that $2 = x^2 = (a/b)^2 = a^2/b^2$, which can be rewritten as $2b^2 = a^2$.

This equation tells us that a^2 is even.

$\boxed{a^2 \text{ being even implies } a \text{ is even.}}$

This means $a = 2m$, where $m \in \mathbb{Z}$.

Plugging this into our equation and simplifying yields

$$2b^2 = (2m)^2 = 4m^2$$

$$b^2 = 2m^2$$

This tells us b^2 is even, and so b is even.

Since both numerator, a, and denominator, b, are always divisible by 2, the fraction $x = \frac{a}{b}$ can NEVER be reduced $\Rightarrow\Leftarrow$

ex: Book of Proof, ch. 6

8. Suppose $a, b, c \in \mathbb{Z}$. If $\underline{a^2 + b^2 = c^2}$, then a or b is even.

Proof (by contradiction).

Assume $a^2+b^2=c^2$ and a is odd and b is odd.

Case 1 c is odd. It follows that c^2 is odd.

Similarly, since a + b are odd, a^2 + b^2 are odd.

Because the sum of two odd numbers is even, it follows that $c^2=a^2+b^2$ is even, and so c^2 is both even and odd (which is a contradiction).

Case 2 c is even. This means $c=2m$ for some $m \in \mathbb{Z}$. a, b being odd means $a=2n+1$, $b=2k+1$ for some $n, k \in \mathbb{Z}$.

The equation $a^2+b^2=c^2$ becomes

$$4n^2+4n + 4k^2+4k+2 = 4m^2$$

which can be rewritten as

$$4n^2+4n + 4k^2+4k - 4m^2 = -2$$

$$4(n^2+n+k^2+k-m^2) = -2$$

The integer on the left side is divisible by 4.

However, -2 is not divisible by 4.

This is a contradiction: $4 \mid (-2)$ and $4 \nmid (-2)$.

$\Rightarrow\Leftarrow$

Proof by Contradiction Outline (general)

Proposition. S

Proof. (By Contradiction)

(First Step) Suppose the entire proposition is false
In other words, assume $\neg S$

(Intermediate Steps) Use facts and definitions about $\neg S$
to find a contradiction – *any* contradiction.

⋮

(Last Step) End the proof once a contradiction is established. $\Rightarrow\Leftarrow$

$\left.\begin{array}{l}\text{Direct Proof}\\ \text{Contra. Pos. Proof}\end{array}\right\}$ are for $P \Rightarrow Q$

Proof By $\Rightarrow\Leftarrow$ ← for $P \Rightarrow Q$ & others!