CSE 16   7-5-23

1.7 Introduction to Proofs

Definitions

- We say $n \in \mathbb{Z}$ is <u>even</u> iff there exists $k \in \mathbb{Z}$ such that $n = 2k$.

$$\exists k : n = 2k \qquad (n \text{ free})$$

Even(n)

- We say $n \in \mathbb{Z}$ is <u>odd</u> iff there exists $k \in \mathbb{Z}$ such that $n = 2k+1$

$$\exists k : n = 2k+1 \qquad (n \text{ free})$$

Odd(n)

<u>note</u>: every $n \in \mathbb{Z}$ is either even or odd, but not both. (Proof later).

- We say $d \in \mathbb{Z}$ $(d \neq 0)$ <u>divides</u> $n \in \mathbb{Z}$ iff there exists $k \in \mathbb{Z}$ s.t. $n = kd$.

$$(d \neq 0) \wedge (\exists k : n = kd) \qquad (n, d \text{ free})$$

Divides(n,d)

<u>notation</u>: $d \mid n$, <u>read</u>: 'd divides n'

- We say $x \in \mathbb{R}$ is <u>rational</u> iff there exists $p, q \in \mathbb{Z}$ $(q \neq 0)$ s.t. $x = \frac{p}{q}$.

$$\exists p \, \exists q : (q \neq 0) \wedge x = \frac{p}{q} \qquad (x \text{ free})$$

What is a Proof?

A finite sequence of propositions, starting with the <u>hypothesis</u>, ending with a <u>conclusion</u>, in which each proposition follows from previous ones by some inference rule (i.e. tautology), or a previously proved fact.

<u>Direct Proof of $p \to q$</u>

Assume p is true, prove (as above) that q is true.

Ex. (direct)

show for any $n, m \in \mathbb{Z}$, if both n and m are even, then $n \cdot m$ is even.

$$\forall n \forall m : \underbrace{\text{Even}(n) \land \text{Even}(m)}_{p} \rightarrow \underbrace{\text{Even}(n \cdot m)}_{q}$$

Proof.

Let $n, m \in \mathbb{Z}$. Assume both n and m are even. Then there exist $k_1 \in \mathbb{Z}$, and $k_2 \in \mathbb{Z}$ s.t.

$$n = 2k_1 \quad \text{and} \quad m = 2k_2 .$$

Thus

$$n \cdot m = (2k_1)(2k_2) = 2(2k_1 k_2) .$$

Since $2k_1k_2 \in \mathbb{Z}$, we have nm is even also. ∎

Exercise

Prove each row

n	m	$n+m$	$n \cdot m$
odd	odd	even	odd
odd	even	odd	even
even	odd	odd	even
even	even	even	even ✓

Ex (direct)

If $n \in \mathbb{Z}$ is even, then n^2 is even.

$$\forall n : \text{Even}(n) \longrightarrow \text{Even}(n^2)$$

Proof.

Let $n \in \mathbb{Z}$ and assume n is even.
Let $m = n$ in the previous theorem.
It follows that $n^2 = m \cdot n$ is also even. ∎

Indirect Proof of $p \to q$ (contraposition)

Prove (directly) the contrapositive stmt $\neg q \to \neg p$. Why is this valid?

Because $p \to q \equiv \neg q \to \neg p$.

Ex. $\forall n :$ Odd$(n^2) \to$ Odd(n)

Proof.

Let $n \in \mathbb{Z}$. We prove

$$\neg \text{Odd}(n) \to \neg \text{Odd}(n^2).$$

Recall not odd $\equiv$ even. So we prove

$$\text{Even}(n) \to \text{Even}(n^2).$$

But this was previously proved. ∎

Ex. (contraposition)

$$\forall n: \text{Even}(n^2) \rightarrow \text{Even}(n).$$

Proof.

Let $n \in \mathbb{Z}$. We prove that if n is odd, then n^2 is also odd.

Assume n is odd. Then

$$n = 2k+1$$

for some $k \in \mathbb{Z}$. Therefore

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$
$$= 2(2k^2+2k)+1.$$

Since $2k^2+2k \in \mathbb{Z}$, we have n^2 is odd. $\blacksquare$

<u>Note</u>: we've shown

$$\forall n: \text{Even}(n) \leftrightarrow \text{Even}(n^2).$$

<u>Exercise</u>: $\forall n: \text{Odd}(5n+4) \rightarrow \text{Odd}(n)$

Prove indirectly.

<u>Ex.</u> (direct)

For all $x, y \in \mathbb{R}$, if x and y are rational, then $x+y$ is also rational.

<u>Proof.</u>

Let $x, y \in \mathbb{R}$. Assume x, y are rational. Then

$$x = \frac{a}{b} \quad \text{and} \quad y = \frac{c}{d}$$

for some $a, b, c, d \in \mathbb{Z}$ with $b \neq 0$, $d \neq 0$.

Then

$$x+y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

Since $ad+bc$, $bd \in \mathbb{Z}$, and since $bd \neq 0$ (since neither $b=0$ nor $d=0$), we have $x+y$ is rational. ∎

Exercise

let $x, y \in \mathbb{R}$ be rational, show

(1) $x-y$ is rational

(2) $x \cdot y$ is rational

(3) $\frac{x}{y}$ (where $y \neq 0$) is rational.

Notation

$\mathbb{Q} = \{\text{rational numbers}\}$

$\mathbb{R} - \mathbb{Q} = \{\text{irrational numbers}\}$.

Proof by Contradiction

To prove p by contradiction, we prove $\neg p \to q$, where q is a contradiction. Usually q is of the form: $q = r \vee \neg r$.

Why is this valid? Because

$$\neg p \to F \equiv p \quad \checkmark$$

Check:

p	$\neg p$	F	$\neg p \to F$
0	1	0	0
1	0	0	1

Ex. show that $\sqrt{2}$ is irrational.

Proof (contradiction)

Assume $\sqrt{2}$ is rational. Then there exist $a, b \in \mathbb{Z}$ $(b \neq 0)$ s.t.

$$\sqrt{2} = \frac{a}{b}.$$

If a, b have any common factors we may cancel them. Suppose that's already done, so in particular:

$*$ a and b are not both even.

Then from $\frac{a}{b} = \sqrt{2}$, we get

$$\frac{a^2}{b^2} = 2$$

$\therefore \quad a^2 = 2b^2$

$\therefore \quad a^2$ is even

$\therefore \quad \underline{a \text{ is even}}$ (Previous Proof.)

$\therefore \quad a = 2k$ for some $k \in \mathbb{Z}$.

Thus

$$4k^2 = a^2 = 2b^2$$

$\therefore \quad b^2 = 2k^2$

$\therefore \quad b^2$ is even

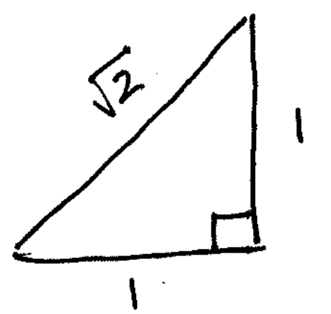
$\therefore \quad \underline{b \text{ is even}}$

Therefore

** both a and b are even

This contradiction shows our assumption was false, hence

$$\sqrt{2} \notin \mathbb{Q} \qquad \blacksquare$$



Fact (proof later, ch4)

for any $n \in \mathbb{Z}$, exactly one of the following is true

- $n = 3k$ $\}$ $3 \mid n$
- $n = 3k+1$
- $n = 3k+2$ $\Big\}$ $3 \nmid n$

for some $k \in \mathbb{Z}$.

Exercise

(1) show $3 \mid n$ $\overset{\longrightarrow}{\underset{\longleftarrow}{\text{iff}}}$ $3 \mid n^2$. (use above fact.)

(2) show $\sqrt{3}$ is irrational

1.8 Proof Methods

An <u>existence proof</u> is a proof of a proposition of the form

$$\exists x \; P(x)$$

where $P(x)$ is some prop. fcn. with domain U.

Two kinds:

- constructive
- non-constructive.