CSE 16 7-2-24

1.7 Introduction to Proofs

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

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

- we say $n \in \mathbb{Z}$ is <u>odd</u> iff there exists $k \in \mathbb{Z}$ s.t. $n = 2k+1$

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

<u>Note</u>: every $n \in \mathbb{Z}$ is either even or odd, and no n is 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. $n = kd$.

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

<u>Notation</u>: $d \mid n$

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

$$\exists a \exists b : (b \neq 0) \wedge x = \frac{a}{b} \qquad (x \text{ free})$$

In general, if $P(x)$ is a Prop. fcn. on universe U, then $P(x)$ defines a property possesed by some elements $x \in U$.

Direct Proof of $p \Rightarrow q$

Assume p is true. Use inference rules (i.e. logical identities) and previously proved theorems to show that q is also true.

<u>Ex.</u>

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

$$\forall n \, \forall m \; : \; \underbrace{Even(n) \wedge Even(m)}_{p} \rightarrow \underbrace{Even(n \cdot m)}_{q}$$

<u>Proof</u>

Let $n, m \in \mathbb{Z}$. Assume both n and m are even. Then there exist $k_1, k_2 \in \mathbb{Z}$ such that $n = 2k_1$ and $m = 2k_2$.

Therefore

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

Since $2k_1 k_2 \in \mathbb{Z}$, we have $n \cdot m$ is even. ∎

Exercise

Prove each row of the table

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

note: $n+m=m+n$, $n \cdot m = m \cdot n$ don't need to be proved

Ex.
Show that if n is even, then n^2 is also even.

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

<u>Proof</u>

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

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

Prove (directly) the contrapositive
statement : $\neg q \rightarrow \neg p$.

<u>Ex.</u> $\forall n : Odd(n^2) \rightarrow Odd(n)$

Proof

Let $n \in \mathbb{Z}$. We will show that if n is not odd, then n^2 is not even. Recall every $m \in \mathbb{Z}$ is either even or odd, but not both. Thus its sufficient to show that if n is even, then n^2 is even. But this was previously proved. ∎

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

Proof (contraposition)
We show if n is odd, then n^2 is odd.

Let $n \in \mathbb{Z}$. assume n is odd.

Then there exists $k \in \mathbb{Z}$ s.t.

$n = 2k+1$. Therefore

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

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

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

<u>EX.</u> $\forall n : Odd(5n+4) \rightarrow Odd(n)$

<u>Proof</u> (contraposition)

we show: $\forall n : Even(n) \rightarrow Even(5n+4)$.

Let $n \in \mathbb{Z}$. Assume n is even.

Then $n = 2k$ for some $k \in \mathbb{Z}$.

Thus

$$
\begin{aligned}
5n+4 &= 5 \cdot 2k + 4 \\
&= 10k + 4 \\
&= 2(5k+2).
\end{aligned}
$$

Since $5k+2 \in \mathbb{Z}$, we have $5n+4$ is even. ■

<u>Ex.</u>

Show that for all $n, a, b \in \mathbb{Z}^+$, if $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof. (indirect)

Let n, a, b be positive integers.

Assume both $a > \sqrt{n}$ and $b > \sqrt{n}$.

Then

$$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

showing that $ab \neq n$. Therefore we have if $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. ∎

Ex.
for all $x, y \in \mathbb{R}$, if x, y are rational, then $x+y$ is rational.

<u>Proof</u> (direct)

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

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

where $a, b, c, d \in \mathbb{Z}$ and $b \neq 0, d \neq 0$.

Thus

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

Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{Z}$ and $bd \neq 0$, we have $x + y$ rational.

$\blacksquare$

Exercise

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

(1) $x+y$ is rational

(2) $x-y$ " "

(3) $x \cdot y$ " "

(4) if $y \neq 0$, then $\frac{x}{y}$ is rational.

Notation

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

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

Proof by contradiction

To prove a proposition p by contradiction, we prove

$$\neg p \to q$$

where q is a contradiction, usually q is of the form $q = r \wedge \neg r$.

note: $\neg p \to F \equiv p$

check: $(\neg p \to F) \leftrightarrow p$ is a tautology.

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

we must show that there do not exist $a, b \in \mathbb{Z}$, $b \neq 0$ s.t.

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

Proof (contradiction)

Assume $\sqrt{2}$ is rational, i.e. assume a, b as above do exist.

If a and b have any common factors, we may cancel them. Assume this is done, so

$a, b \in \mathbb{Z}$, $b \neq 0$, and a, b have no common factors, and

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

Then

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

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

$\therefore$ a^2 is even

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

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

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

$$\therefore \quad 4k^2 = 2b^2$$

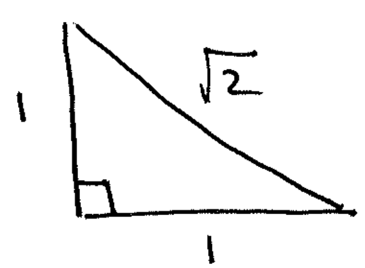
$$\therefore \quad 2k^2 = b^2$$

$\therefore$ b^2 is even

$\therefore$ b is even (previous thm)

We've shown both a and b are even. But also a and b have no common factor.

This contradiction shows our assumption was false. Therefore $\sqrt{2}$ is not rational. ■



Fact (proof in chap. 4)

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

- $n = 3k$ for some $k \in \mathbb{Z}$] $3 \mid n$
- $n = 3k+1$ " " "
- $n = 3k+2$ " " "] $3 \nmid n$

Exercise

using above

(1) $3 \mid n$ iff $3 \mid n^2$

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