1.8 Proof Methods

Recall: To prove $\forall x\, P(x)$, we let $x \in \mathcal{U}$ be arbitrary, then show $P(x)$ is true.

An Existence Proof is a proof of a statement of the form

$$\exists x\, P(x)$$

There are two kinds of such proofs

- <u>constructive</u>
  Find, display or construct an element $a \in U$ such that $P(a)$ is true.

- <u>non-constructive</u>
  Procedes in some other way, often by contradiction.

<u>Ex.</u> Show there exist $x, y \in \mathbb{R} - \mathbb{Q}$ s.t. $x + y \in \mathbb{Q}$.

<u>*Proof*</u> (constructive)
Let $x = \sqrt{2}$, $y = 1 - \sqrt{2}$. We showed x is

irrational. If y were rational, then $y = 1-\sqrt{2} = r \in \mathbb{Q}$, and

$$\sqrt{2} = 1 - r \in \mathbb{Q},$$

which is false. Therefore y is irrational. Then

$$x + y = \sqrt{2} + (1-\sqrt{2}) = 1 \in \mathbb{Q}.$$

$\blacksquare$

Ex.

Show there exist $x, y \in \mathbb{R} - \mathbb{Q}$ s.t. $x^y \in \mathbb{Q}$.

Proof

Either $\sqrt{2}^{\sqrt{2}}$ is rational, or it is not. (note $p \vee \neg p$ is a tautology)

Case 1: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$

Let $x = y = \sqrt{2}$. Then

$$x^y = \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}.$$

Case 2: $\sqrt{2}^{\sqrt{2}} \in \mathbb{R} - \mathbb{Q}$

Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2 \in \mathbb{Q}$$

Since one of these cases must hold, there exist irrational x, y s.t. x^y is rational. ∎

Note: This was non-constructive since we don't know which case holds.

Actually $\sqrt{2}^{\sqrt{2}}$ is irrational, but proof is difficult.

We can prove the last result constructively though.

Lemma

$\log_2(9)$ is irrational.

Proof (contradiction)

Assume $\log_2(9) \in \mathbb{Q}$, i.e.

$$\log_2(9) = \frac{a}{b}$$

for some $a, b \in \mathbb{Z}$, $b \neq 0$. Then

$$2^{\log_2(9)} = 2^{\frac{a}{b}}$$

$$\therefore \quad 9 = (2^a)^{\frac{1}{b}}$$

$$\therefore \quad 9^b = 2^a$$

But the LHS is odd while RHS is even. $\times$ $\therefore \log_2(9) = \mathbb{R} - \mathbb{Q}$. ∎

Theorem

There exist $x, y \in \mathbb{R} - \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof (constructive)

Let $x = \sqrt{2}$ and $y = \log_2(9)$. Then

$$
\begin{aligned}
x^y &= \sqrt{2}^{\log_2(9)} \\
&= \sqrt{2}^{\log_2(3^2)} \\
&= \sqrt{2}^{2 \cdot \log_2(3)} \\
&= \left(\sqrt{2}^{2}\right)^{\log_2(3)} \\
&= 2^{\log_2(3)} \\
&= 3 \in \mathbb{Q}.
\end{aligned}
$$

$\blacksquare$

Read

- exhaustive proofs, proof by cases
  Ex. 1–9
- existence proofs Ex. 10–12
- tilings Ex. 18–22

Backward Reasoning

Ex. 14 on p. 100

<u>Theorem</u> (Arithmetic-Geometric Mean inequality (AGM))

Any two distinct positive real numbers satisfy

$$\sqrt{xy} < \frac{x+y}{2}$$

<u>Note</u>

we call $\sqrt{xy}$ the <u>geometric mean</u> of x, y, and $\frac{x+y}{2}$ the <u>arithmetic mean</u> of x, y.

To discover a proof, reason backwards:

$$\sqrt{xy} < \frac{x+y}{2}$$

$$xy < \frac{(x+y)^2}{4}$$

$$4xy < x^2 + 2xy + y^2$$

$$0 < x^2 - 2xy + y^2$$

$$0 < (x-y)^2 \quad \text{true since } x \neq y$$

<u>Exercise</u> Write the proof.

<u>Note</u>:

the AGM inequality becomes equality iff $x = y$, i.e.

$$\sqrt{xy} = \frac{x+y}{2}$$

(do same steps)

2.1 Sets

Defn

A <u>set</u> is an unordered collection of objects, called its <u>elements</u> or <u>members</u>.

notation

write $x \in S$ to mean x is an element of a set S.

<u>note</u> this defn leads to a Paradox (see P. 126 # 46).

Ex.

- $\{1,2,3\} = \{2,1,3\} = \{3,2,1\} = \cdots$
- $\{1,2,3,\ldots\ldots,100\}$
- $\{1,2,3,\ldots\ldots\}$

Special sets

- $\mathbb{N} = \{0,1,2,3,\ldots\ldots\}$
- $\mathbb{Z} = \{\ldots\ldots,-2,-1,0,1,2,\ldots\ldots\}$
- $\mathbb{Z}^+ = \{1,2,3,\ldots\ldots\}$

- $\mathbb{Q}$ = {rational numbers}
- $\mathbb{R}$ = {real numbers}
- $\mathbb{C}$ = {complex numbers}

Two sets are equal iff they have exactly same members.

$$A = B \text{ iff } \forall x : x \in A \leftrightarrow x \in B$$

$$\text{iff } \forall x : (x \in A \rightarrow x \in B) \land (x \in B \rightarrow x \in A)$$

Another way to specify a set is Set Builder Notation

Let $P(x)$ be a Prop. function on domain U, and define

$$S = \{ x \in U \mid P(x) \}$$

or

$$S = \{ x \mid P(x) \}$$

if U is understood.

Ex.

- $\mathbb{Q} = \{x \in \mathbb{R} \mid \exists a, b \in \mathbb{Z} : (b \neq 0) \wedge (x = \frac{a}{b})\}$
- $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$
- $S = \{n \in \mathbb{Z} \mid 0 \leq n \leq 5\} = \{0, 1, 2, 3, 4, 5\}$

Defn

The empty set is the set with no members.

$$\emptyset = \{\ \}$$

<u>Defn</u>

We say a set A is a <u>subset</u> of a set B iff every element of A is also a member of B. i.e.

$$\forall x : x \in A \rightarrow x \in B$$

<u>Notation</u>: $A \subseteq B$

We say A is a <u>proper subset</u> of B iff both

$$A \subseteq B \text{ and } A \neq B$$

<u>Notation</u>: $A \subsetneqq B$

<u>Note</u>: book uses $A \subset B$ for proper subset.

Observe that for any set S:

- $\emptyset \subseteq S$: $\forall x$: $x \in \emptyset \rightarrow x \in S$
- $S \subseteq S$: $\forall x$: $x \in S \rightarrow x \in S$

<u>Remark</u>: 'contains' may mean different things

- $x \in S$: 'S contains x (as a member)'
- $A \subseteq S$: 'S contains A (as a subset)'

Ex. $S = \emptyset$

subsets: $\emptyset$

Ex $S = \{1\}$

subsets: $\emptyset, \{1\}$

Ex. $S = \{1, 2\}$

subsets: $\emptyset, \{1\}, \{2\}, \{1, 2\}$

Defn
The set of all subsets of S is called the *power set* of S.

notation: $\mathbb{P}(S)$ or 2^S

Ex. $S = \{1, 2, 3\}$

$$\mathbb{P}(S) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Defn

If $n \in \mathbb{N}$ and S has n distinct members, we say S is finite, and call n the cardinality of S.

notation: $|S| = n$

If S is not finite its called infinite.

Ex. infinite sets

$$\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$