CSE 16 7-6-23

Two kinds of existence proofs

$$\exists x : P(x)$$

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

- non-constructive
  Procede by any other method, usually by contradiction.

Ex. We know $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$. Also $1 - \sqrt{2} \in \mathbb{R} - \mathbb{Q}$. Why?

Pf (contradiction)
If $1-\sqrt{2} \in \mathbb{Q}$, then

$$1 - \sqrt{2} = \frac{a}{b}$$

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

$$\sqrt{2} = 1 - \frac{a}{b} = \frac{b-a}{b} \in \mathbb{Q} \quad \times$$

$\therefore$ $1-\sqrt{2}$ is irrational. ∎

Ex. (constructive)
Show there exist $x, y \in \mathbb{R} - \mathbb{Q}$ such that $x + y \in \mathbb{Q}$.

Proof: Let $x = \sqrt{2}$ and $y = 1 - \sqrt{2}$. Then $x + y = 1 \in \mathbb{Q}$. ∎

Ex. (non-constructive)

show there exist $x, y \in \mathbb{R} - \mathbb{Q}$

such that $x^y \in \mathbb{Q}$

Proof

either $\sqrt{2}^{\sqrt{2}}$ is rational, or it is not.

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

Let $x = y = \sqrt{2}$. Then x, y are irrational, but $x^y = \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$.

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

Let $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$. Then x, y are irrational, but

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

In both cases, pair x, y exists. $\blacksquare$

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

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

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

$$\therefore \quad 9^b = \left(2^{\frac{a}{b}}\right)^b = 2^{\frac{a}{\cancel{b}} \cdot \cancel{b}}$$

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

But LHS is odd while RHS is even ※.

This ※ shows no such a, b exist,

so $\log_2(9) \in \mathbb{R} - \mathbb{Q}$ ∎

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 $x, y \in \mathbb{R} - \mathbb{Q}$, and

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

$\blacksquare$

Read

- exhaustive proof, proof by cases.

  Ex. 1–9

- existence proofs. Ex. 10–12

- tilings. Ex. 18–22

Backward Reasoning

Ex. 14 P.100

Theorem (AGM)

Arithmetic-Geometric mean inequality

Any two distinct positive $x, y \in \mathbb{R}$ satisfy

$$\underbrace{\sqrt{xy}}_{GM} < \underbrace{\frac{x+y}{2}}_{AM}$$

To discover a proof, reason backwards from the conclusion, to hypothesis.

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

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

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

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

$$0 < (x-y)^2$$

Exercise:

write proof in forward logical direction.

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

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

2.1 Sets

Defn

A set is an unordered collection of objects, called its elements or members.

notation $x \in S$

read: 'x is an element of S'.

To specify a set, we can list its members

Ex.

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

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

special sets

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

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

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

$\mathbb{R} = \{\text{real}\}$

$\mathbb{C} = \{\text{complex}\}$

Two sets are equal iff they contain the same members.

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

<u>set builder notation</u>

let $P(x)$ be a Prop. fcn on U.

Then

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

or

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

(if U is understood).

This defines S as the set of all $x \in \mathcal{U}$ s.t. $P(x)$ is true.

<u>Ex.</u>

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

<u>Defn</u> The <u>empty set</u> ϕ is the set with no members.

$$\phi = \{ \ \}$$

<u>Defn</u>

we say A is a <u>subset</u> of B iff every element of A is an element of B.

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

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

<u>Defn</u>

we say A is a <u>proper subset</u> of B iff $A \subseteq B$ and $A \neq B$

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

<u>Rmk</u>: Book uses $\subset$ for proper subset.

Observe for any set S:

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

  $F \Rightarrow P$ is a tautology

- $S \subseteq S$: $(\forall x : x \in S \rightarrow x \in S)$

  $P \Rightarrow P$ is a tautology.

Remark

the word 'contains' has 2 meanings.

- $x \in S$: 'S contains x'
- $A \subseteq S$: 'S contains A'

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

subsets of S:

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

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

subsets of S:

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}$$

$$\{1, 3\}, \{2, 3\}, \{1, 2, 3\}$$

note: $1 \neq \{1\} \neq \{\{1\}\}$

<u>Defn</u>

The set of all subsets of S is called the <u>Power set</u> of S

<u>notation</u>: $\mathbb{P}(S)$

<u>Ex.</u> $S = \{1, 2\}$

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

<u>Defn</u>

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

<u>notation</u>: $|S| = n$

If S is not finite its called `infinite.

Ex. $\mathbb{N}, \mathbb{Z}, \mathbb{Z}^+, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ are infinite sets.

- can an infinite set be a subset of a finite set? NO
- can an infinite set be an element of a finite set?

YES Ex. $S = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}\}$

Theorem

If S is finite, then so is $\mathbb{P}(S)$ and

$$|\mathbb{P}(S)| = 2^{|S|}$$

Exercise:

let $S = \{1, 2, 3, 4\}$. check that

$$|\mathbb{P}(S)| = 2^{4} = 16 .$$

<u>Defn</u>

An ordered collection of n objects is called an <u>ordered n-tuple</u>.

<u>notation</u>: $(x_1, x_2, x_3, \ldots, x_n)$

$n=2$: (x_1, x_2) ordered pair

$n=3$: (x_1, x_2, x_3) " triple

$n=4$: (x_1, x_2, x_3, x_4) " 4-tuple

$\vdots$

<u>Defn</u>

The <u>cartesian product</u> of sets A, B

$$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}.$$