Theorem: Let m and n be positive integers. Then $\overset{p}{\overline{m = n}}$ if and only if $\underset{q}{\underline{m|n \text{ and } n|m}}$.

Proof (*proof of equivalence*): To prove $p \Leftrightarrow q$, we need to prove i) $p \Rightarrow q$ and ii) $q \Rightarrow p$.

i) ($p \Rightarrow q$): Suppose $m = n$ ($m, n \in \mathbb{Z}^+$).

Since $m = n$, we have $m \cdot 1 = n$. So $m|n$.

Similarly $m = n$, we have $m = n \cdot 1$. So $n|m$.

This completes the proof of i).

ii) ($q \Rightarrow p$): Suppose that $m|n$ and $n|m$ where $n, m \in \mathbb{Z}^+$. Since $m|n$, we have $n = k_1 m$ ($k_1 \in \mathbb{Z}^+$). (I)

Since $n|m$, we have $m = k_2 n$ ($k_2 \in \mathbb{Z}^+$). (II)

substitute

Then $m = k_2 k_1 m$, (where $k_2, k_1 \in \mathbb{Z}^+$)

$\Rightarrow k_2 \cdot k_1 = 1$

So $k_2 = 1$, $k_1 = 1$.

Then, from (I) we get $n = 1 \cdot m$.

So, $n = m$.

This finishes the proof of ii).

By parts i) & ii), we have completed the proof.

Theorem: If $0 > 1$, then 3 is an even number.

Proof (*vacuous proof*):

$0 > 1$ is false, so the result follows vacuously.

Theorem: If $0 < 1$, then $\sqrt{4}$ is a rational number.

Proof (*trivial proof*):

$\sqrt{4} = 2$, so $\sqrt{4}$ is a rational number. Therefore, the result follows trivially.

P

Theorem: There is no integer that is both even and odd.

Proof: (Proof by contradiction)

Suppose (to get a contradiction) that there is an integer, say n, that is both even and odd.

Since n is even, $n = 2k$ $(k \in \mathbb{Z})$; and since n is odd $n = 2m+1$ $(m \in \mathbb{Z})$.

So $\underline{2k} = n = \underline{2m+1}$.

Therefore, $2k = 2m+1$.

Then, $2k - 2m = 1$, and so $2\underbrace{(k-m)}_{\in \mathbb{Z}} = 1$. So, it follows that

↯ 1 is an even integer.

Contradiction. Therefore, it is not true that there is an integer that is both even and odd. So we proved that there are no integers that is both even and odd.

Want to show

1 <=> 2

1 <=> 3

2 <=> 3

Strategy: show

1 => 2 and

2 => 3 and

3 => 1

Other types of proofs (mixed types) maybe: Let a and b be real numbers. Then the following statements are equivalent.

1) $a < b$

2) $a < \dfrac{a+b}{2}$

3) $\dfrac{a+b}{2} < b$.

1 => 2

2 => 1   2 => 3 ∧ 3 => 1

1 => 2 ∧ 2 => 3

1 => 3   3 => 1

2 => 3   3 => 2

3 => 1 ∧ 1 => 2

Proof: When showing the equivalence of more than one statements, one can go in a circular fashion. It suffices to prove that 1) → 2), 2) → 3) and 3) → 1).

[Why is this sufficient?]

(1 => 2): Suppose $a<b$ $(a, b \in \mathbb{R})$.

Add a to both sides, to get $2a < a+b$.

Dividing by 2, we get $\frac{2a}{2} < \frac{a+b}{2} \Rightarrow a < \frac{a+b}{2}$.

(2 => 3): Suppose $a < \frac{a+b}{2}$.

$$a < \frac{a+b}{2} \quad / -\frac{a}{2}$$

$$\Rightarrow \frac{a}{2} < \frac{b}{2} \quad /+\frac{b}{2} \quad \Rightarrow \frac{a+b}{2} < b$$

(3 => 1): Suppose $\frac{a+b}{2} < b$.

Multiplying both sides by 2, we get $a+b < 2b$; and subtracting b from both sides we get $a<b$.

(1 => 2), (2 => 3) and (3 => 1) collectively finish the proof.

Sets

Defn: A **set** is a collection of distinct objects; these objects are then called **elements** of the set. A set can have a finite (even zero) or an infinite number of elements. Conventionally we use capital letters to denote sets. To express that an element x is in a set A, we write $x \in A$.

The elements of a set can be numbers, functions, and pretty much anything else.

Examples: $A = \{$elephant, monkey, chipmunk, Aras$\}$

set of natural numbers $\{1, 2, 3, 4, \ldots\}$

set of rational numbers

Important sets of numbers: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}^-, \mathbb{Z}^+$ → positive integers

→ set of integers

There are two common ways of denoting sets:

→ set of reals numbers

(i) **list notation**

Example: $S = \{8, 12, 16, 20\}$

(ii) **set-builder notation**

Example: $S = \{4i | i \in \mathbb{Z}, 2 \leq i \leq 5\}$ or $S = \{4i : i \in \mathbb{Z}, 2 \leq i \leq 5\}$

"such that" "such that"

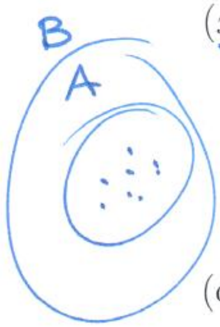
$\emptyset \qquad \{\ \}$

Defns: The set that has no elements is called the **empty set**, denoted by $\emptyset$ or $\{\}$.

$x \in A \Rightarrow x \in B$

A set A is called a **subset** of a set B, denoted by $A \subseteq B$, if $(x \in A \Rightarrow x \in B)$ for all x. subset

Note that a subset A of a set B can possibly be equal to B.



In fact, two sets A and B are **equal** if and only if $A \subseteq B$ and $B \subseteq A$.

A subset A of a set B is called a **proper subset**, denoted by $A \subset B$ (or $A \subsetneq B$), if $A \subseteq B$ and $A \neq B$.

$A \subseteq B$

Examples:

If a set is finite, then we can count its elements. The number of elements in a finite set A is referred to as the **cardinality** of A, denoted by $|A|$.

The set of subsets of a set A is called the **power set** of A, denoted by $\mathcal{P}(A)$.

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$. (WHY?)