Real Numbers and the Power of Continuum Part 1

Theorem 1

The unit interval $I = [0, 1]$ is nondenumerable.

Proof. Let I is denumerable. Then

$$I = \{x_1, x_2, x_3, \ldots\}$$

that is, the elements of I can be written in a sequence. So

$$x_1 = 0.a_{11}a_{12}a_{13}\ldots a_{1n}\ldots$$
$$x_2 = 0.a_{21}a_{22}a_{23}\ldots a_{2n}\ldots$$
$$x_3 = 0.a_{31}a_{32}a_{33}\ldots a_{3n}\ldots$$
$$\vdots$$
$$x_n = 0.a_{n1}a_{n2}a_{n3}\ldots a_{nn}\ldots$$

Here $a_{ij} \in \{0, 1, 2, \ldots 9\}$

$0 = 0.000\ldots$
$0.1 = 0.0999\ldots$
$0.5 = 0.4999\ldots$
$1 = 0.999\ldots$

Theorem 1

Now construct the real number

$$y = 0.b_1 b_2 b_3 \ldots b_n \ldots$$

which will belong to I in the following way:

choose b_1 so $b_1 \neq a_{11}$ and $b_1 \neq 0$

choose b_2 so $b_2 \neq a_{22}$ and $b_2 \neq 0$

choose b_3 so $b_3 \neq a_{33}$ and $b_3 \neq 0$ and so on

Note that $y \neq x_1$ since $b_1 \neq a_{11}$.

and $y \neq x_2$ since $b_2 \neq a_{22}$ and so on.

That is $y \neq x_n$ for all $n \in P$.

Thus $y \notin I$, which contradicts the fact that $y \in I$. Thus the assumption that I is denumerable is wrong. Hence I is nondenumerable.

Power of the Continuum

A set A is said to have the power of the continuum if A has the same cardinality as the unit interval $I = [0, 1]$.

For example, $[a, b] \approx [0, 1]$.

Hence closed interval $[a, b]$ has the power of continuum. Similarly, $[a, b)$, $(a, b]$ and (a, b) also have the power of continuum.

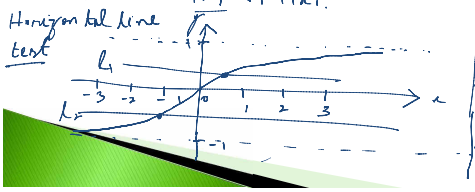
Power of the Continuum

Real Numbers and the Power of Continuum Part 2

Theorem 1

Prove that the set R of real numbers has the power of continuum.

Proof. Consider the function $f : R \to (-1,1)$ defined by $f(x) = \frac{x}{1+|x|}$. Clearly values of f belong to $(-1,1)$ since $|x| < 1+|x|$.



$\therefore R \approx (-1,1)$

$(-1,1) \approx [0,1]$

Then $R \approx [0,1]$.

$f(1) = \frac{1}{1+1} = \frac{1}{2} \in (-1,1)$

$f(-2) = \frac{-2}{1+2} = -\frac{2}{3} \in (-1,1)$

By the horizontal line test, $f(x)$ is bijective. Hence, R has the power of continuum.

Theorem 1

Cardinal Numbers

Definition

Each set A is assigned a symbol in such a way that two sets A and B are assigned the same symbol if and only if they are equipotent. This symbol is called the cardinality or cardinal number of A, and it is denoted by

$|A|$, $n(A)$ or $\text{card}(A)$

Thus,

$|A| = |B|$ iff $A \approx B$.

Finite Cardinal Numbers

0 is assigned to the empty set ø, and n is assigned to the set $\{1, 2, \ldots n\}$. Thus,

$|A| = n$ iff $A \approx \{1, 2, \ldots, n\}$

$|A| = 3$ iff $A \approx \{1,2,3\}$, eg $A = \{2,3,4\}$

Alternatively, the symbols 0, 1, 2, 3,… are assigned, respectively, to the sets

$\emptyset$, $\{\emptyset\}$, $[\emptyset, \{\emptyset\}]$, $[\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}]$, …

Transfinite Cardinal Numbers

Cardinal numbers of infinite sets are called infinite or transfinite cardinal numbers.

The cardinal number of the infinite set P of positive integers is $\aleph_0$ (aleph-nought)

Thus,

$|A| = \aleph_0$ iff $A \approx P$.

In particular, $|\mathbb{Z}| = \aleph_0$ since $\mathbb{Z} \approx P$.

and $|\mathbb{Q}| = \aleph_0$ since $\mathbb{Q} \approx P$

Transfinite Cardinal Numbers

The cardinal number of the unit interval $I = [0, 1]$ is denoted by $\mathbf{c}$ and it is called the power of continuum. Thus: $|A| = c$ iff $A \approx I$.

In particular, we have $|R| = \mathbf{c}$, and the cardinal number of any interval is $\mathbf{c}$.

For example, $|(2,3)| = c$ since $(2,3) \approx [0,1]$

$|[-1,5]| = c$ // $[-1,5] \approx [0,5]$

Some Important Statements

(a) A is denumerable or countably infinite means $|A| = \aleph_0$

(b) A is countable means $|A|$ is finite or $|A| = \aleph_0$

(c) A has the power of continuum if $|A| = \mathbf{c}$.

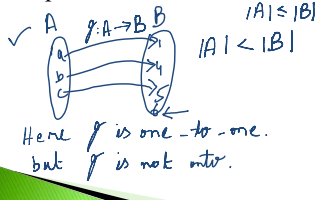
$|R| = c$

Ordering of Cardinal Numbers

Definition

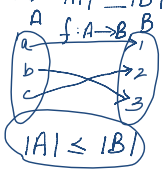
Let A and B be two sets. We say that $|A| \leq |B|$ if there exists a one-to-one(injective) function $f: A \to B$.

The above relation between cardinal numbers are well defined, that is, the relations are independent of the particular sets involved. Namely, if $A \approx A'$ and $B \approx B'$, $|A| \leq |B|$ iff $|A'| \leq |B'|$ / $|A| = |B|$



$|A| < |B|$

Here g is one-to-one. but g is not onto.



$|A| \leq |B|$

Example 1

Let B be a proper subset of a finite set A.

For example, $A = \{1,2,3,4\}$, then $B = \{1,2\}$

Here $|B| < |A|$.

Example 2

Let n be a finite cardinal. Let A be a finite subset of $P = \{1,2,3,\cdots\}$. Then $|A| \neq |P|$. Thus $|A| < |P|$. $n < \aleph_0$

We may write

$0 < 1 < 2 < \cdots < \aleph_0$

Example 3

Consider the set P of positive integers and the unit interval I, that is, consider the sets $P = \{1,2,3,\cdots\}$ and $I = [0,1] = \{x \in R : 0 \leq x \leq 1\}$

The function $f: P \to I$ defined by $f(n) = 1/n$ is one-to-one.(prove it.)

Let $f(n_1) = f(n_2)$

$\Rightarrow 1/n_1 = 1/n_2$

$\Rightarrow n_1 = n_2$ Proved

$f(1) = 1/1 = 1 \in I$

$f(2) = 1/2 = 0.5 \in I$

$f(3) = 1/3 = 0.3\ldots \in I$

$f(4) =$ different

$|P| = \aleph_0$, $|I| = c$

Therefore, $|P| \le |I|$. ✓

On the other hand $|P| \ne |I|$. Therefore $|P| < |I|$.

Accordingly we may write $\Rightarrow \aleph_0 < c$.

$0 < 1 < 2 < \cdots < \aleph_0 < c$.

Example 4

Let A be any infinite set. So A contains a subset which is denumerable. Accordingly, for any infinite set A, we always have

$\aleph_0 \le |A|$. $\{P = \{1,2,3,\ldots\}$, $E \subseteq P$.

$|P| = |E|$

$\aleph_0 = \aleph_0$

$\mathbb{R}$ = infinite set, $P \subseteq \mathbb{R}$. Here P is denumerable. $|P| \not> |\mathbb{R}|$, $\aleph_0 \not< c$.

Cantor's Theorem

Theorem 1

If A has 3 elements, then $P(A)$ has 8 elements. $2^3 = 8$

For any set A, we have $|A| < |P(A)|$.

Proof. Let $f: A \to P(A)$ defined by $f(x) = \{x\}$, $\forall x \in A$.

We need to prove that f is one-to-one but not onto.

Let $f(x_1) = f(x_2)$

$\Rightarrow \{x_1\} = \{x_2\}$

$\Rightarrow x_1 = x_2$

Hence f is one-to-one.

$|P| < |P(P)|$, $\aleph_0 < 2^{\aleph_0}$

$|\mathbb{R}| < |P(\mathbb{R})|$, $c < 2^c$

Theorem 1

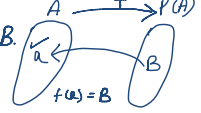
Suppose $f: A \to P(A)$ is onto. Now consider the set

$B = \{x \in A : x \notin f(x)\}$ ✓

For example, if $A = \{1,2,3\}$, then

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

clearly B is a subset of A, so $B \in P(A)$. Also since f is onto, so there exists $a \in A$ such that $f(a) = B$. Now we have two possibilities, either $a \in B$ or $a \notin B$.



Theorem 1

1) If $a \in B$, then $a \in f(a)$. Then, by the definition of set B, we have $a \notin B$, which is a contradiction.

2) If $a \notin B$, then $a \notin f(a)$. Then $a \in B$, which is a contradiction.

Hence, our assumption that f is onto is wrong. Thus f is not onto. Therefore,

$|A| < |P(A)|$.

Theorem 2

Prove that $2^{\aleph_0} = c$.

Theorem 2

$2^{\aleph_0} = c$

Continuum Hypothesis

There exists no cardinal number β such that

$\aleph_0 < \beta < c$.

$\aleph_0$, c

$\aleph_0 < c$.

$\aleph_0 < 2^{\aleph_0} = c$.

same

Cardinal Arithmetic Part 1

Cardinal Addition

Addition and multiplication of the counting numbers N are sometimes treated from the point of view of set theory. The interpretation of 2+3 = 5, for example, is the union of two disjoint sets, one having two elements and the other having three elements, is a set with five elements. This idea leads to a completely general definition of addition of cardinal numbers.

Cardinal Addition

Definition: Let α and β be cardinal numbers and let A and B be disjoint sets with $\alpha = |A|$ and $\beta = |B|$. Then the sum of α and β is denoted and defined by

$$\alpha + \beta = |(A \cup B)|$$

For example, Let $A = \{1,2,3\}$, $B = \{a,b,c\}$.
Here $|A| = 3$, $|B| = 3$. Now, $A \cup B = \{1,2,3,a,b,c\}$, $|A \cup B| = 6$
$= |A| + |B|$

Note:(1) This definition is well-defined.
Let A' and B' with same cardinal numbers.
means $|A'| = \alpha$, $|B'| = \beta$. Then $|A' \cup B'| = |A \cup B|$

(2) If A and B are any two sets, then
$A \times \{1\}$ and $B \times \{2\}$ are disjoint sets.

Examples

(a) Let m and n be finite cardinal numbers. Then $m + n$ corresponds to the usual addition in N.

(b) Let n be a finite cardinal number.

Let $A = \{1,2,3,\cdots,n\}$. Then $|A| = n$

$B = \{n+1, n+2, n+3, \cdots\}$. Then $|B| = \aleph_0$

Here $B \approx P$

Now, $A \cup B = \{1,2,3,\cdots,n,n+1,n+2,\cdots\}$. Then $|A \cup B| = \aleph_0$

But $|A \cup B| = n + \aleph_0$

$\Rightarrow \boxed{\aleph_0 = n + \aleph_0}$

Examples

c) Let $C = [0, \frac{1}{2}]$, $D = (\frac{1}{2}, 1]$

Here $C \approx I$ and $D \approx I = [0,1]$.

So, $|C| = c$, $|D| = c$.

Now, $C \cup D = [0, \frac{1}{2}] \cup (\frac{1}{2}, 1] = [0,1]$

$\Rightarrow |C \cup D| = c$.

Thus, $\boxed{c + c = c}$

d) Let $E = \{2,4,6,\cdots\}$ and $F = \{1,3,5,\cdots\}$

$\Rightarrow |E| = \aleph_0$ and $|F| = \aleph_0$

Now, $E \cup F = \{1,2,3,4,5,6,\cdots\} = P$

$|E \cup F| = \aleph_0$ $\boxed{\aleph_0 + \aleph_0 = \aleph_0}$

Cardinal Arithmetic Part 2

Cardinal Multiplication

Let α and β be cardinal numbers and let A and B be sets with $\alpha = |A|$ and $\beta = |B|$. *Then the product* α *and* β is denoted and defined by

$$\alpha\beta = |A \times B|$$

For example, Let $A = \{2,3,4\}$, $B = \{4,5\}$.

Here $|A| = 3$ and $|B| = 2$.

Now, $A \times B = \{(2,4),(2,5),(3,4),(3,5),(4,4),(4,5)\}$

$\therefore |A \times B| = 6 = 2 \times 3 = |A| \times |B| = \alpha\beta$

Examples

(a) Let m and n be finite cardinal numbers. Them mn corresponds to the usual multiplication in N.

(b) Since $N \times N$ is denumerable, so $|N \times N| = \aleph_0$

$N \times N \approx P$ or $|N \times N| = |P| \Rightarrow \boxed{\aleph_0 \times \aleph_0 = \aleph_0}$

(c) The Cartesian plane $R^2 = R \times R$ has the same cardinality as R. That is, **$\boxed{cc = c.}$**

$|R \times R| = R$

$cc = c$

Theorem 1

Let α and β be nonzero cardinal numbers such that β is infinite and $\alpha \leq \beta$. Then

$$\alpha + \beta = \alpha\beta = \beta$$

We know that $\aleph_0 < c$.

It means, $\aleph_0 + c = c$.

and $\aleph_0 c = c$

Ordered Sets

Definition

Suppose R is a relation on a set S satisfying the following three properties:

1) (Reflexive) For any $a \in S$, we have $a \, R \, a$.
2) (Antisymmetric) If $a \, R \, b$ and $b \, R \, a$, then $a = b$.
3) (Transitive) If $a \, R \, b$ and $b \, R \, c$, then $a \, R \, c$.

Then R is called a partial order or, simply an order relation, and R is said to define a partial ordering of S. The set S with partial ordering R is called a partially ordered set or, simply an ordered set. Poset

Notation

1) If $a \in P$, then $a \leq a$.
2) If $a \leq b$ and $b \leq a$, then $a = b$.
3) If $a \leq b$ and $b \leq c$, then $a \leq c$.

The most familiar order relation, called the usual order, is the relation $\leq$ on the positive integers P or, more generally on any subset of the real numbers R. For this reason, a partial ordering relation is frequently denoted by $\leq = R$

With this notation, the above three properties of a partial order appear in the following usual form:

1) (Reflexive) For any $a \in S$, we have $a \leq a$. or aRa.
2) (Antisymmetric) If $a \leq b$ and $b \leq a$, then $a = b$.
3) (Transitive) If $a \leq b$ and $b \leq c$, then $a \leq c$.

Notation

Although an ordered set consists of two things, a set S and the partial ordering R, one usually simply write S to denote the ordered sets as long as the partial ordering is fixed in the context of the discussion; otherwise the ordered set is denoted by the pair $(S, \leq)$

Suppose S is an ordered set. Then the statement $a \leq b$ is read "a precedes b".

In this context we also write:

$a < b$ means $a \leq b$ and $a \neq b$. (a strictly precedes b)
$b \geq a$ mean "b succeeds a"
$b > a$ means $b < a$ and $a \neq b$. (b strictly succeed a")

Example 1

3) If $A \subseteq B$, $B \subseteq C$, then $A \subseteq C$

1) Let C be any collection of sets. The relation of set inclusion $\subseteq$ is a partial ordering of C. Specifically,
   1) For any $A \in C$, $A \subseteq A$ or ARA.
   2) For any $A, B \in C$, we have $A \subseteq B$ and $B \subseteq A$, then $A = B$.
2) Consider the set P of positive integers. We say "a *divides* b", written $a|b$, if there exists an integer c such that $ac = b$. For example, $2|4$, $3|12$, $7|21$, and so on. This relation of divisibility is a partial ordering of P.
   1) If $a \in P$, $a|a$ or aRa.
   2) If $a|b$ and $b|a$, then $a = b$.
   3) If $a|b$, $b|c$, then $a|c$. ($3|12, 12|24 \Rightarrow 3|24$.)

Example 1

3) The relation "|" of divisibility is not an ordering of the set Z of integers. Specifically, the relation is not antisymmetric. For instance,

For example, $a = 2$, $b = -2$
$2|-2$ and $-2|2$
but $2 \neq -2$.

Example 1

Comparability and Linearly Ordered Sets

Comparability

Suppose a and b are distinct elements in a partially ordered set S. We say a and b are comparable if

$a \leq b$ or $b < a$.

Thus a and b are noncomparable written

$a \| b$

if $a \not< b$ or $b \not< a$.

Linearly Ordered Sets and Chain

Suppose that every pair of elements of S are comparable. Then S is said to be linearly or totally ordered.

Although an ordered set S may not be linearly ordered, it is still possible for a subset A of S to be linearly ordered. Such a linearly ordered subset A of an ordered set S is called a chain in S.

Example 1

a) Consider the set P of positive integers ordered by divisibility. Then 21 and 7 are comparable since $7 \mid 21$. Here 3 and 5 are non comparable because neither $3 \mid 5$ nor $5 \mid 3$. Thus P is not linearly ordered by divisibility. Observe that $A = \{2, 6, 12, 36\}$ is a chain.

b) The set P of positive integers with the usual order $\leq$ is linearly ordered and hence every ordered subset of P is also linearly ordered. $P = \{1, 2, 3, \ldots\}$, Now $B = \{2, 5, 7\}$

Example 1

c) The power set $P(A)$ of a set A with 2 or more elements is not linearly ordered by set inclusion. For example, $a, b \in A$, then $\{a\}$ and $\{b\}$ are noncomparable. Let $B \subseteq P(A)$ such that $B = \{\phi, \{a\}, A\}$. Here $\phi < \{a\} < A$ or $\phi \subseteq \{a\} \subseteq A$ so set B is a chain.

d) Consider the set $A = \{1, 2, 3, 4, 6, 12, 24\}$ ordered by divisibility. Then clearly A is not linearly ordered as for instance, 3 and 4 are not comparable. Observe that the sets $\{1, 2, 4, 12, 24\}$, $\{1, 2, 6, 12, 24\}$ and $\{1, 3, 6, 12, 24\}$ are all chains.

Example 2

Let $P = \{1, 2, 3, \ldots\}$ be ordered by divisibility. State whether each of the following is a chain in P.

a) $A = \{24, 2, 6\}$, it is a chain.
Here $2 < 6 < 24$ or $2 | 6 | 24$

b) $B = \{3, 15, 5\}$, so it is not a chain
Here $3 \nmid 5$

c) $C = \{2, 8, 32, 4\}$, it is a chain.
$2 < 4 < 8 < 32$

d) $D = \{7\}$, it is a chain.

Partially Ordered Sets and Hasse Diagrams

Immediate Predecessor and Immediate Successor

Let S be a partially ordered set, and suppose $a, b \in S$. We say that a is an immediate predecessor of b, or that b is an immediate successor of a, or that b is a cover of a, written $a << b$, if $a < b$ but no element in S lies between a and b, that is, there exists no element c in S such that $a < c < b$.

For example, consider the set $P = \{1, 2, 3, 4, \ldots\}$ with the order $<$. Then we can see that $1 << 2$, $2 << 3$, and so on.

Immediate Predecessor and Immediate Successor

Suppose S is a finite partially ordered set. Then the order on S is completely known once we know all pairs a, b in S such that $a << b$. This follows from the fact that $x < y$ if and only if $x << y$ or there exists elements

$x << a_1 < a_2 < \cdots < a_m < y$

For example, consider the set $A = \{1, 2, 3, 4, 6, 12, 24\}$ ordered by the relation "x *divides* y". Then we can write

$2 << 4$, $2 << 6$, $3 << 6$, $4 << 12$, $6 << 12$, $12 << 24$.

Also $1 << 2 << 4 << 12 << 24$ or $1 << 2 << 6 << 12 << 24$ or $1 << 3 << 6 << 12 << 24$.

Hasse Diagrams



The Hasse diagram of a finite partially ordered set S is a graphical representation of S as follows. The elements of S are represented by points in the plane and there is a directed line segment(arrow) drawn from a to b whenever $a << b$ in S. Instead of drawing an arrow from a to b, we sometimes place b higher than a and draw a line between them.

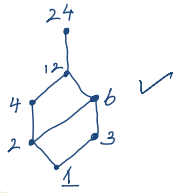
The Hasse diagram of an ordered set S is a picture of S. Sometimes we define a partially ordered set by simply presenting its Hasse diagram.

Example 1

Draw the Hasse diagram representing the divisibility relation on set $A = \{1, 2, 3, 4, 6, 12, 24\}$.

Solution. As we saw $1 << 2 << 4 << 12 << 24$ or $1 << 2 << 6 << 12 << 24$ or $1 << 3 << 6 << 12 << 24$. We can draw its Hasse diagram as follows:

Here $1 < 24$



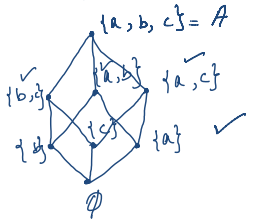
Example 2

Let $A=\{a,b,c\}$. Draw the Hasse diagram representing the subset relation $\subseteq$ on the power set $P(A)$.

- Solution. The power set $P(A)$ contains all subsets of A:
- $P(A)=\{\emptyset,\{a\},\{b\},\{c\},\{a,b\},\{b,c\},\{a,c\},\{a,b,c\}\}$. $2^3=8$
- We place the empty set $\emptyset$ at the bottom of the diagram. The subsets with one element $\{a\},\{b\},\{c\}$ are placed on the first level, and the subsets with two elements $\{a,b\},\{b,c\},\{a,c\}$ are placed on the next level. The element $\{a,b,c\}$ occupies the top of the diagram. Finally we connect the subsets with their immediate successor with respect to the inclusion relation. The resulting diagram is shown in the next slide.

Example 2

Here $\{b\}<<\{b,c\}$ because $\{b\}\subseteq\{b,c\}$
$\{b\}<<\{a,b\}$, $\{c\}<<\{b,c\}$, $\{c\}<<\{a,c\}$
$\{a\}<<\{a,b\}$, $\{a\}<<\{a,c\}$



Example 3

Let $A=\{1,2,3,4,5\}$ and $R=\{(1,1),(1,3),(1,4),(1,5),(2,2),(2,3),(2,4),(2,5),(3,3),(3,4),(3,5),(4,4),(5,5)\}$. Show that the relation R is a partial order and draw its Hasse diagram.

Solution.

- The relation R is reflexive since it contains all reflexive pairs: $(1,1),(2,2),(3,3),(4,4),(5,5)$.
- R is antisymmetric since all non-reflexive elements do not have the corresponding inverse pairs: $(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5)$.

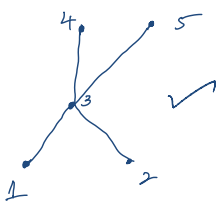
Example 3

- R is transitive:
- $(1,3)\in R,(3,4)\in R\rightarrow(1,4)\in R$;
- $(1,3)\in R,(3,5)\in R\rightarrow(1,5)\in R$;
- $(2,3)\in R,(3,4)\in R\rightarrow(2,4)\in R$;
- $(2,3)\in R,(3,5)\in R\rightarrow(2,5)\in R$.

Hence, the relation R is a partial order and we can draw its Hasse diagram, which is represented below.

Example 3

$R=\{(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5)\}$



Minimal and Maximal Elements

Minimal Element

Let S be a partially ordered set. An element $a \in S$ is called a minimal element of S if no element of S strictly precedes(is less than) a; that is, if

$$x \leq a \text{ implies } x = a$$

For example, let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ be ordered by divisibility. Then we can see that A has only one minimal element, 1.

Maximal Element

Let S be a partially ordered set. An element $b \in S$ is called a maximal element of S if no element of S strictly succeeds(is greater than) b; that is, if

$$x \geq b \text{ implies } x = b$$

For example, let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ be a set ordered by divisibility. Then we can see that A has two maximal elements, 18 and 24.

Geometrical Meaning

Geometrically speaking, a is a minimal element of S if no edge enters a(from below), and b is a maximal element of S if no edge leaves b (in an upward direction).

Note: S can have more than one minimal and more than one maximal element. Hasse diagram of divisibility relation on set $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ is given below:

Minimal and Maximal Element of an Infinite and Finite Set

If S is infinite, then S may have no minimal and maximal element. For instance, the set Z of integers with the usual order $\leq$ has no minimal and maximal element. On the other hand, if S is finite, then S has atleast one minimal and one maximal element.

First and Last Element

An element $a \in S$ is called a first element of S if $a \leq x$ for every $x \in S$, that is, if a precedes every other element in S.

Similarly, an element b $\in S$ is called a last element of S if $y \leq b$ for every $y \in S$, that is, b succeeds every other element in S.

For example, let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ be a set ordered by divisibility. 1 is minimal element of A which is also the first element of A. Set A has two maximal element and neither is a last element.

First and Last Element

Note: We note that S can have at most one first element which must be a minimal element of S, and S can have at most one last element which must be a maximal element of S. Generally speaking, S may have neither a first nor a last element, even when S is finite.

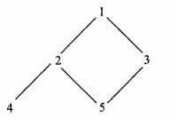
Examples

a) Consider the set $P = \{1, 2, 3, \ldots\}$ with the usual order $\leq$.

b) Let A be any nonempty set and let $P(A)$ be the power set of A ordered by set inclusion.

Examples

c) Consider the ordered set A in the figure below:



1) Find all minimal and maximal elements of A.
2) Does A have a first element or a last element?

Supremum and Infimum

Upper Bound and Supremum

Let S be a partially ordered set, and let A be a subset of S. An element m in S is called an upper bound of A if m succeeds every element of A, that is, for every $x \in A$, we have

$$x \leq m$$

If an upper bound of A precedes every other upper bound of A, then it is called the supremum of A and it is denoted by $sup(A)$.

Lower Bound and Infimum

Let S be a partially ordered set, and let A be a subset of S. An element n in S is called a lower bound of A if n precedes every element of A, that is, for every $y \in A$, we have

$$y \geq n$$

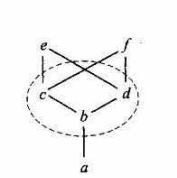
If a lower bound of A succeeds every other lower bound of A, then it is called the infimum of A and it is denoted by $inf(A)$.

Bounded Above and Bounded Below

If A has an upper bound we say A is bounded above, and if A has a lower bound we say A is bounded below. In particular, A is bounded if A has an upper and lower bound.

Example 1

Let $S = \{a, b, c, d, e, f\}$ be ordered as in the Hasse diagram below and let $A = \{b, c, d\}$.



Example 2

Let $S = \{1, 2, 3, \ldots, 8\}$ be ordered as in the Hasse diagram below and let $A = \{4, 5, 7\}$.

Example 3

Consider the set Q of rational numbers, and its subset

Similar Ordered Sets

Similar Mapping

Suppose X and Y are partially ordered sets. A one-to-one(injective) function $f : X \rightarrow Y$ is called a similar mapping from X into Y if f preserves the order relation, that is, if the following conditions holds for any pair a, $b \in X$:

$$a \leq b \text{ in } X \text{ if and only if } f(a) \leq f(b) \text{ in } Y$$

The above condition is equivalent to the following two conditions:

Similar Ordered Sets

Two ordered sets X and Y are said to be order-isomorphic or isomorphic or similar, written

if there exists a one-to-one correspondence $f : X \rightarrow Y$ which preserves the order relations. Such a function f is then called an order-isomorphism or isomorphism from X onto Y.

Example 1

Suppose $S = \{a, b, c, d\}$ is ordered by the diagram below and suppose $T = \{1, 2, 6, 8\}$ is ordered by divisibility. Determine whether S

Example 2

The set of positive integers $P = \{1, 2, 3, \ldots\}$ is order-isomorphic to the set of even positive integers $E = \{2, 4, 6, \ldots\}$ since the function $f : P \to E$ defined by $f(x) = 2x$ is an isomorphism between P and E.

Example 3

Consider the usual ordering $\leq$ of the positive integers $P = \{1, 2, 3,\ldots\}$ and the negative integers $A = \{-1, -2, -3, \ldots\}$. Then P is not order-isomorphic to A.

Proof.

Well Ordered Sets and Initial Segment

Definition

Let A be an ordered set. Then A is said to be well-ordered if every subset of A contains a first element.

Note: Any well-ordered set A is linearly ordered.

Proof. Let A be a well ordered set. Also, Let $a, b \in A$, then the subset $\{a, b\}$ of A has a first, which, therefore, must precede the other. Hence any two elements of A are comparable.

Theorem 1

Let A be a well-ordered set. Then:

(i) Every subset of A is well-ordered.

(ii) If B is similar to A, then B is well-ordered.

Example 1

Consider the following two subsets of well-ordered set P:

$A_1 = \{1, 3, 5, \ldots\}$ and $A_2 = \{2, 4, 6, \ldots\}$

Then A_1 and A_2 are also well-ordered.

Suppose the union

$S = A_1 \cup A_2 = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$

is ordered from left to right. Then S is also well-ordered.

Initial Segments

Let A be a well-ordered set. The initial segment $s(a)$ of an element $a \in A$ consists of all elements in A which strictly precedes a. In other words,

$$s(a) = \{x : x \in A, x < a\}$$

Consider the well-ordered set S as in previous example, that is, $S = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$ ✓

Then $s(1) = \phi$, $s(5) = \{1, 3\}$,

$s(2) = \{1, 3, 5, \ldots\}$

$s(8) = \{1, 3, 5, \ldots, 2, 4, 6\}$

Theorem 2

Let $S(A)$ denote the collection of all initial segments of elements in a well-ordered set A, and let $S(A)$ be ordered by set inclusion $\subseteq$. Then A is similar to $S(A)$ and, in particular, the function $f: A \to S(A)$ defined by $f(x) = s(x)$ is a similarity mapping between A and $S(A)$.

Consider the set $A = \{1, 2, 3\}$ with usual ordering.

Here $s(1) = \phi$, $s(2) = \{1\}$, $s(3) = \{1, 2\}$

Now $S(A) = \{\phi, \{1\}, \{1, 2\}\}$ ✓

Let $f: A \to S(A)$ defined by $f(x) = s(x)$.

Means $f(1) = s(1) = \phi$, $f(2) = s(2) = \{1\}$,

$f(3) = s(3) = \{1, 2\}$.

Theorem 2

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

Here $1 < 2 \Rightarrow f(1) < f(2)$

$\phi \subset \{1\}$

$2 < 3 \Rightarrow f(2) < f(3)$

$\Rightarrow \{1\} \subseteq \{1, 3\}$

$1 < 3 \Rightarrow f(1) < f(3)$

$\Rightarrow \phi \subseteq \{1, 3\}$

Transfinite Induction and Limit Elements

Principle of Transfinite Induction

Let S be a subset of a well-ordered set A with the following two properties:

Limit Elements

An element a in a well-ordered set A is called a limit element if it does not have an immediate predecessor and if it is not the first element.

Consider two finite well-ordered sets:

Comparison of Well-Ordered Sets

Suppose A and B are well-ordered sets, and suppose A is similar to an initial segment of B. Then A is said to be shorter than B, and B is said to be longer than A.

Comparison of Well-Ordered Sets

Ordinal Numbers

Consider a collection C of well-ordered sets. Each well-ordered set A in C is assigned a symbol in such a way that any two well-ordered sets A and B are assigned the same symbol if and only if A and B are similar. This symbol is called the ordinal number of A. We will write

$$\lambda = \text{ord}(A)$$

to indicate that λ is the ordinal number of A.

Finite Ordinal Numbers

The ordinal number of each of the well-ordered sets

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

is denoted by 0, 1, 2, 3,… respectively, and is called a finite ordinal numbers. All other ordinals are called transfinite numbers.

Note: Since any two finite well-ordered sets with the same number of elements are similar, 0, 1, 2, 3, …are the only finite ordinal numbers.

Ordinal Number of *P*

The ordinal number of the set P of counting numbers is denoted by ω.

Inequalities and Ordinal Numbers

Let λ and μ be ordinal numbers and let A and B be two well-ordered sets such that $\lambda = \text{ord}(A)$ and $\mu = \text{ord}(B)$. Then

$$\lambda < \mu$$

if A is similar to an initial segment of B. Accordingly,

Examples

Choice Function and Axiom of Choice

Choice Function

Let C be a non-empty set of non-empty sets. A function $f : C \to \cup C$ is called a choice function for C if $f(A) \in A$ for all $A \in C$.

Example 1

Let C be the set of countries on earth, thinking of each country as a collection of cities. Then $\cup C$ is the set of all cities on earth, and the function f that assigns to each country its capital city is an example of a choice function for C.

$f : C \to \cup C$

For example,

let $A \in C$ denotes Pakistan, then $f(A) =$ Islamabad $\in A$.

$A =$ Pakistan Here $f(A) \in A$

Example 2

$f : C \to \cup C$

Let C be the collection of all pairs of shoes in the world. Then the function that picks the left shoe out of each pair is a choice function for C. Let A = pair of shoes, $f(A)$ = Left shoe $\in A$

Example 3 $N = \{1, 2, 3, \ldots\}$

Let $C = P(N) \setminus \{\emptyset\}$. The function $f(A) = \min(A)$ is a choice function on A.

$A = \{1, 2, 3\}$ then $f(A) = 1 \in A$ so $f(A) \in A$

Notice that in these examples, and in most other examples the reader might think of, the choice function f is defined by some rule: "choose the left shoe", "choose the least element", "choose the capital city", and so on. In all of these we simply define the choice function.

What the axiom of choice does is guarantee that there always exist choice functions, even in the absence of such a rule for defining one easily.

Axiom of Choice

Let C be a non-empty set of non-empty sets. There exists a choice function for C.

The statement seems simple, but this is a subtle idea. To a non-mathematician, we might summarize the statement as, "If you have a bunch of choices, each of which is possible to make, then you can make all of them."

Well Ordering Theorem

Recall that the set of positive numbers with the order $\leq$ is well-ordered. In general, a set with some order is called well-ordered if any nonempty subset has a least element. The set of even numbers and the set {1, 5, 17, 12} with usual order on numbers are two examples of well-ordered sets and you can check this. However, the set of integers with our usual ordering on it is not well-ordered, neither is the set of rational numbers, nor the set of all positive rational numbers.

Whether a set is well-ordered or not depends on how you define the order on the set.

Well Ordering Theorem

Every set can be well-ordered.

Although Z with our usual $\leq$ is not well-ordered, we can define another kind of order on it which does make it well-ordered. Let's call this order $\preceq$ instead $<$. We define it as follows:

$a \prec b$ whenever $|a| < |b|$ or if $|a| = |b|$ and a is negative and b is a positive number. As an example, we have :

$|-9| < |20|$ so $-9 \prec -20$, $|-2| = |2|$ so $-2 \prec 2$,

$|0| < |5|$ so $0 \prec 5$ $\quad Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$|-1| < |-5|$ so $-1 \prec -5$

Zorn's Lemma

Let X be a nonempty partially ordered set in which every chain (linearly ordered subset) has an upper bound in X. Then X contains at least one maximal element.

Consider the partially ordered set $X = \{1, 2, 3, 4, 6, 12, 24\}$ ordered by divisibility. It has three chains $\{1, 2, 4, 12, 24\}$, $\{1, 2, 6, 12, 24\}$ and $\{1, 3, 6, 12, 24\}$. All chains has an upper bound 24. Also maximal element of X is 24.

Theorem

The following are equivalent:

1) Axiom of choice;
2) Well ordering theorem;
3) Zorn's lemma.

Propositions and Compound Propositions

Propositions

A proposition is a declarative sentence which is true or false, but not both. Consider, for example, the following eight sentenes:

(i) Paris is in France.
(ii) 1+1=2
(iii) 2+2=3
(iv) Islamabad is in Sri lanka.
(v) $9 < 6$
(vi) $x = 2$ is a solution of $x^2 = 4$.
(vii) Where are you going?
(viii) Do your homework.

Notation

We use letters to denote propositional variables, that is, variables that represent propositions, just as letters are used to denote numerical variables. The conventional letters used for propositional variables are *p, q, r, s*, ….

The **truth value** of proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition.

Compound Proposition

Many mathematical statements are constructed by combining one or more propositions. New propositions, called compound propositions, are formed from existing propositions using logical operators.

Example:

1) "Roses are red and violets are blue" is a compound proposition.
2) John is intelligent or studies every night.

Basic Logical Operations

Conjunction $p \wedge q$

Any two propositions can be combined by the word "and" to form a compound proposition called the conjunction of the original propositions. Symbolically, $p \wedge q$ read "p and q" denotes the conjunction of p and q.

Truth Value:

Since $p \wedge q$ is a proposition it has a truth value, and this truth value depends on the truth values of p and q. Specifically:

If p and q are true, then $p \wedge q$ is true; otherwise $p \wedge q$ is false.

Conjunction $p \wedge q$

Any two propositions can be combined by the word "and" to form a compound proposition called the conjunction of the original propositions. Symbolically, $p \wedge q$ read "p and q" denotes the conjunction of p and q.

Truth Value:

Since $p \wedge q$ is a proposition it has a truth value, and this truth value depends on the truth values of p and q. Specifically:

If p and q are true, then $p \wedge q$ is true; otherwise $p \wedge q$ is false.

Truth Table of $p \wedge q$ and Examples

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Examples:

1) Paris is in France and $2+2=4$. True

2) Paris is in England and $2+2=4$. False.

3) Paris is in France and $2+2=5$. False.

4) Paris is in England and $2+2=5$. False.

Disjunction $p \vee q$

Any two propositions can be combined by the word "or" to form a compound proposition called the disjunction of the original propositions. Symbolically, $p \vee q$ read "p or q", denotes the disjunction of p and q.

Truth Value:

The truth value of $p \vee q$ depends only on the truth values of p and q as follows:

If p and q are false, then $p \vee q$ is false; otherwise $p \vee q$ is true.

Truth Table of $p \vee q$ and Examples

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

1) Paris is in France or $2+2=4$. T

2) Paris is in England or $2+2=4$. T

3) Paris is in France or $2+2=5$. T

4) Paris is in England or $2+2=5$. F

Negation

Let p be a proposition. The negation of p, denoted by $\sim p$, is the statement "It is not the case that p" The proposition $\sim p$ is read "not p".

Truth Value:

The truth value of the negation of p is the opposite of the truth value of p.

Truth Table of $\sim p$ and Examples

p	$\sim p$
T	F
F	T

Examples:

1) Paris is in France.
Negation is "Paris is not in France".

2) $2+2=5$.
Negation is "$2+2 \neq 5$".

More Logical Operations

Conditional Statement

Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition "if p then q". The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \rightarrow q$, p is called the hypothesis and q is called the conclusion.

Useful Way to Understand the Truth Value:

Consider a statement that a professor might make:

"If you get 100% on the final, then you will get A."

If you manage to get 100% on the final, then you would expect to receive an A. If you do not get 100% you may or may not receive an A. However, if you do get 100%, but the professor does not give you an A, you will feel cheated.

Different Form of Conditional Statement

Because conditional statements play such an essential role in mathematical reasoning, a variety of terminology is used to express $p \rightarrow q$. You will encounter most if not all of the following ways to express this conditional statement:

"if p, then q"
"p implies q"
"p implies q"
"q whenever p"
"p is sufficient for q"
"q if p"
"q when p"

Truth Table of $p \rightarrow q$ and $\sim p \vee q$

1) $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

2) $\sim p \vee q$

p	q	$\sim p$	$\sim p \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

$p \rightarrow q \equiv \sim p \vee q$

Observe that the truth tables of $p \rightarrow q$ *and* $\sim p \vee q$ are identical. Accordingly, $p \rightarrow q$ *and* $\sim p \vee q$ are logically equivalent.

In other words, the conditional statement "If p then q" is logically equivalent to the statement "Not p or q"

$\sim p \vee q$

Example 1

Let p be the statement "Maria learns discrete mathematics" and q the statement "Maria will find a job." Express the statement $p \rightarrow q$ as a statement in English.

Solution: If Maria learns discrete mathematics, then she will find a good job.

There are other ways to express this conditional statement in English.

Maria will find a good job when she learns discrete mathematics. q when p

Biconditional Statement

Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition "p if and only if q." The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise.

Truth table is given below:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Truth table of $(p \rightarrow q) \wedge (q \rightarrow p)$ and $p \leftrightarrow q$

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Example 2

Let p be the statement "You can take the flight," and let q be the statement "You buy a ticket." Then $p \leftrightarrow q$ is the statement

"You can take the flight if and only if you buy a ticket."

Truth Tables of Compound Propositions

We have now introduced four important logical connectives– conjunctions, disjunctions, conditional statements, and biconditional statements– as well as negations. We can use these connectives to build up complicated compound propositions involving any number of propositional variables. We can use truth tables to determine the truth values of these compound propositions.

Example 1

Construct the truth table of the compound proposition $(p \vee \sim q) \rightarrow (p \wedge q)$.

p	q	$\sim q$	$p \vee \sim q$	$p \wedge q$	$(p \vee \sim q) \rightarrow (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Example 2

Construct the truth table of the compound proposition $(p \rightarrow q) \vee (\sim p \rightarrow r)$.

p	q	r	$\sim p$	$p \rightarrow q$	$\sim p \rightarrow r$	$(p \rightarrow q) \vee (\sim p \rightarrow r)$
T	T	T	F	T	T	T
T	T	F	F	T	T	T
T	F	T	F	F	T	T
T	F	F	F	F	T	T
F	T	T	T	T	T	T
F	T	F	T	T	F	T
F	F	T	T	T	T	T
F	F	F	T	F	F	F

Tuatologies and Contradictions

A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called tautology. A compound proposition that is always false is called a contradiction.

Example 1

The proposition $p \vee \sim p$ is a tautology and the proposition $p \wedge \sim p$ is a contradiction.

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
F	T	T	F

Logical Equivalences

Compound propositions that have the same truth values in all possible cases are called logically equivalent. We can also define this notion as follows.

"The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent."

Example 1

One way to determine whether two compound propositions are equivalent is to use a truth table.

Consider the two propositions $\sim(p \vee q)$ and $\sim p \wedge \sim q$. Truth tables for $\sim(p \vee q)$and $\sim p \wedge \sim q$ are given below:

p	q	p ∨ q	~(p ∨ q)	~p	~q	~p ∧ ~q
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

So $\sim(p \vee q) \equiv \sim p \wedge \sim q$

Example 2

Show that $p \rightarrow q$ and $\sim p \vee q$ are logically equivalent. $p \rightarrow q \equiv \sim p \vee q$

p	q	p → q	~p	~p ∨ q
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Proved.

Example 3

Show that $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$ and ~~[illegible]~~ are logically equivalent.

p	q	r	p → q	p → r	(p → q) ∧ (p → r)	q ∧ r	p → (q ∧ r)
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	F	T	F	F	F
T	F	F	F	F	F	F	F
F	T	T	T	T	T	T	T
F	T	F	T	T	T	F	T
F	F	T	T	T	T	F	T
F	F	F	T	T	T	F	T

Proved

Logical Equivalences involving Conditional Statements

1) $p \rightarrow q \equiv \sim p \vee q$
2) $p \rightarrow q \equiv \sim q \rightarrow \sim p$
3) $p \vee q \equiv \sim p \rightarrow q$
4) $p \wedge q \equiv \sim(p \rightarrow \sim q)$
5) $\sim(p \rightarrow q) \equiv p \wedge \sim q$
6) $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
7) $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
8) $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
9) $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Logical Equivalences involving Biconditional Statements

1) $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
2) $p \leftrightarrow q \equiv \sim p \leftrightarrow \sim q$
3) $p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$
4) $\sim(p \leftrightarrow q) \equiv p \leftrightarrow \sim q$

Algebra of Propositions

1) Idempotent Laws
   (1a) $p \vee p \equiv p$ (1b) $p \wedge p \equiv p$
2) Associative Laws
   (2a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$ (2b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
3) Commutative Laws
   (3a) $p \vee q \equiv q \vee p$ (3b) $p \wedge q \equiv q \wedge p$
4) Distributive Laws
   (4a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
   (4b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
5) Identity Laws
   (5a) $p \wedge T \equiv p$ (5b) $p \vee F \equiv p$

p	T	p ∧ T
T	T	T
F	T	F

p	F	p ∨ F
T	F	T
F	F	F

6) Domination Laws
   (6a) $p \vee T \equiv T$ (6b) $p \wedge F \equiv F$
7) Double negation law
   $\sim(\sim p) \equiv p$
8) De Morgan's Laws
   (8a) $\sim(p \wedge q) \equiv \sim p \vee \sim q$
   (8b) $\sim(p \vee q) \equiv \sim p \wedge \sim q$
9) Absorption Laws
   (9a) $p \vee (p \wedge q) \equiv p$ (9b) $p \wedge (p \vee q) \equiv p$
10) Negation laws
   (10a) $p \vee \sim p \equiv T$ (10b) $p \wedge \sim p \equiv F$

Prove $p \vee \sim p \equiv T$.

p	~p	p ∨ ~p ≡ T	p ∧ ~p ≡ F
→ T	F	T	F
→ F	T	T	F

11) Distributive laws
   (11a) $p \vee (q$

Constructing New Logical Equivalences

The logical equivalences that have been established so far can be used to construct additional logical equivalences. This technique is illustrated in the following examples.

Example 1

Show that $\sim(p \to q)$ and $p \wedge \sim q$ are logically equivalent.

Sol We want to prove $\sim(p \to q) \equiv p \wedge \sim q$.

$\sim(p \to q) \equiv \sim(\sim p \vee q)$

$\equiv \sim(\sim p) \wedge \sim q$, by DeMorgan Law

$\equiv p \wedge \sim q$, by the double negation Law.

$p \to q \equiv \sim p \vee q$

Example 2

Show that $\sim(p \vee (\sim p \wedge q))$ and $\sim p \wedge \sim q$ are logically equivalent by developing a series of logical equivalences.

$\sim(p \vee (\sim p \wedge q)) \equiv \sim p \wedge \sim(\sim p \wedge q)$, by the DeMorgan Law

$\equiv \sim p \wedge [\sim(\sim p) \vee \sim q]$, //

$\equiv \sim p \wedge [p \vee \sim q]$, by the double negation Law.

$\equiv (\sim p \wedge p) \vee (\sim p \wedge \sim q)$, by the distributive Law.

$\equiv F \vee (\sim p \wedge \sim q)$

$\equiv \sim p \wedge \sim q$, by the identity Law.

Example 3

$p \vee p \equiv p$

$p \to q \equiv \sim p \vee q$

Show that $(p \wedge q) \to (p \vee q)$ is a tautology.

$(p \wedge q) \to (p \vee q) \equiv \sim(p \wedge q) \vee (p \vee q)$

$\equiv (\sim p \vee \sim q) \vee (p \vee q)$, by the DeMorgan law

$\equiv (\sim p \vee p) \vee (\sim q \vee q)$, by the asso. and the comm. Law

$\equiv T \vee T$

$\equiv T$, by the domination Law.

Example 4

Show that $\sim((p \to q) \wedge p) \vee q$ is a tautology.

$\sim((p \to q) \wedge p) \vee q$

$\equiv \sim((\sim p \vee q) \wedge p) \vee q$

$\equiv \sim((\sim q \vee q) \wedge p) \vee q$

$\equiv \sim(T \wedge p) \vee q$

$\equiv \sim T \vee q$

$\equiv F \vee q$

$\equiv q \vee \sim p$

$\equiv \sim q \vee \sim p$

$\equiv \sim(q \wedge p)$

$\equiv \sim(p \wedge q)$

$\equiv T$

Converse, Contrapositive, and Inverse

We can form some new conditional statements starting with a conditional statement $p \to q$. In particular, there are three related conditional statements that occur so often that they have special names.

Converse of $p \to q$

The proposition $q \to p$ is called the converse of $p \to q$.

Example 1: Write the converse of the conditional statement "The home team wins whenever it is raining". q whenever p = If p then q

"If it is raining, then the home team wins."

Now the converse is:

If the home team wins, then it is raining.

Contrapositive of $p \to q$

The contrapositive of $p \to q$ is the proposition $\sim q \to \sim p$. We first show that the contrapositive, $\sim q \to \sim p$ of a conditional statement $p \to q$ always has the same truth value as $p \to q$.

p	q	$\sim p$	$\sim q$	$p \to q$	$\sim q \to \sim p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

$\therefore p \to q \equiv \sim q \to \sim p$

Example 2: Write the contrapositive of the conditional statement "The home team wins whenever it is raining".

"If it is raining, then the home team wins."

Contrapositive is:

"If the home team does not win, then it is not raining."

Inverse of $p \to q$

The proposition $\sim p \to \sim q$ is called the inverse of $p \to q$. We will show that the converse and the inverse of a conditional statement are also equivalent.

p	q	$\sim p$	$\sim q$	$\sim p \to \sim q$	$q \to p$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	T	T	T

$\therefore \sim p \to \sim q \equiv q \to p$

Example 3: Write the inverse of the conditional statement "The home team wins whenever it is raining".

"If it is raining, then the home team wins."

Inverse is:

If it is not raining, then the home team does not win."

Example 4

State the converse, contrapositive, and inverse ~~of each of~~ of "A positive integer is a prime only if it has no divisors other than 1 and itself."

"If a positive integer is a prime, then it has no divisors other than 1 and itself."

Converse is:

"If a positive integer has no divisors other than 1 and itself, then a positive integer is a prime."

then
If p and q,
or
p only if q.
$p \to q$
converse: $q \to p$
contrapositive: $\sim q \to \sim p$

Example 4

contrapositive is:
"If a positive integer has a divisor other than 1 and itself, then it is not prime".

Inverse is:
"If a positive integer is not prime, then it has a divisor other than 1 and itself."

$p \to q$
Inverse is:
$\sim p \to \sim q$

Argument

Argument and Valid Argument

An argument in propositional logic is a sequence of propositions. All but the final proposition in the argument are called premises and the final proposition is called the conclusion.

An argument is valid if the truth of all its premises implies that the conclusion is true.

It means the argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid, when $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is a tautology.

Example to Understand valid Argument

Consider the following argument involving propositions:

1) "If you have a current password, then you can log onto the network." (p, q)
2) "You have a current password." $= p$

Therefore,

3) "You can log onto the network." (conclusion) $= q$

$p \to q$
p
$\therefore q$

$(p \to q) \wedge p \to q$ is a tautology?

p	q	$p \to q$	$(p \to q) \wedge p$	$((p \to q) \wedge p) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	F	F	T

Example to Understand valid Argument

Suppose
p : You have access to the network.
q : You can change your grade
Also p is true, but $p \to q$ is false.

"If you have access to the network, then you can change your grade"
"You have access to the network."
Therefore,
"You can change your grade".

$p \to q$
p
$\therefore q$

Example to Understand valid Argument

The argument we obtained is a valid argument, but because one of the premises, namely the $p \to q$ is false, we cannot conclude that the conclusion is true.

In next topic, we will see more valid argument forms.

Rules of Inference for Propositional Logic

The tautology $(p \wedge (p \rightarrow q)) \rightarrow q$ is the basis of the rule of inference called modus ponens, or the law of detachment. This tautology leads to the following valid argument form:

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Example 1

Suppose that the conditional statement "If it snows today , then we will go skiing" and its hypothesis, "It is snowing today," are true. Then, by law of detachment, it follows that the conclusion of the conditional statement, "We will go skiing," is true. In notation form, we see that

p : "It is snowing today."
q : "we will go skiing."

$$\begin{array}{l} p \rightarrow q \ \checkmark \\ p \quad \checkmark \\ \hline \therefore q \end{array}$$

We can conclude that by law of detachment that "we will go skiing" is true.

Example 2

Determine whether the argument given here is valid and determine whether its conclusion must be true because of the validity of the argument.

"If $\sqrt{2} > \frac{3}{2}$, then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Consequently, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.

Solution.

Let $p : \sqrt{2} > \frac{3}{2}$ and $q : (\sqrt{2})^2 > (\frac{3}{2})^2$ ($\because 2 < \frac{9}{4}$).

Here $p \rightarrow q$ } = Law of detachment.
$\times p$
$\therefore q$ } Now we want to determine is true or not? Here one of its premises is false, which is $\sqrt{2} > \frac{3}{2}$. We cannot conclude that the conclusion is true.

Rules of Inference

1) $\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$ $(p \wedge (p \rightarrow q)) \rightarrow q$ is a tautology. (Modus ponens)

2) $\begin{array}{l} \sim q \\ p \rightarrow q \\ \hline \therefore \sim p \end{array}$ $((\sim q \wedge (p \rightarrow q)) \rightarrow \sim q$ is a tautology. (Modus tollens)

3) $\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$ $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ is a tautology. (Hypothetical syllogism)

4) $\begin{array}{l} p \vee q \\ \sim p \\ \hline \therefore q \end{array}$ $((p \vee q) \wedge \sim p) \rightarrow q$ is a tautology. (Disjunctive syllogism)

Rules of Inference

5) $\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$ $p \rightarrow (p \vee q)$ is a tautology. (Addition)

6) $\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$ $p \wedge q \rightarrow p$ is a tautology (simplification)

7) $\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$ $(p \wedge q) \rightarrow p \wedge q$ is a tautology (conjunction)

8) $\begin{array}{l} p \vee q \\ \sim p \vee r \\ \hline \therefore q \vee r \end{array}$ $((p \vee q) \wedge (\sim p \vee r)) \rightarrow q \vee r$ is a tautology. (Resolution)

Examples Using Rules of Inference

Example 1

Find the argument form for the following argument and determine whether it is valid. Can we conclude that the conclusion is true if the premises are true?

If Socrates is human, then Socrates is mortal.
Socrates is human.
∴Socrates is mortal. (conclusion)

Let p: Socrates is human.
q: Socrates is mortal.

$$\begin{array}{l} p \rightarrow q \ \checkmark \\ p \ \checkmark \\ \hline \therefore q \ \checkmark \end{array}$$

This is Modus ponens.
Here the conclusion is true if the premises are true because it is a valid argument.

Example 2

What rule of inference is used in each of these arguments?

a) Salman is a mathematics major. Therefore, Salman is either a mathematics major or a computer science major.

Sol: Let p: Salman is a mathematics major.
q: " " computer science major.

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$ Here addition is used.

b) Ezaan is a mathematics major and a computer science major. Therefore, Ezaan is a mathematics major.

Sol: Let p: Ezaan is a mathematics major.
q: Ezaan is a computer science major.

$$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$$ Here simplification is used.

Example 2

c) If it is rainy, then the pool will be closed. It is rainy. Therefore, the pool is closed.

Sol: Let p: it is rainy.
q: the pool is closed.

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

Here Modus ponens is used.

d) If it snows today, the university will close. The university is not closed today. Therefore, it did not snow today.

Sol: Let p: It snows today.
q: the university is closed.

Here the argument is:

$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \neg p \end{array}$$

Here Modus tollens is used.

Example 3

Use rules of inference to show that the hypotheses "Khan works hard," "If Khan works hard, then he is a dull boy," and "If Khan is a dull boy, then he will not get a job" imply the conclusion "Khan will not get the job."

Sol: Let p: Khan works hard.
q: Khan is a dull boy.
r: he will get a job.

Hypothesis are:
p
$p \rightarrow q$
$q \rightarrow \neg r$

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Therefore, we have reached the conclusion.

Now we will use the conclusion q as a hypothesis in the 2nd stage.

$$\begin{array}{l} q \ \checkmark \\ q \rightarrow \neg r \ \checkmark \\ \hline \therefore \neg r \end{array}$$

Propositional Functions

Propositional Functions

Let A be a given set. A propositional function(or an open sentence) defined on A is an expression

$$p(x)$$

which has the property that $p(a)$ is true or false for each $a \in A$. That is, $p(x)$ becomes a statement (with a truth value) whenever any element $a \in A$ is substituted for the variable x.

Domain and Truth Set of $p(x)$

The set A is called the domain of $p(x)$, and the set T_p of all elements of A for which $p(a)$ is true is called the truth set of $p(x)$. In other words,

$$T_p = \{x : x \in A, p(x) \text{ is true}\}$$

Note: Frequently, when A is some set of numbers, the condition $p(x)$ has the form of an equation or inequality involving the variable x.

Example 1

Let $p(x)$ denote the statement "$x > 3$." What are the truth values of $p(4)$ and $p(2)$?

Solution.

Here $p(x): x > 3$

So $p(4): 4 > 3$ is a true statement.

Also $p(2): 2 > 3$ is a false statement.

Hence $p(4)$ is true and $p(2)$ is false.

Example 2

Let $p(x)$ denote the statement "*the word x contains the letter a.*" What are the truth values of $P(orange)$ and $P(lemon)$?

Solution.

Here $p(x)$: the word x contains the letter a.

So $p(orange)$: the word orange contains the letter a, which is a true statement.

and $p(lemon)$: the word lemon contains the letter a, which is a false statement.

Example 3

Let $p(x)$ denote the statement "$x + 2 > 7$." Find the truth set T_p of each propositional function $p(x)$ defined on the set $P = \{1,2,3,\dots\}$.

Solution. Here $p(x): x + 2 > 7$.

So $T_p = \{x : x \in P, x + 2 > 7\} =$

$= \{6, 7, 8, \dots\}$

Example 4

Let $p(x)$ denote the statement "$x + 5 < 3$." Find the truth set T_p of each propositional function $p(x)$ defined on the set $P = \{1,2,3, \dots\}$.

Solution.

Here $p(x): x + 5 < 3$.

Now, $T_p = \{\} = \emptyset$ because $p(x)$ is not true for any value from the domain set P.

Example 5

Let $p(x)$ denote the statement "$x + 5 > 1$." Find the truth set T_p of each propositional function $p(x)$ defined on the set $P = \{1,2,3, \dots\}$.

Solution.

Here $p(x): x + 5 > 1$.

So, $T_p = \{1, 2, 3, \dots\} = P$.

Propositional Function of Two Variables

We can also have expressions that involve more than one variable. For instance, consider the expression "$x = y + 3$." We can denote this expression by $Q(x, y)$, where x and y are variables. When value are assigned to the variables x and y, the statement $Q(x, y)$ has a truth value.

Example 5

Let $Q(x, y)$ denote the statement "$x = y + 3$." What are the truth values of the propositions $Q(1,2)$ and $Q(3,0)$?

Solution.

Here $Q(x,y)$: "$x = y + 3$"

So, $Q(1,2)$: "$1 = 2 + 3$" is a false statement

and $Q(3,0)$: $3 = 0 + 3$ is a true statement.

Propositional Function of n Variables

In general, a statement involving n variables $x_1, x_2, \dots, x_n$ can be denoted by $p(x_1, x_2, \dots, x_n)$.

A statement of the form $p(x_1, x_2, \dots, x_n)$ is the value of the propositional function p at the n-tuple $(x_1, x_2, \dots, x_n)$.

Existential Quantifier

Existential Quantifiers

Let $p(x)$ be a proposition function defined on a set A. Consider the expression

Which reads

Statement in (1) is equivalent to the statement

Example 1

a) The proposition $(\exists n \in P)(n + 4 < 7)$ is true since

b) The proposition $(\exists n \in P)(n + 6 < 4)$ is false since

Example 2

What is the truth value of $\exists x p(x)$, where $p(x)$ is the statement "$x^2 > 10$" and the domain consists of the positive integers not exceeding 4?

Example 3

Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.

a) $\exists x(x^2 = 2)$

b) $\exists x(x^2 = -1)$

c) $\forall x(x^2 + 2 \geq 1)$

d) $\forall x(x^2 \neq x)$

Universal and Existential Quantifier as Conjunction and Disjunction

Consider the propositional function $p(x)$ as "x is prime" with domain set $A = \{2,3,5\}$.

Consider the propositional function $p(x)$ as "$x^2 > 10$" with domain set $A = \{1,2,3,4\}$.

Negation of Quantified Statements

Negation of Universal Quantifier

Consider the propositional function $p(x)$ as "x has taken a course in calculus" and the domain consists of the students in your class. Then the statement:

"Every student in your class has taken a course in calculus." This statement is a universal quantification, namely,

Negation of Universal Quantifier

Negation of Existential Quantifier

Consider the proposition,

"There is a student in this class who has taken a course in calculus." This is the existential quantification, namely,

Negation of Existential Quantifier

Consider the proposition,

"There is a student in this class who has taken a course in calculus." This is the existential quantification, namely,

Example 1

What are the negations of the statements $\forall x(x^2 > x)$ and $\exists x(x^2 = 2)$.

Example 2

Suppose that the domain of the propositional function $p(x)$ consists of the integers 0, 1, 2, 3 and 4. Write out each of these propositions using disjunctions, conjunctions, and negations.

a) $\exists x p(x)$

b) $\forall x p(x)$

c) $\exists x \sim p(x)$

d) $\forall x \sim p(x)$

e) $\sim \exists x p(x)$

f) $\sim \forall x p(x)$

Introduction to Proofs

Some Terminology

Theorem:

Propositions:

Proof:

Axioms

Lemma:

Some Terminology

Corollary:

Conjecture:

Methods of Proving Theorems Part 1

Proving mathematical theorems can be difficult. To construct proofs we need all available ammunition, including a powerful of different proof methods. These methods provide the overall approach and strategy of proofs. Understanding these methods is a key component of learning how to read and construct mathematical proofs.

In this course, we will focus on proving the conditional statements. The followings proofs technique will be discussed here:

1) Direct proofs
2) Indirect proofs

Direct Proofs

A direct proof of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using axioms, definitions, and previously proved theorems, together with rules of inference, to show that q must also be true. Before we give the first example, we need to define some terminology.

Even and Odd Integers

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$.

Example 1

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution:

Example 2

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

Solution:

Example 3

Prove that if n is any even integer, then $(-1)^n = 1$.

Solution:

Example 5

Use a direct proof to show that the product of two rational numbers is rational.

Solution.

Exercise

1) Prove that the product of an even integer and an odd integer is even.
2) Prove that the square of an even integer is even.
3) Prove that if n is an odd integer, then $n^3 + n$ is even.
4) Prove that the sum of any three consecutive integers is divisible by 3.

Methods of Proving Theorems
Part 2

Indirect Proofs

Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion. However, we will see that attempts at direct proofs often reach dead ends. Proofs of theorems that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called indirect proofs.

Proof by Contraposition

Proofs by contraposition make use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive, $\sim q \to \sim p$. In a proof by contraposition of $p \to q$, we take $\sim q$ as premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\sim p$ is true.

Example 1

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution.

Example 2

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or b$\leq \sqrt{n}$.
Solution.

Example 3

Prove that if n is an integer and n^2 is odd, then n is odd.
Solution.

Proof by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\sim p \rightarrow q$ is true. Because q is false, but $\sim p \rightarrow q$ is true, we can conclude that $\sim p$ is false, which means that p is true.

Because the statement $r \wedge \sim r$ is a contradiction whenever r is proposition, we can prove that p is true if we can show that $\sim p \rightarrow (r \wedge \sim r)$ is true. Proofs of this type are called proofs by contradiction.

Example 4

Prove that $\sqrt{2}$ is irrational.

Example 4

Proof by contradiction can be used to prove conditional statements. In such proofs, we first assume the negation of the conclusion. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction.

Example 5

Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

Example 6

Show that if n is an integer and $n^3 + 5$ is odd, then n is even using

a) a proof by contraposition
b) A proof by contradiction

Example 6

Example 7

Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.