SETS AND LOGIC

The basic concepts that we work with are

a) Propositions $\longleftrightarrow$ Boolean Algebra
b) Sets $\longleftrightarrow$ Set Algebra
c) Predicates and quantifiers $\longleftrightarrow$ 1st-order logic

Propositions

• A proposition (or statement) p is an expression which is either TRUE or FALSE.

EXAMPLES

a) $3+5=8$ is a proposition with truth value T.
b) $1+1=3$ is a proposition with truth value F.
c) $2+(10-3)^2$ is an expression but is not a proposition.

• Given the statements p, q we define compound statements as follows

p	q	$p \vee q$	$p \wedge q$	$p \underline{\vee} q$	$\bar{p}$	$p \Rightarrow q$	$p \Leftrightarrow q$
T	T	T	T	F	F	T	T
T	F	T	F	T	F	F	F
F	T	T	F	T	T	T	F
F	F	F	F	F	T	T	T

- Interpretations

$p \vee q$	Disjunction	p is true or q is true (or both) at least one of p or q is true
$p \wedge q$	Conjunction	p is true and q is true
$p \veebar q$	Exclusive Disjunction	either p or q is true (but not both)
$\bar{p}$	Negation	p is false
$p \Rightarrow q$	Implication	if p is true then q is true p implies q p is true only if q is true
$p \Leftrightarrow q$	Equivalence	p is true if and only if q is true p is equivalent to q p, q have the same truth value

↳ Note that if p is false we presume that the compound statement $p \Rightarrow q$ is TRUE regardless of the truth value of q. This is necessary to ensure that $p \Leftrightarrow q$ and $(p \Rightarrow q) \wedge (q \Rightarrow p)$ have the same truth table, as shown below:

p	q	$p \Leftrightarrow q$	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

For example, statements of the form

$1+1=3 \Rightarrow 2=2$

$2+3=8 \Rightarrow 3=2$

are TRUE even though the corresponding hypotheses are false.

Boolean algebra

- A boolean expression is an abstract expression that involves:

a) propositions, represented by lower-case letters (e.g. p, q, r, etc)

b) Boolean operations: $\wedge$ (conjunction), $\vee$ (disjunction), $\veebar$ (exclusive disjunction), $\overline{}$ (negation), $\Rightarrow$ (implication), $\Leftrightarrow$ (equivalence)

c) T : a proposition with truth value fixed at TRUE.

d) F : a proposition with truth value fixed at FALSE

e) Parenthesis, to prioritize the order of boolean operations.

- Given two boolean expressions P, Q:

  $P \equiv Q$: P and Q have the same truth table

  P tautology $\Leftrightarrow P \equiv T$

  P contradiction $\Leftrightarrow P \equiv F$

  The above are an example of "metalogic", i.e. logic about logic!

- With the above terminology we can use truth tables to establish the following properties of Boolean Algebra:

- <u>Commutative</u>

$p \wedge q \equiv q \wedge p$

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

- <u>Associative</u>

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

$p \vee (q \vee r) \equiv (p \vee q) \vee r$

- <u>Distributive</u>

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

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

- <u>Reductions</u> $\longrightarrow$ These properties allow us to rewrite all boolean expressions in terms of conjunction, disjunction, and negation.

$p \veebar q \equiv (p \wedge \bar{q}) \vee (\bar{p} \wedge q)$

$p \Rightarrow q \equiv \bar{p} \vee q$

$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

- <u>Negations</u>:

$$\left.\begin{aligned} \overline{p \wedge q} &\equiv \bar{p} \vee \bar{q} \\ \overline{p \vee q} &\equiv \bar{p} \wedge \bar{q} \end{aligned}\right\} \text{De Morgan's laws}$$

and it follows that

$$\overline{p \Rightarrow q} \equiv \overline{\bar{p} \vee q} \equiv p \wedge \bar{q}$$

and

$$\overline{p \Leftrightarrow q} \equiv \overline{(p \Rightarrow q) \wedge (q \Rightarrow p)} \equiv \overline{(p \Rightarrow q)} \vee \overline{(q \Rightarrow p)}$$
$$\equiv (p \wedge \bar{q}) \vee (\bar{p} \wedge q)$$

- Relationship between equivalence and exclusive disjunction:

$$\overline{p \Leftrightarrow q} \equiv p \veebar q$$
$$\overline{p \veebar q} \equiv p \Leftrightarrow q$$

$\hookrightarrow$ The above properties are established via truth tables, as in the following example.

EXAMPLE

Use truth tables to show that $\overline{p \wedge q} \equiv \bar{p} \vee \bar{q}$.

Solution

We note that

p	q	$p \wedge q$	$\overline{p \wedge q}$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

and

p	q	$\bar{p}$	$\bar{q}$	$\bar{p} \vee \bar{q}$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

It follows that $\overline{p \wedge q} \equiv \bar{p} \vee \bar{q}$ $\square$

<u>Methodology</u>: To show that a boolean expression is a tautology via boolean algebra

- 1 Use the reduction formulas to rewrite the boolean expression in terms of $\wedge$ (conjunction), $\vee$ (disjunction), $^{-}$ (negation)
- 2 Use the De Morgan laws to reduce all negations down to individual statements
- 3 Simplify using the associative, distributive properties in addition to the following self-evident statements:

$p \vee F \equiv p$	$p \wedge T \equiv p$	$p \vee \bar{p} \equiv T$
$p \wedge F \equiv F$	$p \vee T \equiv T$	$p \wedge \bar{p} \equiv F$

EXAMPLE

Show that $[p \wedge (p \Rightarrow q)] \Rightarrow q$ is a tautology.

<u>Solution</u>

$$S \equiv [p \wedge (p \Rightarrow q)] \Rightarrow q \equiv \overline{[p \wedge (p \Rightarrow q)]} \vee q \equiv$$
$$\equiv [\bar{p} \vee \overline{(p \Rightarrow q)}] \vee q \equiv [\bar{p} \vee (p \wedge \bar{q})] \vee q \equiv$$
$$\equiv [(\bar{p} \vee p) \wedge (\bar{p} \vee \bar{q})] \vee q \equiv [T \wedge (\bar{p} \vee \bar{q})] \vee q \equiv$$
$$\equiv (\bar{p} \vee \bar{q}) \vee q \equiv \bar{p} \vee (\bar{q} \vee q) \equiv \bar{p} \vee T \equiv T$$

and therefore $[p \wedge (p \Rightarrow q)] \Rightarrow q$ is a tautology.

EXERCISES

① Evaluate the truth value of the following statements

a) $3+7=10 \vee 1+3=4$

b) $2+1=4 \vee 1+3=5$

c) $3 \neq 4 \wedge 1+1=2$

d) $2+5=8 \wedge 3+3=6$

e) $1+4=5 \Rightarrow 3=2$

f) $3+2=0 \Rightarrow 5=6$

g) $1=2 \Rightarrow 3=3$

h) $2+3=5 \Leftrightarrow 1+1=2$

i) $3+1=2+2 \Leftrightarrow 1=0$

② In the following compound statements replace with letters (e.g. p, q, r, ...) the simple constituent statements and write the structure of the compound statements in terms of the letters you introdued

a) 30 is a multiple of 6 and divisible by 5

b) 5 is either an even or an odd number

c) If $ab=0$, then $a=0$ or $b=0$.

d) 8 is not a prime number

e) The triangles $\overset{\triangle}{ABC}$ and $\overset{\triangle}{DEF}$ are similar if and only if $\hat{A}=\hat{D}$ and $\hat{B}=\hat{E}$ and $\hat{C}=\hat{F}$.

③ Show that the following expressions are tautologies using truth tables

a) $[\bar{p} \wedge (p \vee q)] \Rightarrow q$

b) $\overline{(p \Rightarrow q)} \Leftrightarrow (p \wedge \bar{q})$

c) $\overline{(p \Leftrightarrow q)} \Leftrightarrow (\bar{p} \Leftrightarrow q)$

d $\overline{(p \Leftrightarrow q)} \Leftrightarrow (p \Leftrightarrow \bar{q})$

(4) Show that the following expressions are tautologies using boolean algebra.

a) $(p \wedge q) \Rightarrow q$

b) $p \Rightarrow (p \vee q)$

c) $[\bar{q} \wedge (p \Rightarrow q)] \Rightarrow \bar{p}$

d) $(p \underline{\vee} q) \Rightarrow (p \vee q)$

e) $(\bar{p} \wedge (\bar{q} \Rightarrow p)) \Rightarrow q$

(5) Write the expressions of the previous exercise in English

▸ Methodology: Application to inequalities.

We note that:

$\overline{x<a} \Leftrightarrow x \geq a$	$\overline{x>a} \Leftrightarrow x \leq a$
$\overline{x \leq a} \Leftrightarrow x > a$	$\overline{x \geq a} \Leftrightarrow x < a$

- Weak inequalities are defined via disjunction from strong inequalities:

  $a \leq b \Leftrightarrow (a<b \vee a=b)$

  $a \geq b \Leftrightarrow (a>b \vee a=b)$

- Composite inequalities are equivalent to conjunction of elementary inequalities. For example:

  $$a<b<c \Leftrightarrow a<b \wedge b<c \Leftrightarrow \begin{cases} a<b \\ b<c \end{cases}$$

  The braces notation is used to represent conjunction.

- We can use the above, in conjunction with boolean algebra to negate expressions involving inequalities

EXAMPLE

Negate the statement

$p: \; 0<|x-x_0|<\delta \Rightarrow 0<|y-y_0|<\varepsilon$

Solution

$$\bar{p} \equiv \overline{0<|x-x_0|<\delta \Rightarrow 0<|y-y_0|<\varepsilon}$$
$$\equiv 0<|x-x_0|<\delta \wedge \overline{0<|y-y_0|<\varepsilon}$$
$$\equiv 0<|x-x_0|<\delta \wedge (\overline{0<|y-y_0| \wedge |y-y_0|<\varepsilon})$$
$$\equiv 0<|x-x_0|<\delta \wedge (\overline{0<|y-y_0|} \vee \overline{|y-y_0|<\varepsilon})$$
$$\equiv 0<|x-x_0|<\delta \wedge (0\geq|y-y_0| \vee |y-y_0|\geq\varepsilon)$$
$$\equiv 0<|x-x_0|<\delta \wedge (y=y_0 \vee |y-y_0|\geq\varepsilon)$$

EXERCISES

⑥ Write and simplify the negation to the following statements.

a) $3x<x^2+1<5$

b) $\begin{cases} 2x+y>3 \\ x-y<1 \end{cases}$

c) $2x<1 \Leftrightarrow y>2$

d) $a<b<c \Leftrightarrow b+c+d>2$

e) $x+1<y \veebar x^2<2y<3x+5$

f) $a<b \Rightarrow (c<d \veebar c>e)$

g) $\begin{cases} x<1 \\ y\leq 2 \end{cases} \vee \begin{cases} x\geq 3 \\ y\geq 1 \end{cases}$

h) $\begin{cases} x>2 \veebar y<3 \\ z\leq 1 \end{cases}$

i) $ab\geq c \Rightarrow \begin{cases} b>d \\ a\leq d \end{cases}$

j) $\begin{cases} x\geq 1 \vee y<3 \\ z>y\geq x \end{cases}$

Sets – Definitions

- A set is an unordered collection of an arbitrary number of elements. A set can be an element of another set.

<u>notation</u>: $x \in A$: the element x belongs to A

$x \notin A$: the element x does NOT belong to A.

We also introduce the following abbreviations:

$x, y \in A \Leftrightarrow (x \in A \wedge y \in A)$

$x, y, z \in A \Leftrightarrow (x \in A \wedge y \in A \wedge z \in A)$

and so on.

Definition of sets

- Sets can be defined by providing a <u>belonging condition</u> i.e. a boolean expression $P(x)$ involving a variable x such that

$$x \in A \Leftrightarrow P(x)$$

is a tautology.

e.g. The set with elements $1, 2, 3$ can be defined by the belonging condition

$$x \in A \Leftrightarrow (x = 1 \vee x = 2 \vee x = 3)$$

Equivalently we write $A = \{1, 2, 3\}$.

- The <u>empty set</u> $\emptyset$ is a set that contains no elements. A formal definition is:

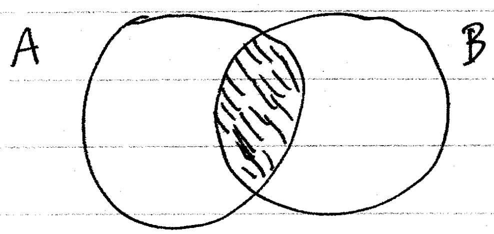
$$x \in \emptyset \Leftrightarrow F$$

▶ Operations with sets

Let A,B be two sets. We use belonging conditions to define:

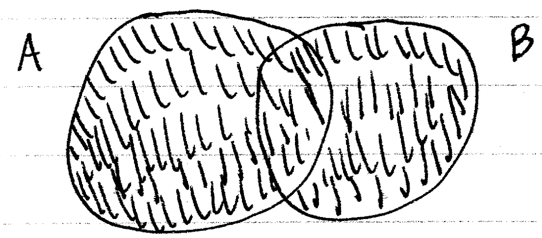
1) Intersection $A \cap B$

$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$



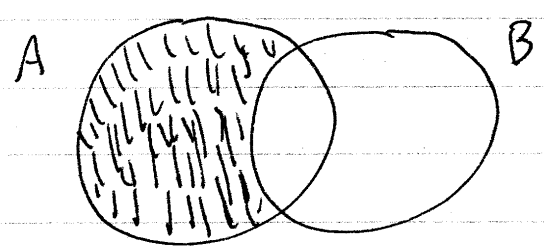
2) Union $A \cup B$

$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$



3) Difference $A - B$

$x \in A - B \Leftrightarrow x \in A \wedge x \notin B$



- <u>Relations between sets</u>

a) <u>Set equality</u>: $A = B$ (i.e. "A is equal to B") means that the sets A, B have the same elements. A formal definition requires using metalogic:

$$\boxed{\begin{aligned} &A = B \Leftrightarrow [(x \in A \Leftrightarrow x \in B) \equiv T] \\ &A \neq B \Leftrightarrow \overline{A = B} \end{aligned}}$$

For any arbitrary boolean expression $P(x)$ we use the notation
$\forall x : P(x)$
as equivalent to $P(x) \equiv T$. In English; this statement reads: "For all x, $P(x)$ is true".
We may therefore rewrite the above definition as

$$\boxed{A = B \Leftrightarrow \forall x : (x \in A \Leftrightarrow x \in B)}$$

This is an example of the fundamental universal quantified statement. Later we will use set equality to define the 3 types of quantified statements that are regularly used in practice. The quantifier $\forall x$ runs over the class V of all elements that can ever be defined within a rigorous set theoretic axiomatic framework (e.g. ZFC).

b) <u>Subset</u> : $A \subseteq B$ means that all elements of A also belong to B (i.e. A is a subset of B).

The formal definition is:

$$\boxed{\begin{aligned} &A \subseteq B \Leftrightarrow [(x \in A \Rightarrow x \in B) \equiv T] \\ &\qquad \Leftrightarrow \forall x : (x \in A \Rightarrow x \in B) \\ &A \not\subseteq B \Leftrightarrow \overline{A \subseteq B} \end{aligned}}$$

Note that $x \in A \Rightarrow x \in A$ and $F \Rightarrow x \in A$ are obvious tautologies and therefore $A \subseteq A$ and $\emptyset \subseteq A$ are always true.

c) <u>Strict subset</u> : $A \subset B$ ("A is a strict subset of B") is defined as:

$$\boxed{\begin{aligned} &A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B) \\ &A \not\subset B \Leftrightarrow \overline{A \subset B} \end{aligned}}$$

► <u>Power set</u>

Given a set A, the power set $\mathcal{P}(A)$ is the set of all subsets of A. We define $\mathcal{P}(A)$ via the following belonging conditions:

$$\boxed{X \in \mathcal{P}(A) \Leftrightarrow X \subseteq A}$$

Note that for all sets A: $\emptyset \in \mathcal{P}(A) \wedge A \in \mathcal{P}(A)$.

EXAMPLES

$A = \{a, b\} \Rightarrow \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

$A = \{a, b, c\} \Rightarrow \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$

$\mathcal{P}(\emptyset) = \{\emptyset\}$

$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$

$\hookrightarrow$ Note that $\emptyset$ and A always belong to $\mathcal{P}(A)$.

► Number sets

We define the following number sets.

a) Natural numbers

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

$\mathbb{N}^* = \{1, 2, 3, \ldots\}$ $\quad [n] = \{1, 2, 3, \ldots, n\}$

b) Integers (from Zahl in German)

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

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

c) Rational numbers

$\mathbb{Q}$ contains all rational numbers

$\mathbb{Q}^* = \mathbb{Q} - \{0\}$

d) Real numbers

$\mathbb{R}$ contains all real numbers; $\mathbb{R}^* = \mathbb{R} - \{0\}$.

Remarks

a) Cantor proposed that starting from the empty set, with set operations, we can represent natural numbers as sets. Then, all other number sets can be constructed from $\mathbb{N}$. Cantor's construction was to define

$$0 = \emptyset$$
$$1 = \{0\} = \{\emptyset\}$$
$$2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$$
$$3 = \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

etc.

Equivalently, Cantor's construction can be represented recursively as:

$$\begin{cases} 0 = \emptyset \\ (n+1) = n \cup \{n\} \end{cases}$$

Then, a "transfinite induction" step is used to round up all natural numbers to build $\mathbb{N}$.

b) The set $\mathbb{Q}$ of the rational numbers can be defined from $\mathbb{N}$ and $\mathbb{Z}$ using definition by mapping, to be explained later.

c) Constructing $\mathbb{R}$ from $\mathbb{Q}$ is a non-trivial problem, and many approaches exist.

EXAMPLES

a) Given $A = ([6]-[3]) \cap [5]$ and $B = ([7]-[4]) \cup [2]$ list the elements of $C = A - B$

Solutions

Since

$$A = ([6]-[3]) \cap [5] =$$
$$= (\{1,2,3,4,5,6\} - \{1,2,3\}) \cap \{1,2,3,4,5\} =$$
$$= \{4,5,6\} \cap \{1,2,3,4,5\} = \{4,5\}$$

and

$$B = ([7]-[4]) \cup [2] =$$
$$= (\{1,2,3,4,5,6,7\} - \{1,2,3,4\}) \cup \{1,2\}$$
$$= \{5,6,7\} \cup \{1,2\} = \{1,2,5,6,7\}$$

it follows that

$$A - B = \{4,5\} - \{1,2,5,6,7\} = \{4\}$$

b) List the elements of $A = \mathcal{P}([6] - ([2] \cup [4]))$.

Solution

$$A = \mathcal{P}([6] - ([2] \cup [4])) =$$
$$= \mathcal{P}(\{1,2,3,4,5,6\} - (\{1,2\} \cup \{1,2,3,4\}))$$
$$= \mathcal{P}(\{1,2,3,4,5,6\} - \{1,2,3,4\})$$
$$= \mathcal{P}(\{5,6\}) = \{\emptyset, \{5\}, \{6\}, \{5,6\}\}$$

c) List the elements of $A = \mathcal{P}(\mathcal{P}(\{1\}))$

<u>Solution</u>

$$
\begin{aligned}
A &= \mathcal{P}(\mathcal{P}(\{1\})) \\
&= \mathcal{P}(\{\emptyset, \{1\}\}) \\
&= \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}
\end{aligned}
$$

EXERCISES

(7) List the elements of $A \cap B$, $A \cup B$, $A - B$, $B - A$ for the following choices of A and B:

a) $A = [6] - [3]$ and $B = [8] - [5]$

b) $A = [3] \cup [5]$ and $B = [4] \cap [2]$

c) $A = [3] \cap [2]$ and $B = [2] - [6]$

(8) List the elements of the following sets

a) $\mathcal{P}([2])$

b) $\mathcal{P}([5] - [4])$

c) $\mathcal{P}([3] - [6])$

d) $\mathcal{P}(([5] - [2]) \cap [4])$

e) $\mathcal{P}(([6] \cap [4]) - [2])$

f) $\mathcal{P}(\mathcal{P}(\emptyset))$

g) $\mathcal{P}(\{1\})$

(9) Which of the following statements is TRUE?

a) $\mathbb{N} \subseteq \mathbb{N}$

b) $\mathbb{N} \subset \mathbb{Z}$

c) $\mathbb{Z} \subseteq \mathbb{N}$

d) $\mathbb{N} \cap \mathbb{Z} = \mathbb{N}$

e) $\mathbb{N} \cap \mathbb{Z} = \mathbb{Z}$

f) $\mathbb{N} \cup \mathbb{Z} = \mathbb{N}$

g) $\mathbb{N} \cup \mathbb{Z} = \mathbb{Z}$

h) $[3] \cap [5] \subseteq [4]$

i) $[4] - [2] \subset [3]$

j) $[2] \cup [6] \subset [6]$

k) $[3] \cap [5] \subseteq [3]$

l) $1 \in \emptyset$

m) $\emptyset \in \mathcal{P}(\emptyset)$

n) $\emptyset \notin \mathcal{P}(\mathcal{P}(\emptyset))$

▼ Proving set properties

Set properties can be proved via logic as follows:

a) Set operations can be reduced using the following tautologies:

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$$

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

$$x \in A - B \Leftrightarrow x \in A \wedge x \notin B$$

b) To show that $A = B$ it is sufficient to show that

$x \in A \Leftrightarrow x \in B$.

This can be done with

1) Direct proof:

$$x \in A \Leftrightarrow p_1(x) \Leftrightarrow p_2(x) \Leftrightarrow \Leftrightarrow \cdots \Leftrightarrow p_n(x) \Leftrightarrow x \in B$$

2) Separate forward / converse proof

($\Rightarrow$): Assume that $x \in A$. Then:

$$x \in A \Rightarrow p_1(x) \Rightarrow p_2(x) \Rightarrow \cdots \Rightarrow p_n(x) \Rightarrow x \in B$$

($\Leftarrow$): Assume that $x \in B$. Then

$$x \in B \Rightarrow q_1(x) \Rightarrow q_2(x) \Rightarrow \cdots \Rightarrow q_n(x) \Rightarrow x \in A$$

From the above: $\begin{cases} A \subseteq B \\ B \subseteq A \end{cases} \Rightarrow A = B$.

c) To show $A \subseteq B$ it is sufficient to show that

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

This requires only the forward argument.

d) To show $A = \emptyset$, it is sufficient to show that

$x \in A \Rightarrow F$

where F is a contradiction (i.e. a universally false statement). The converse statement $F \Rightarrow x \in A$ is also needed, but it is a tautology so it does not require a proof.

For unidirectional arguments (i.e. using "$\Rightarrow$" steps instead of "$\Leftrightarrow$") we are allowed the following additional manipulations:

$p \Rightarrow p \vee q$ (where q is an arbitrary statement)

$p \wedge q \Rightarrow p$

i.e.: we can always ADD an arbitrary statement q using logical OR (disjunction), and from a statement $p \wedge q$ involving the logical AND (conjunction) of multiple statements we can remove any statement we want. However these manipulations are <u>not</u> reversible. More generally:

$p \Rightarrow p \vee q_1 \vee q_2 \vee \cdots \vee q_n$

$p \wedge q_1 \wedge q_2 \wedge \cdots \wedge q_n \Rightarrow p$

EXAMPLES

a) Show that: $G-(A\cap B)=(G-A)\cup(G-B)$.

Solution

Since,

$$
\begin{aligned}
x\in G-(A\cap B) &\Leftrightarrow x\in G\wedge x\notin A\cap B \Leftrightarrow\\
&\Leftrightarrow x\in G\wedge \overline{(x\in A\wedge x\in B)} \Leftrightarrow\\
&\Leftrightarrow x\in G\wedge (x\notin A\vee x\notin B)\Leftrightarrow\\
&\Leftrightarrow (x\in G\wedge x\notin A)\vee(x\in G\wedge x\notin B)\Leftrightarrow\\
&\Leftrightarrow x\in G-A\vee x\in G-B\\
&\Leftrightarrow x\in(G-A)\cup(G-B)
\end{aligned}
$$

it follows that $G-(A\cap B)=(G-A)\cup(G-B)$ $\square$

b) Show that: $A\cap B\subseteq A\cup B$.

Solution

Since,

$$
\begin{aligned}
x\in A\cap B &\Rightarrow x\in A\wedge x\in B\\
&\Rightarrow x\in A \qquad \text{(remark: converse not true)}\\
&\Rightarrow x\in A\vee x\in B \qquad \text{(remark: converse not true)}\\
&\Rightarrow x\in A\cup B
\end{aligned}
$$

it follows that $A\cap B\subseteq A\cup B$ $\square$

↳ The 2nd and 3rd steps cannot be reversed because they are based on the tautologies $p\wedge q\Rightarrow p$ and $p\Rightarrow p\vee q$. The other steps can be reversed, but the proof does not require us to exercise that possibility

c) Show that: $(A-B)\cap B=\emptyset$

<u>Solution</u>

Since,

$$
\begin{aligned}
x\in(A-B)\cap B &\Rightarrow x\in A-B \wedge x\in B \\
&\Rightarrow (x\in A \wedge x\notin B)\wedge x\in B \\
&\Rightarrow x\in A \wedge (x\notin B \wedge x\in B) \\
&\Rightarrow x\in A \wedge F \\
&\Rightarrow F
\end{aligned}
$$

and therefore $(A-B)\cap B=\emptyset$.

EXERCISES

(10) Show the following set identities, given sets A, B, C, D.

a) $C-(C-A) = A\cap C$

b) $(A-B)\cup A = A$

c) $A\cap(B-C) = (A\cap B)-(A\cap C)$

d) $(A-B)\cap(B-A) = \emptyset$

e) $(A-C)\cap(B-C) = (A\cap B)-C$

f) $(B-A)\cap(A\cap B) = \emptyset$

g) $(A\cup B)-B = A-(A\cap B) = A-B$

h) $A-(B-C) = (A-B)\cup(A\cap C)$

i) $(A-B)-C = A-(B\cup C)$

j) $(A-B)\cap(C-D) = (A\cap C)-(B\cup D)$.

▼ Predicates and quantified statements

- A <u>predicate</u> $p(x)$ is a statement about x which is TRUE or FALSE depending on the value of x.
- Assume that $x \in U$ where U is some <u>universal set</u>. Then the <u>truth set</u> of $p(x)$ is the set of all $x \in U$ for which $p(x)$ is true, and is denoted as:

  $$A = \{x \in U \mid p(x)\}$$

  The belonging condition for the truth set A is given by

  $$x \in A \Leftrightarrow x \in U \wedge p(x)$$

► <u>Remark</u>: In algebra, equations, inequalities, systems of equations, systems of inequalities are examples of predicates. For example, consider the predicate consisting of a quadratic equation:

$p(x): \; x^2+3x+2=0$

Solving an equation is equivalent to finding the corresponding truth set:

$$x^2+3x+2=0 \Leftrightarrow (x+1)(x+2)=0 \Leftrightarrow x+1=0 \vee x+2=0 \Leftrightarrow$$
$$\Leftrightarrow x=-1 \vee x=-2 \Leftrightarrow x \in \{-1,-2\}.$$

It follows that

$$S = \{x \in \mathbb{R} \mid x^2+3x+2=0\} = \{-1,-2\}$$

For systems of equations and systems of inequalities we use braces as an abbreviation for conjunction. For example,

$\begin{cases} x+y=3 \\ x-y=2 \end{cases}$ is equivalent to $x+y=3 \wedge x-y=2$.

▶ Quantified statements

Let A be a set and $p(x)$ a predicate. Then, we define:

1) **The universal quantifier $\forall$**
$$(\forall x \in A : p(x)) \Leftrightarrow \{x \in A \mid p(x)\} = A$$

interpretation: "For all $x \in A$, the statement $p(x)$ is true."

2) **The existential quantifier $\exists$**
$$(\exists x \in A : p(x)) \Leftrightarrow \{x \in A \mid p(x)\} \neq \emptyset$$

interpretation: There exists some $x \in A$ such that $p(x)$ is true
There is at least one $x \in A$ such that $p(x)$ is true

3) **The unique-existential quantifier $\exists!$**
$$(\exists! \, x \in A : p(x)) \Leftrightarrow \exists y \in A : \{x \in A \mid p(x)\} = \{y\}$$

interpretation: There is a unique $x \in A$ such that $p(x)$ is true.
There is one and only one $x \in A$ such that $p(x)$ is true.

↳ An equivalent definition of the unique-existential quantifier $\exists!$ reads:

$$\boxed{(\exists! \, x \in A : p(x)) \Leftrightarrow \begin{cases} \forall x_1, x_2 \in A : ((p(x_1) \land p(x_2)) \Rightarrow x_1 = x_2) \\ \exists x \in A : p(x) \end{cases}}$$

Remarks

a) If A is a finite set, then there is a direct correspondance between quantifiers and boolean operations:

$\forall \longleftrightarrow$ generalizes conjunction (i.e. $p \wedge q$)

$\exists \longleftrightarrow$ generalizes disjunction (i.e $p \vee q$)

$\exists! \longleftrightarrow$ generalizes exclusive disjunction (i.e. $p \veebar q$)

For example, for $A = \{a, b, c\}$

$(\forall x \in A : p(x)) \Leftrightarrow p(a) \wedge p(b) \wedge p(c)$

$(\exists x \in A : p(x)) \Leftrightarrow p(a) \vee p(b) \vee p(c)$

Thus, quantifiers function like "summation operators" for conjunction, disjunction, and exclusive disjunction.

b) In a statement of the form $\forall x \in A : p(x)$, the variable x is local, i.e. it exists only inside the quantifier to formulate the statement $p(x)$. However, x does not exist outside the overall statement. Likewise, for the other two quantifiers.

c) Quantifiers can be nested

$\forall x \in A : \exists y \in B : \forall z \in C : p(x, y, z)$

(i.e. for all $x \in A$, there is some $y \in B$ such that for all $z \in C$ we have $p(x, y, z)$)

We also use the following abbreviations:

$\forall x, y \in A : p(x, y) \Leftrightarrow \forall x \in A : \forall y \in A : p(x, y)$

$\exists x, y \in A : p(x, y) \Leftrightarrow \exists x \in A : \exists y \in A : p(x, y)$

and likewise for multiple variables.

▸ Negation of quantified statements

The universal and existential quantified statements can be negated by the following generalization of De Morgan's law:

$$\boxed{\begin{aligned} &\overline{\forall x\in A : p(x)} \iff \exists x\in A : \overline{p(x)} \\ &\overline{\exists x\in A : p(x)} \iff \forall x\in A : \overline{p(x)} \end{aligned}}$$

▸ Quantified statements and limits in Analysis

Historically, quantified statements were introduced to state precisely and concisely the definition of limits in analysis, as well as many other definitions and theorems.

For example, the standard definition of a limit can be written as

$$\lim_{x\to x_0} f(x) = \ell \iff \forall \varepsilon\in(0,+\infty) : \exists \delta\in(0,+\infty) : \forall x\in A :$$
$$: (0<|x-x_0|<\delta \Rightarrow |f(x)-\ell|<\varepsilon)$$

It is standard convention in analysis to replace $\varepsilon\in(0,+\infty)$ with $\varepsilon>0$ and $\delta\in(0,+\infty)$ with $\delta>0$ and rewrite the above definition as:

$$\lim_{x\to x_0} f(x) = \ell \iff$$
$$\iff \forall\varepsilon>0 : \exists\delta>0 : \forall x\in A : (0<|x-x_0|<\delta \Rightarrow |f(x)-\ell|<\varepsilon)$$

Translated in English: " $\lim_{x\to x_0} f(x) = \ell$ if and only if for all $\varepsilon>0$, there is some $\delta>0$ such that for all $x\in A$, if $0<|x-x_0|<\delta$ then $|f(x)-\ell|<\varepsilon$ ".

Using the negation property we can rewrite the definition for $\lim_{x\to x_0} f(x) \neq \ell$ as follows:

$$\lim_{x\to x_0} f(x) \neq \ell \Leftrightarrow$$

$$\Leftrightarrow \overline{\forall \varepsilon > 0 : \exists \delta > 0 : \forall x \in A : (0 < |x - x_0| < \delta \Rightarrow |f(x) - \ell| < \varepsilon)}$$

$$\Leftrightarrow \exists \varepsilon > 0 : \overline{\exists \delta > 0 : \forall x \in A : (0 < |x - x_0| < \delta \Rightarrow |f(x) - \ell| < \varepsilon)}$$

$$\Leftrightarrow \exists \varepsilon > 0 : \forall \delta > 0 : \overline{\forall x \in A : (0 < |x - x_0| < \delta \Rightarrow |f(x) - \ell| < \varepsilon)}$$

$$\Leftrightarrow \exists \varepsilon > 0 : \forall \delta > 0 : \exists x \in A : \overline{(0 < |x - x_0| < \delta \Rightarrow |f(x) - \ell| < \varepsilon)}$$

$$\Leftrightarrow \exists \varepsilon > 0 : \forall \delta > 0 : \exists x \in A : (0 < |x - x_0| < \delta \wedge |f(x) - \ell| \geq \varepsilon).$$

Translated in English: "$\lim_{x\to x_0} f(x) \neq \ell$ if and only if there is some $\varepsilon > 0$ such that for all $\delta > 0$, there is some $x \in A$ such that $0 < |x - x_0| < \delta$ and $|f(x) - \ell| \geq \varepsilon$".

EXERCISES

(10) Write the following statements symbolically using quantifiers

a) Every real number is equal to itself.

b) There is a real number x such that $2x = 3(1-x)$.

c) The equation $x^2+4x+4=0$ has a unique solution on $\mathbb{R}$.

d) For every real number x, there is a natural number n such that $n > x$.

e) For every real number x, there is a complex number z such that $x - z^2 = 0$.

f) For every real number x, there is a unique real number y such that $x+y=0$.

g) For all $\varepsilon > 0$, there is a $\delta > 0$ such that for all real numbers x, if $x_0 - \delta < x < x_0 + \delta$ then $f(x) > 1/\varepsilon$.

h) There is a real number b such that for all natural numbers n we have $a_n < b$.

i) For all $\varepsilon > 0$, there is a natural number n_0 such that for any two natural numbers n_1 and n_2, if $n_1 > n_0$ and $n_2 > n_0$ then we have $|a_{n_1} - a_{n_2}| < \varepsilon$.

j) For any $M > 0$, there is a natural number n_0 such that for any other natural number n, if $n > n_0$ then $a_n > M$.

(11) Write the negations of the statements of the previous exercise, first using quantifier notation, and then in English.

▸ Quantified statements and Euclidean geometry

Quantified statements can be used to encode Hilbert's axioms of Euclidean geometry. Let $\mathbb{P}$ be the set of all <u>points</u> on a <u>plane</u>. Let $\mathbb{L} \subseteq \mathcal{P}(\mathbb{P})$ be the set of all <u>lines</u> of the plane $\mathbb{P}$. Then we can restate some of Hilbert's axioms as follows:

1) For every two points A, B there is a unique line (ℓ) passing through them

$$\forall A \in \mathbb{P} : \forall B \in \mathbb{P} - \{A\} : \exists! (\ell) \in \mathbb{L} : A, B \in (\ell)$$

2) There are at least two points on every line

$$\forall (\ell) \in \mathbb{L} : \exists A, B \in \mathbb{P} : (A \neq B \land A, B \in (\ell))$$

3) There exist at least three points that do not all lie on the same line

$$\exists A, B, C \in \mathbb{P} : \forall (\ell) \in \mathbb{L} : \overline{(A, B, C \in (\ell))}$$

↳ To eliminate the negation, we note that

$$\begin{aligned} \overline{A, B, C \in (\ell)} &\iff \overline{A \in (\ell) \land B \in (\ell) \land C \in (\ell)} \\ &\iff \overline{A \in (\ell)} \lor \overline{B \in (\ell)} \lor \overline{C \in (\ell)} \\ &\iff A \notin (\ell) \lor B \notin (\ell) \lor C \notin (\ell) \end{aligned}$$

and therefore the above statement can be rewritten as:

$$\exists A, B, C \in \mathbb{P} : \forall (\ell) \in \mathbb{L} : (A \notin (\ell) \lor B \notin (\ell) \lor C \notin (\ell)).$$

EXERCISES

(12) In Hilbert's axiomatic formulation of Euclidean Geometry he introduced the statement $A*B*C$ to represent "B is between A and C". This allows defining the line segment AC as

$$AC = \{B \in \mathbb{P} \mid A*B*C\} \cup \{A, C\}$$

Write the following Hilbert axioms using quantified statements.

a) If B is between A and C, then the points A, B, C lie on the same line and B is between C and A.

b) For any points B, D, there are points A, C, E such that B is between A and D, C is between B and D, and D is between B and E.

c) For any three points A, B, C on a line, there exists no more than one point that lies between the other two points.

d) For any line (ℓ) and any point A not on (ℓ), there is exactly one line (ℓ_0) passing through A that is parallel to (ℓ).

(13) Let $A, B \in \mathbb{P}$ be two points and $(\ell) \in \mathbb{L}$ be a line. Write the following statements using quantifiers and set notation.

a) For any points A, B and any line (ℓ), A, B are on the same side of line (ℓ) (notation $A*B*(\ell)$) if and only if AB does not intersect with the line (ℓ).

6) For any 3 points A, B, C and any line (ℓ), if A, B are on the same side of the line (ℓ) and B, C are on the same side of (ℓ), then A, C are on the same side of (ℓ).

Indexed set collections

- Let I be a set. An indexed collection of sets $\{A_a\}_{a\in I}$ represents a collection of sets such that for every $a\in I$, there is a corresponding set A_a. In this context, we say that I is the <u>index set</u> of the collection.
- Let $\{A_a\}_{a\in I}$ be an indexed collection of sets. We define:

$$\boxed{\begin{aligned} x\in \bigcup_{a\in I} A_a &\Leftrightarrow \exists a\in I : x\in A_a \\ x\in \bigcap_{a\in I} A_a &\Leftrightarrow \forall a\in I : x\in A_a \end{aligned}}$$

- The corresponding negation of this definition reads:

$$\boxed{\begin{aligned} x\notin \bigcup_{a\in I} A_a &\Leftrightarrow \forall a\in I : x\notin A_a \\ x\notin \bigcap_{a\in I} A_a &\Leftrightarrow \exists a\in I : x\notin A_a \end{aligned}}$$

- For proofs requiring us to "juggle" with quantified statements, the following factorization rules are helpful.

- **Associative property**

$$p \wedge (\forall x \in A : q(x)) \Leftrightarrow \forall x \in A : (p \wedge q(x))$$
$$p \vee (\exists x \in A : q(x)) \Leftrightarrow \exists x \in A : (p \vee q(x))$$

- **Distributive property**

$$p \vee (\forall x \in A : q(x)) \Leftrightarrow \forall x \in A : (p \vee q(x))$$
$$p \wedge (\exists x \in A : q(x)) \Leftrightarrow \exists x \in A : (p \wedge q(x))$$

↳ Recall that

a) $\forall$ represents an infinite string of $\wedge$

b) $\exists$ represents an infinite string of $\vee$

and note that p is not dependent on the quantifier variable x, although it could be dependent on other variables (not shown).

- **Exchange property**

$$\forall x \in A : \forall y \in B : p(x,y) \Leftrightarrow \forall y \in B : \forall x \in A : p(x,y)$$
$$\exists x \in A : \exists y \in B : p(x,y) \Leftrightarrow \exists y \in B : \exists x \in A : p(x,y)$$

↳ We can exchange similar quantifiers but not opposite quantifiers.

▶ Diagonalization

$$\forall x \in A : (p(x) \land q(x)) \iff \begin{cases} \forall x \in A : p(x) \\ \forall x \in A : q(x) \end{cases}$$

$$\exists x \in A : (p(x) \lor q(x)) \iff (\exists x \in A : p(x)) \lor (\exists x \in A : q(x))$$

▶ Rearrangement

$$\forall x \in A \cup B : p(x) \iff \begin{cases} \forall x \in A : p(x) \\ \forall x \in B : p(x) \end{cases}$$

$$\exists x \in A \cup B : p(x) \iff (\exists x \in A : p(x)) \lor (\exists x \in B : p(x))$$

▶ Extraction / Extension

$$\begin{cases} \exists x \in A : p(x) \\ A \subseteq B \end{cases} \implies \exists x \in B : p(x) \qquad \longleftarrow \text{Extension}$$

$$\begin{cases} \forall x \in B : p(x) \\ A \subseteq B \end{cases} \implies \forall x \in A : p(x) \qquad \longleftarrow \text{Extraction}$$

EXAMPLES

a) Show that: $\bigcup\limits_{a\in I}(B-A_a) = B-\left(\bigcap\limits_{a\in I} A_a\right)$

Proof

$$
\begin{aligned}
x\in \bigcup_{a\in I}(B-A_a) &\Leftrightarrow \exists a\in I : x\in B-A_a \Leftrightarrow\\
&\Leftrightarrow \exists a\in I : (x\in B \wedge x\notin A_a) \Leftrightarrow\\
&\Leftrightarrow x\in B \wedge (\exists a\in I : x\notin A_a) \Leftrightarrow\\
&\Leftrightarrow x\in B \wedge \overline{(\forall a\in I : x\in A_a)} \Leftrightarrow \quad (*)\\
&\Leftrightarrow x\in B \wedge x\notin \bigcap_{a\in I} A_a \Leftrightarrow\\
&\Leftrightarrow x\in B-\left(\bigcap_{a\in I} A_a\right)
\end{aligned}
$$

therefore: $\bigcup\limits_{a\in I}(B-A_a) = B-\left(\bigcap\limits_{a\in I} A_a\right)$. $\square$

b) Show that: $\left(\bigcap\limits_{a\in I} A_a\right)-\left(\bigcup\limits_{a\in I} B_a\right) = \bigcap\limits_{a\in I}\bigcap\limits_{b\in I}(A_a-B_b)$

Proof

$$
\begin{aligned}
x\in \left(\bigcap_{a\in I} A_a\right)-\left(\bigcup_{a\in I} B_a\right) &\Leftrightarrow\\
&\Leftrightarrow x\in \bigcap_{a\in I} A_a \wedge x\notin \bigcup_{b\in I} B_b \Leftrightarrow
\end{aligned}
$$

$$
\begin{aligned}
&\Leftrightarrow (\forall a\in I : x\in A_a) \wedge \overline{(\exists b\in I : x\in B_b)} \Leftrightarrow \\
&\Leftrightarrow (\forall a\in I : x\in A_a) \wedge (\forall b\in I : x\notin B_b) \Leftrightarrow \quad \big\}(*) \\
&\Leftrightarrow \forall a\in I : (x\in A_a \wedge (\forall b\in I : x\notin B_b)) \Leftrightarrow \quad \big\}(*) \\
&\Leftrightarrow \forall a\in I : (\forall b\in I : (x\in A_a \wedge x\notin B_b)) \Leftrightarrow \\
&\Leftrightarrow \forall a\in I : \forall b\in I : x\in A_a - B_b \Leftrightarrow \\
&\Leftrightarrow \forall a\in I : \Big(x\in \bigcap_{b\in I} (A_a - B_b)\Big) \Leftrightarrow \\
&\Leftrightarrow x \in \bigcap_{a\in I} \bigcap_{b\in I} (A_a - B_b).
\end{aligned}
$$

therefore: $\left(\bigcap_{a\in I} A_a\right) - \left(\bigcup_{a\in I} B_a\right) = \bigcap_{a\in I} \bigcap_{b\in I} (A_a - B_b)$. $\square$

↳ We label the use of the associative/distributive properties for quantifiers with $(*)$.

EXERCISES

(14) Let I be an index set and let $\{A_a\}_{a\in I}$, $\{B_a\}_{a\in I}$ be two indexed collections of sets. Prove that:

a) $G - \bigcap_{a\in I} A_a = \bigcup_{a\in I} (G - A_a)$

b) $G - \bigcup_{a\in I} A_a = \bigcap_{a\in I} (G - A_a)$

c) $G \cap \bigcup_{a\in I} A_a = \bigcup_{a\in I} (G \cap A_a)$

d) $G \cup \bigcap_{a\in I} A_a = \bigcap_{a\in I} (G \cup A_a)$

e) $\left[\bigcap_{a\in I} A_a\right] \cup \left[\bigcap_{a\in I} B_a\right] = \bigcap_{a\in I} \bigcap_{b\in I} (A_a \cup B_b)$

f) $\left[\bigcup_{a\in I} A_a\right] \cap \left[\bigcup_{a\in I} B_a\right] = \bigcup_{a\in I} \bigcup_{b\in I} (A_a \cap B_b)$

g) $\left[\bigcap_{a\in I} A_a\right] - G = \bigcap_{a\in I} (A_a - G)$

h) $\left[\bigcup_{a\in I} A_a\right] - G = \bigcup_{a\in I} (A_a - G)$.

Defining sets by description

The fundamental method for defining a set A is by providing a belonging condition of the form

$$x \in A \Leftrightarrow p(x)$$

where $p(x)$ is a predicate about x. That said, there are 3 general methods for defining sets in practice, and we have already encountered the first two:

1) <u>By listing</u>: $A = \{a_1, a_2, a_3, \dots, a_n\}$

The corresponding belonging condition is:

$$x \in A \Leftrightarrow x = a_1 \vee x = a_2 \vee x = a_3 \vee \cdots \vee x = a_n$$

Note that the order by which elements are listed makes no difference.

2) <u>By selection</u>: $A = \{x \in U \mid p(x)\}$

with U a universal set and $p(x)$ a predicate about x. A contains all elements of U that satisfy $p(x)$.

The corresponding belonging condition is:

$$x \in A \Leftrightarrow x \in U \wedge p(x).$$

This condition can be rewritten as a quantified statement as:

$$\forall x \in U : (x \in A \Leftrightarrow p(x)).$$

example

Definition by selection is oftentimes used to define solution sets. For example, the solution set of the inequality $3x - 1 < x^2$ can be written as:

$$S = \{x \in \mathbb{R} \mid 3x - 1 < x^2\}$$

▶ example

Definition by selection can be used to define intervals:

$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$

$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$

and so on.

3) By mapping: $A = \{\varphi(x) \mid x \in U \land p(x)\}$

where U is a universal set, $p(x)$ is a predicate, and $\varphi(x)$ an expression that generates some new element from x. The belonging condition of A is:

$$x \in A \Leftrightarrow \exists a \in U : (p(a) \land \varphi(a) = x).$$

- The elements of A are generated as follows: for each $a \in U$ we test if it satisfies $p(a)$. If it does, then we add the element $\varphi(a)$ to the set A.
- Similar definitions can be made over expressions that use multiple variables. For example:

$A = \{\varphi(a,b) \mid a \in U_1 \land b \in U_2 \land p(a,b)\}$

has belonging condition

$x \in A \Leftrightarrow \exists a \in U_1 : \exists b \in U_2 : (p(a,b) \land \varphi(a,b) = x)$

and

$A = \{\varphi(a,b,c) \mid a \in U_1 \land b \in U_2 \land c \in U_3 \land p(a,b,c)\}$

has belonging condition

$x \in A \Leftrightarrow \exists a \in U_1 : \exists b \in U_2 : \exists c \in U_3 : (p(a,b,c) \land \varphi(a,b,c) = x)$

and so on.

- Another generalization is to include multiple expressions φ_1, φ_2, etc. For example:

$$A = \{\varphi_1(a), \varphi_2(a) \mid a \in U \wedge p(a)\}$$

has belonging condition

$$x \in A \Leftrightarrow \exists a \in U : (p(a) \wedge (\varphi_1(a) = x \vee \varphi_2(a) = x))$$

- We can also have a definition using both multiple variables and multiple expressions. For example

$$A = \{\varphi_1(a,b), \varphi_2(a,b) \mid a \in U_1 \wedge b \in U_2 \wedge p(a,b)\}$$

has belonging condition

$$x \in A \Leftrightarrow \exists a \in U_1 : \exists b \in U_2 : (p(a,b) \wedge (\varphi_1(a,b) = x \vee \varphi_2(a,b) = x))$$

EXAMPLES

a) Set of odd/even numbers

Recall that we defined the set of natural numbers:

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

We can define:

$A = \{2x \mid x \in \mathbb{N}\} = \{0,2,4,6,\dots\}$

$B = \{2x+1 \mid x \in \mathbb{N}\} = \{1,3,5,7,\dots\}$

The corresponding belonging condition is:

$x \in A \Leftrightarrow \exists a \in \mathbb{N} : x = 2a$

$x \in B \Leftrightarrow \exists a \in \mathbb{N} : x = 2a+1$

and since $A \subseteq \mathbb{N}$ and $B \subseteq \mathbb{N}$, the definition of A, B can be rewritten using "definition by selection" as:

$A = \{x \in \mathbb{N} \mid \exists a \in \mathbb{N} : x = 2a\}$

$B = \{x \in \mathbb{N} \mid \exists b \in \mathbb{N} : x = 2a+1\}$

b) The sets $\mathbb{Z}, \mathbb{Q}$

The set of integers $\mathbb{Z}$ and the set of rational numbers $\mathbb{Q}$ can be defined descriptively as:

$\mathbb{Z} = \mathbb{N} \cup \{-x \mid x \in \mathbb{N}\}$

$\mathbb{Q} = \{a/b \mid a,b \in \mathbb{Z} \wedge b \neq 0\}$

The corresponding belonging condition is:

$x \in \mathbb{Z} \Leftrightarrow x \in \mathbb{N} \vee (\exists a \in \mathbb{N} : x = -a)$

$x \in \mathbb{Q} \Leftrightarrow \exists a,b \in \mathbb{Z} : (b \neq 0 \wedge x = a/b)$

c) <u>The sets $\mathbb{C}$ and $\mathbb{I}$</u>

The set of complex numbers $\mathbb{C}$ and the set of imaginary numbers $\mathbb{I}$ can be defined descriptively from the set of real numbers $\mathbb{R}$ as:

$$\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\}$$
$$\mathbb{I} = \{bi \mid b \in \mathbb{R}\}$$

The corresponding belonging conditions are:

$$z \in \mathbb{C} \Leftrightarrow \exists a, b \in \mathbb{R} : z = a+bi$$
$$z \in \mathbb{I} \Leftrightarrow \exists b \in \mathbb{R} : z = bi$$

d) Write the belonging condition and it's negation for the set

$$A = \{a^2+b^2 \mid a \in \mathbb{R} \wedge b \in \mathbb{Q} \wedge a+b<10\}$$

<u>Solution</u>

The belonging condition for A is:

$$x \in A \Leftrightarrow \exists a \in \mathbb{R} : \exists b \in \mathbb{Q} : (a+b<10 \wedge x = a^2+b^2)$$

The corresponding negation is:

$$\begin{aligned}
x \notin A &\Leftrightarrow \overline{\exists a \in \mathbb{R} : \exists b \in \mathbb{Q} : (a+b<10 \wedge x = a^2+b^2)} \\
&\Leftrightarrow \forall a \in \mathbb{R} : \overline{\exists b \in \mathbb{Q} : (a+b<10 \wedge x = a^2+b^2)} \\
&\Leftrightarrow \forall a \in \mathbb{R} : \forall b \in \mathbb{Q} : \overline{(a+b<10 \wedge x = a^2+b^2)} \\
&\Leftrightarrow \forall a \in \mathbb{R} : \forall b \in \mathbb{Q} : (\overline{a+b<10} \vee \overline{x = a^2+b^2}) \\
&\Leftrightarrow \forall a \in \mathbb{R} : \forall b \in \mathbb{Q} : (a+b \geq 10 \vee x \neq a^2+b^2)
\end{aligned}$$

↳ Recall the following negation rules.

$$\overline{p \wedge q} \equiv \bar{p} \vee \bar{q} \qquad \overline{p \Leftrightarrow q} \equiv p \veebar q$$
$$\overline{p \vee q} \equiv \bar{p} \wedge \bar{q} \qquad \overline{p \veebar q} \equiv p \Leftrightarrow q$$
$$\overline{p \Rightarrow q} \equiv p \wedge \bar{q}$$

→ Be careful not to confuse set definitions <u>by mapping</u> with set definitions <u>by description.</u> Here's an example of set definition by description.

e) Write the belonging condition and its negation for
$A = \{x \in \mathbb{R} \mid \exists y \in \mathbb{R} : 2y^2 + y = x + 1\}$

<u>Solution</u>

The belonging condition of A is:

$$\forall x \in \mathbb{R} : (x \in A \Leftrightarrow \exists y \in \mathbb{R} : 2y^2 + y = x + 1)$$

The negation, in <u>detail</u> is <u>derived</u> as follows:

$$\begin{aligned}\forall x \in \mathbb{R} : (x \notin A &\Leftrightarrow \overline{\exists y \in \mathbb{R} : 2y^2 + y = x + 1}\ )\\ &\Leftrightarrow \forall y \in \mathbb{R} : \overline{2y^2 + y = x + 1}\ )\\ &\Leftrightarrow \forall y \in \mathbb{R} : 2y^2 + y \neq x + 1).\end{aligned}$$

and therefore:

$$\forall x \in \mathbb{R} : (x \notin A \Leftrightarrow \forall y \in \mathbb{R} : 2y^2 + y \neq x + 1).$$

EXERCISES

(15) Write the belonging condition and its negation for the following sets, using quantifiers

a) $A=\{x^2+1 \mid x\in\mathbb{Q} \wedge 2x<1\}$

b) $A=\{3x+1 \mid x\in\mathbb{Z} \wedge x \text{ prime number}\}$

c) $A=\{x\in\mathbb{R} \mid x^2+3x\geq 0\}$

d) $A=\{a^3+b^3+c^3 \mid a,b\in\mathbb{R} \wedge c\in\mathbb{Q} \wedge a+b+c=0\}$

e) $A=\{x\in\mathbb{R} \mid x^2+2x<0 \vee 3x+1>-4\}$

f) $A=\{a^2-b^2 \mid a\in\mathbb{N} \wedge b\in\mathbb{R} \wedge a+b\geq 5\}$

g) $A=\{x\in\mathbb{Z} \mid \exists a\in\mathbb{Z} : x=3a\}$

h) $A=\{ab \mid a,b\in\mathbb{R} \wedge (a+b\geq 2 \vee a-b<-3)\}$

i) $A=\{x\in\mathbb{R} \mid \exists y\in\mathbb{R} : y^2+y=x\}$

j) $A=\{x\in\mathbb{R} \mid \forall y\in\mathbb{R} : x<y^2+1\}$

k) $A=\{a+b \mid a,b\in\mathbb{R} \wedge (ab\geq 1 \Rightarrow a^2+b^2\geq 2)\}$

l) $A=\{abc \mid a,b,c\in\mathbb{R} \wedge (a+b\geq 2 \veebar a-c<3)\}$

m) $A=\{2a+3b \mid a,b\in\mathbb{R} \wedge ab\geq 1 \wedge a-b<0\}$

n) $A=\{a^2b,\ a+b \mid a\in\mathbb{Z} \wedge b\in\mathbb{Q} \wedge a-b=3\}$

o) $A=\{3k,\ 3k+1 \mid k\in\mathbb{Z} \wedge k^2-10>0\}$

p) $A=\{ab,\ bc,\ ca \mid a,b,c\in\mathbb{N} \wedge a^2+b^2+c^2<100\}$

q) $A=\{a+b,\ a+3b \mid a,b\in\mathbb{Z} \wedge (a-b\geq 0 \Rightarrow a-3b\geq 0)\}$

Proof methodology with sets

We now consider proofs with sets that involve statements that are more complex that basic set identitites.

▸ Methodology: Dealing with sets

- For proofs involving sets, we use:

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$$
$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$
$$x \in A - B \Leftrightarrow x \in A \wedge x \notin B$$
$$A \subseteq B \Leftrightarrow \forall x \in A : x \in B$$
$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$
$$z \in \{x \in A \mid p(x)\} \Leftrightarrow z \in A \wedge p(z)$$
$$z \in \{\varphi(x) \mid x \in A \wedge p(x)\} \Leftrightarrow \exists x \in A : (p(x) \wedge \varphi(x) = z)$$

- If $A = B$ is given as an assumption (or previously proved) we can deduce:

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

or, in general, replace $x \in A$ with $x \in B$ and vice versa in any boolean expression.

- If $A \subseteq B$ is given as an assumption (or previously proved) we can deduce

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

or, in general, replace $x \in A$ with $x \in B$ in any boolean expression.

▸ <u>Methodology</u>: Extension / Extraction

In a deductive argument we can ADD arbitrary statements with logical OR (disjunction) or remove statements connected with logical AND (conjunction):

$$p \Rightarrow p \vee q_1 \vee q_2 \vee \cdots \vee q_n \qquad \text{(extension)}$$

$$p \wedge q_1 \wedge q_2 \wedge \cdots \wedge q_n \Rightarrow p \qquad \text{(extraction)}$$

The corresponding generalization to quantified statements reads:

$$\boxed{\begin{array}{l} \begin{cases} \forall x \in A : p(x) \\ x_0 \in A \end{cases} \Rightarrow p(x_0) \\ \hline \begin{cases} x_0 \in A \\ p(x_0) \end{cases} \Rightarrow \exists x \in A : p(x) \end{array}} \qquad \begin{array}{l} \text{(extraction)} \\ \\ \text{(extension)} \end{array}$$

▸ <u>Methodology</u>: General proof writing

① → To prove $\boxed{\forall x \in A : p(x)}$

Let $x \in A$ be given.
[Prove $p(x)$]
It follows that $\forall x \in A : p(x)$.

② → To prove $\boxed{\exists x \in A : p(x)}$

▸ 1st method
[Define some $x_0 \in A$]
[Prove $p(x_0)$]
It follows that $\exists x \in A : p(x)$

↳ Note that x_0 can be indirectly defined by deducing a statement of the form $\exists x \in B : q(x)$ via a theorem or by constructing it from other variables that have been indirectly defined via existential statements.

▶ <u>2nd method</u>

[Prove $p(x) \Leftrightarrow \cdots \Leftrightarrow \cdots \Leftrightarrow x \in \$$]

[Choose a specific $x_0 \in \$$]

[Prove $x_0 \in A$]

[Prove $p(x_0)$]

It follows that $\exists x \in A : p(x)$.

3 → To prove $\boxed{p \Rightarrow q}$

▶ <u>Direct method</u>

Assume p is true

[Prove q]

▶ <u>Contrapositive method</u>

We will show that $\bar{q} \Rightarrow \bar{p}$

Assume $\bar{q}$ is true

[Prove $\bar{p}$]

From the above, it follows that $p \Rightarrow q$.

▶ <u>Contradiction method</u>

Assume p is true

To show q, we assume $\bar{q}$, and will derive a contradictio

[Prove r, using $p \wedge \bar{q}$]
[Prove $\bar{r}$] ← Contradiction
It follows that q is true

(4) → To prove $\boxed{p \Leftrightarrow q}$

($\Rightarrow$): [Prove $p \Rightarrow q$]
($\Leftarrow$): [Prove $q \Rightarrow p$]

▸ 2nd method: Occasionally, it is possible to use a direct argument of the form
$p \Leftrightarrow r_1 \Leftrightarrow r_2 \Leftrightarrow \cdots \Leftrightarrow r_n \Leftrightarrow q$
as long as every step can be justified in both directions.

(5) → To prove $\boxed{p \vee q \Rightarrow r}$

▸ Proof by cases
Assume that $p \vee q$. We distinguish between the following cases.
Case 1: Assume that p is true.
[Prove r]
Case 2: Assume that q is true
[Prove r]
From the above it follows that r is true.

▸ Contrapositive
We will show that $\bar{r} \Rightarrow \bar{p} \wedge \bar{q}$. Assume that $\bar{r}$ true

[Prove $\bar{p}$]
[Prove $\bar{q}$]
From the above, it follows that $p \vee q \Rightarrow r$

↳ Proof by cases is used when the hypothesis takes the form $p \vee q$ (or more generally $p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_n$) and we do not really know which of the statements in the disjunction is true. However, for the individual cases we can use any of the proof techniques under 3.

↳ The skeletal structure of any proof combines the above elements as is appropriate.

EXAMPLES

a) Show that $B \subseteq A \Rightarrow A \cup B = A$

Proof

Assume that $B \subseteq A$.

($\Rightarrow$): Let $x \in A \cup B$ be given. Then:

$$\begin{aligned} x \in A \cup B &\Rightarrow x \in A \vee x \in B \\ &\Rightarrow x \in A \vee x \in A \quad [\text{via } B \subseteq A] \\ &\Rightarrow x \in A \end{aligned}$$

($\Leftarrow$): Let $x \in A$ be given. Then:

$$\begin{aligned} x \in A &\Rightarrow x \in A \vee x \in B \\ &\Rightarrow x \in A \cup B \end{aligned}$$

From the above, it follows that

$$\begin{cases} \forall x \in A \cup B : x \in A \\ \forall x \in A : x \in A \cup B \end{cases} \Rightarrow \begin{cases} A \cup B \subseteq A \\ A \subseteq A \cup B \end{cases} \Rightarrow A \cup B = A.$$

↳ Note the following:

a) We declare our assumptions.

b) The structure of the proof is to show

$$\begin{cases} \forall x \in A \cup B : x \in A \\ \forall x \in A : x \in A \cup B \end{cases}$$

from which we deduce the statement $A \cup B = A$. This is the general structure of a proof intended to show that two sets are equal.

b) Show that $A \cup B = A \Rightarrow B \subseteq A$.

Solution

Assume that $A \cup B = A$. Let $x \in B$ be given. Then:

$$\begin{aligned} x \in B &\Rightarrow x \in A \lor x \in B \\ &\Rightarrow x \in A \cup B \\ &\Rightarrow x \in A \qquad [\text{via } A \cup B = A] \end{aligned}$$

It follows that

$(\forall x \in B : x \in A) \Rightarrow B \subseteq A$.

In the context of proving set properties, contradiction proofs often arise when working with statements involving the empty set.

c) Show that $(A-B)-C = \emptyset \Rightarrow A \subseteq B \cup C$.

Solution

Assume that $(A-B)-C = \emptyset$. To show $A \subseteq B \cup C$, we assume that $A \not\subseteq B \cup C$ and will derive a contradiction.

Since,

$$\begin{aligned} A \not\subseteq B \cup C &\Rightarrow \overline{\forall x \in A : x \in B \cup C} \\ &\Rightarrow \exists x \in A : x \notin B \cup C \end{aligned}$$

Choose an $x_0 \in A$ such that $x_0 \notin B \cup C$. Then,

$$\begin{aligned} x_0 \in A \land x_0 \notin B \cup C &\Rightarrow x_0 \in A \land \overline{(x_0 \in B \lor x_0 \in C)} \\ &\Rightarrow x_0 \in A \land (x_0 \notin B \land x_0 \notin C) \\ &\Rightarrow (x_0 \in A \land x_0 \notin B) \land x_0 \notin C \\ &\Rightarrow x_0 \in A - B \land x_0 \notin C \\ &\Rightarrow x_0 \in (A-B) - C \\ &\Rightarrow x_0 \in \emptyset \end{aligned}$$

This is a contradiction, since $x_0 \notin \emptyset$. It follows that $A \subseteq B \cup C$.

d) Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Solution

Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$ be given. It is sufficient to show that $\forall y \in X : y \in A \cup B$. We note that

$$X \in \mathcal{P}(A) \cup \mathcal{P}(B) \Rightarrow X \in \mathcal{P}(A) \vee X \in \mathcal{P}(B) \Rightarrow$$
$$\Rightarrow X \subseteq A \vee X \subseteq B.$$

We distinguish between the following cases.

Case 1: Assume that $X \subseteq A$. Let $y \in X$ be given. Then:

$$\begin{aligned} y \in X &\Rightarrow y \in A \quad [\text{via } X \subseteq A] \\ &\Rightarrow y \in A \vee y \in B \\ &\Rightarrow y \in A \cup B. \end{aligned}$$

Case 2: Assume that $X \subseteq B$. Let $y \in X$ be given. Then

$$\begin{aligned} y \in X &\Rightarrow y \in B \quad [\text{via } X \subseteq B] \\ &\Rightarrow y \in A \vee y \in B \\ &\Rightarrow y \in A \cup B \end{aligned}$$

In both cases we obtain:

$$\begin{aligned} (\forall y \in X : y \in A \cup B) &\Rightarrow X \subseteq A \cup B \\ &\Rightarrow X \in \mathcal{P}(A \cup B). \end{aligned}$$

From the above argument, we have shown that

$$(\forall X \in \mathcal{P}(A) \cup \mathcal{P}(B) : X \in \mathcal{P}(A \cup B)) \Rightarrow \mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B).$$

EXERCISES

(16) Prove that

a) $A \cup B = A \cap B \Rightarrow A = B$

b) $\begin{cases} A \cup B = A \cup C \\ A \cap B = A \cap C \end{cases} \Rightarrow B = C$

(Hint: Distinguish between the cases $x \in A$ and $x \notin A$)

c) $\begin{cases} A \cup B \subseteq C \\ B \cup C \subseteq A \\ C \cup A \subseteq B \end{cases} \Rightarrow A = B = C$

d) $A \cup B = \emptyset \Rightarrow A = \emptyset \wedge B = \emptyset$

e) $A - B = \emptyset \wedge B - A = \emptyset \Rightarrow A = B$

f) $A - (B - C) = \emptyset \Rightarrow A - B = \emptyset \wedge A \cap C = \emptyset$

g) $(A - C) \cap (B - C) = \emptyset \Rightarrow A \cap B \subseteq C$

h) $(A - B) \cap (C - D) = \emptyset \Rightarrow A \cap C \subseteq B \cup D$.

(17) Prove the following equivalences

a) $(B - A) \cup A = B \Leftrightarrow A \subseteq B$

b) $B - (B - A) = A \Leftrightarrow A \subseteq B$

c) $A \cup B = B \Leftrightarrow A \subseteq B$

d) $A \cap B = A \Leftrightarrow A \subseteq B$

e) $A - B = \emptyset \Leftrightarrow A \subseteq B$

(18) Prove that

a) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$

b) $\mathcal{P}(A-B) \subseteq \mathcal{P}(A) - \mathcal{P}(B)$

c) $A \cap B = \emptyset \Rightarrow \mathcal{P}(A-B) = \mathcal{P}(A) - \mathcal{P}(B)$

d) $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$

(19) Prove that

a) $\bigcap_{a\in I} A_a = \bigcup_{a\in I} A_a \Rightarrow \forall a,b \in I:\ A_a = A_b.$

b) $\bigcup_{a\in I} A_a = \emptyset \Rightarrow \forall a \in I:\ A_a = \emptyset$

c) $I \subseteq K \Rightarrow \bigcap_{a\in K} A_a \subseteq \bigcap_{a\in I} A_a$

d) $I \subseteq K \Rightarrow \bigcup_{a\in I} A_a \subseteq \bigcup_{a\in K} A_a$

e) $\bigcap_{a\in I} \mathcal{P}(A_a) = \mathcal{P}\left(\bigcap_{a\in I} A_a\right)$

f) $\bigcup_{a\in I} \mathcal{P}(A_a) \subseteq \mathcal{P}\left(\bigcup_{a\in I} A_a\right)$

g) $(\forall a,b \in I:\ A_a \cap A_b = \emptyset) \Rightarrow \bigcup_{a\in I} \mathcal{P}(A_a) = \mathcal{P}\left(\bigcup_{a\in I} A_a\right)$