Lecture Notes on Intro to Mathematics Proof

Eleftherios Gkioulekas

These notes are constantly updated by the author. If you have not obtained this file from the author's website, it may be out of date. This notice includes the date of latest update to this file. If you are using these notes for a course, I would be very pleased to hear from you, in order to document for my University the impact of this work.
The main online lecture notes website is: https://faculty.utrgv.edu/eleftherios.gkioulekas/
You may contact the author at: drlf@hushmail.com
Last updated: April 24, 2021

Contents

IMP1: Sets and Logic

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	$p\vee q$	$p\wedge q$	$p\veebar q$	$\bar{p}$	$p\Rightarrow q$	$p\Leftrightarrow q$
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 <u>false</u> 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), $-$ (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> $\to$ 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>:

$\left.\begin{array}{l} \overline{p \wedge q} \equiv \bar{p} \vee \bar{q} \\ \overline{p \vee q} \equiv \bar{p} \wedge \bar{q} \end{array}\right\}$ 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 $\overline{p \wedge q} \equiv \bar{p} \vee \bar{q}$ $\square$

Methodology: 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.

Solution

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

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. $p, q, r, \ldots$) 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) $(p \land q) \Rightarrow q$

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

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

d) $(p \veebar q) \Rightarrow (p \lor q)$

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

5. Write the expressions of the previous exercise in English

▸ <u>Methodology</u>: 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:
  $$a \leq b \Leftrightarrow (a<b \lor a=b)$$
  $$a \geq b \Leftrightarrow (a>b \lor a=b)$$
- Composite inequalities are equivalent to conjunction of elementary inequalities. For example:
  $$a<b<c \Leftrightarrow a<b \land b<c$$
  $$\Leftrightarrow \begin{cases} a<b \\ b<c \end{cases}$$
  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

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

<u>Solution</u>

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

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

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

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

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

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.

notation: $x \in A$: the element x belongs to A

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

We also introduce the following abbreviations:

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

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

and so on.

Definition of sets

- Sets can be defined by providing a belonging condition 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

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

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

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

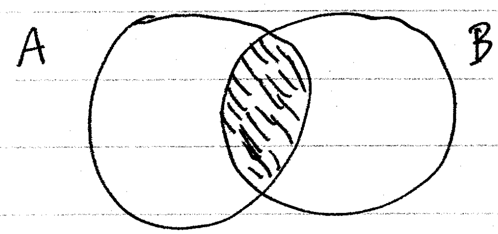
$$x \in \emptyset \Leftrightarrow F$$

▶ Operations with sets

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

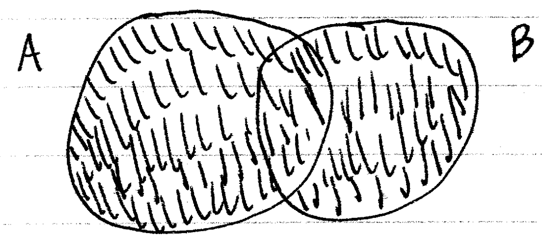
1) Intersection $A \cap B$

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



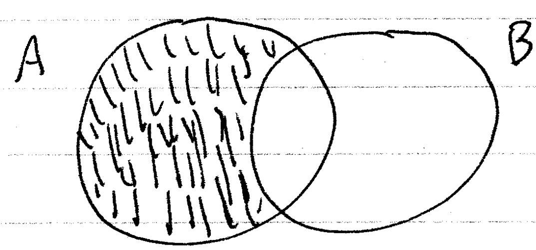
2) Union $A \cup B$

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



3) Difference $A - B$

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



▶ Relations between sets

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:

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

↳ 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:

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

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:

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

▶ <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

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

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

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

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

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

▸ Number sets

We define the following number sets.

a) Natural numbers

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

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

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:

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

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,

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

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,

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

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 $p\land q\Rightarrow p$ and $p\Rightarrow p\lor q$. The other steps can be reversed, but the proof does not require us to exercise that possibility

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

Solution

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) $\boxed{\begin{array}{l}\text{The universal quantifier } \forall \\ (\forall x \in A : p(x)) \Leftrightarrow \{x \in A \mid p(x)\} = A\end{array}}$

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

2) $\boxed{\begin{array}{l}\text{The existential quantifier } \exists \\ (\exists x \in A : p(x)) \Leftrightarrow \{x \in A \mid p(x)\} \neq \emptyset\end{array}}$

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) $\boxed{\begin{array}{l}\text{The unique-existential quantifier } \exists! \\ (\exists!\, x \in A : p(x)) \Leftrightarrow \exists y \in A : \{x \in A \mid p(x)\} = \{y\}\end{array}}$

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:

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

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

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

(i.e. for all $x \in A$, there is some $y \in B$ such that for all $z \in G$ 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:

$$\boxed{\begin{array}{l} \overline{\forall x \in A : p(x)} \Longleftrightarrow \exists x \in A : \overline{p(x)} \\ \overline{\exists x \in A : p(x)} \Longleftrightarrow \forall x \in A : \overline{p(x)} \end{array}}$$

▸ 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

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

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:

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

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 $\lim\limits_{x\to x_0} f(x) \neq \ell$ 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: "$\lim\limits_{x\to x_0} f(x)\neq \ell$ 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 points on a plane. Let $\mathbb{L} \subseteq \mathcal{P}(\mathbb{P})$ be the set of all lines 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 $\{A_\alpha\}_{\alpha\in I}$ represents a collection of sets such that for every $\alpha \in I$, there is a corresponding set A_α. In this context, we say that I is the <u>index set</u> of the collection.
- Let $\{A_\alpha\}_{\alpha\in I}$ be an indexed collection of sets. We define:

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

- The corresponding negation of this definition reads:

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

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

Associative property

$$\boxed{\begin{array}{l} p \wedge (\forall x \in A : q(x)) \Leftrightarrow \forall x \in A : (p \wedge q(x)) \\ p \vee (\exists x \in A : q(x)) \Leftrightarrow \exists x \in A : (p \vee q(x)) \end{array}}$$

Distributive property

$$\boxed{\begin{array}{l} p \vee (\forall x \in A : q(x)) \Leftrightarrow \forall x \in A : (p \vee q(x)) \\ p \wedge (\exists x \in A : q(x)) \Leftrightarrow \exists x \in A : (p \wedge q(x)) \end{array}}$$

↳ 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

$$\boxed{\begin{array}{l} \forall x \in A : \forall y \in B : p(x,y) \Leftrightarrow \forall y \in B : \forall x \in A : p(x,y) \\ \exists x \in A : \exists y \in B : p(x,y) \Leftrightarrow \exists y \in B : \exists x \in A : p(x,y) \end{array}}$$

↳ We can exchange similar quantifiers but not opposite quantifiers.

▸ Diagonalization

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

$$\exists x\in A : (p(x) \vee q(x)) \Longleftrightarrow (\exists x\in A : p(x)) \vee (\exists x \in A : q(x))$$

▸ Rearrangement

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

$$\exists x\in A\cup B : p(x) \Longleftrightarrow (\exists x\in A : p(x)) \vee (\exists x \in B : p(x))$$

▸ Extraction / Extension

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

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

EXAMPLES

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

Proof

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

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

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

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

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

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

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

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

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

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

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

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>: $A = \{a_1, a_2, a_3, \ldots, a_n\}$
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:
$$\forall x \in U : (x \in A \Leftrightarrow p(x)).$$

▸ <u>example</u>
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 : $A = \{\varphi(x) \mid x \in U \wedge p(x)\}$

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:

$$x \in A \Longleftrightarrow \exists a \in U : (p(a) \wedge \varphi(a) = x).$$

- 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:

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

has belonging condition

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

and

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

has belonging condition

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

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:

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

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

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

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

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

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:

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

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

The corresponding belonging condition is:

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

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

c) The sets $\mathbb{C}$ and $\mathbb{I}$

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

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

Solution

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

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

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

Proof methodology with sets

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

▶ Methodology: Dealing with sets

- For proofs involving sets, we use:

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

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

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

  $A \subseteq B \Leftrightarrow \forall x \in A : x \in B$

  $A = B \Leftrightarrow A \subseteq B \land B \subseteq A$

  $z \in \{x \in A \mid p(x)\} \Leftrightarrow z \in A \land p(z)$

  $z \in \{\varphi(x) \mid x \in A \land p(x)\} \Leftrightarrow \exists x \in A : (p(x) \land \varphi(x) = z)$

- 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.

▶ Methodology: 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:

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

▶ Methodology: General proofwriting

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.

▶ 2nd method

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

[Choose a specific $x_0 \in S$]

[Prove $x_0 \in A$]

[Prove $p(x_0)$]

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

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

▶ Direct method

Assume p is true

[Prove q]

▶ Contrapositive method

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

Assume $\bar{q}$ is true

[Prove $\bar{p}$]

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

▶ Contradiction method

Assume p is true

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

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

(4) $\rightarrow$ 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) $\rightarrow$ 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:

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

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 $A \nsubseteq B \cup C$ and will derive a contradiction.

Since,

$$\begin{aligned} A \nsubseteq B \cup C &\Rightarrow \overline{\forall x \in A : x \in B \cup C} \\ &\Rightarrow \exists x \in A : x \notin B \cup C \end{aligned}$$

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

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

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

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

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

IMP2: Integers

INTEGERS

▼ Preliminaries

We recall the following definitions for the set of natural numbers $\mathbb{N}$ and the set of integers $\mathbb{Z}$:

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

$$\mathbb{Z} = \{k, -k \mid k \in \mathbb{N}\} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$$

We also define

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

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

$$[n] = \{k \in \mathbb{N} \mid 1 \leq k \leq n\} = \{1, 2, 3, \ldots, n\}$$

▼ Odd and even integers

We partition the set of integers $\mathbb{Z}$ into even and odd integers as follows:

Def: Let $n \in \mathbb{Z}$ be an integer. We say that

n even $\Leftrightarrow \exists k \in \mathbb{Z} : n = 2k$

n odd $\Leftrightarrow \exists k \in \mathbb{Z} : n = 2k+1$

We note that the statements

$\overline{n \text{ odd}} \Leftrightarrow n$ even

$\overline{n \text{ even}} \Leftrightarrow n$ odd

require the well-ordering principle for their proof, which will be given in the following section.
In the following, we will assume that these statements have already been shown, and we them in our arguments, when needed.

- The following proposition is useful in arguments with integers

$$\boxed{\underline{\text{Prop}}: \forall a,b \in \mathbb{Z}: (ab \text{ even} \Leftrightarrow a \text{ even} \vee b \text{ even})}$$

We also have the contrapositive statement, obtained by negating both sides:

$$\boxed{\underline{\text{Corollary}}: \forall a,b \in \mathbb{Z}: (ab \text{ odd} \Leftrightarrow a \text{ odd} \wedge b \text{ odd})}$$

From both statements, the choice $a=b$ gives.

$$\boxed{\begin{array}{ll} \underline{\text{Corollary}}: & \forall a \in \mathbb{Z}: \ a^2 \text{ even} \Leftrightarrow a \text{ even} \\ & \forall a \in \mathbb{Z}: \ a^2 \text{ odd} \Leftrightarrow a \text{ odd} \end{array}}$$

We now prove the main proposition:
<u>Proof</u>
Let $\underline{a,b \in \mathbb{Z}}$ be given.
$(\Rightarrow)$: We show the contrapositive statement

$$a \text{ odd} \wedge b \text{ odd} \Rightarrow ab \text{ odd}$$

Assume that $\underline{a \text{ odd} \wedge b \text{ odd}}$. Then, we have:

a odd $\Rightarrow \exists k \in \mathbb{Z} : a = 2k+1$

b odd $\Rightarrow \exists k \in \mathbb{Z} : b = 2k+1$

Choose $k, \lambda \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2\lambda + 1$.

Then, we have:

$$ab = (2k+1)(2\lambda+1) = 4k\lambda + 2k + 2\lambda + 1 =$$
$$= 2(2k\lambda + k + \lambda) + 1 \Rightarrow$$
$$\Rightarrow \exists \mu \in \mathbb{Z} : ab = 2\mu + 1 \quad (\text{for } \mu = 2k\lambda + k + \lambda \in \mathbb{Z})$$
$$\Rightarrow \underline{ab \text{ odd}}$$

$(\Leftarrow)$: Assume that $\underline{a \text{ even} \vee b \text{ even}}$. We distinguish between the following cases

$\underline{\text{Case 1}}$: Assume that $\underline{a \text{ even}}$. Then,

a even $\Rightarrow \exists k \in \mathbb{Z} : a = 2k$

Choose $k \in \mathbb{Z}$ such that $a = 2k$. Then, we have

$$ab = (2k)b = 2(kb) \Rightarrow$$
$$\Rightarrow \exists \mu \in \mathbb{Z} : ab = 2\mu \quad (\text{for } \mu = kb \in \mathbb{Z})$$
$$\Rightarrow \underline{ab \text{ even}}.$$

$\underline{\text{Case 2}}$: Assume that $\underline{b \text{ even}}$. Then,

b even $\Rightarrow \exists k \in \mathbb{Z} : b = 2k$

Choose $k \in \mathbb{Z}$ such that $b = 2k$. Then, we have

$$ab = a(2k) = 2(ak) \Rightarrow$$
$$\Rightarrow \exists \mu \in \mathbb{Z} : ab = 2\mu \quad (\text{for } \mu = ak \in \mathbb{Z})$$
$$\Rightarrow \underline{ab \text{ even}}$$

From the above, we conclude that

$\forall a, b \in \mathbb{Z}$: ab even $\Leftrightarrow$ a even $\vee$ b even. $\square$

EXAMPLES

a) Show that
$\forall a,b\in\mathbb{Z}: (a \text{ odd} \wedge b \text{ odd} \Rightarrow a+b \text{ even})$

Solution

Let $a,b\in\mathbb{Z}$ be given and assume that a odd $\wedge$ b odd.
Then, we have:

$$\begin{cases} a \text{ odd} \\ b \text{ odd} \end{cases} \Rightarrow \begin{cases} \exists k\in\mathbb{Z}: a=2k+1 \\ \exists \lambda\in\mathbb{Z}: b=2\lambda+1 \end{cases}$$

Choose $k,\lambda\in\mathbb{Z}$ such that $a=2k+1$ and $b=2\lambda+1$.
It follows that:

$$a+b=(2k+1)+(2\lambda+1)=2k+2\lambda+2=$$
$$=2(k+\lambda+1)\Rightarrow$$
$$\Rightarrow \exists \mu\in\mathbb{Z}: a+b=2\mu \quad (\text{for } \mu=k+\lambda+1\in\mathbb{Z})$$
$$\Rightarrow a+b \text{ even.}$$

From the above, we conclude that
$\forall a,b\in\mathbb{Z}: (a \text{ odd} \wedge b \text{ odd} \Rightarrow a+b \text{ even})$ $\square$

b) Show that: $\forall a\in\mathbb{Z}: (a \text{ odd} \Rightarrow 3a+7 \text{ even})$.

Solution

Let $a\in\mathbb{Z}$ be given and assume that a odd.
Then, we have:

a odd $\Rightarrow \exists k\in\mathbb{Z}: a=2k+1$

Choose $k\in\mathbb{Z}$ such that $a=2k+1$. It follows that:

$3a+7 = 3(2k+1)+7 = 6k+3+7 = 6k+10 = 2(3k+5) \Rightarrow$
$\Rightarrow \exists \mu \in \mathbb{Z} : 3a+7 = 2\mu$
$\Rightarrow \underline{3a+7 \text{ even}}$
We have thus shown that
$\forall a \in \mathbb{Z} : (a \text{ odd} \Rightarrow 3a+7 \text{ even}).$ $\square$

c) Show that:
$\forall x \in \mathbb{Z} : x^3+x^2+x \text{ even} \Leftrightarrow x \text{ even}$
<u>Solution</u>
Let $\underline{x \in \mathbb{Z}}$ be given.
$(\Rightarrow)$: We show the contrapositive statement
$x \text{ odd} \Rightarrow x^3+x^2+x \text{ odd}$
Assume that $\underline{x \text{ odd}}$. Then, we have:
$x \text{ odd} \Rightarrow \exists k \in \mathbb{Z} : x = 2k+1$
Choose $k \in \mathbb{Z}$ such that $x = 2k+1$. It follows that
$x^3+x^2+x = (2k+1)^3 + (2k+1)^2 + (2k+1) =$
$= 8k^3 + 3(2k)^2 + 3(2k) + 1 + (2k)^2 + 2(2k) + 1 + 2k + 1$
$= 8k^3 + 12k^2 + 6k + 1 + 4k^2 + 4k + 1 + 2k + 1$
$= 8k^3 + (12+4)k^2 + (6+4+2)k + (1+1+1)$
$= 8k^3 + 16k^2 + 12k + 3$
$= 2(4k^3 + 8k^2 + 6k + 1) + 1 \Rightarrow$
$\Rightarrow \exists \lambda \in \mathbb{Z} : x^3+x^2+x = 2\lambda+1$ (for $\lambda = 4k^3+8k^2+6k+1 \in \mathbb{Z}$)
$\Rightarrow \underline{x^3+x^2+x \text{ odd}}$
$(\Leftarrow)$: Assume that $\underline{x \text{ even}}$. Then, we have:
$x \text{ even} \Rightarrow \exists k \in \mathbb{Z} : x = 2k$

Choose $k \in \mathbb{Z}$ such that $x = 2k$. It follows that

$$x^3+x^2+x = (2k)^3+(2k)^2+2k = 8k^3+4k^2+2k$$
$$= 2(4k^3+2k^2+k) \Rightarrow$$
$$\Rightarrow \exists \lambda \in \mathbb{Z} : x^3+x^2+x = 2\lambda$$
$$\Rightarrow \underline{x^3+x^2+x \text{ even}}.$$

We have thus shown that

$\forall x \in \mathbb{Z} : (x^3+x^2+x \text{ even} \Leftrightarrow x \text{ even})$. □

d) Show that: $\forall n \in \mathbb{Z} : n^2+3n+5$ odd

<u>Solution</u>

Let $\underline{n \in \mathbb{Z}}$ be given. We distinguish between the following cases.

<u>Case 1:</u> Assume that $\underline{n \text{ even}}$. Then, we have

n even $\Rightarrow \exists k \in \mathbb{Z} : n = 2k$

Choose $k \in \mathbb{Z}$ such that $n = 2k$. It follows that

$$n^2+3n+5 = (2k)^2+3(2k)+5 = 4k^2+6k+5$$
$$= 4k^2+6k+4+1 = 2(2k^2+3k+2)+1 \Rightarrow$$
$$\Rightarrow \exists \lambda \in \mathbb{Z} : n^2+3n+5 = 2\lambda+1 \quad (\text{for } \lambda = 2k^2+3k+2 \in \mathbb{Z})$$
$$\Rightarrow \underline{n^2+3n+5 \text{ odd}}.$$

<u>Case 2:</u> Assume that $\underline{n \text{ odd}}$. Then, we have:

n odd $\Rightarrow \exists k \in \mathbb{Z} : n = 2k+1$

Choose $k \in \mathbb{Z}$ such that $n = 2k+1$. It follows that

$$n^2+3n+5 = (2k+1)^2+3(2k+1)+5$$
$$= 4k^2+4k+1+6k+3+5$$
$$= 4k^2+(4+6)k+(1+3+5)$$

$= 4k^2 + 10k + 9$
$= 4k^2 + 10k + 8 + 1$
$= 2(2k^2 + 5k + 4) + 1 \Rightarrow$
$\Rightarrow \exists \lambda \in \mathbb{Z} : n^2 + 3n + 5 = 2\lambda + 1$ (for $\lambda = 2k^2 + 5k + 4 \in \mathbb{Z}$)
$\Rightarrow$ $\underline{n^2 + 3n + 5 \text{ odd}}$
We have thus shown in both cases that
$\forall n \in \mathbb{Z} : n^2 + 3n + 5$ odd $\square$

EXERCISES

(1) Let $a, b, x \in \mathbb{Z}$ be given. Prove that

a) x odd $\wedge$ $a+b$ odd $\Rightarrow$ $ax+b$ odd

b) x odd $\wedge$ $a+b$ even $\Rightarrow$ $ax+b$ even

c) x even $\wedge$ b odd $\Rightarrow$ $ax+b$ odd

d) x even $\wedge$ b even $\Rightarrow$ $ax+b$ even

(2) Let $a, b, c, x \in \mathbb{Z}$ be given. Prove that

a) x odd $\wedge$ $a+b+c$ odd $\Rightarrow$ ax^2+bx+c odd

b) x odd $\wedge$ $a+b+c$ even $\Rightarrow$ ax^2+bx+c even.

c) x even $\wedge$ c odd $\Rightarrow$ ax^2+bx+c odd

d) x even $\wedge$ c even $\Rightarrow$ ax^2+bx+c even.

(3) Let $a, b, n \in \mathbb{Z}$ be given. Prove that

$$an^3 - bn \text{ odd} \Rightarrow a-b \text{ odd}.$$

(4) Let $x, y \in \mathbb{Z}$ be given. Prove that

a) xy odd $\Rightarrow$ x odd $\wedge$ y odd

b) $(x+1)y^2$ even $\Leftrightarrow$ x odd $\vee$ y even

c) xy even $\wedge$ $x+y$ even $\Rightarrow$ x even $\wedge$ y even

d) $3x+1$ even $\Rightarrow$ $5x+2$ odd

e) x odd $\wedge$ $3x+5y$ even $\Rightarrow$ y odd

▼ The well-ordering principle

- We will now show that
  $\forall n \in \mathbb{Z}: n \text{ odd} \Rightarrow n \text{ not even}$
  $\forall n \in \mathbb{Z}: n \text{ not even} \Rightarrow n \text{ odd}$

  The first statement can be shown with a contradiction argument, however the proof of the second statement requires using the well-ordering principle. Combining the two statements gives
  $\forall n \in \mathbb{Z}: n \text{ odd} \Leftrightarrow n \text{ not even}$
  $\forall n \in \mathbb{Z}: n \text{ even} \Leftrightarrow n \text{ not odd}$
- The well-ordering principle is an axiom of $\mathbb{N}$ that cannot be shown via the obvious laws of algebra.

<u>Axiom</u>: Let S such that $\varnothing \neq S \subseteq \mathbb{N}$ and define the set:
$M = \{m \in S \mid \forall x \in S - \{m\} : m < x\}$
Then $M \neq \varnothing$.

<u>interpretation</u>: If $\varnothing \neq S \subseteq \mathbb{N}$, then S has at least one element that is strictly less than all other elements of S.

We will now prove that M can have only one element. We use the notation $|M|$ to denote the number of elements in M and will show that

> **Prop:** Let S such that $\emptyset \neq S \subseteq \mathbb{N}$ and define the set
> $M = \{m \in S \mid \forall x \in S - \{m\} : m < x\}$
> Then: $|M| = 1$.

Proof

From the well-ordering principle, we have
$\emptyset \neq S \subseteq \mathbb{N} \Rightarrow M \neq \emptyset \Rightarrow |M| > 0 \Rightarrow |M| \geq 1$
To show that $|M| \leq 1$, we assume that $|M| > 1$ and derive a contradiction. Since $|M| > 1 \Rightarrow |M| \geq 2$, we choose $a, b \in M$ such that $a \neq b$. Then, we have:

$$\begin{aligned} a \in M &\Rightarrow a \in S \wedge \forall x \in S - \{a\} : a < x \\ &\Rightarrow \forall x \in S - \{a\} : a < x \\ &\Rightarrow a < b \quad (\text{for } x = b \in M \Rightarrow x \in S) \end{aligned}$$

and

$$\begin{aligned} b \in M &\Rightarrow b \in S \wedge \forall x \in S - \{b\} : b < x \\ &\Rightarrow \forall x \in S - \{b\} : b < x \\ &\Rightarrow b < a \quad (\text{for } x = a \in M \Rightarrow x \in S) \end{aligned}$$

It follows that $a < b \wedge b < a$ which is a contradiction and conclude that $|M| \leq 1$. Then, we have:

$$\begin{cases} |M| \geq 1 \\ |M| \leq 1 \end{cases} \Rightarrow |M| = 1$$

□

▸ __notation:__ Since the set M has a unique element $a \in M$, we denote that element as $\underline{a = \min(S)}$.

We shall now prove our main results:

$\boxed{\text{Prop: } \forall n \in \mathbb{Z} : (n \text{ odd} \Rightarrow n \text{ not even})}$

Proof

Let $n \in \mathbb{Z}$ be given and assume that n odd.
To show that n not even, we assume that n is even in order to derive a contradiction. It follows that

$$\begin{cases} n \text{ odd} \\ n \text{ even} \end{cases} \Rightarrow \begin{cases} \exists k \in \mathbb{Z} : n = 2k+1 \\ \exists \lambda \in \mathbb{Z} : n = 2\lambda \end{cases}$$

Choose $k, \lambda \in \mathbb{Z}$ such that $n = 2k+1$ and $n = 2\lambda$.
Then, we have:

$$\begin{cases} n = 2k+1 \\ n = 2\lambda \end{cases} \Rightarrow 2\lambda = 2k+1 \Rightarrow \lambda = \frac{2k+1}{2} = k + 1/2$$

and therefore

$$k \in \mathbb{Z} \Rightarrow k + 1/2 \notin \mathbb{Z} \Rightarrow \lambda \notin \mathbb{Z}$$

which is a contradiction since λ was chosen with $\lambda \in \mathbb{Z}$. We conclude that n not even.
We have thus shown that
$\forall n \in \mathbb{Z} : (n \text{ odd} \Rightarrow n \text{ not even})$. □

$\boxed{\text{Prop: } \forall n \in \mathbb{Z} : (n \text{ not even} \Rightarrow n \text{ odd})}$

Proof

Let $n \in \mathbb{Z}$ be given and assume that n not even.

- We define the set
  $A = \{n-2x \mid x \in \mathbb{Z} \wedge n-2x \geq 0\}$
  and note that the belonging condition of A is
  $y \in A \Leftrightarrow \exists x \in \mathbb{Z} : (n-2x \geq 0 \wedge y = n-2x)$
- We will apply the well-ordering principle on A and extract $a = \min(A)$, so we must show that $\emptyset \neq A \subseteq \mathbb{N}$.

- <u>Proof of $A \neq \emptyset$</u>

We distinguish between the following cases.

<u>Case 1:</u> Assume that $n \geq 0$. Choose $x = -1$. Then, we have:

$n-2x = n-2(-1) = n+2 \geq 2 > 0 \Rightarrow n-2x \geq 0.$

Choose $y = n-2x$. It follows that

$\exists x \in \mathbb{Z} : (n-2x \geq 0 \wedge y = n-2x)$

$\Rightarrow y \in A \Rightarrow A \neq \emptyset.$

<u>Case 2:</u> Assume that $n < 0$. Choose $x = n-1$. Then, we have

$n-2x = n-2(n-1) = n-2n+2 = -n+2 > 2 > 0$

Choose $y = n-2x$. It follows that

$\exists x \in \mathbb{Z} : (n-2x \geq 0 \wedge y = n-2x)$

$\Rightarrow y \in A \Rightarrow A \neq \emptyset.$

In both cases we have shown that $A \neq \emptyset$.

- <u>Proof of $A \subseteq \mathbb{N}$.</u>

Let $y \in A$ be given. Then, we have

$y \in A \Rightarrow \exists x \in \mathbb{Z} : (n-2x \geq 0 \wedge y = n-2x)$

Choose $x \in \mathbb{Z}$ such that $n - 2x \geq 0$ and $y = n - 2x$.
It follows that

$$\begin{cases} y = n - 2x \geq 0 \\ x \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} y \geq 0 \\ y \in \mathbb{Z} \end{cases} \Rightarrow y \in \mathbb{N}$$

We have thus shown that
$(\forall y \in A : y \in \mathbb{N}) \Rightarrow A \subseteq \mathbb{N}$.

• <u>Main argument</u>: Since $\emptyset \neq A \subseteq \mathbb{N}$, the well-ordering principle applies and we may thus define $a = \min(A)$.
It follows that

$$\begin{aligned} a = \min(A) &\Rightarrow a \in A \\ &\Rightarrow \exists k \in \mathbb{Z} : (n - 2k \geq 0 \land n - 2k = a) \\ &\Rightarrow \exists k \in \mathbb{Z} : n = 2k + a \qquad (1) \end{aligned}$$

▶ We will show that $a > 0$. We note that
$a \in A \Rightarrow a \in \mathbb{N} \Rightarrow a \geq 0$
To show that $a \neq 0$, we assume that $a = 0$ in order to derive a contradiction. From Eq.(1), it follows that
$(\exists k \in \mathbb{Z} : n = 2k) \Rightarrow n$ even
which is a contradiction because by hypothesis n not even. We conclude that $a \neq 0$ and thus
$a \geq 0 \land a \neq 0 \Rightarrow a > 0$

▶ We will show that $a < 2$. To show that $a < 2$, we assume that $a \geq 2$ in order to derive a contradiction.
Define $b = a - 2$. We will show that $b \in A$. From Eq.(1) choose $k \in \mathbb{Z}$ such that $n = 2k + a$. Then, we have:

$b = a-2 = 2k+a-2k-2 = n-2k-2 = n-2(k+1)$

and

$a \geq 2 \Rightarrow b = a-2 \geq 0 \Rightarrow n-2(k+1) \geq 0$

We have thus shown that

$\exists x \in \mathbb{Z} : (n-2x \geq 0 \land b = n-2x) \quad (\text{for } x = k+1 \in \mathbb{Z})$

$\Rightarrow b \in A \Rightarrow b \geq \min(A) = a \Rightarrow b \geq a$

This contradicts $b = a-2 < a$. We conclude that $a < 2$.

From the above, it follows that

$a = 1 \Rightarrow \exists k \in \mathbb{Z} : n = 2k+1$

$\quad \Rightarrow$ <u>n odd.</u>

We have thus shown that

$\forall n \in \mathbb{Z} : (n \text{ not even} \Rightarrow n \text{ odd}).$ $\square$

Division theorem

A generalization of the above argument gives the following theorem

$$\boxed{\forall a \in \mathbb{Z}^* : \forall b \in \mathbb{Z} : \exists! q, r \in \mathbb{Z} : (b = aq + r \land 0 \leq r < |a|)}$$

We say that q is the <u>quotient</u> of the division of b by a and r is the <u>remainder.</u> Both q, r are unique under the constraint $0 \leq r < |a|$.

Divisability.

We begin with the following definition

> **Def:** Let $a \in \mathbb{Z}^*$ and $b \in \mathbb{Z}$. We say that
> $a|b \Leftrightarrow \exists k \in \mathbb{Z} : b = ak$

The notation $a|b$ reads "a divides b" and means that the remainder of the division of b by a is zero.

Properties

① $\boxed{\forall a, b \in \mathbb{Z}^* : \forall c \in \mathbb{Z} : ((a|b \wedge b|c) \Rightarrow a|c)}$

Proof

Let $a, b \in \mathbb{Z}^*$ and $c \in \mathbb{Z}$ be given and assume that $a|b$ and $b|c$. Then, we have

$$\begin{cases} a|b \\ b|c \end{cases} \Rightarrow \begin{cases} \exists x \in \mathbb{Z} : b = ax \\ \exists y \in \mathbb{Z} : c = by \end{cases}$$

Choose $x, y \in \mathbb{Z}$ such that $b = ax$ and $c = by$.
It follows that

$$c = by = (ax)y = a(xy) \Rightarrow$$
$$\Rightarrow \exists \lambda \in \mathbb{Z} : c = a\lambda \quad (\text{for } \lambda = xy \in \mathbb{Z})$$
$$\Rightarrow a|c.$$

We have thus shown that
$\forall a,b \in \mathbb{Z}^* : \forall c \in \mathbb{Z} : ((a|b \wedge b|c) \Rightarrow a|c)$ $\square$

(2) $\boxed{\forall a \in \mathbb{Z}^* : \forall b,c,x,y \in \mathbb{Z} : ((a|b \wedge a|c) \Rightarrow a|(bx+cy))}$

<u>Proof</u>

Let <u>$a \in \mathbb{Z}^*$</u> and <u>$b,c,x,y \in \mathbb{Z}$</u> be given and assume that <u>$a|b$</u> and <u>$a|c$</u>. Then, we have:

$$\begin{cases} a|b \\ a|c \end{cases} \Rightarrow \begin{cases} \exists \lambda \in \mathbb{Z} : b = a\lambda \\ \exists \mu \in \mathbb{Z} : c = a\mu \end{cases}$$

Choose $\lambda,\mu \in \mathbb{Z}$ such that $b = a\lambda$ and $c = a\mu$. Then, we have

$$bx+cy = (a\lambda)x + (a\mu)y = a(\lambda x) + a(\mu y) =$$
$$= a(\lambda x + \mu y) \Rightarrow$$
$$\Rightarrow \exists k \in \mathbb{Z} : bx+cy = ak \quad (\text{for } k = \lambda x + \mu y \in \mathbb{Z})$$
$$\Rightarrow \underline{a|(bx+cy)}$$

We have thus shown that
$\forall a \in \mathbb{Z}^* : \forall b,c,x,y \in \mathbb{Z} : ((a|b \wedge a|c) \Rightarrow a|(bx+cy))$ $\square$

EXAMPLES

a) Show that $\forall x \in \mathbb{Z} : (2 \mid (x^2-1) \Rightarrow 4 \mid (x^2-1))$

Solution

Let $x \in \mathbb{Z}$ be given and assume that $2 \mid (x^2-1)$. It follows that

$$\begin{aligned}
2 \mid (x^2-1) &\Rightarrow \exists k \in \mathbb{Z} : x^2-1 = 2k \\
&\Rightarrow \exists k \in \mathbb{Z} : x^2 = 2k+1 \\
&\Rightarrow x^2 \text{ odd} \\
&\Rightarrow x \text{ odd} \\
&\Rightarrow \exists k \in \mathbb{Z} : x = 2k+1
\end{aligned}$$

Choose $k \in \mathbb{Z}$ such that $x = 2k+1$. Then, we have:

$$\begin{aligned}
x^2-1 &= (2k+1)^2 - 1 = 4k^2+4k+1-1 = 4k^2+4k \\
&= 4(k^2+k)
\end{aligned}$$

$\Rightarrow \exists \lambda \in \mathbb{Z} : x^2-1 = 4\lambda \quad (\text{for } \lambda = k^2+k \in \mathbb{Z})$

$\Rightarrow 4 \mid (x^2-1)$.

We have thus shown that

$\forall x \in \mathbb{Z} : (2 \mid (x^2-1) \Rightarrow 4 \mid (x^2-1))$

b) Show that: $\forall x \in \mathbb{Z} : (\overline{3|x} \Rightarrow 3|(x^2-1))$

<u>Solution</u>

Let $x \in \mathbb{Z}$ be given and assume that $\overline{3|x}$. From the division theorem, it follows that

$\overline{3|x} \Rightarrow \exists a \in \mathbb{Z} : x = 3a+1 \vee x = 3a+2$

Choose $a \in \mathbb{Z}$ such that $x = 3a+1 \vee x = 3a+2$. We distinguish between the following cases.

<u>Case 1:</u> Assume that $x = 3a+1$. Then, we have

$x^2 - 1 = (3a+1)^2 - 1 = (3a+1-1)(3a+1+1) = 3a(3a+2)$

$\Rightarrow \exists k \in \mathbb{Z} : x^2 - 1 = 3k \quad (\text{for } k = a(3a+2) \in \mathbb{Z})$

$\Rightarrow 3 | (x^2-1)$

<u>Case 2:</u> Assume that $x = 3a+2$. Then, we have

$x^2 - 1 = (3a+2)^2 - 1 = (3a+2-1)(3a+2+1)$

$= (3a+1)(3a+3) = 3(3a+1)(a+1)$

$\Rightarrow \exists k \in \mathbb{Z} : x^2 - 1 = 3k \quad (\text{for } k = (3a+1)(a+1) \in \mathbb{Z})$

$\Rightarrow 3 | (x^2-1)$

In both cases, we have shown that $3|(x^2-1)$.

We conclude that

$\forall x \in \mathbb{Z} : (\overline{3|x} \Rightarrow 3|(x^2-1))$ $\square$

EXERCISES

(5) Let $a, b \in \mathbb{Z}$ be given. Show that

a) $a | b \Rightarrow a^2 | b^2$

b) $a | b \wedge b | a \Rightarrow a = b \vee a = -b$

c) $3 \nmid a \wedge 3 \nmid b \Rightarrow 3 | (a^2 - b^2)$

d) $3 | (2a^2 + 1) \Rightarrow 3 \nmid a$

e) $4 | (a^2 + b^2) \Rightarrow a$ even $\vee\ b$ even

f) $3 | (a^3 - a)$

g) $5 | (a^5 - 5a^3 + 4a)$

(6) Let $a, b, c \in \mathbb{Z}$ such that
$3 | c \wedge 3 | (a+b+c) \wedge 3 | (3a+b)$
Prove that $\forall x \in \mathbb{Z}: 3 | (ax^2 + bx + c)$.

(7) Let $a, b, x \in \mathbb{Z}$ be given. Prove that

a) $4 | 2a+b \wedge 4 | x-2 \Rightarrow 4 | ax+b$

b) $5 | 2a-b \wedge 5 | x-3 \Rightarrow 5 | ax^3 - b$

(8) Let $a, b, c \in \mathbb{Z}$ be given such that
$4 | c \wedge 4 | (a+b+c) \wedge 4 | 3a+b \wedge 4 | 5a+b$
Prove that $\forall x \in \mathbb{Z}: 4 | (ax^2 + bx + c)$.

▼ Method of induction

Let $a \in \mathbb{Z}$ and define $\mathbb{Z}_a = \{x \in \mathbb{Z} \mid x \geq a\}$. The method of induction can be used to prove statements of the form: $\forall x \in \mathbb{Z}_a : p(x)$.

It is based on Peano's theorem:

<u>Thm</u> : Let $a \in \mathbb{Z}$. Then:

$$\boxed{\left.\begin{array}{l} p(a) \text{ true} \\ \forall x \in \mathbb{Z}_a : (p(x) \Rightarrow p(x+1)) \end{array}\right\} \Rightarrow \forall x \in \mathbb{Z}_a : p(x)}$$

This theorem can be shown via the well-ordering principle.

▶ <u>Method</u> : To show $\forall x \in \mathbb{Z}_a : p(x)$ true

- •1 For $x = a$, show that $p(x)$ is true
- •2 Assume that for $x = k > a$, $p(k)$ is true
- •3 Show that $p(k+1)$ true
- •4 It follows that $\forall x \in \mathbb{Z}_a : p(x)$ true.

EXAMPLES

a) Show that $1+2+3+\dots+n = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N} - \{0\}$

<u>Proof</u>

For $n=1$: $LHS = 1$

$$RHS = \frac{n(n+1)}{2} = \frac{1\cdot 2}{2} = 1$$

thus the statement is true.

For $n=k$, assume that

$$1+2+3+\cdots+k = \frac{k(k+1)}{2}$$

For $n=k+1$, we will show that

$$1+2+3+\cdots+(k+1) = \frac{(k+1)(k+2)}{2}$$

Since:

$$1+2+3+\cdots+(k+1) = [1+2+3+\cdots+k] + (k+1) =$$

$$= \frac{k(k+1)}{2} + (k+1) = (k+1)(k/2+1)$$

$$= (k+1)\frac{k+2}{2} = \frac{(k+1)(k+2)}{2}$$

It follows that $\forall n \in \mathbb{N}-\{0\}: 1+2+3+\cdots+n = \frac{n(n+1)}{2}$ $\square$

b) Show that $\forall n \in \mathbb{N}: 3 \mid (2^{2n}-1)$.

Proof

For $n=0$: $2^{2n}-1 = 2^0 - 1 = 1-1 = 0 = 3\cdot 0 \Rightarrow 3 \mid 2^{2n}-1$.

For $n=k$: assume that $3 \mid (2^{2k}-1)$.

For $n=k+1$: we will show that $3 \mid (2^{2(k+1)}-1)$.

We have:

$3 \mid (2^{2k}-1) \Rightarrow \exists a \in \mathbb{Z} : 2^{2k} - 1 = 3a$

$\Rightarrow \exists a \in \mathbb{Z} : 2^{2k} = 3a+1$

Choose $a \in \mathbb{Z}$ such that $2^{2k} = 3a+1$. It follows that:

$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^{2k} \cdot 4 - 1 = 4(3a+1) - 1 =$

$= 12a + 4 - 1 = 12a + 3 = 3(4a+1)$

$\Rightarrow \exists \lambda \in \mathbb{Z} : 2^{2(k+1)} - 1 = 3\lambda$ (for $\lambda = 4a+1 \in \mathbb{Z}$)

$\Rightarrow 3 \mid (2^{2(k+1)} - 1)$

We conclude, by induction, that

$\forall n \in \mathbb{N} : 3 \mid (2^{2n} - 1)$ $\square$

EXERCISES

(9) Prove the following identities for $n \in \mathbb{N}$, $n > 0$. by induction

a) $1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + n(n+1) = (1/3)\,n(n+1)(n+2)$, $n > 0$

b) $1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2$

c) $2 + 4 + 6 + \cdots + 2n = n(n+1)$

d) $1\cdot 2^2 + 2\cdot 3^2 + \cdots + n(n+1)^2 = (1/12)\,n(n+1)(n+2)(3n+5)$

e) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$, $n \geq 2$

f) $2^3 + 4^3 + 6^3 + \cdots + (2n)^3 = 2n^2(n+1)^2$, $n > 1$

g) $2 + 2^2 + 2^3 + \cdots + 2^n = 2\cdot(2^n - 1)$, $n \geq 3$

h) $\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$, $n \geq 2$

i) $1\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + \cdots + n5^n = \dfrac{5 + (4n-1)\cdot 5^{n+1}}{16}$

(10) Prove the following statements by induction

a) $\forall n \in \mathbb{N} - \{0\}:\ 49 \mid (4\cdot 8^n + 21n - 4)$

b) $\forall n \in \mathbb{N} - \{0\}:\ 9 \mid (2^{2n} + 15n - 1)$

c) $\forall n \in \mathbb{N} - \{0\}:\ 288 \mid (7^{2n+1} - 48n - 7)$

d) $\forall n \in \mathbb{N} - \{0\}:\ 64 \mid (7^{2n} + 16n - 1)$

e) $\forall n \in \mathbb{N} - \{0\}:\ 4 \mid (5^n - 1)$

f) $\forall n \in \mathbb{N} - \{0\}:\ 81 \mid (10^{n+1} - 9n - 10)$

g) $\forall n \in \mathbb{N} - \{0\}:\ 7 \mid (3^{2n} - 2^n)$

(11) Show that $A_n = (1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$ is an even integer for $n \in \mathbb{N} - \{0\}$.

IMP3: Relations and Mappings

RELATIONS AND FUNCTIONS

▼ Cartesian product

- An ordered pair (a,b) is defined as an ordered collection of two elements a and b such that it satisfies the axiom:
  $(a_1, b_1) = (a_2, b_2) \Leftrightarrow a_1 = a_2 \wedge b_1 = b_2$.
- Ordered pairs can be represented as sets:
  $(a,b) = \{a, \{a,b\}\}$
  Then ordered pair equality corresponds to set equality.
- Let A, B be two sets. We define the cartesian product $A \times B$ as:
  $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$
  The corresponding belonging condition is:
  $x \in A \times B \Leftrightarrow \exists a \in A : \exists b \in B : x = (a,b)$.
  however, in practice we find it more useful to use the following statement
  $(a,b) \in A \times B \Leftrightarrow a \in A \wedge b \in B$.
- We also define $A^2 = A \times A$.
- It is easy to see that
  $\varnothing \times A = \varnothing$
  $A \times \varnothing = \varnothing$.

EXAMPLES

a) For $A = \{1,2\}$ and $B = \{2,3\}$, evaluate $A \times B$, $B \times A$ and A^2.

Solution

$$A \times B = \{1,2\} \times \{2,3\} =$$
$$= \{(1,2), (1,3), (2,2), (2,3)\}$$
$$B \times A = \{2,3\} \times \{1,2\} =$$
$$= \{(2,1), (2,2), (3,1), (3,2)\}$$
$$A^2 = A \times A = \{1,2\} \times \{1,2\} =$$
$$= \{(1,1), (1,2), (2,1), (2,2)\}$$

b) Let A, B, C be sets. Show that
$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

Solution

Since,
$$(x,y) \in A \times (B \cup C) \Leftrightarrow x \in A \wedge y \in B \cup C$$
$$\Leftrightarrow x \in A \wedge (y \in B \vee y \in C)$$
$$\Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C)$$
$$\Leftrightarrow (x,y) \in A \times B \vee (x,y) \in A \times C$$
$$\Leftrightarrow (x,y) \in (A \times B) \cup (A \times C),$$
it follows that
$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

c) Show that; for sets A, B, C:

$(C \neq \emptyset \wedge A \times C = B \times C) \Rightarrow A = B.$

Solution

Assume that $C \neq \emptyset$ and $A \times C = B \times C$.

Since $C \neq \emptyset$, choose a $y \in C$.

Let $x \in A$ be given. Then:

$$\begin{aligned} x \in A \wedge y \in C &\Rightarrow (x, y) \in A \times C && [\text{definition}] \\ &\Rightarrow (x, y) \in B \times C && [A \times C \subseteq B \times C] \\ &\Rightarrow x \in B \wedge y \in C && [\text{definition}] \\ &\Rightarrow x \in B \end{aligned}$$

and therefore:

$(\forall x \in A : x \in B) \Rightarrow A \subseteq B.$ (1)

Let $x \in B$ be given. Then

$$\begin{aligned} x \in B \wedge y \in C &\Rightarrow (x, y) \in B \times C \\ &\Rightarrow (x, y) \in A \times C \\ &\Rightarrow x \in A \wedge y \in C \\ &\Rightarrow x \in A \end{aligned}$$

and therefore

$(\forall x \in B : x \in A) \Rightarrow B \subseteq A.$ (2)

From (1) and (2): $A = B$.

d) Let A, B be sets with $A \neq \emptyset$ and $B \neq \emptyset$. Show that
$A \times B = B \times A \Rightarrow A = B$.

<u>Solution</u>

Assume that $A \neq \emptyset$ and $B \neq \emptyset$ and $A \times B = B \times A$.
Let $x \in A$ be given.
Since $B \neq \emptyset$, choose a $y \in B$. Then

$$\begin{aligned} x \in A \wedge y \in B &\Rightarrow (x,y) \in A \times B \\ &\Rightarrow (x,y) \in B \times A \quad [\text{via } A \times B \subseteq B \times A] \\ &\Rightarrow x \in B \wedge y \in A \\ &\Rightarrow x \in B. \end{aligned}$$

and therefore:

$(\forall x \in A : x \in B) \Rightarrow A \subseteq B.$ (1)

Let $x \in B$ be given.
Since $A \neq \emptyset$, choose a $y \in A$. Then

$$\begin{aligned} x \in B \wedge y \in A &\Rightarrow (x,y) \in B \times A \\ &\Rightarrow (x,y) \in A \times B \quad [\text{via } B \times A \subseteq A \times B] \\ &\Rightarrow x \in A \wedge y \in B \\ &\Rightarrow x \in A. \end{aligned}$$

and therefore

$(\forall x \in B : x \in A) \Rightarrow B \subseteq A.$ (2)

From (1) and (2): $A = B$.

e) Let $\{A_a\}_{a\in I}$, $\{B_a\}_{a\in I}$ be indexed set collections and let G be a set. Show that

$$C\times\left[\bigcup_{a\in I}(A_a-B_a)\right]\subseteq\bigcup_{a\in I}\left[(C\times A_a)-(C\times B_a)\right]$$

Solution

Since

$$(x,y)\in G\times\left[\bigcup_{a\in I}(A_a-B_a)\right]\Rightarrow$$

$$\Rightarrow x\in G\wedge y\in\bigcup_{a\in I}(A_a-B_a)\Rightarrow$$

$$\Rightarrow x\in G\wedge\exists a\in I: y\in A_a-B_a$$

$$\Rightarrow x\in G\wedge\exists a\in I:(y\in A_a\wedge y\notin B_a)$$

$$\Rightarrow\exists a\in I:(x\in G\wedge y\in A_a\wedge y\notin B_a)$$

$$\Rightarrow\exists a\in I:[(x\in G\wedge y\in A_a)\wedge(x\notin G\vee y\notin B_a)]\qquad(!!!)$$

$$\Rightarrow\exists a\in I:((x,y)\in G\times A_a\wedge(\overline{x\in C\wedge y\in B_a}))$$

$$\Rightarrow\exists a\in I:((x,y)\in G\times A_a\wedge(x,y)\notin G\times B_a)$$

$$\Rightarrow\exists a\in I:(x,y)\in(G\times A_a)-(G\times B_a)$$

$$\Rightarrow(x,y)\in\bigcup_{a\in I}\left[(G\times A_a)-(G\times B_a)\right]$$

it follows that:

$$C\times\left[\bigcup_{a\in I}(A_a-B_a)\right]\subseteq\bigcup_{a\in I}\left[(G\times A_a)-(G\times B_a)\right]$$

↳ Note that the (!!) step is valid but cannot be reversed.

EXERCISES

① Let $A = \{x \in \mathbb{Z} \mid 1 \leq x \leq 3\}$
$B = \{3x - 1 \mid x \in \mathbb{Z} \wedge 0 < x < 4\}$
List the elements of $A \times B$.

② Prove that for A, B, C sets
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

③ Prove the following
a) $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$
b) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
c) $(A \times B) \cap (C \times D) = \emptyset \Leftrightarrow A \cap C = \emptyset \vee B \cap D = \emptyset$.

④ Prove the following.
a) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$
b) $\{p, q\} \subseteq A \Rightarrow (A \times \{p\}) \cup (\{q\} \times A) \subseteq A \times A$

⑤ Prove the following:
a) $A \times B = B \times A \Leftrightarrow A = \emptyset \vee B = \emptyset \vee A = B$
b) $A \neq \emptyset \neq B \wedge (A \times B) \cup (B \times A) = C \times C \Rightarrow A = B = C$.

⑥ Let $\{A_a\}_{a\in I}$ and $\{B_a\}_{a\in I}$ be indexed set collections and let C be a set. Prove the following:

a) $$\left(\bigcup_{a\in I} A_a\right)\times C = \bigcup_{a\in I}(A_a\times C)$$

b) $$\left(\bigcap_{a\in I} A_a\right)\times C = \bigcap_{a\in I}(A_a\times C)$$

c) $$\bigcap_{a\in I}(A_a\times B_a) = \left(\bigcap_{a\in I} A_a\right)\times\left(\bigcap_{a\in I} B_a\right)$$

⑦ Show that for A, B sets

$$\bigcup_{S\in\mathcal{P}(A)}\left[\bigcup_{T\in\mathcal{P}(B)}\{S\times T\}\right]\subseteq\mathcal{P}(A\times B)$$

▼ Relations

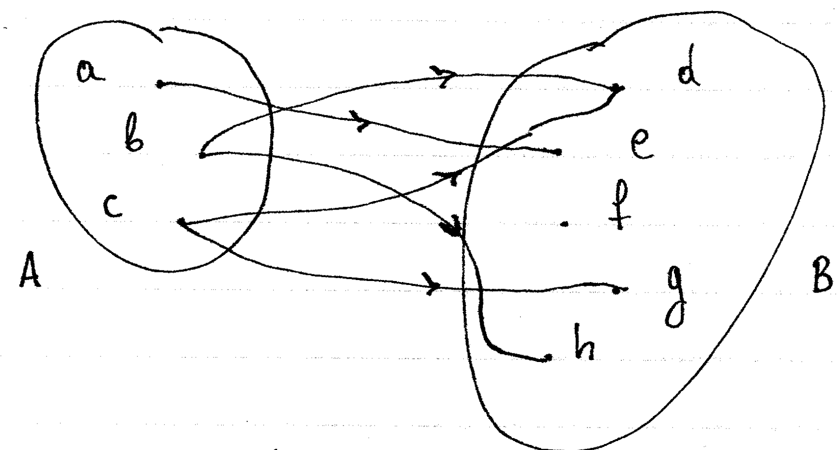
- Let A, B be two sets with $A \neq \emptyset$ and $B \neq \emptyset$. We define the set of all relations from A to B via the following belonging condition:
$$R \in \mathrm{Rel}(A,B) \iff R \subseteq A \times B$$
- If $R \in \mathrm{Rel}(A,B)$, we say that R is a <u>relation</u> from A to B.
- Let $R \in \mathrm{Rel}(A,B)$ be a relation and let $x \in A$ and $y \in B$. Then we define the statements xRy and $x\not{R}y$ as follows:
$$\forall x \in A : \forall y \in B : (xRy \iff (x,y) \in R)$$
$$\forall x \in A : \forall y \in B : (x\not{R}y \iff (x,y) \notin R)$$
We say that:
xRy : x is related with y via relation R.
$x\not{R}y$: x is NOT related with y via relation R.

EXAMPLE

Let $A = \{a, b, c\}$ and $B = \{d, e, f, g, h\}$. Then
$R = \{(a,e), (b,d), (c,g), (b,h), (c,d)\}$
is a relation from A to B (i.e. $R \in \mathrm{Rel}(A,B)$). Then

$(a,e) \in R \Rightarrow aRe$ $\qquad$ $(b,h) \in R \Rightarrow bRh$
$(b,d) \in R \Rightarrow bRd$ $\qquad$ $(c,d) \in R \Rightarrow cRd$
$(c,g) \in R \Rightarrow cRg$

↳ The relation R can be represented geometrically using a <u>Venn diagram</u>, as follows:



Each ordered pair (x,y) is represented by an arrow from x to y.

↳ Domain and range of a relation

- Let $R \in Rel(A,B)$ be a relation from A to B. We define the domain $dom(R)$ and range $ran(R)$ of R as:

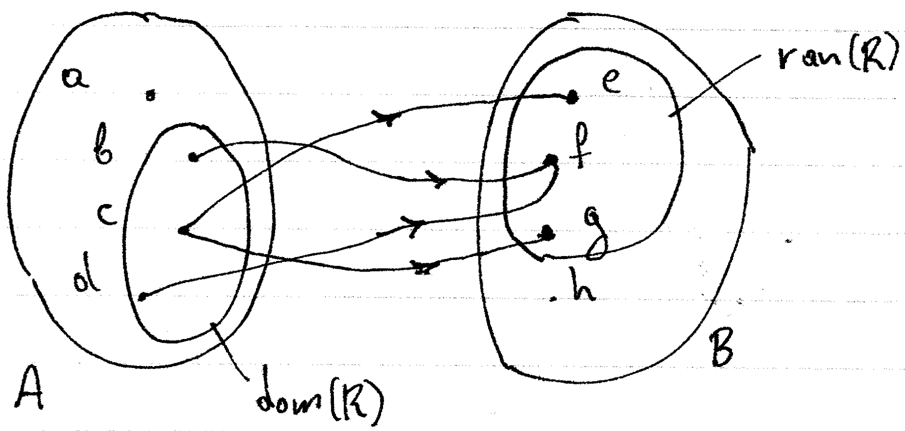
$$dom(R) = \{x \in A \mid \exists y \in B : xRy\} \subseteq A$$
$$ran(R) = \{y \in B \mid \exists x \in A : xRy\} \subseteq B$$

- $dom(R)$ contains all the elements of A that are related with some element of B. In terms of Venn diagrams, $dom(R)$ has all the elements of A that have an outgoing arrow.
- $ran(R)$ contains all the elements of B that are related with some element of A. In terms of Venn diagrams,

ran(R) has all the elements of B that have an incoming arrow.

EXAMPLE

For $A=\{a,b,c,d\}$ and $B=\{e,f,g,h\}$, let $R\in Rel(A,B)$ be a relation from A to B with
$R=\{(b,f),(c,e),(d,f),(c,g)\}$.
Then: $dom(R)=\{b,c,d\}$ and
$ran(R)=\{e,f,g\}$



Relations on A

We define $Rel(A)=Rel(A,A)$. Then:

$$R\in Rel(A) \Leftrightarrow R\subseteq A\times A$$

and we say that R is a <u>relation on A</u>.

Equivalence relations

- Let $R \in Rel(A)$ be a relation on A with $A \neq \emptyset$.
  We say that
  R reflexive $\Leftrightarrow \forall x \in A : xRx$
  R symmetric $\Leftrightarrow \forall x,y \in A : (xRy \Rightarrow yRx)$
  R transitive $\Leftrightarrow \forall x,y,z \in A : ((xRy \wedge yRz) \Rightarrow xRz)$
  and:

$$R \text{ equivalence} \Leftrightarrow \begin{cases} R \text{ reflexive} \\ R \text{ symmetric} \\ R \text{ transitive} \end{cases}$$

EXAMPLE

a) Let $R \in Rel(\mathbb{Z})$ such that

$$xRy \Leftrightarrow 11x - 5y \text{ even.}$$

Show that R is an equivalence.

Proof

- Reflexive

Let $x \in \mathbb{Z}$ be given. Then:

$11x - 5x = 6x = 2(3x)$

and therefore, for $\mu = 3x$:

$$(\exists \mu \in \mathbb{Z} : 11x - 5x = 2\mu) \Rightarrow 11x - 5x \text{ even}$$
$$\Rightarrow xRx$$

It follows that: $(\forall x \in \mathbb{Z} : xRx) \Rightarrow R$ reflexive. (1)

• Symmetric

Let $\underline{x,y \in \mathbb{Z}}$ be given. Assume that $\underline{xRy}$. Then

$$xRy \Rightarrow 11x - 5y \text{ even}$$
$$\Rightarrow \exists k \in \mathbb{Z} : 11x - 5y = 2k$$

Choose $k \in \mathbb{Z}$ such that $11x - 5y = 2k$. Then, we have:

$$11y - 5x = -5y + 16y + 11x - 16x = (11x - 5y) + (16y - 16x)$$
$$= 2k + (16y - 16x) = 2(k + 8y - 8x)$$

Then, for $\mu = k + 8y - 8x \in \mathbb{Z}$:

$$(\exists \mu \in \mathbb{Z} : 11y - 5x = 2\mu) \Rightarrow 11y - 5x \text{ even}$$
$$\Rightarrow \underline{yRx}$$

It follows that

$$(\forall x, y \in \mathbb{Z} : (xRy \Rightarrow yRx)) \Rightarrow R \text{ symmetric.} \quad (2)$$

• Transitive

Let $x, y, z \in \mathbb{Z}$ be given. Assume that $xRy \wedge yRz$. Then

$$xRy \Rightarrow 11x - 5y \text{ even}$$
$$\Rightarrow \exists k \in \mathbb{Z} : 11x - 5y = 2k$$
$$yRz \Rightarrow 11y - 5z \text{ even}$$
$$\Rightarrow \exists \lambda \in \mathbb{Z} : 11y - 5z = 2\lambda$$

Choose $k, \lambda \in \mathbb{Z}$ such that $11x - 5y = 2k$ and $11y - 5z = 2\lambda$. Then,

$$11x - 5z = (11x - 5y) + (11y - 5z) - 6y$$
$$= 2k + 2\lambda - 6y = 2(k + \lambda - 3y)$$

Then, for $\mu = k + \lambda - 3y \in \mathbb{Z}$:

$$(\exists \mu \in \mathbb{Z} : 11x - 5z = 2\mu) \Rightarrow 11x - 5z \text{ even}$$
$$\Rightarrow xRz$$

It follows that: $(\forall x, y, z \in \mathbb{Z} : ((xRy \wedge yRz) \Rightarrow xRz)) \Rightarrow$

$\Rightarrow R$ transitive. (3)

From (1), (2), (3):

$$\left.\begin{cases} R \text{ reflexive} \\ R \text{ symmetric} \\ R \text{ transitive} \end{cases}\right. \Rightarrow R \text{ equivalence.}$$

b) Let $R \in Rel(A)$ be a relation on A. Show that

R reflexive $\Rightarrow dom(R) = A$

Proof

Assume that R reflexive. Since

$dom(R) = \{x \in A \mid \exists y \in A : xRy\} \Rightarrow \underline{dom(R) \subseteq A}$ (1)

$\Rightarrow$ Sufficient to show that $A \subseteq dom(R)$.

Let $\underline{x \in A}$ be given. Then:

R reflexive $\Rightarrow xRx$

$\Rightarrow \exists y \in A : xRy$ (for $y = x$)

It follows that since:

$$\begin{cases} x \in A \\ \exists y \in A : xRy \end{cases} \Rightarrow \underline{x \in dom(R)}.$$

and therefore

$(\forall x \in A : x \in dom(R)) \Rightarrow \underline{A \subseteq dom(R)}$ (2)

From (1) and (2):

$$\begin{cases} dom(R) \subseteq A \\ A \subseteq dom(R) \end{cases} \Rightarrow dom(R) = A.$$

$\hookrightarrow$ For $R \in Rel(A, B)$ note the belonging conditions:

$$x \in dom(R) \Leftrightarrow x \in A \wedge (\exists y \in B : xRy)$$
$$y \in ran(R) \Leftrightarrow y \in B \wedge (\exists x \in A : xRy)$$

These belonging conditions are used in the proofs above.

c) Let $R \in Rel(A)$. We define

R circular $\Leftrightarrow \forall x, y, z \in A : ((xRy \wedge yRz) \Rightarrow zRx)$

Show that:

(R transitive $\wedge$ R symmetric) $\Rightarrow$ R circular.

<u>Proof</u>

Assume that R transitive $\wedge$ R symmetric.

Let <u>$x, y, z \in A$</u> be given and assume that <u>$xRy \wedge yRz$</u>. Then

$$\left.\begin{cases} xRy \\ yRz \end{cases}\right. \Rightarrow xRz \quad [R \text{ is transitive}]$$
$$\Rightarrow \underline{zRx} \quad [R \text{ is symmetric}]$$

From the above, it follows that

$\forall x, y, z \in A : ((xRy \wedge yRz) \Rightarrow zRx)$

$\Rightarrow$ R circular.

EXERCISES

(8) Show that the following relations are equivalences:

a) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow a+b$ even

b) $R \in Rel(\mathbb{N}^*)$ with $aRb \Leftrightarrow a^2+b^2$ even

c) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow 3a-7b$ even

d) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow 3 \mid (a+2b)$

e) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow 4 \mid (a^3-b^3)$

f) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow 5 \mid (2a+3b)$

(9) Show that the following relations on $\mathbb{R}^* \times \mathbb{R}^*$ are equivalences:

a) $(x_1,y_1) R (x_2,y_2) \Leftrightarrow x_1y_2 - x_2y_1 = 0$

b) $(x_1,y_1) R (x_2,y_2) \Leftrightarrow \exists \lambda \in \mathbb{R}^* : \begin{cases} x_1 = \lambda x_2 \\ y_1 = \lambda y_2 \end{cases}$

(Recall that $\mathbb{R}^* = \mathbb{R} - \{0\}$).

(10) Let $R \in Rel(A)$ be a relation on A. Show that

a) R reflexive $\Rightarrow ran(R) = A$

b) R symmetric $\Rightarrow dom(R) = ran(R)$

c) (R circular $\wedge$ R symmetric) $\Rightarrow R$ transitive

d) R equivalence $\Leftrightarrow$ (R reflexive $\wedge$ R circular)

$\hookrightarrow$ We use the definition:

R circular $\Leftrightarrow \forall x,y,z \in A : ((xRy \wedge yRz) \Rightarrow zRx)$

(11) Let $R \in Rel(A)$ be a relation on A. Write the definitions, using quantifiers for the following statements:

a) R is not reflexive

b) R is not symmetric

c) R is not transitive.

Equivalence classes

- Let $R \in \text{Rel}(A)$ be an equivalence relation on A, and let $a \in A$. We define the equivalence class $R(a)$ as:
  $$R(a) = \{x \in A \mid x R a\}$$
  The belonging condition of $R(a)$ is given by:
  $$x \in R(a) \Leftrightarrow x \in A \land x R a$$
- The set of all possible equivalence classes of R is denoted as A/R:
  $$A/R = \{R(a) \mid a \in A\}$$

Properties of equivalence classes

- Let $R \in \text{Rel}(A)$ be an equivalence relation. Then

$$\boxed{\begin{array}{l} 1)\ \forall a,b \in A : R(a) = R(b) \Leftrightarrow a R b. \\ 2)\ \forall a,b \in A : R(a) \cap R(b) = \emptyset \Leftrightarrow a \not R b \end{array}}$$

<u>Proof of (1)</u>

Let $a, b \in A$ be given.

<u>($\Rightarrow$)</u>: Assume that <u>$R(a) = R(b)$</u>. Then.

$$\begin{aligned} R \text{ equivalence} &\Rightarrow R \text{ reflexive} && [\text{definition}] \\ &\Rightarrow aRa && [\text{definition}] \\ &\Rightarrow a \in R(a) && [\text{belonging condition}] \\ &\Rightarrow a \in R(b) && [\text{hypothesis } R(a) = R(b)] \\ &\Rightarrow \underline{aRb} && [\text{belonging condition}]. \end{aligned}$$

($\Leftarrow$): Assume that aRb. Let $x \in R(a)$ be given. Then

$$\begin{aligned}
x \in R(a) &\Rightarrow xRa &&[\text{belonging condition}]\\
&\Rightarrow xRb &&[aRb \wedge R \text{ transitive}]\\
&\Rightarrow x \in R(b) &&[\text{belonging condition}]
\end{aligned}$$

It follows that $(\forall x \in R(a) : x \in R(b)) \Rightarrow \underline{R(a) \subseteq R(b)}$. (1)

Let $x \in R(b)$ be given. Then

$$\begin{aligned}
x \in R(b) &\Rightarrow xRb &&[\text{belonging condition}]\\
&\Rightarrow bRx &&[R \text{ symmetric}]\\
&\Rightarrow aRx &&[aRb \wedge R \text{ transitive}]\\
&\Rightarrow xRa &&[R \text{ symmetric}]\\
&\Rightarrow x \in R(a) &&[\text{belonging condition}]
\end{aligned}$$

It follows that:

$(\forall x \in R(b) : x \in R(a)) \Rightarrow \underline{R(b) \subseteq R(a)}$ (2)

From (1) and (2):

$$\begin{cases} R(a) \subseteq R(b) \\ R(b) \subseteq R(a) \end{cases} \Rightarrow \underline{R(a) = R(b)}.$$

From the above argument it follows that

$\forall a, b \in A : (R(a) = R(b) \Leftrightarrow aRb)$.

Proof of (2)

Let $a, b \in A$ be given.

($\Rightarrow$): Assume that $R(a) \cap R(b) = \emptyset$. To show that $a \not R b$, assume that aRb. Then:

$aRb \Rightarrow a \in R(b)$ (1)

and

R equivalence $\to R$ reflexive $\Rightarrow aRa$

$\Rightarrow a \in R(a) \qquad (2)$

From (1) and (2):

$a \in R(a) \wedge a \in R(b) \Rightarrow a \in R(a) \cap R(b)$

$\Rightarrow R(a) \cap R(b) \neq \emptyset \leftarrow$ Contradiction

because by hypothesis: $R(a) \cap R(b) = \emptyset$.

It follows that $\underline{a \not R b}$.

$\underline{(\Leftarrow)}$: Assume that $\underline{a \not R b}$. To show that $R(a) \cap R(b) = \emptyset$, assume that $R(a) \cap R(b) \neq \emptyset$. We may therefore choose some $x \in R(a) \cap R(b)$. Then:

$$x \in R(a) \cap R(b) \Rightarrow \begin{cases} x \in R(a) \\ x \in R(b) \end{cases} \Rightarrow \begin{cases} xRa \\ xRb \end{cases} \Rightarrow \begin{cases} aRx \\ xRb \end{cases}$$

$\Rightarrow aRb \longleftarrow$ Contradiction,

because by hypothesis $a \not R b$.

It follows that $R(a) \cap R(b) = \emptyset$.

From the above argument it follows that

$\forall a, b \in A : (R(a) \cap R(b) = \emptyset \Leftrightarrow a \not R b)$.

EXAMPLE

We have previously shown that the relation $R \in \mathrm{Rel}(\mathbb{Z})$ defined as:

$$xRy \Leftrightarrow 11x - 5y \text{ even}$$

is an equivalence. Find the equivalence classes of R.

For this type of problem it is useful to know and use the following previously proven statements:

$$\boxed{\begin{array}{l} \forall a, b \in \mathbb{Z}: \ ab \text{ even} \Leftrightarrow (a \text{ even} \lor b \text{ even}) \\ \forall a, b \in \mathbb{Z}: \ ab \text{ odd} \Leftrightarrow (a \text{ odd} \land b \text{ odd}) \end{array}}$$

Solution

Try $R(0) = \{x \in \mathbb{Z} \mid xR0\}$.

$$\begin{aligned} x \in R(0) &\Leftrightarrow xR0 \Leftrightarrow 11x - 5 \cdot 0 \text{ even} \Leftrightarrow 11x \text{ even} \\ &\Leftrightarrow 11 \text{ even} \lor x \text{ even} \\ &\Leftrightarrow x \text{ even} \end{aligned}$$

and therefore $R(0) = \{x \in \mathbb{Z} \mid x \text{ even}\}$.

Try $R(1) = \{x \in \mathbb{Z} \mid xR1\}$. Let $x \in \mathbb{Z}$ be given.

$$\begin{aligned} x \in R(1) &\Leftrightarrow xR1 \Leftrightarrow 11x - 5 \cdot 1 \text{ even} \Leftrightarrow \\ &\Leftrightarrow \exists k \in \mathbb{Z}: 11x - 5 = 2k \\ &\Leftrightarrow \exists k \in \mathbb{Z}: 11x = 2k + 5 = 2k + 4 + 1 = 2(k+2) + 1 \\ &\Leftrightarrow \exists \lambda \in \mathbb{Z}: 11x = 2\lambda + 1 \quad (\text{for } \lambda = k + 2) \\ &\Leftrightarrow 11x \text{ odd} \Leftrightarrow 11 \text{ odd} \land x \text{ odd} \Leftrightarrow x \text{ odd} \end{aligned}$$

and therefore

$R(1) = \{x \in \mathbb{Z} \mid x \text{ odd}\}$.

Since $R(0) \cup R(1) = \mathbb{Z}$, it follows that we have all equivalence classes and therefore

$A/R = \{R(0), R(1)\}$

EXERCISE

(12) The following relations were previously shown to be equivalences. Find the corresponding equivalence classes.

a) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow a+b$ even

b) $R \in Rel(\mathbb{N}^*)$ with $aRb \Leftrightarrow a^2+b^2$ even

c) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow 3a-7b$ even

d) $R \in Rel(\mathbb{Z})$ with $aRb \Leftrightarrow 3 \mid a+2b$

Methodology for writing proofs

Proving implications

(1) To prove $\boxed{p \Rightarrow q}$

- **Direct Method**

  Assume p is true.
  [Prove q]

- **Contrapositive Method**

  We will show that $\bar{q} \Rightarrow \bar{p}$
  Assume $\bar{q}$ is true.
  [Prove $\bar{p}$]
  It follows that $p \Rightarrow q$

- **Contradiction Method**

  Assume p is true.
  To derive a contradiction, assume $\bar{q}$.
  [Prove r, using $p \wedge \bar{q}$]
  [Prove $\bar{r}$] ← Contradiction.
  It follows that q is true.

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

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

Proofs involving sets

Let A, B be two sets.

1. To prove $\boxed{A \subseteq B}$

[We prove $x \in A \Rightarrow x \in B$]

2. To prove $\boxed{A = B}$

[We prove $x \in A \Rightarrow x \in B$]
It follows that $A \subseteq B$ (1)
[We prove $x \in B \Rightarrow x \in A$]
It follows that $B \subseteq A$ (2)
From (1) and (2): $A = B$.

- For proofs involving sets, we recall that

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

Proofs involving identities

Let a, b be two expressions.
To prove $a = b$.

▸ Direct Method

$$a = \cdots = \cdots = \\ = \cdots = \cdots = b$$

▸ Indirect Method

$a = \cdots = \cdots = c$ (1)
$b = \cdots = \cdots = c$ (2)
From (1) and (2): $a = b$.

Proofs involving quantified statements

(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 an $x \in A$]
[Prove that $p(x)$ is true]
It follows that $\exists x \in A : p(x)$

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

▷ <u>2nd method</u>

$p(x) \Leftrightarrow \cdots \Leftrightarrow \cdots \Leftarrow x \in S$

Choose an $x \in S$. Show that $x \in A \wedge p(x)$.

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

IMP4: Mappings and Functions

MAPPINGS AND FUNCTIONS

▼ Basic Definitions

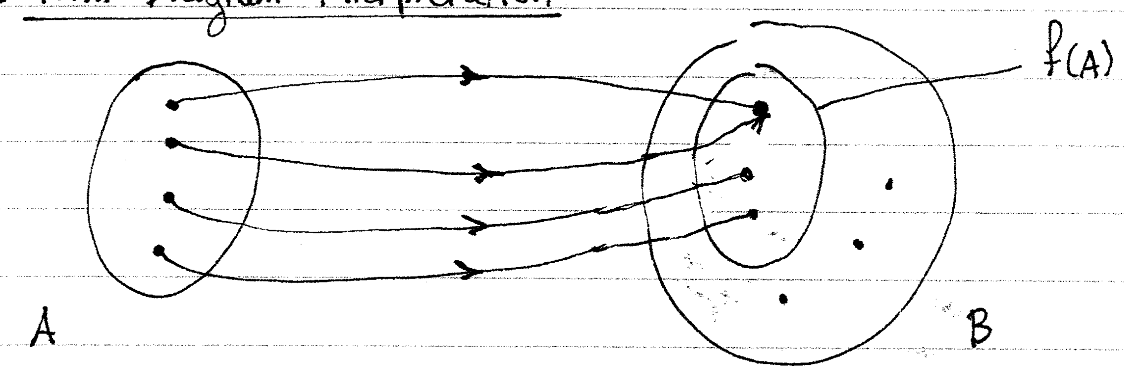
• Let A, B be two arbitrary sets. We say that f is a mapping that maps A to B (notation: $f: A \to B$) if and only if the following conditions are satisfied:

a) f is a relation $f \in \mathrm{Rel}(A, B)$

b) $\forall x \in A : \exists y \in B : (x, y) \in f$

c) $\forall (x_1, y_1), (x_2, y_2) \in f : (x_1 = x_2 \Rightarrow y_1 = y_2)$

▶ Venn Diagram interpretation



Conditions (b) and (c) above have the following interpretations:

b) All elements of A have an outgoing arrow to some element of B

c) No element of A can have more than one outgoing arrow

Note that there are no restrictions on where the arrows go to as long as they go to some element of B.

▶ Special cases

- We denote the set of all mappings $f: A \to B$ as
$\mathrm{Map}(A,B) = \{f \in \mathrm{Rel}(A,B) \mid f: A \to B\}$
- For $A \subseteq \mathbb{R}$ we define the set of all functions with domain A:
  $F(A) = \mathrm{Map}(A, \mathbb{R})$.
- Also relevant are the following definitions
  $F(\mathbb{N})$ = the set of all real-valued sequences
  $\mathrm{Map}(\mathbb{R}^n, \mathbb{R})$ = the set of all scalar fields
  $\mathrm{Map}(\mathbb{R}^n, \mathbb{R}^n)$ = the set of all vector fields

▶ $f(x)$ notation

For every element $x \in A$, there is a unique $y \in B$ such that $(x,y) \in f$. We denote this unique y as $y = f(x)$.

EXAMPLE

For $f = \{(1,7),(2,5),(3,7)\}$, it follows that
$f(1) = 7$
$f(2) = 5$
$f(3) = 7$.

▶ $f(S)$ notation

Let $f: A \to B$ and let $S \subseteq A$. We define the image $f(S)$ of S as follows:

$$f(S) = \{f(x) \mid x \in S\}$$

The belonging condition of $f(S)$ is given by

$$y \in f(S) \Leftrightarrow \exists x \in S : y = f(x)$$

We now prove the following lemma:

<u>Lemma:</u> $\boxed{(f : A \to B \wedge S \subseteq A) \Rightarrow B \cap f(S) = f(S)}$

<u>Proof</u>

We note that

$\underline{y \in B \cap f(S)} \Rightarrow y \in B \wedge y \in f(S) \Rightarrow \underline{y \in f(S)}$

and therefore $\quad B \cap f(S) \subseteq f(S). \qquad (1)$

Conversely, let $\underline{y \in f(S)} \Rightarrow \exists x \in S : y = f(x)$

Since $y = f(x) \Rightarrow (x, y) \in f \quad$ [by definition]

$\Rightarrow (x, y) \in A \times B \quad$ [because $f \subseteq A \times B$]

$\Rightarrow x \in A \wedge y \in B \quad$ [definition]

$\Rightarrow y \in B \Rightarrow \underline{y \in B \cap f(S)}$

and therefore $\quad f(S) \subseteq B \cap f(S) \qquad (2)$

From (1) and (2): $f(S) = B \cap f(S)$. $\square$

▶ <u>Domain and range of f</u>

Let $f : A \to B$ be given. Since f is also a relation, recall that we have previously defined the <u>domain</u> and <u>range</u> of f as:

$$\mathrm{dom}(f) = \{x \in A \mid \exists y \in B : (x,y) \in f\}$$
$$\mathrm{ran}(f) = \{y \in B \mid \exists x \in A : (x,y) \in f\}$$

We will now show that:

<u>Proposition</u> : $\boxed{f : A \to B \Rightarrow (\mathrm{dom}(f) = A \wedge \mathrm{ran}(f) = f(A))}$

<u>Proof</u>

We assume that $f : A \to B$.

(a) By definition:

$\mathrm{dom}(f) = \{x \in A \mid \exists y \in B : (x,y) \in f\} \Rightarrow \mathrm{dom}(f) \subseteq A$ (1)

Sufficient to show $A \subseteq \mathrm{dom}(f)$.

Assume that $x \in A$. Since $f : A \to B \Rightarrow \exists y \in B : (x,y) \in f$.
it follows that

$x \in A \wedge (\exists y \in B : (x,y) \in f) \Rightarrow$
$\Rightarrow x \in \mathrm{dom}(f)$

and therefore $A \subseteq \mathrm{dom}(f)$ (2)

From (1) and (2): $\underline{A = \mathrm{dom}(f)}$.

(b) To show $\mathrm{ran}(f) = f(A)$, we note that

$$\begin{aligned} y \in \mathrm{ran}(f) &\Leftrightarrow y \in \{z \in B \mid \exists x \in A : (x,z) \in f\} \\ &\Leftrightarrow y \in B \wedge (\exists x \in A : (x,y) \in f) \\ &\Leftrightarrow y \in B \wedge (\exists x \in A : y = f(x)) \\ &\Leftrightarrow y \in B \wedge y \in f(A) \\ &\Leftrightarrow y \in B \cap f(A). \end{aligned}$$

It follows that $\mathrm{ran}(f) = B \cap f(A) = f(A)$, using the previous lemma in the last step.

EXAMPLES

a) Let $f: A \to B$ be given and let $S \subseteq A$ and $T \subseteq A$.
Show that $f(S \cup T) = f(S) \cup f(T)$.

Solution

($\Rightarrow$): Let $y \in f(S \cup T)$ be given. Then

$y \in f(S \cup T) \Rightarrow \exists x \in S \cup T : f(x) = y$.

Choose $x_0 \in S \cup T$ such that $f(x_0) = y$.

Since $x_0 \in S \cup T \Rightarrow x_0 \in S \vee x_0 \in T$, we distinguish between the following cases:

Case 1 : Assume that $x_0 \in S$. Then

$$\begin{cases} x_0 \in S \\ f(x_0) = y \end{cases} \Rightarrow \exists x \in S : y = f(x) \Rightarrow y \in f(S)$$

$$\Rightarrow y \in f(S) \vee y \in f(T) \Rightarrow y \in f(S) \cup f(T).$$

Case 2 : Assume that $x_0 \in T$. Then

$$\begin{cases} x_0 \in T \\ f(x_0) = y \end{cases} \Rightarrow \exists x \in T : y = f(x) \Rightarrow y \in f(T)$$

$$\Rightarrow y \in f(S) \vee y \in f(T) \Rightarrow y \in f(S) \cup f(T).$$

In both cases we find $y \in f(S) \cup f(T)$ and therefore

$\forall y \in f(S \cup T) : y \in f(S) \cup f(T)$. (1)

($\Leftarrow$) : Let $y \in f(S) \cup f(T)$ be given. Then:

$y \in f(S) \cup f(T) \Rightarrow y \in f(S) \vee y \in f(T) \Rightarrow$

$$\Rightarrow (\exists x \in S : y = f(x)) \vee (\exists x \in T : y = f(x))$$

We distinguish between the following two cases:

<u>Case 1</u>: Assume that $\exists x \in S : y = f(x)$.

Choose $x_0 \in S$ such that $y = f(x_0)$. Then:

$$\begin{cases} x_0 \in S \\ y = f(x_0) \end{cases} \Rightarrow \begin{cases} x_0 \in S \vee x_0 \in T \\ y = f(x_0) \end{cases} \Rightarrow \begin{cases} x_0 \in S \cup T \\ y = f(x_0) \end{cases} \Rightarrow$$

$$\Rightarrow \exists x \in S \cup T : y = f(x)$$

$$\Rightarrow y \in f(S \cup T).$$

<u>Case 2</u>: Assume that $\exists x \in T : y = f(x)$.

Choose $x_0 \in T$ such that $y = f(x_0)$. Then:

$$\begin{cases} x_0 \in T \\ y = f(x_0) \end{cases} \Rightarrow \begin{cases} x_0 \in S \vee x_0 \in T \\ y = f(x_0) \end{cases} \Rightarrow \begin{cases} x_0 \in S \cup T \\ y = f(x_0) \end{cases} \Rightarrow$$

$$\Rightarrow \exists x \in S \cup T : y = f(x)$$

$$\Rightarrow y \in f(S \cup T).$$

In both cases we find $y \in f(S \cup T)$ and therefore

$$\forall y \in f(S) \cup f(T) : y \in f(S \cup T). \quad (2)$$

From Eq.(1) and Eq.(2):

$$\begin{cases} \forall y \in f(S \cup T) : y \in f(S) \cup f(T) \\ \forall y \in f(S) \cup f(T) : y \in f(S \cup T) \end{cases} \Rightarrow \begin{cases} f(S \cup T) \subseteq f(S) \cup f(T) \\ f(S) \cup f(T) \subseteq f(S \cup T) \end{cases}$$

$$\Rightarrow f(S \cup T) = f(S) \cup f(T).$$

b) Let $f: A \to B$ be given. Use a counterexample to explain why we cannot prove that for $S \subseteq A$ and $T \subseteq A$ we have $f(S \cap T) = f(S) \cap f(T)$.

<u>Solution</u>

Consider the mapping

$f = \{(a,x),(b,x),(c,y),(d,y)\}$

and define $S = \{b,c\}$ and $T = \{a,d\}$.

Then:

$$f(S \cap T) = f(\{b,c\} \cap \{a,d\}) = f(\emptyset) = \emptyset \qquad (1)$$

but

$f(b) = x \wedge f(c) = y \Rightarrow f(S) = f(\{b,c\}) = \{x,y\}$

$f(a) = x \wedge f(d) = y \Rightarrow f(T) = f(\{a,d\}) = \{x,y\}$

and therefore

$$f(S) \cap f(T) = \{x,y\} \cap \{x,y\} = \{x,y\} \qquad (2)$$

From Eq. (1) and Eq. (2):

$f(S \cap T) \neq f(S) \cap f(T)$

$\hookrightarrow$ Proof by counterexample can be very challenging. The statement $f(S \cap T) = f(S) \cap f(T)$ can be true for some choices of S, T and false for other choices of S, T. Can you find alternate choices for S, T for which the statement is true?

EXERCISES

① Let $f: A \to B$ be given, and let $S \subseteq A$ and $T \subseteq A$. Show that

a) $f(S \cap T) \subseteq f(S) \cap f(T)$

b) $f(S) - f(T) \subseteq f(S - T)$

② Find a counterexample of an $f: A \to B$ and $S \subseteq A$ and $T \subseteq A$ such that the following statements are false:

a) $f(S \cap T) = f(S) \cap f(T)$

b) $f(S) - f(T) = f(S - T)$

$\hookrightarrow$ We will later show that these statements can be proved if additional assumptions about f are introduced.

③ Let $f: A \to B$ be given and let S_a such that $\forall a \in I: S_a \subseteq A$ with I an index set. Show that

a) $f\left(\bigcup_{a \in I} S_a\right) = \bigcup_{a \in I} f(S_a)$

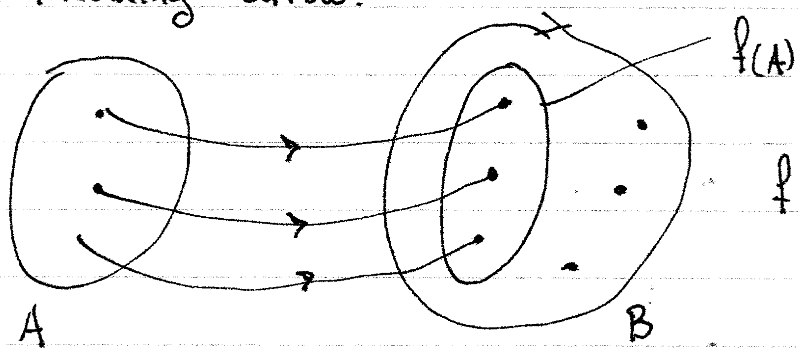
b) $f\left(\bigcap_{a \in I} S_a\right) \subseteq \bigcap_{a \in I} f(S_a)$

One-to-one mappings/functions

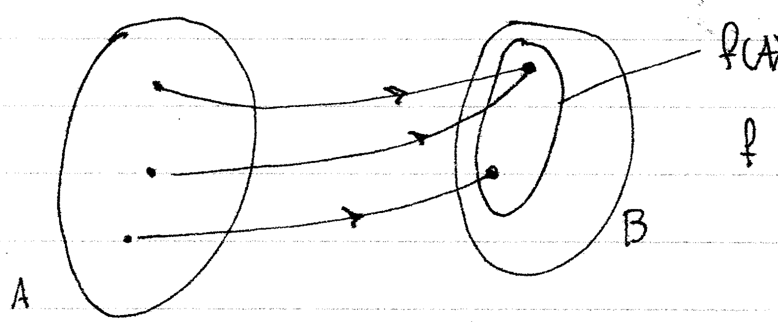
- Let $f: A \to B$ be given. We say that

$$\boxed{f \text{ one-to-one} \Leftrightarrow \forall x_1, x_2 \in A: (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)}$$

▶ Venn diagram interpretation: In a one-to-one mapping, every point in the range $f(A)$ receives only one incoming arrow.



f is one-to-one.



f is NOT one-to-one.

▶ Negated definition

Since $\overline{p \Rightarrow q} \equiv p \wedge \overline{q}$, the negation of the above definition reads:

$$\boxed{f \text{ NOT one-to-one} \Leftrightarrow \exists x_1, x_2 \in A: (f(x_1) = f(x_2) \wedge x_1 \neq x_2)}$$

▸ Methodology

To derive statements of the form $A=B \Rightarrow C=D$ we use the following properties of real numbers

1) We can add / cancel any number to both sides of an equation:
$$\forall a,x,y \in \mathbb{R} : (x=y \Leftrightarrow a+x=a+y)$$
2) We can always add or multiply two equations
$$\forall a,b,x,y \in \mathbb{R} : (a=b \wedge x=y \Rightarrow a+x=b+y)$$
$$\forall a,b,x,y \in \mathbb{R} : (a=b \wedge x=y \Rightarrow ax=by)$$
3) We can multiply any number to both sides of an equation:
$$\forall a,x,y \in \mathbb{R} : (x=y \Rightarrow ax=ay)$$
However the converse does not work for $a=0$. With the restriction $a \neq 0$ we have:
$$\forall x,y \in \mathbb{R} : \forall a \in \mathbb{R}-\{0\} : (x=y \Leftrightarrow ax=ay)$$
4) We can raise both sides of an equation to any integer power:
$$\forall x,y \in \mathbb{R} : \forall n \in \mathbb{N} : (x=y \Rightarrow x^n=y^n)$$
In general, the converse does not work. However, if we require $n \neq 0$ and distinguish between odd and even powers, we have:
$$\forall x,y \in \mathbb{R} : \forall n \in \mathbb{Z} : (x^{2n+1}=y^{2n+1} \Leftrightarrow x=y)$$
$$\forall x,y \in \mathbb{R} : \forall n \in \mathbb{Z}-\{0\} : (x^{2n}=y^{2n} \Leftrightarrow x=y \vee x=-y)$$
5) Factored equation:
$$\forall a,b \in \mathbb{R} : (ab=0 \Leftrightarrow a=0 \vee b=0)$$

EXAMPLES

a) Consider the function

$$\forall x \in \mathbb{R} - \{a\} : f(x) = \frac{x}{x-a}$$

Show that $a \neq 0 \Rightarrow f$ one-to-one.

Solution

Assume that $a \neq 0$. Let $x_1, x_2 \in \mathbb{R} - \{a\}$ be given such that $f(x_1) = f(x_2)$. Then

$$\underline{f(x_1) = f(x_2)} \Rightarrow \frac{x_1}{x_1 - a} = \frac{x_2}{x_2 - a} \Rightarrow$$

$$\Rightarrow (x_1 - a)(x_2 - a) \frac{x_1}{x_1 - a} = (x_1 - a)(x_2 - a) \frac{x_2}{x_2 - a} \Rightarrow$$

$$\Rightarrow x_1(x_2 - a) = x_2(x_1 - a) \Rightarrow x_1 x_2 - a x_1 = x_1 x_2 - a x_2$$

$$\left.\begin{array}{l} \Rightarrow -a x_1 = -a x_2 \\ \quad a \neq 0 \end{array}\right\} \Rightarrow \underline{x_1 = x_2}$$

It follows that

$\forall x_1, x_2 \in \mathbb{R} - \{a\} : (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$

$\Rightarrow f$ one-to-one.

↳ Note that to cancel $-a$ in $-a x_1 = -a x_2$ we need the assumption $a \neq 0$, otherwise the cancellation cannot be justified.

b) Consider the function $f(x) = 2x^2 + 6x - 7,\ \forall x \in \mathbb{R}$

Show that f is not one-to-one.

Solution

Solve $f(x) = -7 \Leftrightarrow 2x^2 + 6x - 7 = -7 \Leftrightarrow 2x^2 + 6x = 0 \Leftrightarrow$

$\Leftrightarrow 2x(x+3) = 0 \Leftrightarrow 2x = 0 \vee x+3 = 0$

$\Leftrightarrow x = 0 \vee x = -3$

It follows that

$f(0) = f(-3) = -7 \wedge 0 \neq -3 \Rightarrow$

$\Rightarrow \exists x_1, x_2 \in \mathbb{R} : f(x_1) = f(x_2) \wedge x_1 \neq x_2$

$\Rightarrow f$ not one-to-one.

c) Let $f: A \to B$ be given and let $S \subseteq A$ and $T \subseteq A$.

Show that

f one-to-one $\Rightarrow f(S \cap T) = f(S) \cap f(T)$.

Solution

Assume that f is one-to-one.

($\Rightarrow$): Let $y \in f(S \cap T)$ be given. Then,

$y \in f(S \cap T) \Rightarrow \exists x \in S \cap T : f(x) = y$

Choose $x_0 \in S \cap T$ such that $f(x_0) = y$. It follows that

$$\begin{cases} x_0 \in S \cap T \\ f(x_0) = y \end{cases} \Rightarrow \begin{cases} x_0 \in S \wedge x_0 \in T \\ f(x_0) = y \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} x_0 \in S \\ f(x_0) = y \end{cases} \wedge \begin{cases} x_0 \in T \\ f(x_0) = y \end{cases} \Rightarrow$$

$$\Rightarrow (\exists x \in S : f(x) = y) \wedge (\exists x \in T : f(x) = y)$$

$$\Rightarrow y \in f(S) \wedge y \in f(T) \Rightarrow$$

$$\Rightarrow y \in f(S) \cap f(T).$$

($\Leftarrow$): Let $y \in f(S) \cap f(T)$ be given. Then:

$$y \in f(S) \cap f(T) \Rightarrow y \in f(S) \wedge y \in f(T) \Rightarrow$$

$$\Rightarrow \begin{cases} \exists x \in S : f(x) = y \\ \exists x \in T : f(x) = y. \end{cases}$$

Choose $x_1 \in S$ and $x_2 \in T$ such that $f(x_1) = y$ and $f(x_2) = y$.

Then:

$$\begin{cases} f(x_1) = y = f(x_2) \\ f \text{ one-to-one} \end{cases} \Rightarrow x_1 = x_2 \in T \Rightarrow x_1 \in T.$$

and therefore:

$$\begin{cases} x_1 \in S \wedge x_1 \in T \\ f(x_1) = y \end{cases} \Rightarrow \begin{cases} x_1 \in S \cap T \\ f(x_1) = y \end{cases} \Rightarrow$$

$$\Rightarrow \exists x \in S \cap T : f(x) = y$$

$$\Rightarrow \underline{y \in f(S \cap T)}$$

From the above argument we have:

$$\begin{cases} \forall\, y \in f(S \cap T) : y \in f(S) \cap f(T) \\ \forall\, y \in f(S) \cap f(T) : y \in f(S \cap T) \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} f(S \cap T) \subseteq f(S) \cap f(T) \\ f(S) \cap f(T) \subseteq f(S \cap T) \end{cases} \Rightarrow$$

$$\Rightarrow f(S \cap T) = f(S) \cap f(T).$$

EXERCISES

(4) Show that the following functions are one-to-one

a) $\forall x \in \mathbb{R}: f(x) = 3x^5 + 2$

b) $\forall x \in (0, +\infty): f(x) = 2x^2 + 5$

c) $\forall x \in \mathbb{R}: f(x) = ax + b$ with $a, b \in \mathbb{R} \wedge a \neq 0$

d) $\forall x \in \mathbb{R}: f(x) = (2x^3 + 1)^5$

e) $\forall x \in \mathbb{R} - \{0\}: f(x) = a/x$ with $a \in \mathbb{R} \wedge a \neq 0$

f) $\forall x \in \mathbb{R} - \{-d/c\}: f(x) = \dfrac{ax+b}{cx+d}$ with $a, b, c, d \in \mathbb{R} \wedge ad - bc \neq 0$

(5) Show that for $\forall x \in \mathbb{R}: f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{R}$ and $a \neq 0$ is <u>not</u> one-to-one.

(6) Let $f: A \to B$ be given and let $S \subseteq A$ and $T \subseteq A$. Show that

f one-to-one $\Rightarrow f(S - T) = f(S) - f(T)$.

(7) Let $f: A \to B$ be given and let S_a be a set collection such that $\forall a \in I: S_a \subseteq A$, with I an index set. Show that

f one-to-one $\Rightarrow f\left(\bigcap_{a \in I} S_a\right) = \bigcap_{a \in I} f(S_a)$

Functions and Monotonicity

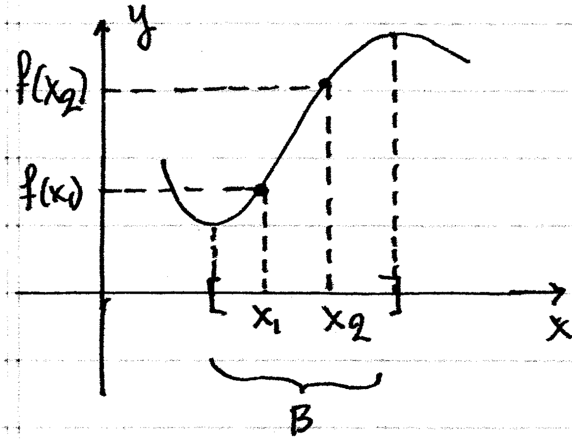
Let f be a function with $f: A \to \mathbb{R}$ and let $B \subseteq A$. We make the following definitions:

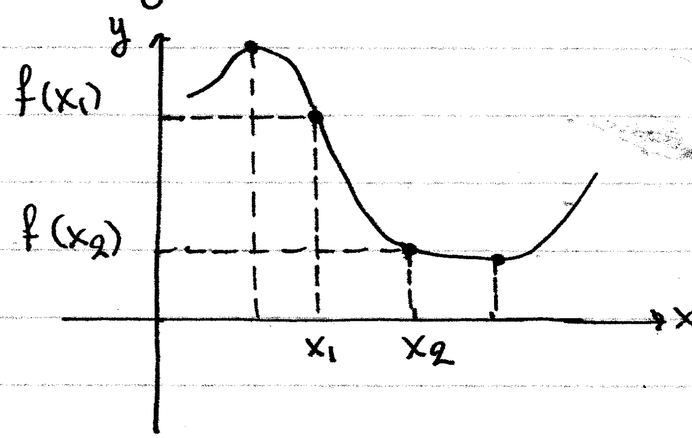
$$\boxed{\begin{array}{l} f \nearrow B \Leftrightarrow \forall x_1, x_2 \in B : (x_1 < x_2 \Rightarrow f(x_1) < f(x_2)) \\ f \searrow B \Leftrightarrow \forall x_1, x_2 \in B : (x_1 < x_2 \Rightarrow f(x_1) > f(x_2)) \end{array}}$$

We read:

$f \nearrow B$: f is strictly increasing in B

$f \searrow B$: f is strictly decreasing in B.





Monotonicity can be determined directly from the definition with 2 methods:

1) Analytic Method
2) Synthetic Method.

In Calculus, monotonicity can also be determined using Differential Calculus.

Analytic Method

To show $f \nearrow B$ or $f \searrow B$.

- •1 Let $x_1, x_2 \in B$ be given with $x_1 < x_2$.
- •2 Calculate and <u>factor</u> $\Delta f(x_1, x_2) = f(x_2) - f(x_1)$
- •3 Determine the sign of each factor of Δf and then conclude whether $\Delta f > 0$ or $\Delta f < 0$.
- •4 Finish the argument.

EXAMPLES

a) Show that $f(x) = 3x+5$ is strictly increasing in $\mathbb{R}$.

<u>Solution</u>

$\mathrm{dom}(f) = \mathbb{R}$.

Let $x_1, x_2 \in \mathbb{R}$ be given with $x_1 < x_2$.

$$\Delta f(x_1, x_2) = f(x_2) - f(x_1) = (3x_2+5) - (3x_1+5) =$$
$$= 3(x_2 - x_1)$$

Since $x_1 < x_2 \Rightarrow x_2 - x_1 > 0 \Rightarrow$

$$\Rightarrow 3(x_2 - x_1) > 0 \Rightarrow$$
$$\Rightarrow f(x_2) - f(x_1) > 0 \Rightarrow$$
$$\Rightarrow \underline{f(x_1) < f(x_2)}$$

- Thus: $\forall x_1, x_2 \in \mathbb{R} : (x_1 < x_2 \Rightarrow f(x_1) < f(x_2)) \Rightarrow f \nearrow \mathbb{R}$.

b) Show that $f(x) = \dfrac{2x}{x-1}$ is strictly decreasing in $(1, +\infty)$.

Solution

Let $x_1, x_2 \in (1, +\infty)$ be given with $x_1 < x_2$.
Then:

$$\Delta f(x_1, x_2) = f(x_2) - f(x_1) = \frac{2x_2}{x_2 - 1} - \frac{2x_1}{x_1 - 1} =$$

$$= \frac{2x_2(x_1 - 1) - 2x_1(x_2 - 1)}{(x_1 - 1)(x_2 - 1)} =$$

$$= \frac{2x_1x_2 - 2x_2 - 2x_1x_2 + 2x_1}{(x_1 - 1)(x_2 - 1)} =$$

$$= \frac{-2x_2 + 2x_1}{(x_1 - 1)(x_2 - 1)} = \frac{2(x_1 - x_2)}{(x_1 - 1)(x_2 - 1)}$$

Since $x_1 < x_2 \Rightarrow x_1 - x_2 < 0$.

$x_1 \in (1, +\infty) \Rightarrow x_1 > 1 \Rightarrow x_1 - 1 > 0$

$x_2 \in (1, +\infty) \Rightarrow x_2 > 1 \Rightarrow x_2 - 1 > 0$

therefore $\Delta f(x_1, x_2) < 0 \Rightarrow f(x_2) - f(x_1) < 0 \Rightarrow$

$\Rightarrow \underline{f(x_1) > f(x_2)}$

Thus:

$\forall x_1, x_2 \in (1, +\infty) : (x_1 < x_2 \Rightarrow f(x_1) > f(x_2)) \Rightarrow$

$\Rightarrow f \searrow (1, +\infty)$.

c) Show that $f(x) = x^2 + 5x + 6$ is strictly increasing in $(-5/2, +\infty)$.

Solution

Let $\underline{x_1, x_2 \in (-5/2, +\infty)}$ be given with $\underline{x_1 < x_2}$

Then

$$\Delta f(x_1, x_2) = f(x_2) - f(x_1) = (x_2^2 + 5x_2 + 6) - (x_1^2 + 5x_1 + 6)$$
$$= (x_2^2 - x_1^2) + 5(x_2 - x_1) =$$
$$= (x_2 - x_1)(x_2 + x_1) + 5(x_2 - x_1) =$$
$$= (x_2 - x_1)(x_2 + x_1 + 5)$$

Since $x_1 < x_2 \Rightarrow x_2 - x_1 > 0 \quad (1)$

$$\left.\begin{array}{l} x_1 \in (-5/2, +\infty) \Rightarrow x_1 > -5/2 \\ x_2 \in (-5/2, +\infty) \Rightarrow x_2 > -5/2 \end{array}\right\} \Rightarrow$$

$\Rightarrow x_1 + x_2 > -5/2 - 5/2 = -5 \Rightarrow x_1 + x_2 + 5 > 0 \quad (2)$

From (1) and (2):

$\Delta f(x_1, x_2) > 0 \Rightarrow f(x_2) - f(x_1) > 0 \Rightarrow \underline{f(x_1) < f(x_2)}$

It follows that:

$\forall x_1, x_2 \in (-5/2, +\infty): (x_1 < x_2 \Rightarrow f(x_1) < f(x_2)) \Rightarrow$

$\Rightarrow f \uparrow (-5/2, +\infty)$.

↳ For quadratics $f(x) = ax^2 + bx + c$, monotonicity changes at the axis of symmetry at $x = -b/2a$.

↳ In addition to the usual properties, it is good to know the following additional properties:

1) We can add two inequalities if they have the same direction:

$$\left.\begin{array}{l} a > b \\ x > y \end{array}\right\} \Rightarrow a + x > b + y$$

2) We can multiply two inequalities if they have the same direction AND all sides are POSITIVE!

$$\left.\begin{array}{l} a > b > 0 \\ x > y > 0 \end{array}\right\} \Rightarrow ax > by$$

3) We can raise an inequality to a positive power if both sides of the inequality are positive

$$\left.\begin{array}{l} a > b > 0 \\ p > 0 \end{array}\right\} \Rightarrow a^p > b^p > 0$$

e.g. $a > b > 0 \Rightarrow \sqrt{a} > \sqrt{b} > 0$ for $p = 1/2$.

4) We can raise an inequality to a negative power if both sides of the inequality are positive but then the direction of the inequality is reversed.

$$\left.\begin{array}{l} a > b > 0 \\ n < 0 \end{array}\right\} \Rightarrow 0 < a^n < b^n$$

e.g. $a > b > 0 \Rightarrow 0 < \frac{1}{a} < \frac{1}{b}$ for $n = -1$.

We rely on these properties heavily for the synthetic method. We also need the following previously mentioned properties:

5) $x < y \Rightarrow x + a < y + a$

6) $\left.\begin{array}{l} x < y \\ p > 0 \end{array}\right\} \Rightarrow px < py$ 7) $\left.\begin{array}{l} x < y \\ n < 0 \end{array}\right\} \Rightarrow nx > ny$.

to add/multiply a constant to both sides of an inequality.

Synthetic Method

To show that $f \nearrow B$ or $f \searrow B$:

- 1 Let $x_1, x_2 \in B$ be given with $x_1 < x_2$.
- 2 Use a sequence of deductions to show that

  $x_1 < x_2 \Rightarrow \dots \Rightarrow \dots \Rightarrow f(x_1) < f(x_2)$

  or

  $x_1 < x_2 \Rightarrow \dots \Rightarrow \dots \Rightarrow f(x_1) > f(x_2)$

  using the above properties of inequalities.
- 3 Wrap up the argument.

EXAMPLES

a) For $f(x) = 3-(1-2x)^2$ show that $f \searrow (1/2, +\infty)$

Solution

Let $x_1, x_2 \in (1/2, +\infty)$ be given with $x_1 < x_2$. Then:

$x_1 < x_2 \Rightarrow -2x_1 > -2x_2 \Rightarrow 1-2x_1 > 1-2x_2 \overset{*}{\Rightarrow}$

$\Rightarrow \underbrace{0 <}_{(!)} 2x_1 - 1 < 2x_2 - 1$ [because $x_1 > 1/2 \wedge x_2 > 1/2$]

$\Rightarrow (2x_1-1)^2 < (2x_2-1)^2 \overset{**}{\Rightarrow} (1-2x_1)^2 < (1-2x_2)^2$

$\Rightarrow -(1-2x_1) > -(1-2x_2)^2 \Rightarrow 3-(1-2x_1)^2 > 3-(1-2x_2)^2$

$\Rightarrow f(x_1) > f(x_2)$.

Thus: $\forall x_1, x_2 \in (1/2, +\infty): (x_1 < x_2 \Rightarrow f(x_1) > f(x_2))$

$\Rightarrow f \searrow (1/2, +\infty)$.

* We multiply inequality with -1 to ensure that both sides are positive before going ahead and squaring it.

** Here we use $x^2 = (-x)^2$.

↳ In the above solution you should be able to identify which inequality property is used at every step.

b) For $f(x) = 3x + 1 + \sqrt{1 - x^2}$, show that $f \nearrow (-1, 0)$

<u>Solution</u>

Let $x_1, x_2 \in (-1, 0)$ be given such that $x_1 < x_2$. Then

$x_1 < x_2 \Rightarrow 3x_1 < 3x_2 \Rightarrow 3x_1 + 1 < 3x_2 + 1 \qquad (1)$

Also note that

$$x_1 < x_2 \Rightarrow -x_1 > -x_2 > 0 \Rightarrow (-x_1)^2 > (-x_2)^2 \Rightarrow x_1^2 > x_2^2$$
$$\Rightarrow -x_1^2 < -x_2^2 \Rightarrow 1 - x_1^2 < 1 - x_2^2 \qquad (2)$$

and

$$x_1 \in (-1, 0) \Rightarrow -1 < x_1 < 0 \Rightarrow 1 > -x_1 > 0 \Rightarrow 1 > (-x_1)^2 \Rightarrow$$
$$\Rightarrow 1 > x_1^2 \Rightarrow 1 - x_1^2 > 0 \qquad (3)$$

and similarly

$$x_2 \in (-1, 0) \Rightarrow \cdots \Rightarrow 1 - x_2^2 > 0. \qquad (4)$$

From (2), (3), (4), it follows that

$$0 < 1 - x_1^2 < 1 - x_2^2 \Rightarrow \sqrt{1 - x_1^2} < \sqrt{1 - x_2^2} \qquad (5)$$

From (1) and (5), adding the inequalities:

$3x_1+1+\sqrt{1-x_1^2} < 3x_2+1+\sqrt{1-x_2^2} \Rightarrow$

$\Rightarrow \underline{f(x_1) < f(x_2)}$

Thus $\forall x_1, x_2 \in (-1,0): (x_1<x_2 \Rightarrow f(x_1)<f(x_2))$

$\Rightarrow f \nearrow (-1,0)$.

↳ Note that before we raise an inequality to any power we have to ensure/check that both sides of the inequality are positive. Thus in the above:

$x_1 < x_2 \Rightarrow x_1^2 < x_2^2$ is WRONG

since $x_1<0$ and $x_2<0$. Be careful!!

↳ Note that it was necessary to interrupt the main line of the argument:

$x_1<x_2 \Rightarrow \cdots \Rightarrow \sqrt{1-x_1^2} < \sqrt{1-x_2^2}$

to show that $1-x_1^2>0$ and $1-x_2^2>0$. Note the careful use of equation labels to interrupt and restart our main argument.

c) For $f(x) = \dfrac{1}{x^2-2}$, show that $f \nearrow (-\infty, -\sqrt{2})$

<u>Solution</u>

Let $\underline{x_1, x_2 \in (-\infty, -\sqrt{2})}$ be given with $\underline{x_1 < x_2}$.

Then

$$x_1 < x_2 \Rightarrow -x_1 > -x_2 > 0 \Rightarrow (-x_1)^2 > (-x_2)^2 \Rightarrow x_1^2 > x_2^2$$
$$\Rightarrow x_1^2 - 2 > x_2^2 - 2 \qquad (1)$$

Also note that

$$x_1 \in (-\infty, -\sqrt{2}) \Rightarrow x_1 < -\sqrt{2} \Rightarrow -x_1 > \sqrt{2} \Rightarrow (-x_1)^2 > 2 \Rightarrow$$
$$\Rightarrow x_1^2 > 2 \Rightarrow x_1^2 - 2 > 0. \qquad (2)$$

and similarly $x_2 \in (-\infty, -\sqrt{2}) \Rightarrow x_2^2 - 2 > 0$ (3).

From (1), (2), and (3):

$$x_1^2 - 2 > x_2^2 - 2 > 0 \Rightarrow \frac{1}{x_1^2 - 2} < \frac{1}{x_2^2 - 2} \Rightarrow \underline{f(x_1) < f(x_2)}$$

It follows that

$$\forall x_1, x_2 \in (-\infty, -\sqrt{2}) : (x_1 < x_2 \Rightarrow f(x_1) < f(x_2))$$
$$\Rightarrow f \nearrow (-\infty, -\sqrt{2}).$$

EXERCISES

(8) Use the analytic method to determine the monotonicity of the following functions

a) $f(x) = 3x+2$ on $\mathbb{R}$

b) $f(x) = 5-4x$ on $\mathbb{R}$

c) $f(x) = x^2-4x+5$ on $(-\infty, 2)$

d) $f(x) = \dfrac{3x+1}{x+2}$ on $(-2, +\infty)$

e) $f(x) = \dfrac{x+8}{3x+1}$ on $(-\infty, -1/3)$

f) $f(x) = (2x+5)^2-3$ on $(-\infty, -5/2)$

g) $f(x) = (x-1)(2x+1)$ on $(1, +\infty)$

(9) Use the synthetic method to determine the monotonicity of the following functions

a) $f(x) = 5x-3$ on $\mathbb{R}$

b) $f(x) = 2-7x$ on $\mathbb{R}$

c) $f(x) = (2x+3)^2+1$ on $(0, +\infty)$

d) $f(x) = (2-5x)^3-2$ on $(0, +\infty)$

e) $f(x) = \dfrac{-2}{2x^2+3}$ on $(0, +\infty)$

f) $f(x) = \sqrt{2x-1}$ on $(1, +\infty)$

g) $f(x) = 2-3\sqrt{4-x^2}$ on $(0, 2)$

h) $f(x) = -1 + 2\sqrt{9-(x+1)^2}$ on $(-4,-1)$

i) $f(x) = 3x+2+\sqrt{x+1}$ on $(0,+\infty)$

j) $f(x) = (2x-1)\sqrt{2x+1}$ on $(1,+\infty)$

(10) Let $f(x) = -1/x$, $\forall x \in (-\infty,0) \cup (0,+\infty)$

a) Show that $f \nearrow (-\infty,0)$ and $f \nearrow (0,+\infty)$.

b) Now, show that the statement $f \nearrow (-\infty,0) \cup (0,+\infty)$ is FALSE!

$\hookrightarrow$ This exercise provides a counterexample to the false conjecture

$f \nearrow A_1 \wedge f \nearrow A_2 \Rightarrow f \nearrow A_1 \cup A_2 \longleftarrow$ FALSE!!

(11) Consider the function

$$\forall x \in \mathbb{R} - \{-d/c\} : f(x) = \frac{ax+b}{cx+d}$$

and define $D = ad - bc$. Show that

a) $D > 0 \Rightarrow (f \nearrow (-\infty,-d/c) \wedge f \nearrow (d/c,+\infty))$

b) $D < 0 \Rightarrow (f \searrow (-\infty,-d/c) \wedge f \searrow (d/c,+\infty))$

(12) Let $f : A \to \mathbb{R}$ with $A \subseteq \mathbb{R}$ be a function. Show that

a) $f \nearrow A \Rightarrow f$ one-to-one

b) $f \searrow A \Rightarrow f$ one-to-one

(Hint: Use proof by contradiction).

Algebra and properties of mappings/functions

- To properly define a mapping or function f, we have to define both the domain $\mathrm{dom}(f)$ of f and the expression $f(x)$.

Equality and restriction of mappings

- Let f, g be two mappings. We say that

$$f = g \Leftrightarrow \begin{cases} \mathrm{dom}(f) = \mathrm{dom}(g) = A \\ \forall x \in A : f(x) = g(x) \end{cases}$$

- Let $f : A \to B$ be a mapping and let $S \subseteq A$. We define the restriction $f \upharpoonright S$ as follows:

$$\begin{cases} \mathrm{dom}(f \upharpoonright S) = S \\ \forall x \in S : (f \upharpoonright S)(x) = f(x) \end{cases}$$

Algebra of functions

- Let $f \in F(A)$ and $g \in F(B)$ be two real-valued functions and let $\lambda \in \mathbb{R}$. We define $f+g$, λf, fg as follows:

$$\begin{cases} \mathrm{dom}(f+g) = \mathrm{dom}(f) \cap \mathrm{dom}(g) = A \cap B \\ \forall x \in A \cap B : (f+g)(x) = f(x) + g(x) \end{cases}$$

$$\begin{cases} \mathrm{dom}(\lambda f) = \mathrm{dom}(f) = A \\ \forall x \in A : (\lambda f)(x) = \lambda f(x) \end{cases}$$

$$\begin{cases} \mathrm{dom}(fg) = \mathrm{dom}(f) \cap \mathrm{dom}(g) = A \cap B \\ \forall x \in A \cap B : (fg)(x) = f(x) g(x) \end{cases}$$

- Note that if the domain of f, g is not given, then by default we assume the widest possible subset of $\mathbb{R}$ for which $f(x)$ can be evaluated.

▶ odd and even functions

- Let $f: A \to \mathbb{R}$ with $A \subseteq \mathbb{R}$ be a function. We say that

$$f \text{ even} \Leftrightarrow \forall x \in A: (-x \in A \wedge f(-x) = f(x))$$
$$f \text{ odd} \Leftrightarrow \forall x \in A: (-x \in A \wedge f(-x) = -f(x))$$

- Note that in order for f to be even or odd, a necessary condition is that its domain A has to be symmetric around the origin, i.e. $\forall x \in A: -x \in A$.
If the domain is not symmetric, then the function can be neither even nor odd.

▶ Bounded functions

- Let $f: A \to \mathbb{R}$ with $A \subseteq \mathbb{R}$ be a function and let $S \subseteq A$. We say that:

$$f \text{ upper bounded on } S \Leftrightarrow \exists a \in \mathbb{R}: \forall x \in S: f(x) \leq a$$
$$f \text{ lower bounded on } S \Leftrightarrow \exists a \in \mathbb{R}: \forall x \in S: f(x) \geq a$$
$$f \text{ bounded on } S \Leftrightarrow \begin{cases} f \text{ upper bounded on } S \\ f \text{ lower bounded on } S \end{cases}$$

- We will now show that

Thm: f bounded on $S \Leftrightarrow \exists a \in (0, +\infty): \forall x \in S: |f(x)| \leq a$.

Proof

$(\Rightarrow)$: Assume that f bounded on S. Then.

$$f \text{ bounded on } S \Rightarrow f \text{ lower bounded on } S$$
$$\Rightarrow \exists a_1 \in \mathbb{R}: \forall x \in S: f(x) \geq a_1$$
$$f \text{ bounded on } S \Rightarrow f \text{ upper bounded on } S$$
$$\Rightarrow \exists a_2 \in \mathbb{R}: \forall x \in S: f(x) \leq a_2$$

Choose $a_1, a_2 \in \mathbb{R}$ such that $\forall x \in S: a_1 \leq f(x) \leq a_2$.

Define $a = \max\{|a_1|, |a_2|\}$.
We will show that $\forall x \in S : |f(x)| \leq a$.
Let $x \in S$ be given. Then

$$f(x) \leq a_2 \leq |a_2| \leq \max\{|a_1|, |a_2|\} = a \Rightarrow f(x) \leq a \quad (1)$$

$$f(x) \geq a_1 \geq -|a_1| \geq -\max\{|a_1|, |a_2|\} = -a \Rightarrow f(x) \geq -a \quad (2)$$

From (1) and (2):

$$-a \leq f(x) \leq a \Rightarrow |f(x)| \leq a$$

and therefore $\forall x \in S : |f(x)| \leq a$

We have thus shown that $\underline{\exists a \in (0, +\infty) : \forall x \in S : |f(x)| \leq a}$.

($\Leftarrow$): Assume that $\underline{\exists a \in (0, +\infty) : \forall x \in S : |f(x)| \leq a}$

Let $x \in S$ be given. Then $f(x) \leq |f(x)| \leq a$ and $f(x) \geq -|f(x)| \geq -a$. It follows that

$$\begin{cases} \forall x \in S : f(x) \leq a \\ \forall x \in S : f(x) \geq -a \end{cases} \Rightarrow \begin{cases} f \text{ upper bounded on } S \\ f \text{ lower bounded on } S \end{cases} \Rightarrow$$

$$\Rightarrow \underline{f \text{ bounded on } S.} \quad \square$$

↳ In arguments involving absolute values, we use the following properties:

$\forall a \in \mathbb{R} : -|a| \leq a \leq |a|$

$\forall a, b \in \mathbb{R} : |a+b| \leq |a| + |b|$

$\forall a, b \in \mathbb{R} : |a-b| \leq |a| + |b|$

$\forall a, b \in \mathbb{R} : |ab| = |a||b|$

$\forall a \in \mathbb{R} : \forall b \in \mathbb{R} - \{0\} : \left|\dfrac{a}{b}\right| = \dfrac{|a|}{|b|}$

EXAMPLES

a) Given the functions $f_1, f_2 \in F(A)$ and $g_1, g_2 \in F(B)$ show that

$$f_1 = f_2 \wedge g_1 = g_2 \Rightarrow f_1 + g_1 = f_2 + g_2$$

Solution

Assume that $f_1 = f_2 \wedge g_1 = g_2$. Then

$$\left.\begin{array}{l} \mathrm{dom}(f_1+g_1) = \mathrm{dom}(f_1) \cap \mathrm{dom}(g_1) = A \cap B \\ \mathrm{dom}(f_2+g_2) = \mathrm{dom}(f_2) \cap \mathrm{dom}(g_2) = A \cap B \end{array}\right\} \Rightarrow$$

$$\Rightarrow \mathrm{dom}(f_1+g_1) = \mathrm{dom}(f_2+g_2) \qquad (1)$$

We will show: $\forall x \in A \cap B : (f_1+g_1)(x) = (f_2+g_2)(x)$.

Let $x \in A \cap B$ be given. We note that:

$$f_1 = f_2 \Rightarrow f_1(x) = f_2(x) \qquad (2)$$

$$g_1 = g_2 \Rightarrow g_1(x) = g_2(x) \qquad (3)$$

and therefore:

$$\begin{aligned} (f_1+g_1)(x) &= f_1(x) + g_1(x) && [\text{definition}] \\ &= f_2(x) + g_2(x) && [\text{eq. } (2), (3)] \\ &= (f_2+g_2)(x) && [\text{definition}] \end{aligned}$$

It follows that $\forall x \in A \cap B : (f_1+g_1)(x) = (f_2+g_2)(x)$ (4)

From (1) and (4): $f_1 + g_1 = f_2 + g_2$.

$\rightarrow$ To show that two functions are equal, we have to show that

a) They have the same domain

b) They have the same formula.

b) Let A, B be two sets with $A \cap B \neq \emptyset$. Show that:

$$\forall a, b \in \mathbb{R} : \forall f \in \mathcal{F}(A) : \forall g \in \mathcal{F}(B) : (af)(bg) = (ab)(fg)$$

<u>Solution</u>

Let $a, b \in \mathbb{R}$ and $f \in \mathcal{F}(A)$ and $g \in \mathcal{F}(B)$ be given. Then

$$\operatorname{dom}((af)(bg)) = \operatorname{dom}(af) \cap \operatorname{dom}(bg) = \operatorname{dom}(f) \cap \operatorname{dom}(g)$$
$$= A \cap B \qquad (1)$$

and

$$\operatorname{dom}((ab)(fg)) = \operatorname{dom}(fg) = \operatorname{dom}(f) \cap \operatorname{dom}(g) = A \cap B \qquad (2)$$

From (1) and (2): $\operatorname{dom}((af)(bg)) = \operatorname{dom}((ab)(fg))$ (3).

Let $x \in A \cap B$ be given. Then

$$[(af)(bg)](x) = (af)(x) \cdot (bg)(x) = af(x)\, bg(x) =$$
$$= ab\, f(x) g(x) = ab\,(fg)(x) =$$
$$= [(ab)(fg)](x).$$

and therefore $\forall x \in A \cap B : [(af)(bg)](x) = [(ab)(fg)](x)$. (4)

From (3) and (4): $(af)(bg) = (ab)(fg)$

and it follows that

$$\forall a, b \in \mathbb{R} : \forall f \in \mathcal{F}(A) : \forall g \in \mathcal{F}(B) : (af)(bg) = (ab)(fg).$$

c) Let f, g be two functions. Show that

f even $\wedge$ g odd $\Rightarrow$ fg odd

<u>Solution</u>

Assume that f even $\wedge$ g odd.

Define $A = \text{dom}(f)$ and $B = \text{dom}(g)$.

f even $\Rightarrow \forall x \in A : (-x \in A \wedge f(-x) = f(x))$ (1)

g odd $\Rightarrow \forall x \in B : (-x \in B \wedge g(-x) = -g(x))$ (2)

Note that $\text{dom}(fg) = \text{dom}(f) \cap \text{dom}(g) = A \cap B$.

Let $\underline{x \in A \cap B}$ be given. Then:

$$\begin{aligned} x \in A \cap B &\Rightarrow x \in A \wedge x \in B && [\text{definition}] \\ &\Rightarrow -x \in A \wedge -x \in B && [\text{from } (1),(2)] \\ &\Rightarrow \underline{-x \in A \cap B} \end{aligned}$$

and

$$\begin{aligned} \underline{(fg)(-x)} &= f(-x)g(-x) = f(x)[-g(x)] = -f(x)g(x) \\ &= \underline{-(fg)(x)}. \end{aligned}$$

It follows that

$\forall x \in A \cap B : (-x \in A \cap B \wedge (fg)(-x) = -(fg)(x))$

$\Rightarrow fg$ odd.

d) Define $\forall x \in \mathbb{R} : f(x) = 2\sin x\,(\cos(2x) + \cos(3x))$
Show that f bounded in $\mathbb{R}$.

Solution

Let $x \in \mathbb{R}$ be given. Then

$$|f(x)| = |2\sin x\,[\cos(2x) + \cos(3x)]| =$$
$$= 2|\sin x| \cdot |\cos(2x) + \cos(3x)|$$
$$\leq 2|\cos(2x) + \cos(3x)| \leq 2(|\cos(2x)| + |\cos(3x)|)$$
$$\leq 2(1+1) = 2 \cdot 2 = 4 \Rightarrow |f(x)| \leq 4.$$

It follows that

$\forall x \in \mathbb{R} : |f(x)| \leq 4 \Rightarrow f$ bounded in $\mathbb{R}$.

e) Let $f, g \in F(\mathbb{R})$ be two functions, both bounded on $\mathbb{R}$.
Define h as:
$\forall x \in \mathbb{R} : h(x) = f(x)(2 + \cos x) - g(x)(1 - \sin x)^3$
Show that h is bounded in $\mathbb{R}$.

Solution

f bounded on $\mathbb{R} \Rightarrow \exists a \in (0, +\infty) : \forall x \in \mathbb{R} : |f(x)| \leq a$

g bounded on $\mathbb{R} \Rightarrow \exists b \in (0, +\infty) : \forall x \in \mathbb{R} : |g(x)| \leq b$

Choose $a, b \in (0, +\infty)$ such that $\forall x \in \mathbb{R} : (|f(x)| \leq a \wedge |g(x)| \leq b)$.

Let $x \in \mathbb{R}$ be given. Then:

$$|h(x)| = |f(x)(2 + \cos x) - g(x)(1 - \sin x)^3|$$
$$\leq |f(x)(2 + \cos x)| + |g(x)(1 - \sin x)^3|$$
$$= |f(x)||2 + \cos x| + |g(x)|(|1 - \sin x|)^3$$
$$\leq a|2 + \cos x| + b|1 - \sin x|^3$$
$$\leq a(2 + |\cos x|) + b(1 + |\sin x|)^3$$

$$\leq a(2+1) + b(1+1)^3 = 3a + 8b.$$

and therefore

$\forall x \in \mathbb{R} : (|h(x)| \leq 3a + 8b) \Rightarrow$

$\Rightarrow h$ bounded at $\mathbb{R}$.

↳ In addition to properties of absolute values, we also use:

$\forall x \in \mathbb{R} : \ |\sin x| \leq 1$

$\forall x \in \mathbb{R} : \ |\cos x| \leq 1.$

f) Let $f, g \in F(\mathbb{R})$ be two functions that are upper bounded on $\mathbb{R}$. Show that $f+g$ are upper bounded on $\mathbb{R}$.

<u>Solution</u>

f upper bounded on $\mathbb{R} \Rightarrow \exists a \in \mathbb{R} : \forall x \in \mathbb{R} : f(x) \leq a$ (1)

g upper bounded on $\mathbb{R} \Rightarrow \exists b \in \mathbb{R} : \forall x \in \mathbb{R} : g(x) \leq b$ (2)

Let $x \in \mathbb{R}$ be given. Then:

$$\begin{aligned}(f+g)(x) &= f(x) + g(x) && [\text{definition}] \\ &\leq a + g(x) && [\text{via eq. (1)}] \\ &\leq a + b && [\text{via eq. (2)}]\end{aligned}$$

and therefore

$\forall x \in \mathbb{R} : (f+g)(x) \leq a + b$

$\Rightarrow f+g$ upper bounded on $\mathbb{R}$.

g) Let $f,g \in F(\mathbb{R})$ be two functions. Show that

$$f \uparrow \mathbb{R} \land g \uparrow \mathbb{R} \Rightarrow f+g \uparrow$$

Solution

1st method: Let $x_1, x_2 \in \mathbb{R}$ be given with $x_1 < x_2$. Then

$f \uparrow \mathbb{R} \Rightarrow f(x_1) < f(x_2)$ (1)

$g \uparrow \mathbb{R} \Rightarrow g(x_1) < g(x_2)$ (2)

From (1) and (2):

$f(x_1) + g(x_1) < f(x_2) + g(x_2) \Rightarrow$

$\Rightarrow (f+g)(x_1) < (f+g)(x_2)$

It follows that

$\forall x_1, x_2 \in \mathbb{R}: (x_1 < x_2 \Rightarrow (f+g)(x_1) < (f+g)(x_2)) \Rightarrow$

$\Rightarrow f+g \uparrow \mathbb{R}$.

2nd method: Let $x_1, x_2 \in \mathbb{R}$ be given with $x_1 < x_2$. Then

$$\begin{aligned} \Delta(x_1, x_2) &\equiv (f+g)(x_2) - (f+g)(x_1) \\ &= [f(x_2) + g(x_2)] - [f(x_1) + g(x_1)] \\ &= [f(x_2) - f(x_1)] + [g(x_2) - g(x_1)] > 0 \end{aligned}$$

because:

$x_1 < x_2 \Rightarrow f(x_1) < f(x_2) \Rightarrow f(x_2) - f(x_1) > 0$

$x_1 < x_2 \Rightarrow g(x_1) < g(x_2) \Rightarrow g(x_2) - g(x_1) > 0$

It follows that $(f+g)(x_1) < (f+g)(x_2)$, and therefore:

$\forall x_1, x_2 \in \mathbb{R}: (x_1 < x_2 \Rightarrow (f+g)(x_1) < (f+g)(x_2))$

$\Rightarrow f+g \uparrow \mathbb{R}$.

EXERCISES

(13) Let A, B be two sets with $A \cap B \neq \emptyset$. Show that

a) $\forall f \in \mathcal{F}(A) : \forall g \in \mathcal{F}(B) : (-f)(-g) = fg$

b) $\forall a, b \in \mathbb{R} : \forall f \in \mathcal{F}(A) : \forall g, h \in \mathcal{F}(B) : (ag + bh)f = a(fg) + b(fh)$

c) $\forall f, g \in \mathcal{F}(A) : \forall h \in \mathcal{F}(B) : (f = g \Rightarrow f + h = g + h)$

d) $\forall f, g \in \mathcal{F}(A) : \forall h \in \mathcal{F}(B) : (f = g \Rightarrow fh = gh)$

(14) Let $f, g \in \mathcal{F}(\mathbb{R})$ be two functions. Show that:

a) f even $\wedge$ g even $\Rightarrow$ $f + g$ even

b) f even $\wedge$ g even $\Rightarrow$ fg even

c) f odd $\wedge$ g odd $\Rightarrow$ $f + g$ odd

d) f odd $\wedge$ g odd $\Rightarrow$ fg even

e) f odd $\wedge$ $f \nearrow [0, +\infty) \Rightarrow f \nearrow \mathbb{R}$

(Hint: use proof by cases)

f) f even $\wedge$ $f \nearrow [0, +\infty) \Rightarrow f \searrow (-\infty, 0)$

(15) Let $f : A \to \mathbb{R}$ be a function. Show that

a) $f \nearrow A \Rightarrow f$ one-to-one

b) $f \searrow A \Rightarrow f$ one-to-one

c) f even $\Rightarrow f$ not one-to-one

(16) Show that the following functions are bounded in $\mathbb{R}$.

a) $\forall x \in \mathbb{R} : f(x) = \sin x (\cos x + \sin x)$

b) $\forall x \in \mathbb{R} : f(x) = (1 - \sin x)^2 \cos x + \sin x$

c) $\forall x \in \mathbb{R}: f(x) = (1-\cos x)(1-\sin x) + \sin x$

(17) Let $f, g \in F(\mathbb{R})$ be two functions bounded in $\mathbb{R}$. Show that $h \in F(\mathbb{R})$, defined as follows, is also bounded in $\mathbb{R}$.

a) $\forall x \in \mathbb{R}: h(x) = f(x)\, g(x) \cos x$

b) $\forall x \in \mathbb{R}: h(x) = f(x)\,(1+\sin x) + g(x) \cos^2 x$

c) $\forall x \in \mathbb{R}: h(x) = \sin(f(x)) + g(x) \cos(g(x))$

d) $\forall x \in \mathbb{R}: h(x) = f(g(x))\,[\sin x + g(x) \cos(\sin x)]$

(18) Let $f \in F(\mathbb{R})$ be defined as:

$\forall x \in \mathbb{R}: f(x) = ax^2 + bx + c$

Show that $g = f \upharpoonright [-1,1]$ is bounded on $[-1,1]$.

(19) Let $f \in F(\mathbb{R})$ be a general polynomial function defined by:

$$\forall x \in \mathbb{R}: f(x) = \sum_{K=1}^{n} a_K x^k$$

and let $a, b \in \mathbb{R}$ be given with $a < b$. Show that $g = f \upharpoonright [a,b]$ is bounded in $[a,b]$.

(Hint: For $x \in [a,b]$, first show that $|x| \leq \max\{|a|, |b|\}$.

(20) Let $f, g, h \in F(\mathbb{R})$ be three functions. Show that

a) $\begin{cases} h = f + 3g \\ f, g \text{ lower bounded on } \mathbb{R} \end{cases} \Rightarrow h$ lower bounded on $\mathbb{R}$.

b) $\begin{cases} h = 2f - 5g \\ f \text{ upper bounded on } \mathbb{R} \\ g \text{ lower bounded on } \mathbb{R} \end{cases} \Rightarrow h$ upper bounded on $\mathbb{R}$.

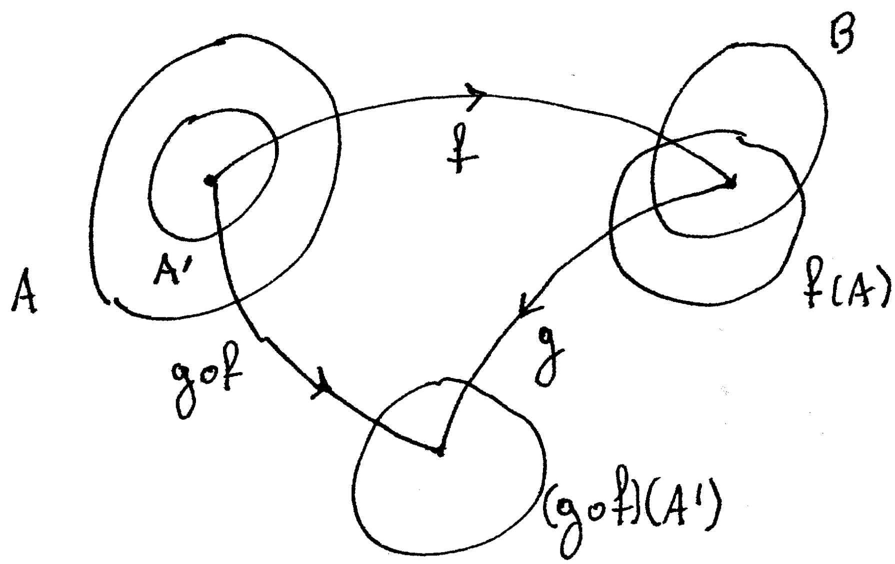
c) $\begin{cases} h = fg \\ f \text{ upper bounded on } \mathbb{R} \\ \forall x \in \mathbb{R} : 0 < g(x) < 1 \end{cases} \Rightarrow h$ upper bounded on $\mathbb{R}$.

d) $\begin{cases} h = fg \\ f \text{ lower bounded on } \mathbb{R} \\ \forall x \in \mathbb{R} : 0 < g(x) < 2 \end{cases} \Rightarrow h$ lower bounded on $\mathbb{R}$.

Function composition

- Let $f: A \to \mathbb{R}$ and $g: B \to \mathbb{R}$ be two functions. We assume that $f(A) \cap B \neq \emptyset$. Let A' be the subset of A whose elements are mapped by f into the intersection $f(A) \cap B$. Thus A' is given by
$$A' = \{x \in A \mid f(x) \in B\}.$$
We may therefore define the function $g \circ f: A' \to \mathbb{R}$ as follows:

$$\boxed{\begin{array}{l} \mathrm{dom}(g\circ f) = \{x \in \mathrm{dom}(f) \mid f(x) \in \mathrm{dom}(g)\} = A' \\ \forall x \in A': \ (g\circ f)(x) = g(f(x)) \end{array}}$$



- We note that the belonging condition for $g\circ f$ is

$$\boxed{x \in \mathrm{dom}(g\circ f) \iff \begin{cases} x \in \mathrm{dom}(f) \\ f(x) \in \mathrm{dom}(g) \end{cases}}$$

Properties of mapping composition

- Let f, g, h be 3 mappings. Then

$$\boxed{(f \circ g) \circ h = f \circ (g \circ h)} \quad \text{(associative)}$$

Proof

First we establish that the domains are equal.

$x \in \mathrm{dom}((f \circ g) \circ h) \Leftrightarrow$

$\Leftrightarrow x \in \mathrm{dom}(h) \wedge h(x) \in \mathrm{dom}(f \circ g)$

$\Leftrightarrow x \in \mathrm{dom}(h) \wedge [h(x) \in \mathrm{dom}(g) \wedge g(h(x)) \in \mathrm{dom}(f)]$

$\Leftrightarrow (x \in \mathrm{dom}(h) \wedge h(x) \in \mathrm{dom}(g)) \wedge (g \circ h)(x) \in \mathrm{dom}(f)$

$\Leftrightarrow x \in \mathrm{dom}(g \circ h) \wedge (g \circ h)(x) \in \mathrm{dom}(f)$

$\Leftrightarrow x \in \mathrm{dom}(f \circ (g \circ h))$.

therefore,

$$\mathrm{dom}((f \circ g) \circ h) = \mathrm{dom}(f \circ (g \circ h)) = A$$

Let $x \in A$ be given. Then

$$\left.\begin{aligned} [(f \circ g) \circ h](x) &= (f \circ g)(h(x)) = f(g(h(x))) \\ [f \circ (g \circ h)](x) &= f((g \circ h)(x)) = f(g(h(x))) \end{aligned}\right\} \Rightarrow$$

$$\Rightarrow [(f \circ g) \circ h](x) = [f \circ (g \circ h)](x), \forall x \in A.$$

It follows that $(f \circ g) \circ h = f \circ (g \circ h)$. □

- In general, it is usually <u>not true</u> that $f \circ g = g \circ f$, although exceptions are possible for specific choices of f, g.

- Let f, g be two mappings. Then

$$\boxed{\begin{cases} f \text{ one-to-one} \\ g \text{ one-to-one} \end{cases} \Rightarrow f \circ g \text{ one-to-one.}}$$

<u>Proof</u>

Let $A = \mathrm{dom}(f \circ g)$. Let $x_1, x_2 \in A$ be given such that $(f \circ g)(x_1) = (f \circ g)(x_2)$. Then,

$$\begin{aligned} (f \circ g)(x_1) = (f \circ g)(x_2) &\Rightarrow f(g(x_1)) = f(g(x_2)) && [\text{definition}] \\ &\Rightarrow g(x_1) = g(x_2) && [f \text{ one-to-one}] \\ &\Rightarrow x_1 = x_2 && [g \text{ one-to-one}] \end{aligned}$$

and it follows that

$$\forall x_1, x_2 \in A : ((f \circ g)(x_1) = (f \circ g)(x_2) \Rightarrow x_1 = x_2)$$

$\Rightarrow f \circ g$ one-to-one.

<u>Methodology</u>

•$_1$ To define a function f, we have to define both the expression $f(x)$ and the domain $\mathrm{dom}(f)$ of f.

•$_2$ When the domain of a function is not given, the <u>implied domain</u> is the widest possible subset of $\mathbb{R}$ for which the function formula $f(x)$ can be evaluated. To derive the belonging condition of the domain, we note that

a) We cannot DIVIDE BY ZERO

b) We cannot take the SQUARE ROOT OF A NEGATIVE NUMBER.

•$_3$ To find the domain of $f \circ g$:

a) First we find $\mathrm{dom}(f)$ and $\mathrm{dom}(g)$

b) The belonging condition of $\mathrm{dom}(f \circ g)$ is given by

$$x \in \mathrm{dom}(f \circ g) \Leftrightarrow \begin{cases} x \in \mathrm{dom}(g) \\ g(x) \in \mathrm{dom}(f) \end{cases} \Leftrightarrow \cdots$$

EXAMPLE

a) Given $f(x) = \sqrt{1-x}$ and $g(x) = 1-3x$, define the functions $h_1 = f \circ g$ and $h_2 = g \circ f$.

Solution

• Domain of f

Require $1-x \geq 0 \Leftrightarrow x \leq 1 \Leftrightarrow x \in (-\infty, 1]$.

It follows that $\operatorname{dom}(f) = (-\infty, 1]$.

• Domain of g.

There are no requirements, therefore $\operatorname{dom}(g) = \mathbb{R}$.

• Definition of $h_1 = f \circ g$.

$$x \in \operatorname{dom}(f \circ g) \Leftrightarrow \begin{cases} x \in \operatorname{dom}(g) \\ g(x) \in \operatorname{dom}(f) \end{cases} \Leftrightarrow \begin{cases} x \in \mathbb{R} \\ (1-3x) \in (-\infty, 1] \end{cases} \Leftrightarrow$$

$$\Leftrightarrow (1-3x) \in (-\infty, 1] \Leftrightarrow 1-3x \leq 1 \Leftrightarrow -3x \leq 0 \Leftrightarrow$$

$$\Leftrightarrow x \geq 0 \Leftrightarrow x \in [0, +\infty).$$

and therefore $\operatorname{dom}(f \circ g) = [0, +\infty)$.

$$\forall x \in [0, +\infty) : (f \circ g)(x) = f(g(x)) = f(1-3x) = \sqrt{1-(1-3x)}$$
$$= \sqrt{1-1+3x} = \sqrt{3x}$$

thus $\forall x \in [0, +\infty) : (f \circ g)(x) = \sqrt{3x}$.

• Definition of $h_2 = g \circ f$.

$$x \in \operatorname{dom}(g \circ f) \Leftrightarrow \begin{cases} x \in \operatorname{dom}(f) \\ f(x) \in \operatorname{dom}(g) \end{cases} \Leftrightarrow \begin{cases} x \in (-\infty, 1] \\ \sqrt{1-x} \in \mathbb{R} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow x \in (-\infty, 1]$$

and therefore: $\operatorname{dom}(g \circ f) = (-\infty, 1]$.

$$\forall x \in (-\infty, 1] : (g \circ f)(x) = g(f(x)) = g(\sqrt{1-x}) = 1 - 3\sqrt{1-x}$$

b) Let $f: \mathbb{R} \to \mathbb{R}$ and $g: \mathbb{R} \to \mathbb{R}$ be two functions.

Show that: $f \searrow \mathbb{R} \wedge g \nearrow \mathbb{R} \Rightarrow f \circ g \searrow \mathbb{R}$.

Solution

Assume that $f \searrow \mathbb{R}$ and $g \nearrow \mathbb{R}$.

Since $\mathrm{dom}(f) = \mathbb{R}$ and $\mathrm{dom}(g) = \mathbb{R}$, it follows that

$$\mathrm{dom}(f \circ g) = \{x \in \mathrm{dom}(g) \mid g(x) \in \mathrm{dom}(f)\} =$$
$$= \{x \in \mathbb{R} \mid g(x) \in \mathbb{R}\} = \mathbb{R}.$$

Let $x_1, x_2 \in \mathbb{R}$ be given with $x_1 < x_2$. Then

$$\begin{aligned} x_1 < x_2 &\Rightarrow g(x_1) < g(x_2) && [g \nearrow \mathbb{R}] \\ &\Rightarrow f(g(x_1)) > f(g(x_2)) && [f \searrow \mathbb{R}] \\ &\Rightarrow (f \circ g)(x_1) > (f \circ g)(x_2) && [\text{definition}] \end{aligned}$$

and therefore:

$$\forall x_1, x_2 \in \mathbb{R} : (x_1 < x_2 \Rightarrow (f \circ g)(x_1) > (f \circ g)(x_2))$$
$$\Rightarrow f \circ g \searrow \mathbb{R}$$

c) Let $f: \mathbb{R} \to \mathbb{R}$ and $g: \mathbb{R} \to \mathbb{R}$ be two functions.

Show that f even $\wedge$ g odd $\Rightarrow f \circ g$ even.

Solution

Assume that f even and g odd. Since $\mathrm{dom}(f) = \mathbb{R}$ and $\mathrm{dom}(g) = \mathbb{R}$, it follows that

$$\mathrm{dom}(f \circ g) = \{x \in \mathrm{dom}(g) \mid g(x) \in \mathrm{dom}(f)\} =$$
$$= \{x \in \mathbb{R} \mid g(x) \in \mathbb{R}\} = \mathbb{R}$$

which is symmetric: $\forall x \in \mathbb{R} : -x \in \mathbb{R}$.

Let $x \in \mathbb{R}$ be given. Then:

$$
\begin{aligned}
(f\circ g)(-x) &= f(g(-x)) && [\text{definition}]\\
&= f(-g(x)) && [g \text{ odd}]\\
&= f(g(x)) && [f \text{ even}]\\
&= (f\circ g)(x) && [\text{definition}]
\end{aligned}
$$

and therefore $\forall x \in \mathbb{R} : (f\circ g)(-x) = (f\circ g)(x)$. (2)

From (1) and (2):

$\forall x \in \mathbb{R} : (-x \in \mathbb{R} \wedge (f\circ g)(-x) = (f\circ g)(x))$

$\Rightarrow f\circ g$ even.

d) Let $f : \mathbb{R} \to \mathbb{R}$ be a function. Show that

f odd $\wedge$ f bounded on $[0, +\infty) \Rightarrow f$ bounded on $\mathbb{R}$.

<u>Solution</u>

Assume that f odd and f bounded on $[0, +\infty)$. Since:

f bounded on $[0, +\infty) \Rightarrow \exists a \in (0, +\infty) : \forall x \in [0, +\infty) : |f(x)| \leq a$. (1)

Let $x \in \mathbb{R}$ be given. We distinguish the following cases:

<u>Case 1</u>: If $x \in [0, +\infty)$, then from (1): $|f(x)| \leq a$.

<u>Case 2</u>: If $x \in (-\infty, 0)$, then

$$
\begin{aligned}
|f(x)| &= |-f(x)| =\\
&= |f(-x)| && [f \text{ odd}]\\
&\leq a && [\text{eq. (1) and } -x \in [0, +\infty)]
\end{aligned}
$$

It follows that

$(\forall x \in \mathbb{R} : |f(x)| \leq a) \Rightarrow f$ bounded on $\mathbb{R}$.

EXERCISES

(21) Define the functions $f \circ g$ and $g \circ f$ for f, g given by:

a) $f(x) = 3x+2$, $g(x) = x^2+5x+3$

b) $f(x) = x^2+1$, $g(x) = \sqrt{3-x}$

c) $f(x) = \sqrt{4-x^2}$, $g(x) = \sqrt{1-x^2}$

d) $f(x) = \dfrac{x+2}{x-1}$, $g(x) = \dfrac{2x-1}{x+3}$

(22) Let $f, g, h \in F(\mathbb{R})$ be three functions. Show that $f = g \Rightarrow f \circ h = g \circ h$.

(23) Let $f, g \in F(\mathbb{R})$ be two functions. Show that

a) f even $\wedge$ g even $\Rightarrow$ $f \circ g$ even

b) f odd $\wedge$ g odd $\Rightarrow$ $f \circ g$ odd

c) f even $\wedge$ g odd $\Rightarrow$ $f \circ g$ even

d) $f \nearrow \mathbb{R} \wedge g \nearrow \mathbb{R} \Rightarrow f \circ g \nearrow \mathbb{R}$

e) $f \nearrow \mathbb{R} \wedge g \searrow \mathbb{R} \Rightarrow f \circ g \searrow \mathbb{R}$

f) $f \searrow \mathbb{R} \wedge g \searrow \mathbb{R} \Rightarrow g \circ f \nearrow \mathbb{R}$

g) f odd $\wedge$ $f \nearrow [0, +\infty) \Rightarrow f \nearrow \mathbb{R}$

h) f even $\wedge$ $f \nearrow (0, +\infty) \Rightarrow f \searrow (-\infty, 0)$.

i) f even $\wedge$ f bounded on $[0, +\infty) \Rightarrow f$ bounded on $\mathbb{R}$

▼ Inverse mappings

- Let $f : A \to B$ and $g : B \to A$ be two mappings. We say that

$$\boxed{\begin{array}{l} g \text{ left inverse of } f \Leftrightarrow \forall x \in A : (g \circ f)(x) = x \\ g \text{ right inverse of } f \Leftrightarrow \forall x \in B : (f \circ g)(x) = x \end{array}}$$

- These definitions can be abbreviated if written in terms of the identity mapping $id[A] : A \to A$ defined as: $\forall x \in A : id[A](x) = x$.
  Then, it follows that for $f : A \to B$ and $g : B \to A$
  g left inverse of $f \Leftrightarrow g \circ f = id[A]$
  g right inverse of $f \Leftrightarrow f \circ g = id[B]$
- We note that in general:
  $$f \circ id[\mathcal{S}] = f \upharpoonright \mathcal{S}$$
  $$id[\mathcal{S}] \circ f = f \upharpoonright \{x \in dom(f) \mid f(x) \in \mathcal{S}\}$$
  To eliminate the need for restrictions, for $f : A \to B$ we have:
  $$f \circ id[A] = f$$
  $$id[f(A)] \circ f = f$$

Criteria for existence of left/right inverse

Let $f : A \to B$ be a mapping. Recall that we defined 1-1 mappings as follows:

$$\boxed{f \text{ one-to-one} \Leftrightarrow \forall x_1, x_2 \in A : (\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2)}$$

We now introduce the following definitions:

$$\boxed{\begin{array}{l} f \text{ onto} \Leftrightarrow f(A) = B \\ f \text{ bijection} \Leftrightarrow f \text{ onto} \wedge f \text{ one-to-one} \end{array}}$$

We will now show that

Thm : Let $f : A \to B$ be a mapping. Then:

a) f has a left inverge $g : B \to A \Leftrightarrow f$ one-to-one

b) f has a right inverse $g : B \to A \Leftrightarrow f$ onto

Proof

a) $(\Rightarrow)$: Assume that f has a left inverse $g : B \to A$.
Let $x_1, x_2 \in A$ be given with $f(x_1) = f(x_2)$. Then:

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow g(f(x_1)) = g f(x_2)) \\ &\Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2) && [\text{Definition}] \\ &\Rightarrow id[A](x_1) = id[A](x_2) && [g \text{ left inverse of } f] \\ &\Rightarrow x_1 = x_2 && [\text{Definition}] \end{aligned}$$

It follows that

$\forall x_1, x_2 \in A : (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$

$\Rightarrow f$ one-to-one.

$(\Leftarrow)$: Assume that f is one-to-one.

▸ Definition of $g : B \to A$

Let $y \in f(A)$ be given. Since $y \in f(A) \Rightarrow \exists x \in A : f(x) = y$ we choose an $x \in A$ and define $h(y) = x$ such that $f(x) = y$. Consequently, we may define a mapping $h : f(A) \to A$ such that

$$\forall y \in f(A) : f(h(y)) = y \qquad (1)$$

We now define $g : B \to A$ as:

$$\forall y \in B : g(y) = \begin{cases} h(y) & , \text{ if } y \in f(A) \\ y & , \text{ if } y \in B - f(A) \end{cases}$$

• <u>Analysis:</u> We now show g left inverse of f.

Let $x \in A$ be given. Define $y = f(x) \in f(A)$ and $x_0 = g(y)$. Note that it is not yet obvious that $x_0 = x$. Since

$$\begin{aligned} y \in f(A) \Rightarrow f(h(y)) &= y && [\text{Eq. } (1)] \\ &= f(x) && [\text{Definition}] \end{aligned}$$

and therefore,

$$\left.\begin{array}{l} f(h(y)) = f(x) \\ f \text{ one-to-one} \end{array}\right\} \Rightarrow h(y) = x \qquad (2)$$

consequently,

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) && [\text{Definition}] \\ &= g(y) && [\text{Definition}] \\ &= h(y) && [\text{because } y \in f(A)] \\ &= x && [\text{Eq. } (2)] \end{aligned}$$

It follows that

$\forall x \in A : (g \circ f)(x) = x$

$\Rightarrow g$ left inverse of f.

b) <u>($\Rightarrow$)</u>: Assume that $g : B \to A$ is a right inverse of f. By definition, we know that $f(A) \subseteq B$. We claim that $B \subseteq f(A)$. Let $y \in B$ be given. Define $x = g(y) \in A$. Then:

$$\begin{aligned} f(x) &= f(g(y)) && [\text{because } x = g(y)] \\ &= (f \circ g)(y) && [\text{definition}] \\ &= \mathrm{id}[B](y) && [g \text{ right inverse of } f] \\ &= y && [\text{definition}] \end{aligned}$$

It follows that

$$(\exists x \in A : y = f(x)) \Rightarrow y \in f(A).$$

and therefore $\forall y \in B : y \in f(A) \Rightarrow B \subseteq f(A)$

Since $\left\{ \begin{array}{l} f(A) \subseteq B \\ B \subseteq f(A) \end{array} \right. \Rightarrow f(A) = B \Rightarrow f$ onto.

($\Leftarrow$): Assume that f onto.

- Definition of $g : B \to A$

f onto $\Rightarrow f(A) = B \Rightarrow B \subseteq f(A) \Rightarrow \forall y \in B : y \in f(A)$
$\Rightarrow \forall y \in B : \exists x \in A : f(x) = y \quad (1)$

Let $y \in B$ be given. From (1), we choose an $x \in A$ such that $f(x) = y$, and define $g(y) = x$.
It follows that we have thus defined a $g : B \to A$ such that $\forall y \in B : (g(y) = x \Rightarrow f(x) = y)$

- Analysis

Let $y \in B$ be given. Define $x = g(y)$. Then $f(x) = y$.
It follows that

$$\begin{aligned} (f \circ g)(y) &= f(g(y)) && [\text{definition}] \\ &= f(x) && [\text{because } x = g(y)] \\ &= y && [\text{because } f(x) = y] \end{aligned}$$

and therefore

$$(\forall y \in B : (f \circ g)(y) = y) \Rightarrow g \text{ right inverse of } f. \quad \square$$

From the proof of this theorem we see that the left and right inverse do not have to be unique. However we will show that when both exist, they have to be equal to each other.

Prop: Let $f: A \to B$ be a mapping. Then

$$\boxed{\begin{cases} g_1 \text{ left inverse of } f \\ g_2 \text{ right inverse of } f \end{cases} \Longrightarrow g_1 = g_2}$$

Proof

Assume that g_1 left inverse of f and g_2 right inverse of f.

g_1 left inverse of $f \Rightarrow g_1 \circ f = \mathrm{id}[A]$ (1)

g_2 right inverse of $f \Rightarrow f \circ g_2 = \mathrm{id}[B]$. (2)

It follows that

$$\begin{aligned} g_1 &= g_1 \circ \mathrm{id}[B] && [\text{identity mapping}] \\ &= g_1 \circ (f \circ g_2) && [\text{eq. (2)}] \\ &= (g_1 \circ f) \circ g_2 && [\text{associative property}] \\ &= \mathrm{id}[A] \circ g_2 && [\text{eq. (1)}] \\ &= g_2 && [\text{identity mapping}] \end{aligned}$$

and therefore $g_1 = g_2$ □

Definition of inverse mapping

- Let $f: A \to B$ be a mapping. We say that

$$\boxed{g \text{ inverse of } f \Leftrightarrow \begin{cases} g \text{ left inverse of } f \\ g \text{ right inverse of } f \end{cases}}$$

Equivalently, the definition can be rewritten as

$$\boxed{g \text{ inverse of } f \Leftrightarrow \begin{cases} g \circ f = \mathrm{id}[A] \\ f \circ g = \mathrm{id}[B] \end{cases} \Leftrightarrow \begin{cases} \forall x \in A: (g \circ f)(x) = x \\ \forall x \in B: (f \circ g)(x) = x \end{cases}}$$

Existence of inverse of mapping

Thm: Let $f: A \to B$ be a mapping. Then

$$\boxed{\exists g \in \mathrm{Map}(B, A): g \text{ inverse of } f \Leftrightarrow f \text{ bijection}}$$

Proof

($\Rightarrow$): Assume that f has an inverse $g: B \to A$. Then

$$g \text{ inverse of } f \Rightarrow \begin{cases} g \text{ left inverse of } f \\ g \text{ right inverse of } f \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} f \text{ one-to-one} \\ f \text{ onto} \end{cases} \Rightarrow$$

$$\Rightarrow f \text{ bijection.}$$

($\Leftarrow$) : Assume that f is a bijection. Then

f bijection $\Rightarrow f$ one-to-one $\Rightarrow$

$\Rightarrow \exists g_1 \in \mathrm{Map}(B, A) : g_1$ left inverse of f. (1)

f bijection $\Rightarrow f$ onto $\Rightarrow$

$\Rightarrow \exists g_2 \in \mathrm{Map}(B, A) : g_2$ right inverse of f (2)

Choose $g_1, g_2 \in \mathrm{Map}(B, A)$ such that g_1 left inverse and g_2 right inv. of f.

$$\left.\begin{cases} g_1 \text{ left inverse of } f \\ g_2 \text{ right inverse of } f \end{cases}\right. \Rightarrow g_1 = g_2 .$$

Define $g \equiv g_1 = g_2$. Then

$$\left.\begin{cases} g \text{ left inverse of } f \\ g \text{ right inverse of } f \end{cases}\right. \Rightarrow g \text{ inverse of } f. \quad \square$$

Uniqueness of inverse mapping

Thm: Let $f: A \to B$ be a mapping. Then, we have:

$$\left\{\begin{array}{l} g_1 \text{ inverse of } A \\ g_2 \text{ inverse of } A \end{array}\right. \Rightarrow g_1 = g_2$$

Proof

Assume that $g_1 : B \to A$ and $g_2 : B \to A$ are inverses of f. Then, we have:

$$\begin{aligned}
g_1 &= id[A] \circ g_1 && [A \text{ codomain of } g_1] \\
&= (g_2 \circ f) \circ g_1 && [g_2 \text{ left inverse of } f] \\
&= g_2 \circ (f \circ g_1) && [\text{associative property}] \\
&= g_2 \circ id[B] && [g_1 \text{ right inverse of } f] \\
&= g_2 && [B \text{ domain of } g_2]
\end{aligned}$$

and therefore $g_1 = g_2$.

Notation: If $f: A \to B$ is a bijection, then according to the previous two results, there is a unique function g which is the inverse of f. We denote the unique inverse of f as $f^{-1} = g$.

Equivalent characterization of inverse mapping

Thm: Let $f : A \to B$ and $g : B \to A$ be two mappings.
Then:

$$\boxed{g = f^{-1} \Leftrightarrow \forall x \in A : \forall y \in B : (y = f(x) \Leftrightarrow x = g(y))}$$

Proof

($\Rightarrow$): Assume that $g = f^{-1}$. Let $x \in A$ and $y \in B$ be given. We will show that $y = f(x) \Leftrightarrow x = g(y)$.

- To show $y = f(x) \Rightarrow x = g(y)$:

Assume that $y = f(x)$. Then

$$\begin{aligned} x &= id[A](x) = && [\text{Definition of } id] \\ &= (g \circ f)(x) = && [g \text{ left inverse of } f] \\ &= g(f(x)) = && [\text{Definition}] \\ &= g(y) && [\text{Hypothesis } y = f(x)] \end{aligned}$$

- To show $x = g(y) \Rightarrow y = f(x)$:

Assume that $x = g(y)$. Then

$$\begin{aligned} y &= id[B](y) = && [\text{Definition of } id] \\ &= (f \circ g)(y) = && [g \text{ right inverse of } f] \\ &= f(g(y)) = && [\text{Definition}] \\ &= f(x). && [\text{Hypothesis } x = g(y)] \end{aligned}$$

It follows that $\forall x \in A : \forall y \in B : (y = f(x) \Leftrightarrow x = g(y))$.

($\Leftarrow$): Assume that $\forall x \in A : \forall y \in B : (y = f(x) \Leftrightarrow x = g(y))$

We will show that $f \circ g = id[B]$ and $g \circ f = id[A]$.

Let $x \in A$ be given. Define $y = f(x)$. Then, by hypothesis, we have $x = g(y)$, and

$$
\begin{aligned}
(g \circ f)(x) &= g(f(x)) && [\text{Definition}] \\
&= g(y) && [\text{Definition } y = f(x)] \\
&= x && [\text{because } x = g(y)]
\end{aligned}
$$

It follows that $\forall x \in A : (g \circ f)(x) = x$ (1)

Let $y \in B$ be given. Define $x = g(y)$. By hypothesis, it follows that $y = f(x)$ and

$$
\begin{aligned}
(f \circ g)(y) &= f(g(y)) && [\text{Definition}] \\
&= f(x) && [\text{because } x = g(y)] \\
&= y && [\text{because } y = f(x)]
\end{aligned}
$$

It follows that $\forall y \in B : (f \circ g)(y) = x$ (2)

From (1) and (2)

$$
\begin{cases} g \circ f = id[A] \\ f \circ g = id[B] \end{cases} \Rightarrow \begin{cases} g \text{ left inverse of } f \\ g \text{ right inverse of } f \end{cases} \Rightarrow
$$

$$\Rightarrow g = f^{-1}. \quad \square$$

EXAMPLES

a) Let $f: A \to B$ be a mapping. Show that if:

$$\left\{\begin{array}{l} f \text{ odd} \\ g \text{ inverse of } f \end{array}\right. \Rightarrow g \text{ odd}.$$

Solution

Assume that f odd and $g: B \to A$ is an inverse of f.
It is sufficient to show that $\forall y \in B : (-y \in B \land g(-y) = -g(y))$.
Let $y \in B$ be given.

- Proof that $-y \in B$.

We first note that:

f has an inverse $\Rightarrow f$ bijection $\Rightarrow f$ onto $\Rightarrow f(A) = B$.

Since $y \in B \Rightarrow y \in f(A)$ [because $f(A) = B$]

$\Rightarrow \exists x \in A : f(x) = y$ [definition of $f(A)$]

We note that $x \in A \land f$ odd $\Rightarrow -x \in A$.

We may therefore evaluate:

$f(-x) = -f(x)$ [f odd]

$= -y \Rightarrow$ [because $f(x) = y$]

$\Rightarrow \exists x' \in A : f(x') = -y \Rightarrow -y \in f(A)$ [Definition]

$\Rightarrow \underline{-y \in B}$. [because $f(A) = B$]

We also note that

f bijection $\Rightarrow f$ one-to-one.

and

$f(g(-y)) = (f \circ g)(-y) =$ [Definition]

$= -y =$ [g right inverse on f]

$$= -(f \circ g)(y) = \qquad [g \text{ right inverse of } f]$$
$$= -f(g(y)) = \qquad [\text{definition}]$$
$$= f(-g(y)) \qquad [f \text{ odd}]$$

and therefore:

$$\left\{\begin{array}{l} f \text{ one-to-one} \\ f(g(-y)) = f(-g(y)) \end{array}\right. \Rightarrow \underline{g(-y) = -g(y).}$$

We have thus shown that

$$\forall y \in B : (-y \in B \wedge g(-y) = -g(y))$$
$$\Rightarrow g \text{ odd}.$$

b) Let $f: A \to B$ be a bijection with $A \subseteq \mathbb{R}$ and $B \subseteq \mathbb{R}$.
Show that: $f \uparrow A \Rightarrow f^{-1} \uparrow B$.

<u>Solution</u>

Assume that $f \uparrow A$. Let $\underline{y_1, y_2 \in B}$ be given with $\underline{y_1 < y_2.}$
To derive a contradiction, assume that $f^{-1}(y_1) \geq f^{-1}(y_2)$. Then:

$$f^{-1}(y_1) \geq f^{-1}(y_2) \Rightarrow f(f^{-1}(y_1)) \geq f(f^{-1}(y_2)) \qquad [f \uparrow A]$$
$$\Rightarrow (f \circ f^{-1})(y_1) \geq (f \circ f^{-1})(y_2) \qquad [\text{definition}]$$
$$\Rightarrow y_1 \geq y_2 \quad (1) \qquad [f^{-1} \text{ right inverse}]$$

Eq. (1) contradicts the hypothesis $y_1 < y_2$. It follows that
$\underline{f^{-1}(y_1) < f^{-1}(y_2)}$, and therefore

$$\forall y_1, y_2 \in B : (y_1 < y_2 \Rightarrow f^{-1}(y_1) < f^{-1}(y_2))$$
$$\Rightarrow f^{-1} \uparrow B.$$

EXERCISES

(24) Study the preceding proofs on inverse mappings, and learn how to reproduce them, for the following statements:

a) f has a left inverse $\Leftrightarrow$ f one-to-one

b) f has a right inverse $\Leftrightarrow$ f onto

c) $\left\{ \begin{array}{l} g_1 \text{ left inverse of } f \\ g_2 \text{ right inverse of } f \end{array} \right. \Rightarrow g_1 = g_2$

d) f has an inverse $\Leftrightarrow$ f bijection

e) $\left\{ \begin{array}{l} f \text{ bijection} \\ g_1 \text{ inverse of } f \\ g_2 \text{ inverse of } f \end{array} \right. \Rightarrow g_1 = g_2$

f) $g = f^{-1} \Leftrightarrow \forall x \in A : \forall y \in B : (y = f(x) \Leftrightarrow g(y) = x)$

(25) Let $f : A \to B$ be a bijection with $A \subseteq \mathbb{R}$ and $B \subseteq \mathbb{R}$. Show that $f \searrow A \Rightarrow f^{-1} \searrow B$.

(26) Let $f : B \to C$ and $g : A \to B$ be bijections. Show that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

(27) Let $f : B \to C$ and $g : A \to B$ be two mappings. Show that for $S \subseteq A$, we have $(f \circ g)(S) = f(g(S))$

$\hookrightarrow$ This statement was used in the proof that the inverse mapping is unique. Prove it!

(28) Let $f : A \to B$ be a mapping. Show that
$S \subseteq T \subseteq A \Rightarrow f(S) \subseteq f(T)$.

(29) Let $f : B \to C$ and $g : A \to B$ be two mappings.
Show that
$$\begin{cases} f \circ g \text{ onto} \\ g \text{ not onto} \end{cases} \Rightarrow f \text{ not one-to-one.}$$
(Hint: Exercise 28 can help shorten the proof for this very challenging problem).

Cardinality

- Given two finite sets A, B, if there is a bijection $f: A \to B$ then A and B have to have the same number of elements. Cantor proposed extending his observation to infinite sets according to the following definitions:

> Def: Let A, B be two sets. We say that
> $A \sim B \Leftrightarrow \exists f \in \mathrm{Map}(A,B) : f$ bijection

- The statement $A \sim B$ reads "A, B are equipotent", or "A and B have the same cardinality".
- Recall the definition
  $[n] = \{x \in \mathbb{N}^* \mid x \leq n\} = \{1, 2, 3, \ldots, n\}$
  Based on that, we introduce the following characterizations:

$$
\boxed{
\begin{aligned}
&A \text{ finite set} \Leftrightarrow A = \varnothing \vee (\exists n \in \mathbb{N}^* : A \sim [n])\\
&A \text{ infinite set} \Leftrightarrow A \text{ not finite set}\\
&\qquad\qquad\qquad \Leftrightarrow A \neq \varnothing \wedge (\forall n \in \mathbb{N}^* : \overline{A \sim [n]})\\
&A \text{ countable set} \Leftrightarrow \exists B \in \mathcal{P}(\mathbb{N}) : A \sim B\\
&A \text{ countably infinite} \Leftrightarrow A \sim \mathbb{N}\\
&A \text{ uncountable} \Leftrightarrow A \text{ not countable}
\end{aligned}
}
$$

- A relative comparison of sets in terms of cardinality is:

$$\text{finite} \leq \text{count}\underbrace{\text{able} \leq \text{countably infinite} < \text{uncountable}}_{\text{infinite}}$$

It should be stressed that since $\emptyset, \mathbb{N} \in \mathcal{P}(\mathbb{N})$ and
$\forall n \in \mathbb{N}^* : [n] \in \mathcal{P}(\mathbb{N})$
it follows that

A finite $\Rightarrow$ A countable

A countably infinite $\Rightarrow$ A countable

However, the converse statements do not hold.

▶ <u>Interpretation</u>: A countably infinite set contains an infinite number of elements, however the existence of some bijection $f: A \to \mathbb{N}$ allows us to enumerate each element of A by assigning it to a unique natural number from $\mathbb{N}$.

▶ <u>$\mathbb{Z}$ and $\mathbb{Q}$ are countable</u>

Recall that

$$\mathbb{Z} = \mathbb{N} \cup \{-x \mid x \in \mathbb{N}^*\} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$$
$$\mathbb{Q} = \{(a/b) \mid a, b \in \mathbb{Z} \land b \neq 0\}$$

with $\mathbb{Z}$ the set of integers and $\mathbb{Q}$ the set of rational numbers. The remarkable insight of Cantor is that even though $\mathbb{Z}$ and $\mathbb{Q}$ contain "more numbers" than $\mathbb{N}$, in the sense that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$, from the standpoint of cardinality, we can show that $\mathbb{Z} \sim \mathbb{N}$ and $\mathbb{Q} \sim \mathbb{N}$. Equivalently, we can show that

$$\begin{cases} \mathbb{Z} \text{ countably infinite} \\ \mathbb{Q} \text{ countably infinite} \end{cases}$$

▶ <u>$\mathbb{R}$ is uncountable</u>

With some additional theory we can show that the set $\mathbb{R}$ of all real numbers satisfies the following statements:

$$\begin{cases} \mathbb{R} \text{ is uncountable} \\ \mathbb{R} \sim \mathcal{P}(\mathbb{N}) \end{cases}$$

Proof of $\mathbb{Z} \sim \mathbb{N}$ ($\mathbb{Z}$ is countably infinite)

We define the mapping $f: \mathbb{Z} \to \mathbb{N}$ such that

$$\forall x \in \mathbb{Z} : f(x) = \begin{cases} 2x-1 &, \text{if } x>0 \\ -2x &, \text{if } x \leq 0 \end{cases}$$

and note that

$$f = \{(0,0), (1,1), (-1,2), (2,3), (-2,4), (3,5), (-3,6), \ldots\}$$

which indicates that f is a bijection. To prove that, we show that f is one-to-one and that f is onto.

- <u>one-to-one</u>: Sufficient to show that

$$\forall x_1, x_2 \in \mathbb{Z} : (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$$

Let $x_1, x_2 \in \mathbb{Z}$ be given and assume that $f(x_1) = f(x_2)$.

We distinguish between the following cases.

<u>Case 1</u>: Assume that $f(x_1) = -2x_1$ and $f(x_2) = -2x_2$. Then,

$$f(x_1) = f(x_2) \Rightarrow -2x_1 = -2x_2 \Rightarrow x_1 = x_2.$$

<u>Case 2</u>: Assume that $f(x_1) = 2x_1 - 1$ and $f(x_2) = 2x_2 - 1$. Then

$$f(x_1) = f(x_2) \Rightarrow 2x_1 - 1 = 2x_2 - 1 \Rightarrow 2x_1 = 2x_2 \Rightarrow x_1 = x_2$$

<u>Case 3</u>: Assume that $f(x_1) = 2x_1 - 1$ and $f(x_2) = -2x_2$. Then

$$f(x_1) = f(x_2) \Rightarrow 2x_1 - 1 = -2x_2 \Rightarrow 2x_1 + 2x_2 = 1 \Rightarrow$$
$$\Rightarrow 2(x_1 + x_2) = 1 \Rightarrow x_1 + x_2 = 1/2$$

This is a contradiction, because

$$x_1, x_2 \in \mathbb{Z} \Rightarrow x_1 + x_2 \in \mathbb{Z} \Rightarrow x_1 + x_2 \neq 1/2$$

therefore case 3 does not materialize.

From the above cases we conclude that $x_1 = x_2$ and therefore:

$$\forall x_1, x_2 \in \mathbb{Z} : (f(x_1) = f(x_2) \Rightarrow x_1 = x_2) \qquad (1)$$

• <u>Onto:</u> Sufficient to show that $\forall y \in \mathbb{N} : \exists x \in \mathbb{Z} : f(x) = y$.
Let $\underline{y \in \mathbb{N}}$ be given. From the division theorem we have:
$\exists k \in \mathbb{N} : (y = 2k \lor y = 2k+1)$
Choose a $k \in \mathbb{N}$ such that $y = 2k \lor y = 2k+1$ and distinguish between the following cases.
<u>Case 1</u>: Assume that $y = 2k$. Then:

$$k \in \mathbb{N} \Rightarrow k \geq 0 \Rightarrow -k \leq 0 \Rightarrow f(-k) = -2(-k) = 2k = y \Rightarrow$$
$$\Rightarrow \underline{\exists x \in \mathbb{Z} : f(x) = y} \quad (\text{for } x = -k)$$

<u>Case 2</u>: Assume that $y = 2k+1$. Then:

$$k \in \mathbb{N} \Rightarrow k \geq 0 \Rightarrow k+1 > 0 \Rightarrow$$
$$\Rightarrow f(k+1) = 2(k+1) - 1 = 2k+2-1 = 2k+1 = y \Rightarrow$$
$$\Rightarrow \underline{\exists x \in \mathbb{Z} : f(x) = y.} \quad (\text{for } x = k+1)$$

From the above argument, in all cases, we find that

$$(\forall y \in \mathbb{N} : \exists x \in \mathbb{Z} : f(x) = y) \Rightarrow \forall y \in \mathbb{N} : y \in f(\mathbb{Z}) \Rightarrow$$
$$\Rightarrow \mathbb{N} \subseteq f(\mathbb{Z}) \Rightarrow$$
$$\Rightarrow f(\mathbb{Z}) = \mathbb{N} \quad (2)$$

From Eq. (1) and Eq. (2).

$$\begin{cases} \forall x_1, x_2 \in \mathbb{Z} : (f(x_1) = f(x_2) \Rightarrow x_1 = x_2) \\ f(\mathbb{Z}) = \mathbb{N} \end{cases} \Rightarrow$$
$$\Rightarrow \begin{cases} f \text{ one-to-one} \\ f \text{ onto} \end{cases} \Rightarrow f : \mathbb{Z} \to \mathbb{N} \text{ bijection}$$
$$\Rightarrow \mathbb{Z} \sim \mathbb{N} \Rightarrow \mathbb{Z} \text{ countably infinite.}$$

Sketch of proof that $\mathbb{Q} \sim \mathbb{N}$

A bijection $f: \mathbb{Q} \to \mathbb{N}$ can be constructed via the process of diagonalization, originally proposed by Cantor. We will explain this process and the overall argument informally, for the sake of clarity. We sequence the rational numbers using the diagonalizing pattern shown in the table below, making sure to skip any numbers previously encountered in an equivalent fractional representation:

	0	1	2	3	4	...
1	0/1	1/1	2/1	3/1	4/1	...
2	0/2	1/2	2/2	3/2	4/2	...
3	0/3	1/3	2/3	3/3	4/3	...
4	0/4	1/4	2/4	3/4	4/4	...
5	0/5	...	...	...	...	
⋮	⋮					

Consequently, we sequence the rational numbers of $\mathbb{Q}$ as follows:

$\underline{0/1}$, $\underline{1/1}$, $0/2$, $\underline{2/1}$, $\underline{1/2}$, $0/3$, $\underline{3/1}$, $2/2$, $\underline{1/3}$, $0/4$, $\underline{4/1}$, $\underline{3/2}$, $\underline{2/3}$, $\underline{1/4}$, $0/5$, etc.

where we have underlined all rational numbers that appear for the first time and thus are not being skipped. We can thus define a bijection $f: \mathbb{Z} \to \mathbb{Q}$

with the initial assignments:

$f(0) = 0/1 = 0$ $\quad$ $f(4) = 3/1$ $\quad$ $f(8) = 2/3$

$f(1) = 1/1 = 1$ $\quad$ $f(5) = 1/3$ $\quad$ $f(9) = 1/4$

$f(2) = 2/1 = 2$ $\quad$ $f(6) = 4/1$

$f(3) = 1/2$ $\quad$ $f(7) = 3/2$ $\quad$ etc.

The algorithm for generating this bijection is as follows:

for $a = 0, 1, 2, 3, 4, \ldots$
  for $b = 0, 1, 2, \ldots, a$
    if it has not occured previously then add
    the number $(a-b)/(b+1)$ to the sequence.
  end for
end for.

To account for negative rational numbers, we extend the definition by the algorithm above as follows:

$\forall x \in \mathbb{N}^* : f(-x) = -f(x)$

and that completes the bijection $f : \mathbb{Z} \to \mathbb{Q}$. Skipping numbers that occured previously ensures that f is one-to-one. It is also clear that any rational number will be reached by this algorithm with a finite numbers of steps, which ensures that f is onto. Thus, it follows that

$f : \mathbb{Z} \to \mathbb{Q}$ bijection $\Rightarrow \mathbb{Q} \sim \mathbb{Z}$ [definition]

$\Rightarrow \mathbb{Q} \sim \mathbb{N}$ [via $\mathbb{Z} \sim \mathbb{N}$]

$\Rightarrow \mathbb{Q}$ countable $\quad \square$

EXAMPLE – APPLICATION

The following problem is also a necessary first step towards proving that $\mathbb{R}$ is uncountable.

Show that $\boxed{\mathbb{R} \sim (0,1)}$

Solution

Define $\forall x \in \mathbb{R} : f(x) = (1/2) + (1/\pi)\,\mathrm{Arctan}(x)$.

We will show that $f : \mathbb{R} \to (0,1)$ is a bijection.

- Onto : Sufficient to show $\begin{cases} \forall y \in f(\mathbb{R}) : y \in (0,1) \\ \forall y \in (0,1) : y \in f(\mathbb{R}) \end{cases}$

$(\Rightarrow)$: Let $y \in f(\mathbb{R})$ be given. Then

$y \in f(\mathbb{R}) \Rightarrow \exists x \in \mathbb{R} : f(x) = y$.

Choose $x_0 \in \mathbb{R}$ such that $f(x_0) = y$. Then,

$$-\pi/2 < \mathrm{Arctan}(x_0) < \pi/2 \Rightarrow$$

$$\Rightarrow -1/2 < (1/\pi)\,\mathrm{Arctan}(x_0) < 1/2 \Rightarrow$$

$$\Rightarrow 0 < (1/2) + (1/\pi)\,\mathrm{Arctan}(x_0) < 1 \Rightarrow$$

$$\Rightarrow 0 < f(x_0) < 1 \Rightarrow 0 < y < 1 \Rightarrow \underline{y \in (0,1)}$$

It follows that $\forall y \in f(\mathbb{R}) : y \in (0,1)$. (1)

$(\Leftarrow)$: Let $y \in (0,1)$ be given. Then, we note that

$$f(x) = y \Leftrightarrow (1/2) + (1/\pi)\,\mathrm{Arctan}(x) = y \Leftrightarrow$$

$$\Leftrightarrow (1/\pi)\,\mathrm{Arctan}(x) = y - 1/2$$

$$\Leftrightarrow \mathrm{Arctan}(x) = \pi(y - 1/2) \qquad (2)$$

and also that

$$y \in (0,1) \Rightarrow 0 < y < 1 \Rightarrow -1/2 < y - 1/2 < 1/2 \Rightarrow$$

$$\Rightarrow -\pi/2 < \pi(y - 1/2) < \pi/2 \Rightarrow \tan \text{ is defined at } \pi(y-1/2).$$

Now we can define $x_0 = \tan(\pi(y-1/2))$ and conclude that

$$\mathrm{Arctan}(x_0) = \mathrm{Arctan}(\tan(\pi(y-1/2))) = \pi(y-1/2) \overset{(2)}{\Longrightarrow}$$
$$\Rightarrow f(x_0) = y \Rightarrow \exists x \in \mathbb{R} : f(x) = y \Rightarrow$$
$$\Rightarrow \underline{y \in f(\mathbb{R})}$$

and therefore,

$$\forall y \in (0,1) : y \in f(\mathbb{R}) \qquad (3)$$

From Eq.(2) and Eq.(3):

$$\begin{cases} \forall y \in f(\mathbb{R}) : y \in (0,1) \\ \forall y \in (0,1) : y \in f(\mathbb{R}) \end{cases} \Rightarrow \begin{cases} f(\mathbb{R}) \subseteq (0,1) \\ (0,1) \subseteq f(\mathbb{R}) \end{cases} \Rightarrow f(\mathbb{R}) = (0,1)$$
$$\Rightarrow f \text{ onto.} \qquad (4)$$

- <u>One-to-one</u>

Let $\underline{x_1, x_2 \in \mathbb{R}}$ be given and assume that $\underline{f(x_1) = f(x_2)}$. Then,

$$f(x_1) = f(x_2) \Rightarrow (1/2) + (1/\pi)\mathrm{Arctan}(x_1) = (1/2) + (1/\pi)\mathrm{Arctan}(x_2) \Rightarrow$$
$$\Rightarrow (1/\pi)\mathrm{Arctan}(x_1) = (1/\pi)\mathrm{Arctan}(x_2) \Rightarrow$$
$$\Rightarrow \mathrm{Arctan}(x_1) = \mathrm{Arctan}(x_2) \Rightarrow$$
$$\Rightarrow \tan(\mathrm{Arctan}(x_1)) = \tan(\mathrm{Arctan}(x_2))$$
$$\Rightarrow \underline{x_1 = x_2}$$

and therefore, we have

$$\forall x_1, x_2 \in \mathbb{R} : (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$$
$$\Rightarrow f \text{ one-to-one} \qquad (5)$$

From Eq.(4) and Eq.(5):

$$\begin{cases} f \text{ onto} \\ f \text{ one-to-one} \end{cases} \Rightarrow f : \mathbb{R} \to (0,1) \text{ bijection} \Rightarrow \mathbb{R} \sim (0,1).$$

EXERCISES

(8) Learn the proofs for the following statements

a) $\mathbb{Z}$ is countable

b) $\mathbb{Q}$ is countable

c) $\mathbb{R} \sim (0,1)$

(9) Let A, B be two sets. Show that

A countable $\wedge$ B countable $\Rightarrow$ $A \cup B$ countable.

(10) Let A_a with $a \in \mathbb{N}$ be a set collection. Show that:

a) $(\forall a \in \mathbb{N} : A_a \text{ finite}) \Rightarrow \bigcup_{a \in \mathbb{N}} A_a$ countable

b) Use part (a) to show that

$(\forall a \in \mathbb{N} : A_a \sim \mathbb{N}) \Rightarrow \bigcup_{a \in \mathbb{N}} A_a \sim \mathbb{N}$

(11) Given 3 sets A, B, C show that the set equivalence satisfies the reflexive, symmetric, and transitive properties.

a) $A \sim A$

b) $A \sim B \Rightarrow B \sim A$

c) $A \sim B \wedge B \sim C \Rightarrow A \sim C$

(12) Let $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$ and consider the intervals

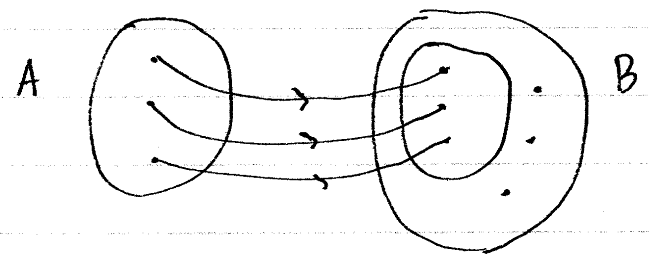
$$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$$

$[c,d] = \{x \in \mathbb{R} \mid c \leq x \leq d\}$

Construct a bijection to show that $[a,b] \sim [c,d]$.

Cardinality inequalities

If we can define a mapping $f: A \to B$ which is one-to-one but not necessarily onto, then from an intuitive standpoint the only conclusion that can be drawn is that either A, B are of "equal cardinality" or "B has greater cardinality than A", as illustrated by the following figure:



$\begin{cases} f \text{ one-to-one} \\ f \text{ not onto} \end{cases}$

Consequently, we propose the following definitions:

$$\boxed{\begin{array}{l} A \leqslant B \iff \exists f \in \mathrm{Map}(A,B) : f \text{ one-to-one} \\ A < B \iff A \leqslant B \wedge A \nsim B \end{array}}$$

Note that it is easy to show that:

$$A \sim B \wedge B \sim C \Rightarrow A \sim C$$
$$A \leqslant B \wedge B \leqslant C \Rightarrow A \leqslant C$$
$$A \subseteq B \Rightarrow A \leqslant B$$

which are left as homework problems. Starting from Cantor, the following two major theorems will be used to show that $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$ and $\mathbb{R}$ uncountable.

① → Cantor's theorem

Thm: For any set A, $A < \mathcal{P}(A)$

Proof

Define $f_0 : A \to \mathcal{P}(A)$ such that $\forall x \in A : f_0(x) = \{x\}$. Then:

$\forall x_1, x_2 \in A : (\{x_1\} = \{x_2\} \Rightarrow x_1 = x_2) \Rightarrow$

$\Rightarrow \forall x_1, x_2 \in A : (f_0(x_1) = f_0(x_2) \Rightarrow x_1 = x_2)$

$\Rightarrow f_0$ one-to-one $\Rightarrow$

$\Rightarrow \exists f \in \mathrm{Map}(A, \mathcal{P}(A)) : f$ one-to-one (for $f = f_0$)

$\Rightarrow A \leqslant \mathcal{P}(A)$. (1)

To show that $A \not\sim \mathcal{P}(A)$, assume that $A \sim \mathcal{P}(A)$. Then

$A \sim \mathcal{P}(A) \Rightarrow \exists f \in \mathrm{Map}(A, \mathcal{P}(A)) : f$ bijection

Choose an $f \in \mathrm{Map}(A, \mathcal{P}(A))$ such that ~~fis~~ $f : A \to \mathcal{P}(A)$ is a bijection. We define a set of "bad elements"

$B = \{x \in A \mid x \notin f(x)\} \subseteq A \Rightarrow B \in \mathcal{P}(A)$.

and note that

f bijection $\Rightarrow f$ onto $\Rightarrow f(A) = \mathcal{P}(A) \Rightarrow \mathcal{P}(A) \subseteq f(A)$

$\Rightarrow \forall y \in \mathcal{P}(A) : y \in f(A) \Rightarrow$

$\Rightarrow \forall y \in \mathcal{P}(A) : \exists x \in A : f(x) = y$

Let $y = B$ and choose a $b \in A$ such that $f(b) = B$.

We distinguish between the following cases.

Case 1: Assume that $b \in B$. Then

$b \in B \Rightarrow b \in \{x \in A \mid x \notin f(x)\} \Rightarrow$

$\Rightarrow b \in A \wedge b \notin f(b) \Rightarrow b \notin f(b) \Rightarrow b \notin B$

which is a contradiction, therefore case 1 does not materialize.

Case 2 : Assume that $b \notin B$. We also now, by definition, that $b \in A$, and therefore:

$$\begin{cases} b \in A \\ b \notin B \end{cases} \Rightarrow \begin{cases} b \in A \\ b \notin f(b) \end{cases} \Rightarrow b \in \{x \in A \mid x \notin f(x)\} \Rightarrow$$

$$\Rightarrow b \in B$$

which is also a contradiction.

Since none of the possible cases materialize, it follows that $A \not\sim \mathcal{P}(A)$. (2)

From Eq.(1) and Eq.(2):

$$\begin{cases} A \not\sim \mathcal{P}(A) \\ A \leqslant \mathcal{P}(A) \end{cases} \Rightarrow A < \mathcal{P}(A).$$

2 → Schroeder – Bernstein theorem

> Thm : Let A, B be two sets. Then
> $$A \leq B \land B \leq A \Rightarrow A \sim B$$

Proof

Assume that $A \leq B$ and $B \leq A$. Then

$$\begin{cases} A \leq B \\ B \leq A \end{cases} \Rightarrow \begin{cases} \exists f \in \text{Map}(A,B) : f \text{ one-to-one} \\ \exists g \in \text{Map}(B,A) : g \text{ one-to-one} \end{cases} \quad (1)$$

Choose $f \in \text{Map}(A,B)$ and $g \in \text{Map}(B,A)$ such that f, g are one-to-one.

Define $C_0 = A - g(B)$ and distinguish between the following two cases.

Case 1 : Assume that $C_0 = \emptyset$. By construction, we have $g \in \text{Map}(B,A) \Rightarrow g(B) \subseteq A$.

We will show that $A \subseteq g(B)$. $\quad (2)$

Let $x \in A$ be given. To show that $x \in g(B)$, assume that $x \notin g(B)$ in order to derive a contradiction. It follows that

$$\begin{cases} x \in A \\ x \notin g(B) \end{cases} \Rightarrow x \in A - g(B) \Rightarrow x \in C_0 \Rightarrow x \in \emptyset$$

which is a contradiction. We conclude that $\underline{x \in g(B)}$

We have thus shown that

$$\forall x \in A : x \in g(B) \Rightarrow A \subseteq g(B) \quad (3)$$

From Eq. (1), Eq. (2), Eq. (3) we conclude that:

$$\begin{cases} A \subseteq g(B) \wedge g(B) \subseteq A \\ g \text{ one-to-one} \end{cases} \Rightarrow \begin{cases} g(B) = A \\ g \text{ one-to-one} \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} g \text{ onto} \\ g \text{ one-to-one} \end{cases} \Rightarrow g : B \to A \text{ bijection}$$

$$\Rightarrow B \sim A \Rightarrow \underline{A \sim B}.$$

<u>Case 2</u> : Assume that $C_0 \neq \emptyset$. Then we define by recursion

$$\forall n \in \mathbb{N} : C_{n+1} = g(f(C_n)) = g(\{f(x) \mid x \in C_n\}) =$$
$$= \{g(f(x)) \mid x \in C_n\}$$

We construct the needed bijection $h : A \to B$ by the following definition:

$$\forall x \in A : h(x) = \begin{cases} f(x) & , \text{ if } \exists n \in \mathbb{N} : x \in C_n \\ g^{-1}(x) & , \text{ if } \forall n \in \mathbb{N} : x \notin C_n \end{cases}$$

Since we do not know if g is a bijection, we need to prove that $A - \bigcup_{n \in \mathbb{N}} C_n \subseteq g(B)$ to ensure that $g^{-1}(x)$ has a unique evaluation.

To show the claim, let $x \in A - \bigcup_{n \in \mathbb{N}} C_n$ be given. Then:

$$x \in A - \bigcup_{n \in \mathbb{N}} C_n \Rightarrow x \in A \wedge x \notin \bigcup_{n \in \mathbb{N}} C_n \Rightarrow x \notin \bigcup_{n \in \mathbb{N}} C_n \Rightarrow$$

$$\Rightarrow \overline{\exists n \in \mathbb{N} : x \in C_n} \Rightarrow$$
$$\Rightarrow \forall n \in \mathbb{N} : x \notin C_n \Rightarrow x \notin C_0.$$

To show that $x \in g(B)$, assume that $x \notin g(B)$. Then

$$\begin{cases} x \in A \\ x \notin g(B) \end{cases} \Rightarrow x \in A - g(B) \Rightarrow x \in C_0$$

which is a contradiction, since we previously showed that $x \notin C_0$.

We conclude that

$$\forall x \in A - \bigcup_{n \in \mathbb{N}} C_n : x \in g(B) \Rightarrow A - \bigcup_{n \in \mathbb{N}} C_n \subseteq g(B)$$

which proves the claim.

• We will show that <u>h is one-to-one.</u>

Let <u>$x_1, x_2 \in A$</u> be given and assume that <u>$h(x_1) = h(x_2)$.</u>

We distinguish between the following subcases.

<u>Case A</u>: Assume that $\begin{cases} \exists n \in \mathbb{N} : x_1 \in C_n \\ \exists n \in \mathbb{N} : x_2 \in C_n \end{cases}$

Then $h(x_1) = h(x_2) \Rightarrow f(x_1) = f(x_2)$ [definition of h]

$\Rightarrow \underline{x_1 = x_2}$ [f one-to-one]

<u>Case B</u>: Assume that $\begin{cases} \forall n \in \mathbb{N} : x_1 \notin C_n \\ \forall n \in \mathbb{N} : x_2 \notin C_n \end{cases}$. Then,

$h(x_1) = h(x_2) \Rightarrow g^{-1}(x_1) = g^{-2}(x_2) \Rightarrow$ [definition of h]

$\Rightarrow g(g^{-1}(x_1)) = g(g^{-1}(x_2)) \Rightarrow$

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

<u>Case C</u>: Assume that $\begin{cases} \exists n \in \mathbb{N} : x_1 \in C_n \\ \forall n \in \mathbb{N} : x_2 \notin C_n \end{cases}$

Choose $n_0 \in \mathbb{N}$ such that $x_1 \in C_{n_0}$. We note that

$$\begin{cases} x_2 \in A \\ \forall n \in \mathbb{N} : x_2 \notin C_n \end{cases} \Rightarrow x_2 \in A - \bigcup_{n \in \mathbb{N}} C_n \Rightarrow g^{-1}(x_2) \text{ is defined}$$

and therefore:

$x_2 = g(g^{-1}(x_2))$

$= g(h(x_2))$ [Definition of h(x) - 2nd case]

$= g(h(x_1))$ [Hypothesis $h(x_1) = h(x_2)$]

$= g(f(x_1))$ [Definition of h(x) - 1st case]

$\Rightarrow \exists x \in C_{n_0} : g(f(x)) = x_2 \Rightarrow$

$\Rightarrow x_2 \in \{g(f(x)) \mid x \in C_{n_0}\}$

$\Rightarrow x_2 \in g(f(C_{n_0}))$

$\Rightarrow x_2 \in C_{n_0+1}$

This is a contradiction because

$(\forall n \in \mathbb{N} : x_2 \notin C_n) \Rightarrow x_2 \notin C_{n_0+1}$

therefore Case C does not materialize. In all of the above cases we conclude that $x_1 = x_2$ and therefore:

$\forall x_1, x_2 \in A : (h(x_1) = h(x_2) \Rightarrow x_1 = x_2)$

$\Rightarrow h$ one-to-one. (4)

•2 We will show that $h(A) = B$.

By definition, we have $h(A) \subseteq B$, so it is sufficient to show that $\forall y \in B : y \in h(A)$. Let $y \in B$ be given. We distinguish between the following cases.

Case 1 : Assume that $\exists n \in \mathbb{N} : y \in f(C_n)$.

Choose $n_0 \in \mathbb{N}$ such that $y \in f(C_{n_0})$. Since

$$
\begin{aligned}
h(C_{n_0}) &= \{h(x) \mid x \in C_{n_0}\} \\
&= \{f(x) \mid x \in C_{n_0}\} \quad [\text{Definition of } h(x) - 1\text{st case}] \\
&= f(C_{n_0})
\end{aligned}
$$

it follows that

$$
\begin{aligned}
y \in f(C_{n_0}) &\Rightarrow y \in h(C_{n_0}) \quad [\text{Because } h(C_{n_0}) = f(C_{n_0})] \\
&\Rightarrow y \in h(A) \quad [\text{because } C_{n_0} \subseteq A]
\end{aligned}
$$

Case 2 : Assume that $\forall n \in \mathbb{N} : y \notin f(C_n)$.

We claim that $\forall n \in \mathbb{N} : g(y) \notin C_n$.

To show the claim, we note that:

$$\forall n \in \mathbb{N}: y \notin f(C_n) \Rightarrow \forall n \in \mathbb{N}: g(y) \notin g(f(C_n))$$
$$\Rightarrow \forall n \in \mathbb{N}: g(y) \notin C_{n+1}$$
$$\Rightarrow \forall n \in \mathbb{N}^*: g(y) \notin C_n \quad (5)$$

For $n=0$, to show that $g(y) \notin C_0$, we will assume that $g(y) \in C_0$ and derive a contradiction. Then:

$$g(y) \in C_0 \Rightarrow g(y) \in A - g(B)$$
$$\Rightarrow g(y) \in A \wedge g(y) \notin g(B)$$
$$\Rightarrow g(y) \notin g(B)$$

which is a contradiction because

$$y \in B \Rightarrow g(y) \in g(B)$$

It follows that $g(y) \notin C_0 \quad (6)$

From Eq.(5) and Eq.(6) we prove the claim. It follows that

$$h(g(y)) = g^{-1}(g(y)) \quad [\text{because } \forall n \in \mathbb{N}: g(y) \notin C_n]$$
$$= y \Rightarrow$$
$$\Rightarrow \exists x \in A: y = h(x) \quad (\text{for } x = g(y))$$
$$\Rightarrow \underline{y \in h(A)}$$

From the above argument we have:

$$\begin{cases} h(A) \subseteq B \\ \forall y \in B: y \in h(A) \end{cases} \Rightarrow \begin{cases} h(A) \subseteq B \\ B \subseteq h(A) \end{cases} \Rightarrow h(A) = B \Rightarrow \underline{h \text{ onto}} \quad (7)$$

From Eq.(4) and Eq.(7):

$$\begin{cases} h \text{ one-to-one} \\ h \text{ onto} \end{cases} \Rightarrow h: A \to B \text{ bijection}$$
$$\Rightarrow A \sim B \qquad \square$$

③ → Uncountability of $\mathbb{R}$

The Schroeder-Bernstein theorem can be used to derive the following characterization for the cardinality of $\mathbb{R}$:

$$\boxed{\mathbb{R} \sim \mathcal{P}(\mathbb{N})}$$

Once this result is established, we can use Cantor's theorem to argue that:

$$\begin{cases} \mathbb{R} \sim \mathcal{P}(\mathbb{N}) \\ \mathcal{P}(\mathbb{N}) > \mathbb{N} \end{cases} \Rightarrow \mathbb{R} > \mathbb{N} \Rightarrow \mathbb{R} \text{ uncountable}$$

The argument below uses the previous result that $\mathbb{R} \sim (0,1)$.

► Proof of $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$

It is sufficient to show that $\mathcal{P}(\mathbb{N}) \leqslant \mathbb{R} \wedge \mathbb{R} \leqslant \mathcal{P}(\mathbb{N})$.

•₁ Proof of $\mathcal{P}(\mathbb{N}) \leqslant \mathbb{R}$.

We define a mapping $f: \mathcal{P}(\mathbb{N}) \to [0,1]$ as follows.
Given $X \in \mathcal{P}(\mathbb{N})$ we define $f(X)$ via the expansion

$$f(X) = (0.a_0 a_1 a_2 \cdots)_{10} = \sum_{n=0}^{+\infty} a_n 10^{-n-1}$$

with

$$\forall n \in \mathbb{N}: \ a_n = \begin{cases} 1 & , \text{if } n \in X \\ 0 & , \text{if } n \notin X \end{cases}$$

To show that f is one-to-one, it is necessary to define it using a base representation that is greater than binary (i.e. base 2) while restricting the digits used to 0 and 1. This way, a number that terminates with an infinite sequence of 1s (e.g. 0.101111...) will not have an second alternate representation, as it would have in the binary system. We may therefore now argue as follows: Let $X_1, X_2 \in \mathcal{P}(\mathbb{N})$ be given and assume that $f(X_1) = f(X_2)$. Define the sequences (a_n) and (b_n) via the decimal representations:

$$f(X_1) = 0.a_0 a_1 a_2 \dots = \sum_{n=0}^{+\infty} a_n \cdot 10^{-n-1}$$

$$f(X_2) = 0.b_0 b_1 b_2 \dots = \sum_{n=0}^{+\infty} b_n \cdot 10^{-n-1}$$

We note that

$$f(X_1) = f(X_2) \Rightarrow 0.a_0 a_1 a_2 \dots = 0.b_0 b_1 b_2 \dots \Rightarrow$$
$$\Rightarrow \forall n \in \mathbb{N} : a_n = b_n.$$

We use this result to show that

$$\begin{aligned} n \in X_1 &\Leftrightarrow a_n = 1 && [\text{definition of } a_n] \\ &\Leftrightarrow b_n = 1 && [\text{via } a_n = b_n] \\ &\Leftrightarrow n \in X_2 && [\text{definition of } b_n] \end{aligned}$$

It follows that $\underline{X_1 = X_2}$. We have thus shown that

$$\forall X_1, X_2 \in \mathcal{P}(\mathbb{N}) : (f(X_1) = f(X_2) \Rightarrow X_1 = X_2)$$
$$\Rightarrow f \text{ one-to-one} \Rightarrow \mathcal{P}(\mathbb{N}) \preccurlyeq [0,1]$$

We also have: $[0,1] \subseteq \mathbb{R} \Rightarrow [0,1] \preccurlyeq \mathbb{R}$

and therefore

$$\left\{\begin{array}{l} \mathcal{P}(\mathbb{N}) \leqslant [0,1] \\ [0,1] \leqslant \mathbb{R} \end{array}\right. \Rightarrow \underline{\mathcal{P}(\mathbb{N}) \leqslant \mathbb{R}}. \qquad (1)$$

•₂ Proof of $\mathbb{R} \leqslant \mathcal{P}(\mathbb{N})$.

We define a mapping $g : [0,1] \to \mathcal{P}(\mathbb{N})$ as follows.
Let $x \in [0,1]$ be given with binary representation

$$x = (0.a_0 a_1 a_2 \cdots)_2 = \sum_{n=0}^{+\infty} a_n 2^{-n-1}$$

To ensure uniqueness, we do not allow terminating the binary representation of x with an infinite sequence of 1s except for $x = 1$ (represented as $x = (0.1111\cdots)_2$)
Define $g(x) = \{n \in \mathbb{N} \mid a_n = 1\}$
Let $\underline{x_1, x_2 \in [0,1]}$ be given and assume that $\underline{g(x_1) = g(x_2)}$.
Define the sequences (a_n) and (b_n) via the unique binary representations (as explained above)

$$x_1 = (0.a_0 a_1 a_2 \cdots)_2$$
$$x_2 = (0.b_0 b_1 b_2 \cdots)_2$$

To show that $x_1 = x_2$, we assume that $x_1 \neq x_2$ and derive a contradiction. Then, we have

$$\begin{aligned} x_1 \neq x_2 &\Rightarrow \underline{(0.a_0 a_1 a_2 \cdots)_2} \neq (0.b_0 b_1 b_2 \cdots)_2 \\ &\Rightarrow \overline{\forall n \in \mathbb{N} : a_n = b_n} \\ &\Rightarrow \exists n \in \mathbb{N} : a_n \neq b_n \end{aligned}$$

Choose $n_0 \in \mathbb{N}$ such that $a_{n_0} \neq b_{n_0}$. It follows that

$$a_{n_0} \neq b_{n_0} \Rightarrow \left\{\begin{array}{l} a_{n_0} = 1 \\ b_{n_0} = 0 \end{array}\right. \veebar \left\{\begin{array}{l} a_{n_0} = 0 \\ b_{n_0} = 1 \end{array}\right. \Rightarrow$$

$$\Rightarrow \begin{cases} n_0 \in g(x_1) \\ n_0 \notin g(x_2) \end{cases} \veebar \begin{cases} n_0 \notin g(x_1) \\ n_0 \in g(x_2) \end{cases} \Rightarrow$$

$$\Rightarrow \underline{(\exists n \in g(x_1) : n \notin g(x_2))} \vee \underline{(\exists n \in g(x_2) : n \notin g(x_1))}$$

$$\Rightarrow \overline{(\forall n \in g(x_1) : n \in g(x_2))} \veebar \overline{(\forall n \in g(x_2) : n \in g(x_1))}$$

$$\Rightarrow g(x_1) \not\subseteq g(x_2) \veebar g(x_2) \not\subseteq g(x_1)$$

which is a contradiction because

$$g(x_1) = g(x_2) \Rightarrow \begin{cases} g(x_1) \subseteq g(x_2) \\ g(x_2) \subseteq g(x_1) \end{cases}$$

We have thus shown that $\underline{x_1 = x_2}$

From the above argument we have show that

$$\forall x_1, x_2 \in [0,1] : (g(x_1) = g(x_2) \Rightarrow x_1 = x_2)$$

$$\Rightarrow g \text{ one-to-one} \Rightarrow [0,1] \leqslant \mathcal{P}(\mathbb{N}).$$

and therefore:

$$\begin{aligned} \mathbb{R} &\sim (0,1) && [\text{previous result}] \\ &\leqslant [0,1] && [\text{via } (0,1) \subseteq [0,1]] \\ &\leqslant \mathcal{P}(\mathbb{N}) && [\text{above proof}] \end{aligned}$$

$$\Rightarrow \underline{\mathbb{R} \leqslant \mathcal{P}(\mathbb{N})} \qquad (2)$$

From Eq.(1) and Eq.(2) via the Schroeder-Bernstein theorem, it follows that

$$\begin{cases} \mathcal{P}(\mathbb{N}) \leqslant \mathbb{R} \\ \mathbb{R} \leqslant \mathcal{P}(\mathbb{N}) \end{cases} \Rightarrow \mathbb{R} \sim \mathcal{P}(\mathbb{N}). \qquad \square$$

EXERCISES

(13) Study the proofs for
a) The Cantor theorem
b) The Schroder – Bernstein theorem
c) The statement $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$.

(14) Use Exercise 9 and the previous results that $\mathbb{Q} \sim \mathbb{N}$ and $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$ to show that $\mathbb{R} - \mathbb{Q}$ (the set of irrational numbers) is uncountable.
(Hint: Use proof by contradiction)

(15) Show that, given 3 sets A, B, C, we have:
a) $A \preccurlyeq B \wedge B \preccurlyeq C \Rightarrow A \preccurlyeq C$
b) $(A \preccurlyeq B \preccurlyeq C \wedge A \sim C) \Rightarrow (B \sim C \wedge A \sim B)$
c) $A \sim B \wedge B \subseteq C \Rightarrow A \preccurlyeq C$.

(16) Consider the sets

$$\mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}$$
$$\mathbb{R}_-^* = \{x \in \mathbb{R} \mid x < 0\}$$

Use the Schroder – Bernstein theorem to show that $\mathbb{R} \sim \mathbb{R}_+^*$ and $\mathbb{R} \sim \mathbb{R}_-^*$
(Hint: The needed one-to-one mappings can be constructed using the exponential function)
(Another hint: It is sufficient to show $\mathbb{R}_+^* \succcurlyeq \mathbb{R}$ and $\mathbb{R}_-^* \succcurlyeq \mathbb{R}$).

(17) Use Exercise 16 to show that given two sets A, B we have:

$$A \sim \mathbb{R} \wedge B \sim \mathbb{R} \Rightarrow A \cup B \sim \mathbb{R}.$$

(Hint: Distinguish between the following cases. For case 1 assume that $A \cap B = \emptyset$. For Case 2 assume that $A \cap B \neq \emptyset$. Define $B_1 = B - A$, show that $A \cup B = A \cup B_1$ and use Case 1 and the Schroeder–Bernstein theorem to show that $A \cup B_1 \sim \mathbb{R}$).

(18) Use the Schoeder–Bernstein theorem to show that $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$.

(Hint: Use binary or decimal representations to show that $[0,1] \times [0,1] \sim [0,1]$ by defining one-to-one mappings $f : [0,1] \times [0,1] \to [0,1]$ and $g : [0,1] \to [0,1] \times [0,1]$. Then uplift this result to the statement $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$)

Cardinal numbers

- To introduce the concept of cardinality and cardinal numbers, we note first that

$$\forall n, m \in \mathbb{N}^*: \left(\begin{cases} A \sim [n] \\ A \sim [m] \end{cases} \Rightarrow n = m \right)$$

Thus, for finite sets A, we can define a unique integer $|A|$ such that $A \sim [|A|]$.

- $|A|$ is the number of elements in A and we call it the cardinality of A.
- Cantor proposed introducing "transfinite cardinal numbers" to denote the cardinality $|A|$ of infinite sets. A key requirement of this cardinal number arithmetic is that it should satisfy:

$$A \sim B \Leftrightarrow |A| = |B|$$
$$A \lesssim B \Leftrightarrow |A| \leq |B|$$
$$A \lnsim B \Leftrightarrow |A| < |B|$$

The Schroeder-Bernstein theorem ensures self-consistent behaviour of inequalities in cardinal arithmetic.

- Since $\mathbb{N} \sim \mathbb{Z} \sim \mathbb{Q}$, Cantor introduced the cardinal number $\aleph_0$ to represent the cardinality of countably infinite sets. Consequently, we may write

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$$

- Aleph sequence: Cantor proposed defining a sequence of cardinalities $\aleph_1, \aleph_2, \aleph_3, \ldots$ as follows.

Let $\mathbb{V}$ be the set of <u>all sets that</u> exist. We define:

$|A| = \aleph_1 \iff \forall B_1 \in \mathbb{V} : \overline{\mathbb{N} < B_1 < A}$

$|A| = \aleph_2 \iff \forall B_1, B_2 \in \mathbb{V} : \overline{\mathbb{N} < B_1 < B_2 < A}$

$|A| = \aleph_3 \iff \forall B_1, B_2, B_3 \in \mathbb{V} : \overline{\mathbb{N} < B_1 < B_2 < B_3 < A}$

etc.

- <u>Beth sequence</u> : Another sequence of cardinal numbers is thee beth sequence. It is based on the Cantor theorem that tells us that $A < \mathcal{P}(A)$. The beth sequence is defined as follows:

  $\beth_0 = \aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$

  $\beth_1 = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$

  $\beth_2 = |\mathcal{P}(\mathcal{P}(\mathbb{N}))|$

  $\beth_3 = |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|$

  etc.

- <u>Continuum hypothesis</u> : With the above definitions, Cantor posed the question of whether the aleph and beth sequences coincide. This leads to two questions:

a) Continuum Hypothesis: The claim that $\beth_1 = \aleph_1$.

b) General Continuum Hypothesis: The claim that $\beth_a = \aleph_a$ for all a.

It was later found that these hypotheses are undecidable, i.e. it can neither be proved true or false. The underlying problem is that for the case of infinite sets, the mechanism for generating the powerset $\mathcal{P}(A)$ of an infinite set A is not precisely given. As a result, we have no way of deducing the correct "size" of $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, etc.

References

The following references were consulted during the preparation of these lecture notes.

(1) P.B. Bhattacharya and S.K. Jain and S.R. Naaul (1994), "Basic abstract algebra", 2nd ed.,Cambridge University Press
(2) G. Chartrand, A.D. Polimeni, and P. Zhang (2003), "Mathematical Proofs: A Transition to Advanced Mathematics", Addison-Wesley.
(3) A. Pistofides (1989), "Algebra. II", unpublished lecture notes.
(4) D.A. Santos (2007), "Number theory", unpublished lecture notes.
(5) E. Zakon (1973), "Basic concepts of mathematics", The Trillia Group

Lecture notes by Pistofides are available for download at

http://www.math.utpa.edu/lf/OGS/pistofides.html

Lecture notes by Santos are available for download at

http://faculty.ccp.edu/faculty/dsantos/lecture_notes.html