Lecture Notes in Foundations of Mathematics

Dr. Abdullah Al-Azemi

Mathematics Department
Kuwait University

June 1, 2023

Contents

Chapter

1 Logic and Proofs

Section 1.1: Propositions and Connectives

Definition 1.1.1

A **proposition P** is a sentence which is either true **T** or false **F**. That is, the truth values of propositions are **T** or **F**.

Example 1.1.1

Consider the following sentences:

- Propositions:

  a) $\frac{1}{2}$ is a rational number. [**T**].

  b) $2 + 4 = 1$. [**F**].

- Not propositions:

  c) How are you doing? [not a proposition].

  d) $x^2 = 36$. [where is x coming from?].

  e) This sentence is false. [depends on the given sentence!].

The previous propositions studied in *a* and *b* are called **simple** propositions. **Compound** propositions can be formed by **connectives** with simple propositions. For example,

Compound proposition: $1 + 2 = 5$ "and" the sun is made of an orange.

Definition 1.1.2

Let **P** and **Q** be two propositions. Then,

1. the **conjunction** of **P** and **Q**, denoted by $\mathbf{P} \wedge \mathbf{Q}$, is the proposition "**P** and **Q**". $\mathbf{P} \wedge \mathbf{Q}$ is true exactly when both **P** and **Q** are true.

2. the **disjunction** of $\mathbf{P}$ and $\mathbf{Q}$, denoted by $\mathbf{P} \vee \mathbf{Q}$, is the proposition "$\mathbf{P}$ or $\mathbf{Q}$". $\mathbf{P} \vee \mathbf{Q}$ is true exactly when at least one of $\mathbf{P}$ or $\mathbf{Q}$ is true.
3. the **negation** of $\mathbf{P}$, denoted by $\sim \mathbf{P}$, is the proposition "not $\mathbf{P}$". $\sim \mathbf{P}$ is true exactly when $\mathbf{P}$ is false.

Example 1.1.2

Let $\mathbf{P}$ be "Kuwait is an island" and let $\mathbf{Q}$ be "Sea water contains salt". Discuss $\mathbf{P} \wedge \mathbf{Q}$, $\mathbf{P} \vee \mathbf{Q}$, and $\sim \mathbf{P}$.

Solution:

It is clear the $\mathbf{P}$ is false and $\mathbf{Q}$ is true. Thus,

1. $\mathbf{P} \wedge \mathbf{Q}$: Kuwait is an island and sea water contains salt. [**F**].
2. $\mathbf{P} \vee \mathbf{Q}$: Kuwait is an island or sea water contains salt. [**T**].
3. $\sim \mathbf{P}$: It is not the case that Kuwait is an island. [**T**].

$\mathbf{P}$	$\mathbf{Q}$	$\mathbf{P} \wedge \mathbf{Q}$	$\mathbf{P} \vee \mathbf{Q}$	$\sim \mathbf{P}$	$\sim \mathbf{Q}$
T	**T**	**T**	**T**	**F**	**F**
T	**F**	**F**	**T**	**F**	**T**
F	**T**	**F**	**T**	**T**	**F**
F	**F**	**F**	**F**	**T**	**T**

Definition 1.1.3

A **propositional form** is an expression involving finitely many propositions connected by connectives such as $\wedge$, $\vee$, and $\sim$.

Example 1.1.3

Let $\mathbf{P}$, $\mathbf{Q}$, and $\mathbf{R}$ be propositions. Write down the truth table of the propositional form $\big((\mathbf{P} \wedge \mathbf{Q}) \vee (\mathbf{P} \vee (\sim \mathbf{R}))\big)$.

Solution:

$\mathbf{P}$	$\mathbf{Q}$	$\mathbf{R}$	$\sim \mathbf{R}$	$\mathbf{P} \wedge \mathbf{Q}$	$\mathbf{P} \vee (\sim \mathbf{R})$	$\big((\mathbf{P} \wedge \mathbf{Q}) \vee (\mathbf{P} \vee (\sim \mathbf{R}))\big)$
T	**T**	**T**	**F**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**	**T**	**T**
T	**F**	**T**	**F**	**F**	**T**	**T**
T	**F**	**F**	**T**	**F**	**T**	**T**
F	**T**	**T**	**F**	**F**	**F**	**F**
F	**T**	**F**	**T**	**F**	**T**	**T**
F	**F**	**T**	**F**	**F**	**F**	**F**
F	**F**	**F**	**T**	**F**	**T**	**T**

Definition 1.1.4

Two propositional forms $\mathbf{P}$ and $\mathbf{Q}$ are called **equivalent** if and only if their truth tables are identical. In that case, we write $\mathbf{P} \equiv \mathbf{Q}$.

Definition 1.1.5

A **denial** of a proposition $\mathbf{P}$ is any proposition equivalent to $\sim \mathbf{P}$.

A proposition $\mathbf{P}$ has only one negation "$\sim \mathbf{P}$", but it has many denials. For instance, $\sim \mathbf{P}$, $\sim\sim\sim \mathbf{P}$, and $\sim\sim\sim\sim\sim \mathbf{P}$ are all examples of denials. Note that $\sim(\sim \mathbf{P})$ is simply $\mathbf{P}$.

Example 1.1.4

Let $\mathbf{P}$ be "π is an irrational number". Find the negation of $\mathbf{P}$, and give some examples of denials of $\mathbf{P}$.

Solution:

- negation $\sim \mathbf{P}$: It is not the case that π is irrational.
- denials of $\mathbf{P}$: a. π is rational. b. π is the quotient of two integers r/s. c. π has a finite decimal expansion.

Note that since $\mathbf{P}$ is true, all of its denials are false.

Definition 1.1.6

A propositional form is called a **tautology** if it is true for all possible truth values of its components. It is called a **contradiction** if it is the negation of a tautology.

Example 1.1.5

Show that $\big((\mathbf{P} \vee \mathbf{Q}) \vee ((\sim \mathbf{P}) \wedge (\sim \mathbf{Q}))\big)$ is a tautology for any propositions **P** and **Q**.

Solution:

$\mathbf{P}$	$\mathbf{Q}$	$\sim \mathbf{P}$	$\sim \mathbf{Q}$	$\mathbf{P} \vee \mathbf{Q}$	$(\sim \mathbf{P}) \wedge (\sim \mathbf{Q})$	$\big((\mathbf{P} \vee \mathbf{Q}) \vee ((\sim \mathbf{P}) \wedge (\sim \mathbf{Q}))\big)$
T	**T**	**F**	**F**	**T**	**F**	**T**
T	**F**	**F**	**T**	**T**	**F**	**T**
F	**T**	**T**	**F**	**T**	**F**	**T**
F	**F**	**T**	**T**	**F**	**T**	**T**

Moreover, it can be seen that the negation of $\big((\mathbf{P} \vee \mathbf{Q}) \vee ((\sim \mathbf{P}) \wedge (\sim \mathbf{Q}))\big)$ is a contradiction.

Remark 1.1.1

The negation of a tautology is a contradiction, and the negation of a contradiction is a tautology.

Section 1.2: Conditionals and Biconditionals

Definition 1.2.1

Given two propositions $\mathbf{P}$ and $\mathbf{Q}$, the conditional sentence $\mathbf{P} \Rightarrow \mathbf{Q}$ (reads "$\mathbf{P}$ implies $\mathbf{Q}$") is the proposition "if $\mathbf{P}$, then $\mathbf{Q}$". In that case, $\mathbf{P}$ is called **antecedent** and $\mathbf{Q}$ is called **consequent**.

Remark 1.2.1

The proposition $\mathbf{P} \Rightarrow \mathbf{Q}$ is true whenever $\mathbf{P}$ is false or $\mathbf{Q}$ is true. In general, $\mathbf{P} \Rightarrow \mathbf{Q}$ is equivalent to $(\sim \mathbf{P}) \vee \mathbf{Q}$.

Example 1.2.1

Consider the following propositions:

a) if "x is an odd integer", then "$x + 1$ is an even integer". [**T**].

b) if "$2 + 1 = 0$", then "$1 + 1 = 0$". [**T**].

c) if "$1 - 1 = 0$", then "$2 + 9 = 1$". [**F**].

Definition 1.2.2

For propositions $\mathbf{P}$ and $\mathbf{Q}$, the **converse** of $\mathbf{P} \Rightarrow \mathbf{Q}$ is $\mathbf{Q} \Rightarrow \mathbf{P}$, and the **contrapositive** of $\mathbf{P} \Rightarrow \mathbf{Q}$ is $(\sim \mathbf{Q}) \Rightarrow (\sim \mathbf{P})$.

Theorem 1.2.1

For any propositions $\mathbf{P}$ and $\mathbf{Q}$, we have

(i) $\mathbf{P} \Rightarrow \mathbf{Q}$ is equivalent to $(\sim \mathbf{Q}) \Rightarrow (\sim \mathbf{P})$, and (ii) $\mathbf{P} \Rightarrow \mathbf{Q}$ is not equivalent to $\mathbf{Q} \Rightarrow \mathbf{P}$.

Proof:

We prove both results in the following truth table.

P	Q	$\sim$ P	$\sim$ Q	P $\Rightarrow$ Q	Q $\Rightarrow$ P	$\sim$ Q $\Rightarrow \sim$ P
T	T	F	F	T	T	T
T	F	F	T	F	T	F
F	T	T	F	T	F	T
F	F	T	T	T	T	T

Definition 1.2.3

Let **P** and **Q** be two propositions. The **biconditional** sentence **P** $\Leftrightarrow$ **Q** is "**P** if and only if (iff.) **Q**". **P** $\Leftrightarrow$ **Q** is true exactly when both **P** and **Q** have the same truth value.

Remark 1.2.2

The following phrases are translated as **P** $\Rightarrow$ **Q** for any propositions **P** and **Q**:

• if **P**, then **Q**.	• if $a > 5$, then $a > 3$.
• **P** implies **Q**.	• $a > 5$ implies $a > 3$.
• **P** is sufficient for **Q**.	• $a > 5$ is sufficient for $a > 3$.
• **P** only if **Q**.	• $a > 5$ only if $a > 3$
• **Q**, if **P**.	• $a > 3$, if $a > 5$.
• **Q** whenever **P**.	• $a > 3$ whenever $a > 5$.
• **Q** is necessary for **P**.	• $a > 3$ is necessary for $a > 5$.
• **Q**, when **P**.	• $a > 3$, when $a > 5$.

Remark 1.2.3

Moreover, the following phrases are translated as **P** $\Leftrightarrow$ **Q** for any propositions **P** and **Q**:

• **P** if and only if **Q**.	• $\|x\| = 2$ iff $x^2 = 4$.
• **P** if, but only if, **Q**.	• $\|x\| = 2$ if, but only if, $x^2 = 4$.
• **P** is equivalent to **Q**.	• $\|x\| = 2$ is equivalent to $x^2 = 4$.
• **P** is necessary and sufficient for **Q**.	• $\|x\| = 2$ is necessary and sufficient for $x^2 = 4$.

Theorem 1.2.2

Let $\mathbf{P}$, $\mathbf{Q}$, and $\mathbf{R}$ be propositions. Then,

a. $\mathbf{P} \Rightarrow \mathbf{Q} \equiv (\sim \mathbf{P}) \vee \mathbf{Q}$.

b. $\mathbf{P} \Leftrightarrow \mathbf{Q} \equiv (\mathbf{P} \Rightarrow \mathbf{Q}) \wedge (\mathbf{Q} \Rightarrow \mathbf{P})$.

c. $\sim (\mathbf{P} \wedge \mathbf{Q}) \equiv (\sim \mathbf{P}) \vee (\sim \mathbf{Q})$.

d. $\sim (\mathbf{P} \vee \mathbf{Q}) \equiv (\sim \mathbf{P}) \wedge (\sim \mathbf{Q})$.

e. $\sim (\mathbf{P} \Rightarrow \mathbf{Q}) \equiv \mathbf{P} \wedge (\sim \mathbf{Q})$.

f. $\sim (\mathbf{P} \wedge \mathbf{Q}) \equiv \mathbf{P} \Rightarrow (\sim \mathbf{Q})$.

g. $\mathbf{P} \wedge (\mathbf{Q} \vee \mathbf{R}) \equiv (\mathbf{P} \wedge \mathbf{Q}) \vee (\mathbf{P} \wedge \mathbf{R})$.

h. $\mathbf{P} \vee (\mathbf{Q} \wedge \mathbf{R}) \equiv (\mathbf{P} \vee \mathbf{Q}) \wedge (\mathbf{P} \vee \mathbf{R})$.

Proof:

b.

$\mathbf{P}$	$\mathbf{Q}$	$\mathbf{P} \Leftrightarrow \mathbf{Q}$	$\mathbf{P} \Rightarrow \mathbf{Q}$	$\mathbf{Q} \Rightarrow \mathbf{P}$	$(\mathbf{P} \Rightarrow \mathbf{Q}) \wedge (\mathbf{Q} \Rightarrow \mathbf{P})$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

g.

$\mathbf{P}$	$\mathbf{Q}$	$\mathbf{R}$	$\mathbf{Q} \vee \mathbf{R}$	$\mathbf{P} \wedge (\mathbf{Q} \vee \mathbf{R})$	$\mathbf{P} \wedge \mathbf{Q}$	$\mathbf{P} \wedge \mathbf{R}$	$(\mathbf{P} \vee \mathbf{Q}) \vee (\mathbf{P} \vee \mathbf{R})$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Section 1.3: Quantifiers

⋆ NOTATIONS:

- $\mathbb{N} = \{1, 2, 3, \cdots\}$ is the set of **natural numbers**.
- $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ is the set of **integer numbers**.
- $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0\}$ is the set of **rational numbers**.
- $\mathbb{R}$ is the set of **real numbers**.

The sentence $x \geq 5$ is not a proposition, unless we assign a value to x. It is an open sentence. In general, an open sentence with n variables is denoted by $P(x_1, x_2, \cdots, x_n)$. For example, the open sentence $P(x_1, x_2, x_3)$: "x_1 equals to $x_2 + x_3$" is an open sentence. On the other hand, $P(7, 3, 4)$ and $P(7, 2, 3)$ are propositions with true and false values, respectively.

Definition 1.3.1

The set of objects for which an open sentence is true is called the **truth set**, and is denoted by $\mathcal{T}$.
On the other hand, the set from where the objects can be taken from is called the **universe**, and is denoted by $\mathcal{U}$. In particular, two open sentences are said to be equivalent for a particular universe if and only if their truth sets are equal.

Example 1.3.1

Let $\mathcal{U} = \mathbb{N}$. Then, $P(x) : x + 3 > 7$ is equivalent to $Q(x) : x > 4$, since $\mathcal{T} = \{5, 6, 7, \cdots\}$ for both P and Q.
Also, $P(x) : x^2 = 4$ is equivalent to $Q(x) : x = 2$. However, if $\mathcal{U}$ was the set of all integers, then $P(x) : x^2 = 4$ with truth set $\{-2, 2\}$ is not equivalent to $Q(x) : x = 2$ with truth set $\{2\}$.

Definition 1.3.2

Let $\mathbf{P}(x)$ be an open sentence with variable $x \in \mathcal{U}$. Then,

a) The sentence "$(\forall x)\mathbf{P}(x)$" reads as "for all x, $\mathbf{P}(x)$". It is true iff $\mathcal{T} = \mathcal{U}$ for $\mathbf{P}(x)$. "$\forall$" is called the **universal quantifiers**.

b) The sentence "$(\exists x)\mathbf{P}(x)$" reads as "there exists x such that $\mathbf{P}(x)$". It is true iff $\mathcal{T} \neq \emptyset$ (the empty set). "$\exists$ is called the **existential quantifiers**.

c) The sentence "$(\exists! x)\mathbf{P}(x)$" reads as "there exists a unique x such that $\mathbf{P}(x)$". It is true iff $\mathcal{T}$ contains only one element. "$\exists!$ is called the **unique existential quantifiers**.

Example 1.3.2

Let $\mathcal{U} = \mathbb{R}$. Decide the truth value and the truth set for each of the following.

Solution:

Consider the following table where we different sentences along with its truth value as true or false and the corresponding truth set.

sentence	**T** or **F**	$\mathcal{T}$
a. $(\forall x)(x \geq 3)$	**F**	$[3, \infty)$.
b. $(\forall x)(\lvert x\rvert > 0)$	**F**	$\mathbb{R}\backslash\{0\}$.
c. $(\forall x)(x - 1 < x)$	**T**	$\mathbb{R}$.
d. $(\exists x)(x \geq 3)$	**T**	$[3, \infty)$.
e. $(\exists! x)(\lvert x\rvert = 0)$	**T**	$\{0\}$.
f. $(\exists! x)(\lvert x\rvert = 2)$	**F**	$\{-2, 2\}$.
g. $(\exists x)(x^2 = -4)$	**F**	$\emptyset$.
h. $(\exists x)(\exists y)(2x + y = 0 \wedge x - y = 1)$	**T**	$\{x = \frac{1}{3}, y = -\frac{2}{3}\}$.
i. $(\exists! x)(\exists! y)(2x + y = 0 \vee x - y = 1)$	**F**	$(x, y) \in \Big\{(0,0), (1,0), (3,2), \cdots\Big\}$.
j. $(\forall x)(\forall y)(x^2 + y^2 > 0)$	**F**	$\mathbb{R}^2\backslash(0,0)$.

Definition 1.3.3

Two quantified sentences are equivalent for a particular universe $\mathcal{U}$ iff they have the same truth set in $\mathcal{U}$. Two quantified sentences are equivalent iff they are equivalent in every universe.

For instance, $(\forall x)(\mathbf{P}(x) \wedge \mathbf{Q}(x))$ is equivalent to $(\forall x)(\mathbf{Q}(x) \wedge \mathbf{P}(x))$ and $(\forall x)[\mathbf{P}(x) \Rightarrow \mathbf{Q}(x)]$ is equivalent to $(\forall x)[\sim \mathbf{Q}(x) \Rightarrow \sim \mathbf{P}(x)]$.

Theorem 1.3.1

Let $\mathbf{P}(x)$ be an open sentence with a variable $x \in \mathcal{U}$ for some $\mathcal{U}$. Then,

a. $\sim (\forall x)[\mathbf{P}(x)]$ is equivalent to $(\exists x)[\sim \mathbf{P}(x)]$.

b. $\sim (\exists x)[\mathbf{P}(x)]$ is equivalent to $(\forall x)[\sim \mathbf{P}(x)]$.

Proof:

(a.) The sentence $\sim (\forall x)[\mathbf{P}(x)]$ is true iff $(\forall x)[\mathbf{P}(x)]$ is false iff the truth set for $\mathbf{P}(x)$ is not the entire universe, i.e. $\mathcal{T} \neq \mathcal{U}$ iff there exists an $x \in \mathcal{U}$ such that $\mathbf{P}(x)$ is false iff $(\exists x)[\sim \mathbf{P}(x)]$ is true.

(b.) The sentence $\sim (\exists x)[\mathbf{P}(x)]$ is true iff $(\exists x)[\mathbf{P}(x)]$ is false iff the truth set of $\mathbf{P}(x)$ is empty iff $(\forall x)[\sim \mathbf{P}(x)]$ is true.

Remark 1.3.1

Let $\mathbf{P}(x)$ be an open sentence with a variable $x \in \mathcal{U}$ for some $\mathcal{U}$. Then,

$$(\exists! x)\mathbf{P}(x) \equiv (\exists x)\Big[\mathbf{P}(x) \wedge (\forall y)[\mathbf{P}(y) \Rightarrow x = y]\Big].$$

Example 1.3.3

Find a denial (or the negation) for "$(\forall x)[\mathbf{P}(x) \Rightarrow \mathbf{Q}(x)]$".

Solution:

Using Theorem 1.3.1 and Theorem 1.2.2 (part e), we conclude

$$\sim (\forall x)[\mathbf{P}(x) \Rightarrow \mathbf{Q}(x)] \equiv (\exists x)[\sim (\mathbf{P}(x) \Rightarrow \mathbf{Q}(x))] \equiv (\exists x)[\mathbf{P}(x) \wedge (\sim \mathbf{Q}(x))].$$

Example 1.3.4

Find a denial (or the negation) for "$(\exists! x)\mathbf{P}(x)$".

Solution:

Using Remark 1.3.1 and Theorem 1.2.2, we conclude

$$\begin{aligned}
\sim (\exists! x)\mathbf{P}(x) &\equiv \sim (\exists x)\Big[\mathbf{P}(x) \wedge (\forall y)[\mathbf{P}(y) \Rightarrow x = y]\Big] \\
&\equiv (\forall x)\Big[\sim \Big(\mathbf{P}(x) \wedge (\forall y)[\mathbf{P}(y) \Rightarrow x = y]\Big)\Big] \\
&\equiv (\forall x)\Big[\sim \mathbf{P}(x) \vee \sim (\forall y)[\mathbf{P}(y) \Rightarrow x = y]\Big] \\
&\equiv (\forall x)\Big[\sim \mathbf{P}(x) \vee (\exists y) \sim [\mathbf{P}(y) \Rightarrow x = y]\Big] \\
&\equiv (\forall x)\Big[\sim \mathbf{P}(x) \vee (\exists y)[\mathbf{P}(y) \wedge \sim (x = y)]\Big] \\
&\equiv (\forall x)\Big[\sim \mathbf{P}(x) \vee (\exists y)[\mathbf{P}(y) \wedge x \neq y]\Big]
\end{aligned}$$

Example 1.3.5

Find a denial (or the negation) for

$$(\forall z)(\exists x)(\exists y)\Big[\Big((x > z) \wedge (y > z)\Big) \wedge \sim (\exists w)\Big(x + y < w < xz\Big)\Big]. \tag{1.3.1}$$

Solution:

Using Theorem1.3.1 and Theorem 1.2.2, we conclude

$$\begin{aligned}
\sim \text{Equation}(1.3.5) &\equiv \sim (\forall z)(\exists x)(\exists y)\Big[\Big((x > z) \wedge (y > z)\Big) \wedge \sim (\exists w)\Big(x + y < w < xz\Big)\Big] \\
&\equiv (\exists z)(\forall x)(\forall y) \sim \Big[\Big((x > z) \wedge (y > z)\Big) \wedge \sim (\exists w)\Big(x + y < w < xz\Big)\Big] \\
&\equiv (\exists z)(\forall x)(\forall y)\Big[\Big((x > z) \wedge (y > z)\Big) \Rightarrow \sim\sim (\exists w)\Big(x + y < w < xz\Big)\Big] \\
&\equiv (\exists z)(\forall x)(\forall y)\Big[\Big((x > z) \wedge (y > z)\Big) \Rightarrow (\exists w)\Big(x + y < w < xz\Big)\Big].
\end{aligned}$$

Example 1.3.6

Let $\mathcal{U} = \mathbb{R}$. Decide the truth value and the truth set for each of the following.

Solution:

sentence	**T** or **F**	$\mathcal{T}$
a. $(\forall y)(\exists x)[x + y = 0]$	**T**	for any y, $x = -y$ is a solution.
b. $(\exists x)(\forall y)[x + y = 0]$	**F**	given $x = 0$ not all $y \in \mathbb{R}$ is a solution.
c. $(\exists x)(\exists y)[x^2 + y^2 = 10]$	**T**	for $x \in \mathbb{R}$ there is $y = \sqrt{10 - x^2} \in \mathbb{R}$.
d. $(\forall y)(\exists x)(\forall z)[xy = xz]$	**T**	for any $y \in \mathbb{R}$, $x = 0$ for any $z \in \mathbb{R}$.
e. $(\forall y)(\exists! x)[x = y^2]$	**T**	for any $y \in \mathbb{R}$, $x = y^2$ is a solution.

Section 1.4: Mathematical Proofs

Definition 1.4.1

A **proof** is a justification of the truth of a given statement called theorem, proposition, claim, or lemma.

Remark 1.4.1

Tools of proofs: We may use any of the following:

- Axioms: Initial statements which are assumed to be true.
- Theorems: Some previously proved statement can be use.
- Assumptions: Assumed fact about the problem at hand.
- Tautologies: Examples follow:

a. $\mathbf{P} \vee (\sim \mathbf{P})$ .... (Excluded Middle).

b. $(\mathbf{P} \Rightarrow \mathbf{Q}) \Leftrightarrow (\sim \mathbf{Q} \Rightarrow \sim \mathbf{P})$ .... (Contrapositive).

c. $\left.\begin{array}{l} \mathbf{P} \vee (\mathbf{Q} \vee \mathbf{R}) \Leftrightarrow (\mathbf{P} \vee \mathbf{Q}) \vee \mathbf{R} \\ \mathbf{P} \wedge (\mathbf{Q} \wedge \mathbf{R}) \Leftrightarrow (\mathbf{P} \wedge \mathbf{Q}) \wedge \mathbf{R} \end{array}\right\}$ .... (Associativity).

d. $\left.\begin{array}{l} \mathbf{P} \wedge (\mathbf{Q} \vee \mathbf{R}) \Leftrightarrow (\mathbf{P} \wedge \mathbf{Q}) \vee (\mathbf{P} \wedge \mathbf{R}) \\ \mathbf{P} \vee (\mathbf{Q} \wedge \mathbf{R}) \Leftrightarrow (\mathbf{P} \vee \mathbf{Q}) \wedge (\mathbf{P} \vee \mathbf{R}) \end{array}\right\}$ .... (Distributivity).

e. $(\mathbf{P} \Leftrightarrow \mathbf{Q}) \Leftrightarrow [(\mathbf{P} \Rightarrow \mathbf{Q}) \wedge (\mathbf{Q} \Rightarrow \mathbf{P})]$ .... (Biconditional).

f. $\sim (\mathbf{P} \Rightarrow \mathbf{Q}) \Leftrightarrow (\mathbf{P} \wedge \sim \mathbf{Q})$ .... (Denial of Implication).

g. $\left.\begin{array}{l} \sim (\mathbf{P} \wedge \mathbf{Q}) \Leftrightarrow (\sim \mathbf{P} \vee \sim \mathbf{Q}) \\ \sim (\mathbf{P} \vee \mathbf{Q}) \Leftrightarrow (\sim \mathbf{P} \wedge \sim \mathbf{Q}) \end{array}\right\}$ .... (De Morgan's Laws).

h. $\mathbf{P} \Leftrightarrow [\sim \mathbf{P} \Rightarrow (\mathbf{Q} \wedge \sim \mathbf{Q})]$ .... (Contradiction).

i. $[(\mathbf{P} \Rightarrow \mathbf{Q}) \wedge (\mathbf{Q} \Rightarrow \mathbf{R})] \Leftrightarrow (\mathbf{P} \Rightarrow \mathbf{R})$ .... (Transitivity).

j. $[\mathbf{P} \wedge (\mathbf{P} \Rightarrow \mathbf{Q})] \Rightarrow \mathbf{Q}$ .... (Modus Ponens).

In what follows, we consdier different types of proof.

1.4.1 Type 1: Direct Proof

Direct proof $\mathbf{P} \Rightarrow \mathbf{Q}$: Assume $\mathbf{P}$, then $\cdots$ $\cdots$. Therefore, $\mathbf{Q}$.

Example 1.4.1

Let n be an integer. Show that if n is odd, then $n+1$ is even.

Solution:

Assume that $n = 2k+1$ for some integer k. Then, $n+1 = (2k+1)+1$. That is $n+1 = 2k+2 = 2(k+1)$. Therefore, $n+1$ is even.

Example 1.4.2

Assume that $\sin(x)$ is an odd funtion, i.e. $\sin(-x) = -\sin(x)$. Show that $f(x) = \sin^2(x)$ for any $x \in \mathbb{R}$ is an even function, i.e. $f(-x) = f(x)$.

Solution:

$f(-x) = (\sin(-x))^2 = (-\sin(x))^2 = \sin(x) = f(x)$. Therefore, $f(x)$ is an even function.

Theorem 1.4.1

Suppose that a, b, and c are integers. If a divides b and b divides c, then a divides c.

Proof:

Since a divides b $(a \mid b)$, then there is an integer k such that $b = ka$. Also, since $b \mid c$ there is an integer h such that $c = hb$. Thus, $c = hb = h(ka) = (hk)a$, and therefore $a \mid c$.

Theorem 1.4.2

Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid b \pm c$.

Proof:

Since $a \mid b$, $\exists k \in \mathbb{Z}$ such that $b = ka$, and since $a \mid c$, $\exists h \in \mathbb{Z}$ such that $c = ha$. Thus,

$$b \pm c = ka \pm ha = (k \pm h)a.$$

Therefore, $a \mid b \pm c$.

1.4.2 Type 2: Proof By Contradiction

Contradiction to proof **P**: Suppose $\sim$ **P**, then $\cdots\cdots$. Thus **Q**. Then, $\cdots\cdots$. Therefore, $\sim$ **Q**, contradiction.

This technique uses the tautology $\mathbf{P} \Leftrightarrow [\sim \mathbf{P} \Rightarrow (\mathbf{Q} \wedge \sim \mathbf{Q})]$.

Example 1.4.3

The equation $x^3 + x - 1 = 0$ has at most one real root.

Solution:

Let $f(x) = x^3 + x - 1$. Suppose that $f(x)$ has two real roots a and b, then $f(a) = f(b) = 0$. f is continuouse on $[a, b]$ and is differentiable on (a, b) since it is a polynomial. Then, by Rolle's Theorem, there is a $c \in (a, b)$ such that $f'(c) = 0$. But $f'(c) = 3c^2 + 1 \neq 0$ for all $c \in \mathbb{R}$. This is a contradiction. Therefore, f has at most one real root.

Remark 1.4.2

- Any square integer has an even number of 2's as prime factors.
- All natural number greater than 1 has a prime divisor $q > 1$.

Example 1.4.4

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

Solution:

Recall the fact that any square integer number has an even number of 2's as prime factors. Suppose that $\sqrt{2}$ is rational number. Then, $\sqrt{2} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$. Thus, $2 = \frac{p^2}{q^2}$ or $p^2 = 2q^2$. Since p^2 and q^2 are both square numbers, p^2 contains an even number of 2's as prime factors (might be 0 times for odd numbers) and q^2 contains an even number of 2's as prime factors. But then $2q^2$ has an odd number of 2's as prime factors and thus p^2 has an odd number of 2's as prime factors because $p^2 = 2q^2$. This is a contradiction. Thus, $\sqrt{2}$ is an irrational number.

Theorem 1.4.3

The set of primes in $\mathbb{N}$ is infinite.

Proof:

Suppose that the set of primes $W = \{p_1, p_2, \cdots, p_k\}$ is finite for some $k \in \mathbb{N}$. Let $n = p_1p_2\cdots p_k + 1 \in \mathbb{N}$. (fact) All natural number has a prime divisor $q > 1$. So, $q \mid n$, and since q is a prime, then $q \in W$ and $q \mid p_1p_2\cdots p_k$ (because $q = p_i$ for some $1 \leq i \leq k$). Also, $q \mid n$. Therefore, $q \mid (n - p_1p_2\cdots p_k)$, but $n - p_1p_2\cdots p_k = 1$. Thus $q = 1$, Contradition. Thus W is infinite.

1.4.3 Type 3: Contrapositive Proofs

Contraposition to show $\mathbf{P} \Rightarrow \mathbf{Q}$: Suppose $\sim \mathbf{Q}$, then $\cdots\cdots$. Thus $\sim \mathbf{P}$. Therefore, $\mathbf{P} \Rightarrow \mathbf{Q}$. This technique uses the tautology $(\mathbf{P} \Rightarrow \mathbf{Q}) \Leftrightarrow (\sim \mathbf{Q} \Rightarrow \sim \mathbf{P})$.

Example 1.4.5

Let $m \in \mathbb{Z}$. If m^2 is odd, then m is odd.

Solution:

Assume that m is even. Then $m = 2k$ for some $k \in \mathbb{Z}$ and $m^2 = 4k^2 = 2(2k^2)$ which is even. By contraposition, the result is proved.

Example 1.4.6

Let $x, y \in \mathbb{R}$ such that $x < 2y$. Show that if $7xy \leq 3x^2 + 2y^2$, then $3x \leq y$.

Solution:

Assume that $x < 2y$. By contraposition, assume that $3x > y$. Then, $2y - x > 0$ and $3x - y > 0$, but

$$(2y - x)(3x - y) = 7xy - 3x^2 - 2y^2 > 0 \quad \Rightarrow \quad 7xy > 3x^2 + 2y^2.$$

Therefore, if $7xy \leq 3x^2 + 2y^2$, then $3x \leq y$.

1.4.4 Type 4: Two-Directions Proofs

Two directions to show $\mathbf{P} \Leftrightarrow \mathbf{Q}$: By any method, (i) Show that $\mathbf{P} \Rightarrow \mathbf{Q}$. (ii) Show that $\mathbf{Q} \Rightarrow \mathbf{P}$. Therefore, $\mathbf{P} \Leftrightarrow \mathbf{Q}$.

Theorem 1.4.4

Let a be a prime number, and let b and c be positive integers. Prove that $a \mid bc$ if and only if $a \mid b$ or $a \mid c$.

Proof:

We show the result by two direction: „ $\Rightarrow$ " and „ $\Leftarrow$ ".

„ $\Rightarrow$ ": Assume that $a \mid bc$. By Fundamental Theorem of Arithmetic, b and c can be written uniquely as products of primes. Assume $b = p_1p_2 \cdots p_k$ and $c = q_1q_2 \cdots q_h$ for some $h, k \in \mathbb{N}$. But then $bc = p_1p_2 \cdots p_kq_1q_2 \cdots q_h$. Since $a \mid bc$ and a is a prime, a is one of the prime factors. If $a = p_i$ for some $1 \le i \le k$, then $a \mid b$ or if $a = q_i$ for some $1 \le i \le h$, then $a \mid c$. Thus, either $a \mid b$ or $a \mid c$.

„ $\Leftarrow$ ": Assume that $a \mid b$ or $a \mid c$. Thus,

Case 1: $a \mid b$ then $b = ka$ for some $k \in \mathbb{Z}$ and hence $bc = (ka)c = (kc)a$. Thus $a \mid bc$.

Case 2: $a \mid c$ then $c = ha$ for some $h \in \mathbb{Z}$ and hence $bc = b(ha) = (bh)a$. Thus $a \mid bc$.

In either cases, $a \mid bc$.

1.4.5 Type 5: Proofs By Cases (Exhaustion)

Contradiction to show $(\mathbf{P}_1 \vee \mathbf{P}_2) \Rightarrow \mathbf{Q}$: By any method, (i) Show that $\mathbf{P}_1 \Rightarrow \mathbf{Q}$ and (ii) show that $\mathbf{P}_2 \Rightarrow \mathbf{Q}$. Using the tautology $[(\mathbf{P}_1 \vee \mathbf{P}_2) \Rightarrow \mathbf{Q}] \Leftrightarrow [(\mathbf{P}_1 \Rightarrow \mathbf{Q}) \wedge (\mathbf{P}_2 \Rightarrow \mathbf{Q})]$.

Example 1.4.7

Show that for any $x, y \in \mathbb{Z}$, if either x or y is even, then xy is even.

Solution:

We have two cases:

Case 1: Assume x-even. Then $x = 2k$ for some $k \in \mathbb{Z}$. That is $xy = 2(ky)$ which is even.

Case 2: Assume y-even. Then $y = 2h$ for some $h \in \mathbb{Z}$. That is $xy = 2(xh)$ which is even.

Thus, in both cases, xy is even.

Example 1.4.8

Let $x, y \in \mathbb{Z}$. If x and y are both odd, then xy is odd.

Solution:

a. Direct Proof: Assume x and y are odd integers. Then, there are m and n in $\mathbb{Z}$ such that $x = 2m+1$ and $y = 2n+1$. Thus, $xy = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$. Therefore, xy is odd as well.

b1. Proof by Contradiction: Assume that xy is even. Thus $2 \mid xy$ which implies that $2 \mid x$ or $2 \mid y$ (since 2 is a prime number) which is a contradiction both ways since both of x and y are odd.

b2. Another Proof by Contradiction: Assume that xy is even. Since x and y are odd, there are m and n in $\mathbb{Z}$ such that $x = 2m+1$ and $y = 2n+1$. Thus, $xy = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$ which is odd, contradiction. Therefore, xy is odd.

c. Proof by Contraposition: We use $\sim$ (xy is odd) $\Rightarrow \sim$ (x is odd and y is odd) which is equivalent to (xy is even) $\Rightarrow$ [(x is even) or (y is even)].

Assume that xy is even. Thus, $2 \mid xy$. Since 2 is a prime number, we have either $2 \mid x$ or $2 \mid y$. Thus, either x is even or y is even. Therefore, if x and y are odd, then xy is odd.

Exercise 1.4.1

Let $a, b \in \mathbb{Z}$. Use a contrapositive proof to show that if ab-odd, then a - odd and b-odd.

Section 1.6: Proofs Involving Quantifiers

1.6.1 Type 1: Proof of $(\exists x)\mathbf{P}(x)$

- Direct proof: Name or construct an element $x \in \mathcal{U}$ which has the property $\mathbf{P}(x)$.
- Proof by contradiction: Suppose $\sim (\exists x)\mathbf{P}(x)$. Then $(\forall x)(\sim \mathbf{P}(x))$ ... ... .Therefore, $\mathbf{Q}(x) \wedge \sim \mathbf{Q}(x)$, contradiction. Hence, $\sim (\exists x)\mathbf{P}(x)$ is false, then $(\exists x)\mathbf{P}(x)$ is true.

Example 1.6.1

Show that there is an even prime number.

Solution:

2 is a prime even number.

Example 1.6.2

Let $\mathcal{U} = \mathbb{R}$. Show that $(\exists x)[x^3 + 3x^2 + x - 1 = 0]$.

Solution:

Using direct proof: $x = -1$ is a solution. On the other hand, using a proof by contradiction:

Assume $\sim (\exists x)[x^3 + 3x^2 + x - 1 = 0] \equiv (\forall x)[x^3 + 3x^2 + x - 1 \neq 0]$. Therefore, either:

Case 1: $(\forall x)[x^3 + 3x^2 + x - 1 > 0]$ which is false for if $x = -10$, or

Case 2: $(\forall x)[x^3 + 3x^2 + x - 1 < 0]$ which is false for if $x = 10$.

Therefore, $(\exists x)[x^3 + 3x^2 + x - 1 = 0]$.

1.6.2 Type 2: Proof of $(\forall x)\mathbf{P}(x)$

- Direct proof: Let $x \in \mathcal{U}$ be arbitrary, then ... . Hence, $\mathbf{P}(x)$ is true. Since x was arbitrary chosen, $(\forall x)\mathbf{P}(x)$ is true.
- Proof by contradiction: Suppose $\sim (\forall x)\mathbf{P}(x)$. Then $(\exists x)(\sim \mathbf{P}(x))$ ... ... .Therefore, $\mathbf{Q}(x) \wedge \sim \mathbf{Q}(x)$, contradiction. Hence, $\sim (\forall x)\mathbf{P}(x)$ is false, then $(\forall x)\mathbf{P}(x)$ is true.

Example 1.6.3

Let $\mathcal{U} = \mathbb{Z}$. Show that $(\forall x)$, if x is even, then x^2 is even.

Solution:

Assume that $x \in \mathbb{Z}$ so that $x = 2k$ for some integer k. Then $x^2 = \left(2k\right)^2 = 2\left(2k^2\right)$ which is even.

Example 1.6.4

Show that for all rational numbers p and q, $\dfrac{p+q}{2}$ is rational.

Solution:

Assume that $p = \frac{x}{y}$ and $q = \frac{u}{v}$ where $x, y, u, v \in \mathbb{Z}$ with $y, v \neq 0$. Then,

$$\frac{p+q}{2} = \frac{1}{2}\left(\frac{x}{y} + \frac{u}{v}\right) = \frac{1}{2}\left(\frac{xv + yu}{yv}\right) = \frac{xv + yu}{2yv},$$

which is rational.

1.6.3 Type 3: Proof of $(\exists! x)\mathbf{P}(x)$

1. Prove that $(\exists x)\mathbf{P}(x)$ by any method.
2. Assume that $x, y \in \mathcal{U}$ such that $\mathbf{P}(x)$ and $\mathbf{P}(y)$ are true ... . Thus, $x = y$. Therefore, $(\exists! x)\mathbf{P}(x)$.

Example 1.6.5

Prove that every nonzero real number has a unique multiplicative inverse.

Solution:

Let x be any nonzero real number. We want to show that $xy = 1$ for exactly one real number y. Let $y = \frac{1}{x}$, then y is a real number. Since $x \neq 0$, then $xy = x\frac{1}{x} = 1$. Thus, x has a multiplicative inverse.

Assume that y and z are two real numbers such that $xy = xz = 1$. Since $x \neq 0$, $xy = xz$ implies that $y = z$. Therefore, every nonzero real number has a unique multiplicative inverse.

Exercise 1.6.1

Prove that every nonsingular matrix has a unique inverse.

Chapter

2 Set Theory

Section 2.1: Basic Notations of Set Theory

Definition 2.1.1

A **set** is a collection of objects called elements. Sets are usually denoted by capital letters $A, B, C, \cdots$ while elements are usually denoted by small letters $a, b, c, \cdots$.

- If a is an element of a set A, then we write $a \in A$. Otherwise, we write $a \notin A$.
- The empty set $\phi := \{x : x \neq x\}$. That is, ϕ is a set with no elements.
- A set B is a **subset** of A, denoted by $B \subseteq A$, if and only if every elements of B is also an element of A. That is, $\forall b \in B \Rightarrow b \in A$.
- A set B is called a **proper subset** of set A, if $B \subseteq A$ and $B \neq \phi$, but $B \neq A$. In this case, we write $B \subset A$.
- Two subsets A and B are equal , denoted by $A = B$, if and only of $A \subseteq B$ and $B \subseteq A$.
- If a set A contains n elements, we say that $|A| = n$.

Theorem 2.1.1

For any sets A, B, and C, we have:

1) $\phi \subseteq A$,
2) $A \subseteq A$, and
3) if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof:

The first two results are trivial so we leave those. For part 3) let a be any element of A. Since $A \subseteq B$, $a \in B$. But since $B \subseteq C$, $a \in C$. Thus, if $a \in A \Rightarrow a \in C$. Thus, $A \subseteq C$.

Definition 2.1.2

Let A be a set. The **power set** of A is the set whose elements are all the subsets of A and is denoted by $\mathcal{P}(A)$. Thus,

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

Example 2.1.1

Let $A = \{a, b, c\}$. Find $\mathcal{P}(A)$.

Solution:

$\mathcal{P}(A) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$.

Remark 2.1.1

Let A be any given set. Then,

a. Theorem: If $|\,A\,| = n$, then $|\,\mathcal{P}(A)\,| = 2^n$.

b. $A \nsubseteq \mathcal{P}(A)$, but $A \in \mathcal{P}(A)$.

Example 2.1.2

Let $A = \{1, \{1, 3\}, \{2, 3\}\}$. Find $\mathcal{P}(A)$.

Solution:

$$\mathcal{P}(A) = \{\,\phi, \{1\}, \{\,\{\,1, 3\,\}\,\}, \{\,\{\,2, 3\,\}\,\}, \{\,1, \{\,1, 3\,\}\,\}, \{\,1, \{\,2, 3\,\}\,\}, \{\,\{\,1, 3\,\}, \{\,2, 3\,\}\,\}, A\,\}.$$

Note that, $1 \in A$, while $2 \notin A$ and $3 \notin A$. Also, $\{1\} \notin A$ where $\{2, 3\} \in A$ and $\{\{2, 3\}\} \subseteq A$ hence $\{\{2, 3\}\} \in \mathcal{P}(A)$. Moreover, $1 \notin \mathcal{P}(A)$, $\{1\} \in \mathcal{P}(A)$, and $\{\{1\}\} \subseteq \mathcal{P}(A)$. Also, $\phi \subseteq A$, $\phi \in \mathcal{P}(A)$ and $\{\phi\} \subseteq \mathcal{P}(A)$. Finally, $\{1, 3\} \notin \mathcal{P}(A)$, but $\{\{1, 3\}\} \in \mathcal{P}(A)$ and $\{\{\{1, 3\}\}\} \subseteq \mathcal{P}(A)$.

Theorem 2.1.2

Let A and B be two sets. Then, $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof:

„ $\Rightarrow$ ": Assume that $A \subseteq B$. Let $X \in \mathcal{P}(A)$. Then, $X \subseteq A \subseteq B$. That is, $X \in \mathcal{P}(B)$. Thus, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

„ $\Leftarrow$ ": Assume that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Since $A \in \mathcal{P}(A) \subseteq \mathcal{P}(B)$, we have $A \in \mathcal{P}(B) \Rightarrow A \subseteq B$.

Exercise 2.1.1

Let $A = \{ 9^n : n \in \mathbb{Z} \}$ and $B = \{ 3^n : n \in \mathbb{Z} \}$. Show that $A \subsetneqq B$.

Exercise 2.1.2

Let $A = \{ 9^n : n \in \mathbb{Q} \}$ and $B = \{ 3^n : n \in \mathbb{Q} \}$. Show that $A = B$.

Exercise 2.1.3

Find $\mathcal{P}(\phi)$, $\mathcal{P}(\mathcal{P}(\phi))$, and $\mathcal{P}(\mathcal{P}(\mathcal{P}(\phi)))$.

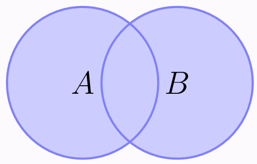
Section 2.2: Set Operations

Definition 2.2.1

Let A and B be two sets. Then,

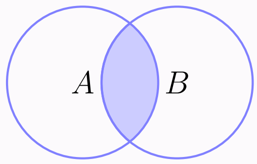
1. **Union**: $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
   What is the meaning of $x \notin A \cup B$?

$A \cup B$



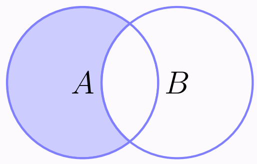
2. **intersection**: $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
   What is the meaning of $x \notin A \cap B$?

$A \cap B$



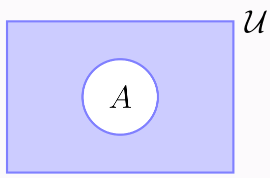
3. **Difference**: $A - B = \{x : x \in A \text{ and } x \notin B\}$.
   What is the meaning of $x \notin A - B$?

$A - B$



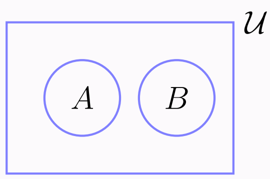
4. **Complement**: If $\mathcal{U}$ is the universal, then
   $\widetilde{A} = \{x : x \notin A\} = \{x : x \in \mathcal{U} - A\}$.

$\widetilde{A} = \mathcal{U} - A$



5. **Disjoint**: A and B are called **disjoint** if $A \cap B = \phi$.

$A \cap B = \phi$



Theorem 2.2.1

Let A, B, and C be sets. Then,

1. $A \subseteq A \cup B$.
2. $A \cap B \subseteq A$.
3. $A \cap \phi = \phi$.
4. $A \cup \phi = A$.

5. $A \cap A = A$.
6. $A \cup A = A$.
7. $A \cup B = B \cup A$.
8. $A \cap B = B \cap A$.
9. $A - \phi = A$.
10. $\phi - A = \phi$.
11. $A \cup (B \cup C) = (A \cup B) \cup C$.
12. $A \cap (B \cap C) = (A \cap B) \cap C$.
13. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
14. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
15. $A \subseteq B$ if and only if $A \cup B = B$.
16. $A \subseteq B$ if and only if $A \cap B = A$.
17. if $A \subseteq B$, then $A \cup C \subseteq B \cup C$.
18. if $A \subseteq B$, then $A \cap C \subseteq B \cap C$.

Proof:

Proof of (13): Using the fact "$\mathbf{P} \wedge (\mathbf{Q} \vee \mathbf{R}) = (\mathbf{P} \wedge \mathbf{Q}) \vee (\mathbf{P} \wedge \mathbf{R})$" as follows.

$$\begin{aligned} x \in A \cap (B \cup C) \quad & \text{iff} \quad x \in A \text{ and } x \in B \cup C \\ & \text{iff} \quad x \in A \text{ and } (x \in B \text{ or } x \in C) \\ & \text{iff} \quad (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ & \text{iff} \quad x \in A \cap B \text{ or } x \in A \cap C \\ & \text{iff} \quad x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Proof of (15): „ $\Rightarrow$ ": Assume that $A \subseteq B$. By part (1), $B \subseteq A \cup B$ so we only show that $A \cup B \subseteq B$. Let $x \in A \cup B$, then $x \in A \subseteq B$ or $x \in B$. In both cases, $x \in B$. Thus, $A \cup B \subseteq B$. Therefore, $B = A \cup B$.

„ $\Leftarrow$ ": Assume that $A \cup B = B$. By part (1) $A \subseteq A \cup B = B$. Thus, $A \subseteq B$.

Proof of (18): Assume that $A \subseteq B$. Let $x \in A \cap C$, then $x \in A \subseteq B$ and $x \in C$. Thus, $x \in B$ and $x \in C$, which implies that $x \in B \cap C$. Therefore, $A \cap C \subseteq B \cap C$.

Theorem 2.2.2

Let A and B be two subsets of the universe $\mathcal{U}$. Then:

1. $\widetilde{\widetilde{A}} = A$.
2. $A \cup \widetilde{A} = \mathcal{U}$.
3. $A \cap \widetilde{A} = \phi$.
4. $A - B = A \cap \widetilde{B}$.
5. $A \subseteq B$ iff $\widetilde{B} \subseteq \widetilde{A}$.
6. $A \cap B = \phi$ iff $A \subseteq \widetilde{B}$.
7. a. $\widetilde{A \cup B} = \widetilde{A} \cap \widetilde{B}$.
   b. $\widetilde{A \cap B} = \widetilde{A} \cup \widetilde{B}$. } ....(De Morgan's Laws).

Proof:

Proof of (2): If $x \in A \cup \widetilde{A}$ then $x \in A \subseteq \mathcal{U}$ or $x \in \widetilde{A} = \mathcal{U} - A$. In either cases, $x \in \mathcal{U}$. Thus, $A \cup \widetilde{A} \subseteq \mathcal{U}$.

Assume now that $x \in \mathcal{U}$. Thus, $x \in A$ or $x \in \mathcal{U} - A = \widetilde{A}$ which implies $x \in A \cup \widetilde{A}$. Thus $\mathcal{U} \subseteq A \cup \widetilde{A}$. Therefore, $\mathcal{U} = A \cup \widetilde{A}$.

Proof of (5): Using a contrapositive proof as follows:

$$\begin{aligned} A \subseteq B \quad & \text{iff} \quad (\forall x)(x \in A \Rightarrow x \in B) \\ & \text{iff} \quad (\forall x)(x \notin B \Rightarrow x \notin A) \\ & \text{iff} \quad (\forall x)(x \in \widetilde{B} \Rightarrow x \in \widetilde{A}) \\ & \text{iff} \quad \widetilde{B} \subseteq \widetilde{A}. \end{aligned}$$

Proof of (7.b): Recall that $\sim (\mathbf{P} \wedge \mathbf{Q}) = \sim \mathbf{P} \vee \sim \mathbf{Q}$:

$$\begin{aligned} x \in \widetilde{A \cap B} \quad & \text{iff} \quad x \notin A \cap B \\ & \text{iff} \quad \sim (x \in A \text{ and } x \in B) \\ & \text{iff} \quad x \notin A \text{ or } x \notin B \\ & \text{iff} \quad x \in \widetilde{A} \text{ or } x \in \widetilde{B} \\ & \text{iff} \quad x \in \widetilde{A} \cup \widetilde{B}. \end{aligned}$$

Example 2.2.1

Let $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ be the universe and let $A = \{1, 5, 7\}$, $B = \{2, 5, 8\}$, and $C = \{3, 4, 5, 6, 7\}$ Answer Each of the following:

1. $A \cap B = \{5\}$.
2. $B \cup C = \{2, 3, 4, 5, 6, 7, 8\}$.
3. $(A \cap B) \cup (A \cap C) = \{5\} \cup \{5, 7\} = \{5, 7\}$.
4. $A - C = \{1\}$.
5. $(A \cup C) - (B \cap C) = \{1, 3, 4, 5, 6, 7\} - \{5\} = \{1, 3, 4, 6, 7\}$.
6. $\tilde{A} = \mathcal{U} - A = \{2, 3, 4, 6, 8\}$.
7. $\tilde{A} \cap \tilde{B} = \{2, 3, 4, 6, 8\} \cap \{1, 3, 4, 6, 7\} = \{3, 4, 6\}$.

Example 2.2.2

Let $A \subseteq B \cup C$ and $A \cap B = \phi$. Show that $A \subseteq C$.

Solution:

Let $x \in A$. Since $A \subseteq B \cup C$, $x \in B$ or $x \in C$. If $x \in B$, then $x \in A \cap B$, contradiction. Thus, $x \in C$ and therefore, $A \subseteq C$.

Example 2.2.3

Show that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Solution:

$$\begin{aligned}
\text{Let } X \in \mathcal{P}(A \cap B) &\text{ iff } X \subseteq A \cap B \\
&\text{ iff } X \subseteq A \text{ and } X \subseteq B \\
&\text{ iff } X \in \mathcal{P}(A) \text{ and } X \in \mathcal{P}(B) \\
&\text{ iff } X \in \mathcal{P}(A) \cap \mathcal{P}(B).
\end{aligned}$$

Example 2.2.4

Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Is $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ in general? Explain.

Solution:

$$\begin{aligned} \text{Let } X \in \mathcal{P}(A) \cup \mathcal{P}(B) \quad &\Rightarrow \quad X \in \mathcal{P}(A) \text{ or } X \in \mathcal{P}(B) \\ &\Rightarrow \quad X \subseteq A \text{ or } X \subseteq B \\ &\Rightarrow \quad X \subseteq A \cup B \\ &\Rightarrow \quad X \in \mathcal{P}(A \cup B). \end{aligned}$$

In general, $\mathcal{P}(A \cup B) \nsubseteq \mathcal{P}(A) \cup \mathcal{P}(B)$ and thus $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

For instance, consider $A = \{a\}$ and $B = \{b\}$. Then $A \cup B = \{a, b\}$, $\mathcal{P}(A) = \{\phi, \{a\}\}$ and $\mathcal{P}(B) = \{\phi, \{b\}\}$. Therefore,

$$\mathcal{P}(A \cup B) = \{\phi, \{a\}, \{b\}, \{a, b\}\} \neq \mathcal{P}(A) \cup \mathcal{P}(B) = \{\phi, \{a\}, \{b\}\}.$$

Remark 2.2.1

If $A \subseteq B$, then $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$.

Exercise 2.2.1

Suppose that A, B, and C are three nonempty sets. Show that if $A \subseteq B$, then $A - C \subseteq B - C$.

Exercise 2.2.2

Suppose that A, and B are two nonempty sets. Show that $A - B = \phi$ iff $A \cap B = A$.

Section 2.3: Extended Set Operations

Definition 2.3.1

Let $\mathcal{I}$ be a nonempty set. Suppose that for each $i \in \mathcal{I}$, there is a corresponding set A_i. Then, the family of sets $\mathcal{A} = \{A_i : i \in \mathcal{I}\}$ is called an **indexed family of sets**. Each $i \in \mathcal{I}$ is called an **index** and $\mathcal{I}$ is called an **indexing set**. Then

1. The **union over** $\mathcal{A}$ is defined by
$$\bigcup_{i\in\mathcal{I}} A_i = \{\, x : (\exists A_i \in \mathcal{A})\,[x \in A_i]\,\} = \{\, x : (\,\exists A_i\,)\,[A_i \in \mathcal{A} \wedge x \in A_i]\,\}.$$
2. the **intersection over** $\mathcal{A}$ is defined by
$$\bigcap_{i\in\mathcal{I}} A_i = \{\, x : (\forall A_i \in \mathcal{A})\,[x \in A_i]\,\} = \{\, x : (\,\forall A_i\,)\,[A_i \in \mathcal{A} \Rightarrow x \in A_i]\,\}.$$
3. The indexed family $\mathcal{A}$ of sets is said to be **pairwise disjoint** if and only if for all i and j in $\mathcal{I}$, either $A_i = A_j$ or $A_i \cap A_j = \phi$.

Example 2.3.1

Let $\mathcal{I} = \{\,1, 2, 3\,\}$, and define $A_i = \{\,i, i+1\,\}$ for each $i \in \mathcal{I}$. Find $\bigcup_{i\in\mathcal{I}} A_i$ and $\bigcap_{i\in\mathcal{I}} A_i$.

Solution:

Note that $A_1 = \{\,1, 2\,\}$, $A_2 = \{\,2, 3\,\}$, and $A_3 = \{\,3, 4\,\}$. Thus, $\bigcup_{i\in\mathcal{I}} A_i = \{\,1, 2, 3, 4\,\}$, and $\bigcap_{i\in\mathcal{I}} A_i = \phi$.

Example 2.3.2

For each $i \in \mathbb{N}$, let $A_i = \{j \in \mathbb{N} : j \leq i\}$. Find $\bigcup_{i\in\mathbb{N}} A_i$ and $\bigcap_{i\in\mathbb{N}} A_i$.

Solution:

Note that $A_1 = \{1\}$, $A_2 = \{1, 2\}$, $\cdots$, $A_n = \{1, 2, \cdots, n\}$ and so on. Thus, $\bigcup_{i\in\mathbb{N}} A_i = \mathbb{N}$ while $\bigcap_{i\in\mathbb{N}} A_i = \{1\}$.

Theorem 2.3.1

Let $\mathcal{A} = \{A_i : i \in \mathcal{I}\}$ be an indexed family of sets. Then,

1. For each $k \in \mathcal{I}$, $A_k \subseteq \bigcup_{i\in\mathcal{I}} A_i$.

2. For each $k \in \mathcal{I}$, $\bigcap_{i\in\mathcal{I}} A_i \subseteq A_k$.

3. a. $\widetilde{\bigcup_{i\in\mathcal{I}} A_i} = \bigcap_{i\in\mathcal{I}} \widetilde{A_i}$.
   b. $\widetilde{\bigcap_{i\in\mathcal{I}} A_i} = \bigcup_{i\in\mathcal{I}} \widetilde{A_i}$.
   .... (De Morgan's Laws).

Proof:

Proof of (1): Let $x \in A_k$. Since $A_k \in \mathcal{A}$, $x \in \bigcup_{i\in\mathcal{I}} A_i$. Thus, $A_k \subseteq \bigcup_{i\in\mathcal{I}} A_i$.

Proof of (2): Let $x \in \bigcap_{i\in\mathcal{I}} A_i$. Then, $x \in A_i$ for every $i \in \mathcal{I}$. Since $k \in \mathcal{I}$, $x \in A_k$. Thus, $\bigcap_{i\in\mathcal{I}} A_i \subseteq A_k$.

Proof of (3.a):

$$\begin{aligned} x \in \widetilde{\bigcup_{i\in\mathcal{I}} A_i} &\Leftrightarrow x \notin \bigcup_{i\in\mathcal{I}} A_i \\ &\Leftrightarrow x \notin A_i \text{ for all } i \in \mathcal{I} \\ &\Leftrightarrow x \in \widetilde{A_i} \text{ for all } i \in \mathcal{I} \\ &\Leftrightarrow x \in \bigcap_{i\in\mathcal{I}} \widetilde{A_i}. \end{aligned}$$

Proof of (3.b): A similar proof as that in part (3.a) can be shown in this part as well. However, we use a different style as follows: Using $A_i = \widetilde{\widetilde{A_i}}$ together with part (3.a) of this theorem, we get

$$\widetilde{\bigcap_{i\in\mathcal{I}} A_i} = \widetilde{\bigcap_{i\in\mathcal{I}} \widetilde{\widetilde{A_i}}} = \widetilde{\widetilde{\bigcup_{i\in\mathcal{I}} \widetilde{A_i}}} = \bigcup_{i\in\mathcal{I}} \widetilde{A_i}.$$

Example 2.3.3

Let $\mathcal{I} = \{1, 2, 3, 4\}$ so that $A_1 = \{1, 2, 7\}$, $A_2 = \{3, 4, 8\}$, $A_3 = \{1, 4, 8\}$, and $A_4 = \{1, 3, 4, 7\}$. If $\mathcal{U} = \{1, 2, 3, \cdots, 10\}$, answer each of the following:

a. $\bigcup_{i\in\mathcal{I}} A_i = \{1, 2, 3, 4, 7, 8\}$.

b. $\bigcap_{i\in\mathcal{I}} A_i = \phi$.

c. $\bigcup_{i\in\mathcal{I}} \widetilde{A_i} = \widetilde{\bigcap_{i\in\mathcal{I}} A_i} = \mathcal{U}$.

d. $\bigcap_{i\in\mathcal{I}} \widetilde{A_i} = \widetilde{\bigcup_{i\in\mathcal{I}} A_i} = \{5, 6, 9, 10\}$.

e. Is $\mathcal{A} = \{A_i : i \in \mathcal{I}\}$ a pairwise disjoint? Explain. Answer: No, $A_3 \cap A_4 = \{1, 4\} \neq \phi$.

Example 2.3.4

Let $\mathcal{U} = \mathbb{N}$ and $\mathcal{I} = \mathbb{N}$. Define $A_i = \mathbb{N} - \{1, 2, \cdots, i\}$ for all $i \in \mathcal{I}$. Find:

a. $A_{10} = \{11, 12, 13, \cdots\}$.

b. $\bigcup_{i\in\mathcal{I}} A_i = \{2, 3, 4, 5, \cdots\}$.

c. $\bigcap_{i\in\mathcal{I}} A_i = \phi$.

Example 2.3.5

If $\mathcal{U} = \mathbb{R}$, let $A_n = [-\frac{1}{n}, 2 + \frac{1}{n})$ for all $n \in \mathbb{N}$. Find:

a. $\bigcup_{n\in\mathbb{N}} A_n = [-1, 3) =: A_1$.

b. $\bigcap_{n\in\mathbb{N}} A_n = [0, 2]$.

c. $\bigcap_{n\in\mathbb{N}} \widetilde{A_n} = \widetilde{\bigcup_{n\in\mathbb{N}} A_n} = \mathbb{R} - [-1, 3)$.

d. $\bigcup_{n\in\mathbb{N}} \widetilde{A_n} = \widetilde{\bigcap_{n\in\mathbb{N}} A_n} = \mathbb{R} - [0, 2]$.

Example 2.3.6

Let $\mathcal{U} = \mathbb{R}$ and define $S_a = (-a, a)$ for all $a \in \mathbb{N}$. Find

a. $\bigcup_{a\in\mathbb{N}} S_a = \mathbb{R}$.

b. $\bigcap_{a\in\mathbb{N}} S_a = (-1,1)$.

Exercise 2.3.1

Let $\mathcal{A} = \{ A_i : i \in \mathcal{I} \}$ be an indexed family of sets for a nonempty set $\mathcal{I}$. Show that if $B \subseteq A_i$ for every $i \in \mathcal{I}$, then $B \subseteq \bigcap_{i\in\mathcal{I}} A_i$.

Exercise 2.3.2

For each natural number $n \geq 3$, let $A_n = \left[\frac{1}{n}, 2+\frac{1}{n}\right]$, and $\mathcal{A} = \{ A_n : n \geq 3 \}$. Find $\bigcap_{n\geq 3} A_n$ and $\bigcup_{n\geq 3} A_n$.

Section 2.4: Proof by Induction

Definition 2.4.1: Principle of Mathematical Induction (PMI)

If S is a subset of $\mathbb{N}$ so that:

1. $1 \in S$, and
2. for all $n \in \mathbb{N}$, if $n \in S$, then $n+1 \in S$,

then $S = \mathbb{N}$.

2.4.1 Proof of $(\forall n \in \mathbb{N})\mathbf{P}(n)$ using PMI

- **Basic Step**: Show that $\mathbf{P}(1)$ is true.
- **Induction Step**: Show that for all $n \in \mathbb{N}$, if $\mathbf{P}(n)$ is true, then $\mathbf{P}(n+1)$ is true.
- **Conclusion**: By step 1 and step 2 and using the PMI, $\mathbf{P}(n)$ is true for all $n \in \mathbb{N}$.

Example 2.4.1

Show that for all $n \in \mathbb{N}$,

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

Solution:

For $n = 1$, clearly $1 = \frac{1(1+1)}{2}$ is true. Assume that for some $n \in \mathbb{N}$, we have

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

Now, we want to show that $1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}$.

$$\begin{aligned}
\overbrace{1 + 2 + 3 + \cdots + n}^{\text{use our assumption}} + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

Example 2.4.2

Show that for all $n \in \mathbb{N}$, $\sum_{i=1}^{n}(2i-1) = n^2$.

Solution:

For $n = 1$, $2(1) - 1 = 1 = 1^2$, which is true. Assume that for some $n \in \mathbb{N}$, we have $\sum_{i=1}^{n}(2i-1) = n^2$. We want to show that $\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$. Thus,

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + 2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2.$$

Example 2.4.3

Show that for all $n \in \mathbb{N}$, $n + 3 < 5n^2$.

Solution:

For $n = 1$ we have $1 + 3 = 4 < 5$ which is true. So, assume that for n, $n + 3 < 5n^2$ is true. For $n + 1$, we want to show that $(n + 1) + 3 < 5(n + 1)^2 = 5n^2 + 10n + 5$. Then,

$$(n + 1) + 3 = (n + 3) + 1 < 5n^2 + 1 < 5n^2 + (10n + 4) + 1 = 5(n + 1)^2.$$

Therefore, for all $n \in \mathbb{N}$, $n + 3 < 5n^2$.

Definition 2.4.2

For $n \in \mathbb{N}$, define $0! = 1$ and $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1$. Then, the **bionomial coefficient "n choose k"**, where $0 \le k \le n$, is

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)(n-3)\cdots(n-k+2)(n-k+1)}{k!}.$$

Moreover, the **bionomial expansion** of any $a, b \in \mathbb{R}$ is given by

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k} a^k\, b^{n-k}.$$

Remark 2.4.1: Pascal's Triangle

Let $a, b \in \mathbb{R}$. Then, the coefficients of the bionomial expansion $(a+b)^n$ can be computed by the Pascal's Triangle for each n.

$$\begin{array}{lccccccccccc}
n=0 & & & & & & 1 & & & & & \\
n=1 & & & & & 1 & & 1 & & & & \\
n=2 & & & & 1 & & 2 & & 1 & & & \\
n=3 & & & 1 & & 3 & & 3 & & 1 & & \\
n=4 & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n=5 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

Example 2.4.4

Show that for all $n \in \mathbb{N}$, $\dfrac{n^3}{3} + \dfrac{n^5}{5} + \dfrac{7n}{15}$ is an integer.

Solution:

$\dfrac{n^3}{3} + \dfrac{n^5}{5} + \dfrac{7n}{15} = \dfrac{5n^3 + 3n^5 + 7n}{15}$ is an integer iff $15 \mid 5n^3 + 3n^5 + 7n$ iff $\exists k \in \mathbb{N}$ such that $5n^3 + 3n^5 + 7n = 15k$.

For $n = 1$, we have $5 + 3 + 7 = 15$ which is true. So assume that there $k \in \mathbb{N}$ such that $5n^3 + 3n^5 + 7n = 15k$. Then, we want to show that

$$5(n+1)^3 + 3(n+1)^5 + 7(n+1) = 15h \tag{2.4.1}$$

for some $h \in \mathbb{N}$. Thus, using the Pascal's Triangle we get

$$\begin{aligned}
\text{Eqn.}(2.4.1) &= 5(n^3 + 3n^2 + 3n + 1) + 3(n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1) + 7n + 7 \\
&= \underbrace{(5n^3 + 3n^5 + 7n)}_{=15k} + \textcircled{15}n^2 + \textcircled{15}n + 5 + \textcircled{15}n^4 \\
&\quad + \textcircled{30}n^3 + \textcircled{30}n^2 + \textcircled{15}n + 3 + 7 \\
&= 15k + 15\left[n^2 + n + n^4 + 2n^3 + 2n^2 + n + 1\right]
\end{aligned}$$

Thus $15 \mid 5(n+1)^3 + 3(n+1)^5 + 7(n+1)$ and $\dfrac{n^3}{3} + \dfrac{n^5}{5} + \dfrac{7n}{15}$ is an integer for all $n \in \mathbb{N}$.

Example 2.4.5

Express the terms of $(2x-4yz^2)^5$ for $x, y, z \in \mathbb{R}$.

Solution:

Let $a = 2x$, $b = -4yz^2$, and $n = 5$. Using the bionomial expansion form, we get

$$\begin{aligned}(2x-4yz^2)^5 &= (2x)^5 + 5(2x)^4(-4yz^2) + 10(2x)^3(-4yz^2)^2 + 10(2x)^2(-4yz^2)^3 \\ &\quad +5(2x)(-4yz^2)^4 + (-4yz^2)^5.\end{aligned}$$

Definition 2.4.3: Generalized Principle of Mathematical Induction (GPMI)

Let k be a natural number. If S is a subset of $\mathbb{N}$ so that:

1. $k \in S$, and
2. for all $n \in \mathbb{N}$ with $n \geq k$, if $n \in S$, then $n+1 \in S$,

then S contains all natural number greater than or equal to k.

Example 2.4.6

Show that for all $n \geq 5$, $n^2 - n - 20 \geq 0$.

Solution:

For $n = 5$, we have $25 - 5 - 20 = 0 \geq 0$ which is true. Assume that for some $n \geq 5$, $n^2 - n - 20 \geq 0$ is true. For $n+1$, we have

$$(n+1)^2 - (n+1) - 20 = n^2 + 2n + \cancel{1} - n - \cancel{1} - 20 = (n^2 - n - 20) + \underbrace{2n}_{\text{positive}} \geq 0.$$

Thus, $n^2 - n - 20 \geq 0$ for all $n \geq 5$.

Example 2.4.7

Let $n \in \mathbb{N}$. Show that $(n+1)! > 2^{n+3}$ for all $n \geq 5$.

Solution:

For $n = 5$, we have $6! = 720 \geq 2^8 = 256$ which is true. Assume that for some $n \geq 5$, $(n+1)! > 2^{n+3}$ is true.

For $n+1$, we want to show that $(n+2)! > 2^{n+4}$ for all $n+1 \geq 5$. Since $n+2 > 2$ for all $n \geq 4$, we get

$$(n+2)! = (n+2)(n+1)! > (n+2)2^{n+3} > 2 \cdot 2^{n+3} = 2^{n+4}.$$

Thus, $(n+1)! > 2^{n+3}$ for all $n \geq 5$.

Exercise 2.4.1

Show that for all $n \in \mathbb{N}$, the polynomial $x - y$ divides the polynomial $x^n - y^n$.

Exercise 2.4.2

Show that for all $n \in \mathbb{N}$, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Exercise 2.4.3

Show that for all $n \in \mathbb{N}$, $3 \mid n^3 + 5n$.

Exercise 2.4.4

Let $x \in \mathbb{R}$ with $x \geq -1$. Show that $(1+x)^n \geq 1 + nx$ for all $n \in \mathbb{N}$.

Exercise 2.4.5

Show that for all natural numbers n, $\displaystyle\prod_{i=1}^{n} (2i-1) = \frac{(2n)!}{n!\,2^n}$.

Chapter

3 Relations

Section 3.1: Cartesian Products and Relations

Definition 3.1.1

Let A and B be two sets. An **ordered pair** is $(a, b) \neq \{a, b\}$ for $a \in A$ and $b \in B$. We say that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Definition 3.1.2

Let A and B be two sets. The (**Cartesian** or **cross**) **product** of A and B, denoted by $A \times B$, is defined by

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

Moreover, if $(a, b) \in A \times B$, then $a \in A$ and $b \in B$. If $(a, b) \notin A \times B$, then either $a \notin A$ or $b \notin B$.

Remark 3.1.1

Let A and B be two given sets. Then,

1. if A has m elements and B has n elements, then $A \times B$ has mn elements.
2. In general, $A \times B \neq B \times A$.

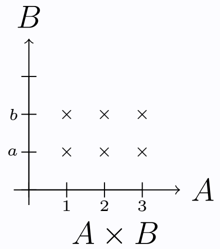
Example 3.1.1

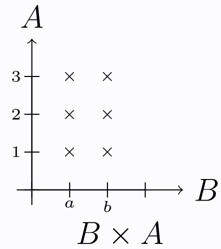
Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$. Find $A \times B$ and $B \times A$.

Solution:

Note that, in general $A \times B \neq B \times A$ as this example shows.

$$\begin{aligned} A \times B &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}, \text{ and} \\ B \times A &= \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}. \end{aligned}$$



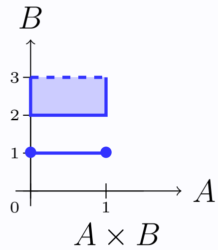


Example 3.1.2

Let $A = [0, 1]$ and $B = \{1\} \cup [2, 3)$. Find $A \times B$.

Solution:

$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.



Theorem 3.1.1

If A and B are nonempty set, then $A \times B = B \times A$ iff $A = B$.

Proof:

„ $\Rightarrow$ ": Assume that $A \neq \phi$, $B \neq \phi$ and $A \times B = B \times A$. Let $a \in A$, then there is $b \in B$ such that $(a, b) \in A \times B = B \times A$ which implies that $a \in B$ Thus, $A \subseteq B$.

Let $b \in B$, then there is $a \in A$ such that $(b, a) \in B \times A = A \times B$ which implies that $b \in A$. Thus, $B \subseteq A$ and therefore $A = B$.

„ $\Leftarrow$ ": if $A = B$, then $A \times B = A \times A = B \times A$.

Theorem 3.1.2

Let A, B, C, and D be sets. Then

$$1. \begin{cases} \text{a. } A \times (B \cup C) & = & (A \times B) \cup (A \times C). \\ \text{b. } (A \cup B) \times C & = & (A \times C) \cup (B \times C). \\ \text{c. } A \times (B \cap C) & = & (A \times B) \cap (A \times C). \\ \text{d. } (A \cap B) \times C & = & (A \times C) \cap (B \times C). \end{cases}$$

2. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

3. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Proof:

Proof of (1.a):

$$\begin{aligned} (x,y) \in A \times (B \cup C) \quad &\text{iff} \quad x \in A \wedge y \in B \cup C \\ &\text{iff} \quad x \in A \wedge (y \in B \vee y \in C) \\ &\text{iff} \quad (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\ &\text{iff} \quad ((x,y) \in A \times B) \vee ((x,y) \in A \times C) \\ &\text{iff} \quad (x,y) \in (A \times B) \vee (A \times C). \end{aligned}$$

Proof of (2):

$$\begin{aligned} (x,y) \in (A \times B) \cap (C \times D) \quad &\text{iff} \quad (x \in A \wedge y \in B) \wedge (x \in C \wedge y \in D) \\ &\text{iff} \quad (x \in A \wedge x \in C) \wedge (y \in B \wedge y \in D) \\ &\text{iff} \quad (x \in A \cap C) \wedge (y \in B \cap D) \\ &\text{iff} \quad (x,y) \in (A \cap C) \times (B \cap D). \end{aligned}$$

Proof of (3): Let $(x,y) \in (A \times B) \cup (C \times D)$, then $(x,y) \in A \times B$ or $(x,y) \in C \times D$.

Case(i): $(x,y) \in A \times B$ implies that $x \in A$ and $y \in B$. Then, $x \in A \cup C$ and $y \in B \cup D$. Thus, $(x,y) \in (A \cup C) \times (B \cup D)$.

Case(ii): $(x,y) \in C \times D$ implies that $x \in C$ and $y \in D$. Then again $x \in A \cup C$ and $y \in B \cup D$. Thus, $(x,y) \in (A \cup C) \times (B \cup D)$.

Therefore, $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Remark 3.1.2

Note that $(A \times B) \cup (C \times D) \neq (A \cup C) \times (B \cup D)$: For instance, Let $A = B = \{0\}$, and $C = D = \{1\}$. Then, $(0,1) \in (A \cup C) \times (B \cup D)$ while $(0,1) \notin (A \times B) \cup (C \times D)$. Therefore, $(A \cup C) \times (B \cup D) \nsubseteq (A \times B) \cup (C \times D)$.

Definition 3.1.3

Let A and B be sets. A **relation** $\mathcal{R}$ from A to B is a subset of $A \times B$. In this case, we write $a\mathcal{R}b$ for $(a,b) \in \mathcal{R}$ and say that "a is related to b". Also, $a\not{\mathcal{R}}b$ means that $(a,b) \notin \mathcal{R} \subseteq A \times B$. Moreover, if $A = B$, then subsets of $A \times A$ are called relations on A.

Definition 3.1.4

If $\mathcal{R} \subseteq A \times B$ is a relation, then the **domain** of $\mathcal{R}$ is $\mathrm{Dom}(\mathcal{R}) = \{a \in A : (a,b) \in \mathcal{R}\}$. Moreover, the **range** of $\mathcal{R}$ is $\mathrm{Rng}(\mathcal{R}) = \{b \in B : (a,b) \in \mathcal{R}\}$.

Example 3.1.3

Let $A = \{1, 2, \{3\}, 4\}$ and $B = \{a, b, c, d\}$. Find the domain and range of $\mathcal{R}$, where

$$\mathcal{R} = \{(1,c), (\{3\},a), (1,d), (2,d)\} \subseteq A \times B.$$

Solution:

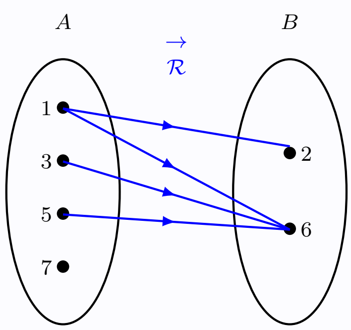
The $\mathrm{Dom}(\mathcal{R}) = \{1, 2, \{3\}\} \subseteq A$ and the $\mathrm{Rng}(\mathcal{R}) = \{a, c, d\} \subseteq B$. Note that $\mathrm{Dom}(\mathcal{R}) \neq A$ and $\mathrm{Rng}(\mathcal{R}) \neq B$.

Example 3.1.4

Let $A = \{1, 3, 5, 7\}$ and $B = \{2, 6\}$. Let $\mathcal{R} \subseteq A \times B$ defined by $\mathcal{R} = \{(a,b) \in A \times B : a < b\}$. Find $\mathcal{R}$ along with its domain and range.

Solution:

$$\mathcal{R} = \{(1,2), (1,6), (3,6), (5,6)\}$$
$$\mathrm{Dom}(\mathcal{R}) = \{1, 3, 5\}$$
$$\mathrm{Rng}(\mathcal{R}) = \{2, 6\}.$$



Example 3.1.5

Let $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2 + 3\}$. Find the domain and the range of the relation $\mathcal{R}$.

Solution:

Domain: $x \in \text{Dom}(\mathcal{R})$ iff $\exists y \in \mathbb{R}$ with $y = x^2 + 3$ which is true for all $x \in \mathbb{R}$. Thus, $\text{Dom}(\mathcal{R}) = \mathbb{R}$. Range: $y \in \text{Rng}(\mathcal{R})$ iff $\exists x \in \mathbb{R}$ with $y = x^2 + 3$ and since $x^2 \geq 0$, we have $y \geq 3$. Therefore, $\text{Rng}(\mathcal{R}) = [3, \infty)$.

Definition 3.1.5

For any set A, the relation $\mathcal{I}_A$ is the **identity relation** on A and is defined by

$$\mathcal{I}_A = \{(a, a) : a \in A\},$$

with $\text{Dom}(\mathcal{I}_A) = A = \text{Rng}(\mathcal{I}_A)$.

Definition 3.1.6

For any sets A and B, if $\mathcal{R} \subseteq A \times B$ is a relation, then the **inverse relation** is

$$\mathcal{R}^{-1} = \{(b, a) : (a, b) \in \mathcal{R}\} \subseteq B \times A,$$

with $\text{Dom}(\mathcal{R}^{-1}) = \text{Rng}(\mathcal{R})$ and $\text{Rng}(\mathcal{R}^{-1}) = \text{Dom}(\mathcal{R})$.

Definition 3.1.7

Let $\mathcal{R} \subseteq A \times B$ be a relation and let $\mathcal{S} \subseteq B \times C$ be a relation. The **composition relation** $\mathcal{S} \circ \mathcal{R}$ is defined by

$$\mathcal{S} \circ \mathcal{R} = \{(a, c) : (\exists b \in B)\big((a, b) \in \mathcal{R} \text{ and } (b, c) \in \mathcal{S}\big)\} \subseteq A \times C.$$

Moreover, $\text{Dom}(\mathcal{S} \circ \mathcal{R}) \subseteq \text{Dom}(\mathcal{R})$.

Example 3.1.6

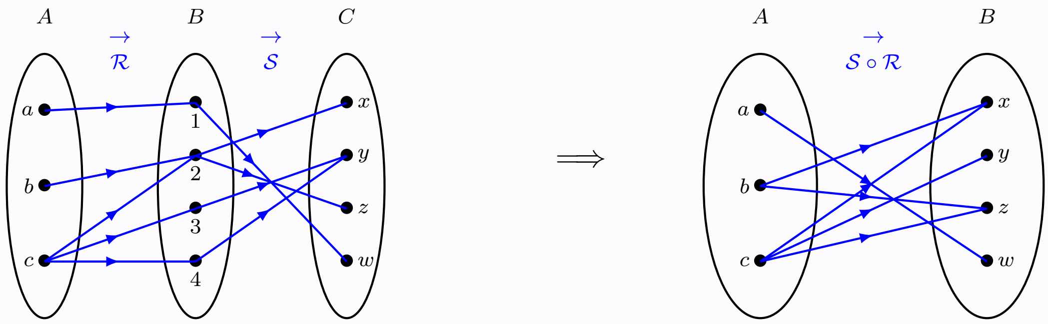
Let $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $C = \{x, y, z, w\}$. Let

$$\mathcal{R} = \{(a,1),(b,2),(c,2),(c,3),(c,4)\} \subseteq A \times B, \text{ and}$$
$$\mathcal{S} = \{(1,w),(2,x),(2,z),(3,y),(4,y)\} \subseteq B \times C.$$

Find $\mathcal{R}^{-1}$, and $\mathcal{S} \circ \mathcal{R}$.

Solution:

$$\begin{aligned} \mathcal{R}^{-1} &= \{(1,a),(2,b),(2,c),(3,c),(4,c)\} \subseteq B \times A. \\ \mathcal{S} \circ \mathcal{R} &= \{(a,w),(b,x),(b,z),(c,x),(c,z),(c,y)\} \subseteq A \times C. \end{aligned}$$



Example 3.1.7

Let $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}$. Find $\mathcal{R}^{-1}$.

Solution:

Note that

$$\begin{aligned} (x,y) \in \mathcal{R}^{-1} \quad &\text{iff} \quad (y,x) \in \mathcal{R} \\ &\text{iff} \quad y < x \\ &\text{iff} \quad x > y. \end{aligned}$$

That is $\mathcal{R}^{-1} = \{\, (x, y) \in \mathbb{R} \times \mathbb{R} : x > y \,\}$.

Example 3.1.8

Let $\mathcal{R} = \{ (x,y) \in \mathbb{R} \times \mathbb{R} : y = x - 1 \}$ and let $\mathcal{S} = \{ (x,y) \in \mathbb{R} \times \mathbb{R} : y = x^2 \}$. Find $\mathcal{S} \circ \mathcal{R}$ and $\mathcal{R} \circ \mathcal{S}$.

Solution:

$$\begin{aligned} \mathcal{S} \circ \mathcal{R} &= \{ (x,y) : (\exists z \in \mathbb{R})((x,z) \in \mathcal{R} \text{ and } (z,y) \in \mathcal{S}) \} \\ &= \left\{ (x,y) : (\exists z \in \mathbb{R}) \left(z = x - 1 \text{ and } y = z^2 \right) \right\} \\ &= \left\{ (x,y) : (\exists z \in \mathbb{R}) \left(y = (x-1)^2 \right) \right\} \end{aligned}$$

$$\begin{aligned} \mathcal{R} \circ \mathcal{S} &= \{ (x,y) : (\exists z \in \mathbb{R})((x,z) \in \mathcal{S} \text{ and } (z,y) \in \mathcal{R}) \} \\ &= \left\{ (x,y) : (\exists z \in \mathbb{R}) \left(z = x^2 \text{ and } y = z - 1 \right) \right\} \\ &= \left\{ (x,y) : (\exists z \in \mathbb{R}) \left(y = x^1 - 1 \right) \right\} \end{aligned}$$

Theorem 3.1.3

Let A, B, C, and D be sets. Let $\mathcal{R} \subseteq A \times B$, $\mathcal{S} \subseteq B \times C$, and $\mathcal{T} \subseteq C \times D$. Then,

1. $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.
2. $\mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) = (\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R}$.
3. $(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$.

Proof:

Proof of part(2): Let $a \in A$ and $d \in D$ so that

$$\begin{aligned} (a,d) \in \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) \quad &\text{iff} \quad (\exists c \in C)\Big[(a,c) \in \mathcal{S} \circ \mathcal{R} \text{ and } (c,d) \in \mathcal{T}\Big] \\ &\text{iff} \quad (\exists c \in C)\Big[(\exists b \in B)\Big((a,b) \in \mathcal{R} \text{ and } (b,c) \in \mathcal{S}\Big) \text{ and } (c,d) \in \mathcal{T}\Big] \\ &\text{iff} \quad (\exists c \in C)(\exists b \in B)\Big[(a,b) \in \mathcal{R} \text{ and } (b,c) \in \mathcal{S} \text{ and } (c,d) \in \mathcal{T}\Big] \\ &\text{iff} \quad (\exists b \in B)\Big[(a,b) \in \mathcal{R} \text{ and } (\exists c \in C)\Big((b,c) \in \mathcal{S} \text{ and } (c,d) \in \mathcal{T}\Big)\Big] \\ &\text{iff} \quad (\exists b \in B)\Big[(a,b) \in \mathcal{R} \text{ and } (b,d) \in \mathcal{T} \circ \mathcal{S}\Big] \\ &\text{iff} \quad (a,d) \in (\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R}. \end{aligned}$$

Proof of part (3): Let $a \in A$ and $c \in C$ so that

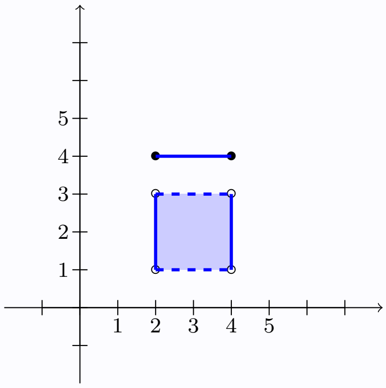
$$\begin{aligned}(c,a) \in (\mathcal{S}\circ\mathcal{R})^{-1} \quad &\text{iff} \quad (a,c) \in \mathcal{S}\circ\mathcal{R}\\ &\text{iff} \quad (\exists b \in B)\big[(a,b) \in \mathcal{R} \text{ and } (b,c) \in \mathcal{S}\big]\\ &\text{iff} \quad (\exists b \in B)\big[(b,a) \in \mathcal{R}^{-1} \text{ and } (c,b) \in \mathcal{S}^{-1}\big]\\ &\text{iff} \quad (\exists b \in B)\big[(c,b) \in \mathcal{S}^{-1} \text{ and } (b,a) \in \mathcal{R}^{-1}\big]\\ &\text{iff} \quad (c,a) \in \mathcal{R}^{-1}\circ\mathcal{S}^{-1}.\end{aligned}$$

Example 3.1.9

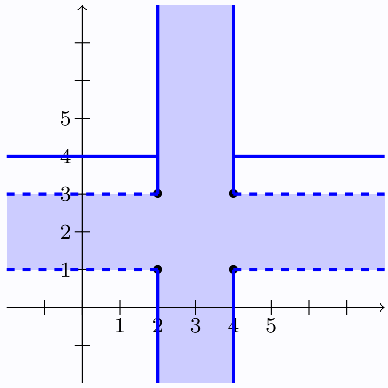
Let $A = [2,4]$ and $B = (1,3) \cup \{4\}$. Let $\mathcal{R}$ be the relation on $A \times \mathbb{R}$ with $x\mathcal{R}y$ iff $x \in A$ and let $\mathcal{S}$ be the relation on $\mathbb{R} \times B$ with $x\mathcal{S}y$ iff $y \in B$. Find $\mathcal{R}\cap\mathcal{S}$ and $\mathcal{R}\cup\mathcal{S}$.

Solution:

By Theorem 3.1.2 part(2), $\mathcal{R}\cap\mathcal{S} = (A\times\mathbb{R})\cap(\mathbb{R}\times B) = (A\cap\mathbb{R})\times(\mathbb{R}\cap B) = A\times B$. Therefore, $\mathcal{R}\cap\mathcal{S} = A\times B = \{(a,b) : a \in A \text{ and } b \in B\}$. On the other hand, $\mathcal{R}\cup\mathcal{S} = \{(a,b) \in \mathbb{R}\times\mathbb{R} : a \in A \text{ or } b \in B\}$.



$\mathcal{R}\cap\mathcal{S}$



$\mathcal{R}\cup\mathcal{S}$

Exercise 3.1.1

Let A and B be two nonempty sets. Show that if $A \times B \subseteq B \times C$, then $A \subseteq C$.

Exercise 3.1.2

Let $\mathcal{R} \subseteq A \times B$ and $\mathcal{S} \subseteq B \times C$ be two relations. Show that $\text{Dom}(\mathcal{S}\circ\mathcal{R}) \subseteq \text{Dom}(\mathcal{R})$.

Section 3.2: Equivalence Relations

Definition 3.2.1

Let A be a set and $\mathcal{R}$ be a relation on A. Then $\mathcal{R}$ is called an **equivalence relation** if and only if:

1. $\mathcal{R}$ is **reflexive** on A: $(\forall x \in A)\ x\mathcal{R}x$.
2. $\mathcal{R}$ is **symmetric** on A: $(\forall x, y \in A)$ if $x\mathcal{R}y$, then $y\mathcal{R}x$.
3. $\mathcal{R}$ is **transitive** on A: $(\forall x, y, z \in A)$ if $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$.

Example 3.2.1

Let $A = \{1, 2, 3, 4\}$ and $\mathcal{R}_1 = \{(1, 2), (2, 3), (1, 3)\}$, $\mathcal{R}_2 = \{(1, 1), (1, 2)\}$, $\mathcal{R}_3 = \{(3, 4)\}$, $\mathcal{R}_4 = \{(1, 2), (2, 1)\}$, and $\mathcal{R}_5 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$. Decide which relation is reflexive, symmetric, transitive.

Solution:

$\mathcal{R}_5$ is reflexive. $\mathcal{R}_4$, and $\mathcal{R}_5$ are symmetric. $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$, and $\mathcal{R}_5$ are transitive. Therefore, $\mathcal{R}_5$ is an equivalence relation on A.

Example 3.2.2

Let $\mathcal{R} = \{(x, y) : xy > 0\}$ be a relation on $\mathbb{Z}$. Discuss whether $\mathcal{R}$ reflexive, symmetric, transitive, and equivalence relation.

Solution:

Clearly, $x\mathcal{R}x$ for all $x \in \mathbb{Z}$ except for $x = 0$, thus $\mathcal{R}$ is not reflexive. If $x\mathcal{R}y$, then $xy > 0$ or $yx > 0$ which imples that $y\mathcal{R}x$. Thus, $\mathcal{R}$ is symmetric. If $x\mathcal{R}y$ and $y\mathcal{R}z$, then $xy > 0$ and $yz > 0$. Considering the cases of $y \in \mathbb{Z} - \{0\}$, we have

1. case 1: $y > 0$, then $x > 0$ and $z > 0$ which implies that $xz > 0$ and thus $x\mathcal{R}z$.
2. case 1: $y < 0$, then $x < 0$ and $z < 0$ which implies that $xz > 0$ and thus $x\mathcal{R}z$.

In either cases, $\mathcal{R}$ is transitive on $\mathbb{Z}$. Note that $\mathcal{R}$ is not reflexive and thus it is not an equivalence relation on $\mathbb{Z}$.

Example 3.2.3

Let $\mathcal{R}$ be the relation on $\mathbb{Z}$ given by $x\mathcal{R}y$ iff $x-y$ is even. Show that $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.

Solution:

Reflexive: Since $x-x=0$ is even, $x\mathcal{R}x$ for all $x\in\mathbb{Z}$. Thus, $\mathcal{R}$ is reflexive.

Symmetric: Assume that $x\mathcal{R}y$, then there is $k\in\mathbb{Z}$ such that $x-y=2k$. Thus, $y-x=2(-k)$ which implies that $y\mathcal{R}x$. Thus, $\mathcal{R}$ is symmetric.

Transitive: Let $x\mathcal{R}y$ and $y\mathcal{R}z$. Then, there are $h,k\in\mathbb{Z}$ such that $x-y=2h$ and $y-z=2k$. Adding these two equations, we get $x-z=2(h+k)$ which is even. Therefore, $x\mathcal{R}z$ and $\mathcal{R}$ is transitive.

Therefore, $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.

Definition 3.2.2

Let $\mathcal{R}$ be an equivalence relation on a set A. For $x\in A$, define the **equivalence class** of x determined by $\mathcal{R}$ as

$$x/\mathcal{R}=\{y\in A : x\mathcal{R}y\},$$

which reads "the class of x modulo $\mathcal{R}$" or "x mod $\mathcal{R}$. The set of all equivalence classes is called A modulo $\mathcal{R}$ and is defined by

$$A/\mathcal{R}=\{x/\mathcal{R} : x\in A\}.$$

Example 3.2.4

Let $\mathcal{R}=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ be an equivalence relation on $A=\{1,2,3\}$. Find:

- $1/\mathcal{R}=\{1,2\}$.
- $2/\mathcal{R}=\{1,2\}$.
- $3/\mathcal{R}=\{3\}$.
- $A/\mathcal{R}=\{\{1,2\},\{3\}\}$.

Example 3.2.5

Let $\mathcal{R}$ be a relation on $\mathbb{N}$ so that $x\mathcal{R}y \Leftrightarrow 2 \mid x+y$. Show that $\mathcal{R}$ is an equivalence relation on $\mathbb{N}$. Calculate all the equivalence classes of $\mathcal{R}$.

Solution:

reflexive: Since $x+x=2x$, $2 \mid x+x$ and thus $x\mathcal{R}x$. So, $\mathcal{R}$ is reflexive.

symmetric: if $x\mathcal{R}y$, then $2 \mid x+y$. Thus, $2 \mid y+x$ as well and $y\mathcal{R}x$. Therefore, $\mathcal{R}$ is symmetric.

transitive: Assume that $x\mathcal{R}y$ and $y\mathcal{R}z$. Then $2 \mid x+y$ and $2 \mid y+z$. Thus, $2 \mid x+z+2y$. But because $2 \mid 2y$, we have $2 \mid x+z$. Thus, $x\mathcal{R}z$ and $\mathcal{R}$ is transitive.

Therefore, $\mathcal{R}$ is an equivalence relation on $\mathbb{N}$.

For $x \in \mathbb{N}$, $x/\mathcal{R} = \{y \in \mathbb{N} : 2 \mid x+y\}$. Thus,

$$\overline{1} = \{1,3,5,7,9,\cdots\} = \overline{3} = \overline{5} = \cdots, \text{ and } \overline{2} = \{2,4,6,8,10,\cdots\} = \overline{2} = \overline{4} = \cdots.$$

Therefore, $\mathbb{N} = \overline{1} \cup \overline{2}$.

Theorem 3.2.1

Let $\mathcal{R}$ be an equivalence relation on a nonempty set A. For all $x, y \in A$,

1. $x/\mathcal{R} \subseteq A$ and $x \in x/\mathcal{R} \neq \phi$.
2. $x\,\mathcal{R}\,y$ iff. $x/\mathcal{R} = y/\mathcal{R}$.
3. $x\not\mathcal{R}y$ iff. $x/\mathcal{R} \cap y/\mathcal{R} = \phi$.

Proof:

1. Clearly, $x/\mathcal{R} \subseteq A$ by the definition. Since$\mathcal{R}$ is reflexive, $x\,\mathcal{R}\,x$ and hence $x \in x/\mathcal{R}$.
2. „ $\Rightarrow$ ": Suppose $x\,\mathcal{R}\,y$. Then $y\,\mathcal{R}\,x$ (since $\mathcal{R}$ is symmetric). To show that $x/\mathcal{R} = y/\mathcal{R}$, we first show that $x/\mathcal{R} \subseteq y/\mathcal{R}$: Let $z \in x/\mathcal{R} \Rightarrow x\,\mathcal{R}\,z$ and $y\,\mathcal{R}\,x$. Hence, $y\,\mathcal{R}\,z$. Hence, $x/\mathcal{R} \subseteq y/\mathcal{R}$. The proof of $y/\mathcal{R} \subseteq x/\mathcal{R}$ is similar.

   „ $\Leftarrow$ ": Suppose $x/\mathcal{R} = y/\mathcal{R}$. Then $x \in x/\mathcal{R} = y/\mathcal{R}$. That is $x\,\mathcal{R}\,y$.
3. „ $\Rightarrow$ ": Suppose $x\not\mathcal{R}y$. We proof by contradiction: Assume that there is $z \in x/\mathcal{R} \cap y/\mathcal{R}$. Then, $z \in x/\mathcal{R}$ and $z \in y/\mathcal{R}$ and hence $x\,\mathcal{R}\,z$ and $z\,\mathcal{R}\,y$. Thus, $x\,\mathcal{R}\,y$, contradiction.

   „ $\Leftarrow$ ": Suppose $x/\mathcal{R} \cap y/\mathcal{R} = \phi$. Then, $x \in x/\mathcal{R}$. Thus, $x \notin y/\mathcal{R}$ and hence $x\not\mathcal{R}y$.

Definition 3.2.3

Let $m \neq 0$ be a fixed integer. Then "$\equiv_m$" denotes the relation on $\mathbb{Z}$ and is defined by

$$\big(x \equiv y \mod m \text{ or } x \equiv_m y\big) \Leftrightarrow m \mid x - y,$$

which reads "x is congruent to y modulo m". That is $\overline{x} = \{y \in \mathbb{Z} : x \equiv_m y \Leftrightarrow m \mid x - y\}$, and the set of equivalence classes for $\equiv_m$ is $\mathbb{Z}$ mod m (denoted $\mathbb{Z}_m$) and is defined by

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}.$$

Example 3.2.6

Find all the equivalence classes of $\mathbb{Z}_3$.

Solution:

Note that $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, where $\overline{x} = \{y \in \mathbb{Z} : x \equiv y \mod 3 \text{ or } 3 \mid x - y\}$. Therefore,

- $\overline{0} = 0/\equiv_3 = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$,
- $\overline{1} = 1/\equiv_3 = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}$,
- $\overline{2} = 2/\equiv_3 = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}$,

Therefore, $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

Theorem 3.2.2

Let $m \neq 0$ be a fixed integer. The relation $\equiv_m$ is an equivalence relation on $\mathbb{Z}$. Moreover, $\mathbb{Z}_m$ has m distinct elements: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$.

Proof:

We only show that $\equiv_m$ is an equivalence relation. reflexive: Since $x - x = 0$ which is divisible by m, $x \equiv_m x$. Thus $\equiv_m$ is reflexive.

symmetric: Assume that $x \equiv_m y$, then $m \mid x - y$ which implies that $m \mid y - x$. Thus, $y \equiv_m x$ and $\equiv_m$ is symmetric.

transitive: Assume that $x \equiv_m y$ and $y \equiv_m z$, then $m \mid x - y$ and $m \mid y - z$. Thus, $m \mid (x - y) + (y - z)$ which implies $m \mid x - z$. Therefore, $x \equiv_m z$ and $\equiv_m$ is transitive. That shows that $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

Exercise 3.2.1

Let $m \neq 0$. For $x, y \in \mathbb{Z}$: Show that $x \equiv_m y$ if and only if $\overline{x} = \overline{y}$.

Exercise 3.2.2

Let $\mathcal{R}$ be a relation on the set A. Prove that $\mathcal{R} \cup \mathcal{R}^{-1}$ is symmetric.

Exercise 3.2.3

Let $\mathcal{R}$ be a relation on $\mathbb{N}$ so that $x\mathcal{R}y$ iff $3 \mid x + y$. Determine whether $\mathcal{R}$ an equivalence relation. Explain.

Exercise 3.2.4

Let $\mathcal{R}$ be a relation on $\mathbb{N}$ so that $x\mathcal{R}y$ iff $3 \mid x + 2y$. Show that $\mathcal{R}$ is an equivalence relation on $\mathbb{N}$. Find the equivalence class of 1.

Exercise 3.2.5

Let $\mathcal{R}$ be a relation on $\mathbb{R}$ so that $x \, \mathcal{R} \, y$ iff $x = y$ or $xy = 1$. Show that $\mathcal{R}$ is an equivalence relation on $\mathcal{R}$. Find the equivalence classes for 2; 0; and $-\frac{1}{5}$.

Section 3.3: Partitions

Definition 3.3.1

Let A be a set and $\mathcal{A}$ be a family of subsets of A. $\mathcal{A}$ is called a **partition** of A if and only if:

1. if $X \in \mathcal{A}$, then $X \neq \phi$.
2. if $X, Y \in \mathcal{A}$, then either $X = Y$ or $X \cap Y = \phi$.
3. $\bigcup\limits_{X \in \mathcal{A}} X = A$.

Example 3.3.1

1. The set of even natural numbers and odd natural numbers is a partition of $\mathbb{N}$.
2. Let $A_0 = \{0\}$ and $A_i = \{-i, i\}$ for all $i \in \mathbb{N}$. Then $\mathcal{A} = \{A_0, A_1, A_2, A_3, \cdots\}$ is a partition of $\mathbb{Z}$.
3. The set $\{0/\equiv_3, 1/\equiv_3, 2/\equiv_3\}$ is a partition of $\mathbb{Z}$.
4. The set $\{\{$ male students, female students $\}\}$ is a partition for the set of all students in Kuwait University.
5. The collection $\{\, B_i : i \in \mathbb{Z}\,\}$, where $B_i = [i, i+1)$ is a partition of $\mathbb{R}$.

Theorem 3.3.1

Let $A \neq \phi$ and let $\mathcal{R}$ be an equivalence relation on A. Then, the family $A/\mathcal{R} = \{x/\mathcal{R} : x \in A\}$ is a partition of A.

Proof:

Do it your self!

Section 3.4: Ordering Relations

Definition 3.4.1

A relation $\mathcal{R}$ on a set A is called **antisymmetric** if for all $x, y \in A$, if $x\mathcal{R}y$ and $y\mathcal{R}x$, then $x = y$.

Definition 3.4.2

A relation $\mathcal{R}$ on a set A is called a **partial order** (or **partial ordering**) for A if $\mathcal{R}$ is reflexive, antisymmetric, and transitive. In that case, A is called a **partially ordered set** or a **poset**.

Example 3.4.1

Show that "$\subseteq$" is a partial order relation on $\mathcal{P}(A)$ for any set A.

Solution:

reflexive: if $X \in \mathcal{P}(A)$, then $X \subseteq A$ and hence $X \subseteq X$ and hence $x\mathcal{R}x$.

antisymmetric: Let $X, Y \in \mathcal{P}(A)$ with $X\mathcal{R}Y$ and $Y\mathcal{R}X$. Then, $X \subseteq Y$ and $Y \subseteq X$. Therefore, $X = Y$ and $\mathcal{R}$ is antisymmetric.

transitive: Assume that $X, Y, Z \in \mathcal{P}(A)$ with $X \subseteq Y$ and $Y \subseteq Z$. Then $X \subseteq Z$ and hence $X\mathcal{R}Z$.

Therefore, $\mathcal{R}$ is a partial order relation on $\mathcal{P}(A)$.

Example 3.4.2

Let $\mathcal{R}$ be a relation on $\mathbb{N}$ so that $a\mathcal{R}b \Leftrightarrow a \mid b$ for all $a, b \in \mathbb{N}$. Show that $\mathcal{R}$ is a partial order on $\mathbb{N}$.

Solution:

reflexive: Since $a = 1 \cdot a$ for all $a \in \mathbb{N}$, then $a \mid a$ and $a\mathcal{R}a$. Hence, $\mathcal{R}$ is reflexive.

antisymmetric: Assume that $a \mid b$ and $b \mid a$. Then, there are $h, k \in \mathbb{N}$ such that $b = ha$ and $a = kb$. Thus, $b = ha = h(kb) = (hk)b$. Then, $hk = 1$ which implies that $h = k = 1$. Therefore, $a = b$ and $\mathcal{R}$ is antisymmetric.

transitive: Assume that $a \mid b$ and $b \mid c$. Then, Theorem 1.4.1 implies that $a \mid c$. Thus, $a\mathcal{R}c$

and $\mathcal{R}$ is transitive. Therefore, $\mathcal{R}$ is a partial order on $\mathbb{N}$.

Example 3.4.3

Let $\mathcal{R}$ be a relation on $\mathbb{N}$ so that $a\mathcal{R}b$ iff $2 \mid a+b$ with $a \leq b$ for all $a, b \in \mathbb{N}$. Show that $\mathbb{N}$ is a poset with respect to $\mathcal{R}$.

Solution:

reflexive: Since $2 \mid a+a = 2a$ with $a \leq a$, $a\mathcal{R}a$ and $\mathcal{R}$ is reflexive.

antisymmetric: Assume that $a\mathcal{R}b$ and $b\mathcal{R}a$. Then, $2 \mid a+b$ with $a \leq b$ and $2 \mid b+a$ with $b \leq a$. Thus, $a \leq b \leq a$ which implies that $a = b$. Thus, $\mathcal{R}$ is antisymmetric.

transitive: Assume that $a\mathcal{R}b$ and $b\mathcal{R}c$. Then, $2 \mid a+b$ with $a \leq b$ and $2 \mid b+c$ with $b \leq c$. Therefore, by Theorem 1.4.1, $2 \mid a+2b+c$ which implies that $2 \mid a+c$ with $a \leq b \leq c$. Thus, $a\mathcal{R}c$ and $\mathcal{R}$ is transitive. Therefore, $\mathbb{N}$ is a poset with respect to $\mathcal{R}$.

3.4.1 Upper and Lower Bounds

Definition 3.4.3

Let $\mathcal{R}$ be a partial order for A and let B be any subset of A. Then,

- $a \in A$ is an **upper bound** for B if for every $b \in B$, $b\mathcal{R}a$. Also, a is called a "**least upper bound**" or "**supremum** for B, denoted by $\sup(B)$, if:
  1. a is an upper bound for B, and
  2. $a\mathcal{R}x$ for every upper bound x for B.
- $a \in A$ is a **lower bound** for B if for every $b \in B$, $a\mathcal{R}b$. Also, a is called a "**greatest upper bound**" or "**infimum** for B, denoted by $\inf(B)$, if:
  1. a is a lower bound for B, and
  2. $x\mathcal{R}a$ for every lower bound x for B.

Theorem 3.4.1

If $\mathcal{R}$ is a partial order for a set A and $B \subseteq A$, then if the least upper bound (or greatest lower bound) for B exists, then it is unique.

Proof:

Assume that x and y are both least upper bound for B. Since x is an upper bound and y is the least upper bound, thus $y\mathcal{R}x$. Similarly, since y is an upper bound and x is the least upper bound, thus $x\mathcal{R}y$. Since $\mathcal{R}$ is antisymmetric, $x\mathcal{R}y$ and $y\mathcal{R}x$, implies $x = y$.

Example 3.4.4

Let $A = [0, 6) \subset \mathbb{R}$ be a poset with respect to "$\leq$", and let $B = \{\frac{1}{2}, 3, 5\}$ and $C = \{1, \frac{1}{2}, \frac{1}{3}, \cdots\}$ be two subsets of A. Find $\sup(B)$, $\inf(B)$, $\sup(C)$, and $\inf(C)$.

Solution:

<u>$\sup(B)$</u>: Note that $5, 5.1, 5.35, 5.9$, and so on are all considered upper bounds for B since for example $b \leq 5$ for all $b \in B$. Then, $\sup(B) = 5$ since $5 \leq x$ for all upper bounds for B.

<u>$\inf(B)$</u>: $0, \frac{1}{2}, \frac{1}{4}, \frac{1}{45}$ and so on are all considered lower bounds for B since for example $\frac{1}{4} \leq b$ for all $b \in B$. Then, $\inf(B) = \frac{1}{2}$ since $\frac{1}{2} \leq x$ for all lower bounds x for B.

<u>$\sup(C)$</u>: The set of upper bounds for C consists of $\{1, 2, 1.5, 3, 5, 5.5, \cdots\}$ while the $\sup(C) = 1$.

<u>$\inf(C)$</u>: The set of upper bounds for C consists of $\{0\}$ and the $\inf(C) = 0$.

Note that, if $A = (0, 6)$, then C would has no $\inf(C)$.

Example 3.4.5

Let $A = \{1, 2, 3, 4, 5, 6\}$ and consider $\mathcal{P}(A)$ with the partial ordering "$\subseteq$". Let $B = \big\{\{1, 2\}, \{1, 2, 3\}, \{1, 2, 6\}\big\}$. Find $\sup(B)$ and $\inf(B)$.

Solution:

Upper bound for B are like $\{1, 2, 3, 6\}$, $\{1, 2, 3, 4, 6\}$, $\{1, 2, 3, 5, 6\}$, and A it self. Therefore, $\sup(B) = \{1, 2, 3, 6\} = \bigcup\limits_{X \in B} X$. On the other hand, ϕ, $\{1\}$, $\{2\}$, and $\{1, 2\}$ are all lower bounds for B while the $\inf(B) = \{1, 2\} = \bigcap\limits_{X \in B} X$.

Exercise 3.4.1

Let $\mathcal{R}$ be a relation on $\mathbb{N}$ so that $x\mathcal{R}y$ iff $y = 2^k x$ for some integer $k \geq 0$. Show that $\mathbb{N}$ is a poset with respect to $\mathcal{R}$.

Chapter

4 Functions

Section 4.1: Functions as Relations

Definition 4.1.1

A **function** f from A to B is a relation from A to B that satisfies

1. $\mathrm{Dom}(f) = A$,
2. if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

Moreover, if $A = B$, we say that f is a function on A.

Remark 4.1.1: Notations

A function (mapping) f from A to B is denoted by $f : A \to B$. The **domain** of f is A and the **codomain** of f is B.

If $(x, y) \in f$, then $y = f(x)$ where we say that y is the **image** of x and that x is the **preimage** of y. The **range** of f is a subset of B and is defined as

$$\mathrm{Rng}(f) = \{y \in B : \exists x \in A \text{ with } y = f(x)\}.$$

Example 4.1.1

Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. Let $\mathcal{R}_1 = \{(1, a), (2, b), (2, c), (3, c)\}$, $\mathcal{R}_2 = \{(1, a), (2, c), (3, b)\}$, and $\mathcal{R}_3 = \{(1, a), (2, c)\}$ be three relations on $A \times B$. Decide whether $\mathcal{R}_1$, $\mathcal{R}_2$, and $\mathcal{R}_3$ a function.

Solution:

$\mathcal{R}_1$ is clearly not a function since $(2, b)$ and $(2, c)$ both are in $\mathcal{R}_1$ where $b \neq c$. $\mathcal{R}_2$ satisfies the conditions of Definition 4.1.1 and so it is a function from A to B.

$\mathcal{R}_3$ is not a function from A to B; however, it is a function from $\{1, 2\}$ to $\{a, c\}$.

Example 4.1.2

Let $\mathcal{S} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}$ be a relation on $\mathbb{R}$. Is $\mathcal{S}$ a function? Explain.

Solution:

Note that for $x = 0$, we have $y = -1$ or $y = 1$ and so $\mathcal{S}$ is not a function. Another reason is that for $x = 5$, $y^2 = -24 \notin \mathbb{R}$.

Example 4.1.3

Let $f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y = x^2\}$. Determine whether f a function on $\mathbb{Z}$.

Solution:

$f : \mathbb{Z} \to \mathbb{Z}$ is a function with $\text{Rng}(f) = \{0, 1, 4, 9, 16, \cdots\}$. That is $f(x) = x^2$ is a function from $\mathbb{Z}$ to $\mathbb{Z}$.

⋆ **Constant Function**: $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = c$ (c is a constant) for all $x \in \mathbb{R}$.

Example 4.1.4

Let $f = \{\,(\,x, y\,) \in \mathbb{R} \times \mathbb{R} : y = 2x + 5\,\}$. Show that f is a function from $\mathbb{R}$ to $\mathbb{R}$.

Solution:

We first show that $\text{Dom}(f) = \mathbb{R}$. Clearly, $\text{Dom}(f) \subseteq \mathbb{R}$ by the definition of f. Next, let $x \in \mathbb{R}$. Then there is $y = 2x + 5 \in \mathbb{R}$ and hence $(x, y) \in f$. That is $x \in \text{Dom}(f)$.
Now assume that $(x, y), (x, z) \in f$, we want to show that $y = z$. But since $y = 2x + 5$ and $z = 2x + 5$, we have $y = z$. Therefore, f is a function from $\mathbb{R}$ to $\mathbb{R}$.

Theorem 4.1.1

Two functions f and g are equal iff (i) $\text{Dom}(f) = \text{Dom}(g)$, and (ii) for all $x \in \text{Dom}(f)$, $f(x) = g(x)$.

Proof:

" $\Rightarrow$ ": Assume that $f = g$. Proof of (i): If $x \in \text{Dom}(f)$, then $(x, y) \in f = g$ for some y and hence $x \in \text{Dom}(g)$. Thus, $\text{Dom}(f) \subseteq \text{Dom}(g)$. Similarly, if $x \in \text{Dom}(g)$, then $(x, y) \in g = f$

for some y and hence $x \in \mathrm{Dom}(f)$. Thus, $\mathrm{Dom}(g) \subseteq \mathrm{Dom}(f)$. Therefore, $\mathrm{Dom}(f) = \mathrm{Dom}(g)$.

Proof of (ii): Let $x \in \mathrm{Dom}(f)$. Then for some y, $(x, y) \in f = g$. Thus, $f(x) = y = g(x)$.

„ $\Leftarrow$ ": Assume that $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ and that for all $x \in \mathrm{Dom}(f)$, $f(x) = g(x)$. Suppose that $(x, y) \in f$, then there is y such that $y = f(x)$ and $x \in \mathrm{Dom}(f) = \mathrm{Dom}(g)$. Thus, $y = f(x) = g(x)$ which implies that $(x, y) \in g$ and hence $f \subseteq g$. Now suppose that $(x, y) \in g$. Then there is y such that $y = g(x) = f(x)$ for $x \in \mathrm{Dom}(f)$. Thus, $y = f(x)$ and $(x, y) \in f$. Hence $g \subseteq f$. Therefore, $f = g$.

Section 4.2: Constructions of Functions

Definition 4.2.1

Let $f : A \to B$ and $g : B \to C$ be two given functions. The **composition function** $g \circ f$ is defined by $g \circ f : A \to C$ where $(g \circ f)(x) = g(f(x))$ for every $x \in A$. Note that $f \circ g \neq g \circ f$, while $(f \circ g) \circ h = f \circ (g \circ h)$ for any three (appropriate) functions f, g, and h.

Example 4.2.1

Let $f(x) = \sin(x)$ and $g(x) = 2x + 1$ for $x \in \mathbb{R}$. Find $f \circ g$ and $g \circ f$.

Solution:

For any $x \in \mathbb{R}$, we have

1. $(f \circ g)(x) = f(g(x)) = f(2x + 1) = \sin(2x + 1)$.
2. $(g \circ f)(x) = g(f(x)) = g(\sin(x)) = 2\sin(x) + 1$.

Definition 4.2.2

Let $f : A \to B$ and let $D \subseteq A$. The "**restriction of f to D**", denoted by $f|_D$, is a function with domain D and is defined as

$$f|_D = \{(x, y) : (x, y) \in f \text{ and } x \in D\}.$$

In that case, we say that f is an **extension** of $f|_D$.

Example 4.2.2

Let $f : A \to B$ be a function where $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, and $f = \{(1, a), (2, a), (3, b), (4, c)\}$. Find $f|_A$, $f|_{\{1\}}$, and $f|_{\{2,4\}}$.

Solution:

Clearly, $f|_A = f$, $f|_{\{1\}} = \{(1, a)\}$, and $f|_{\{2,4\}} = \{(2, a), (4, c)\}$.

Remark 4.2.1

Let $f : A \to B$ and $g : C \to D$ be two functions. Then,

1. $f \cap g$ is a function with $\text{Dom}(f \cap g) = \{x \in A \cap C : f(x) = y = g(x) \in B \cap D\}$.

2. If $A \cap C = \phi$, then $f \cup g$ is a function with domain $A \cup B$.

Example 4.2.3

Let $f = \{(1, 2), (3, 5), (4, 2)\}$ and $g = \{(1, 2), (3, 6), (5, -10)\}$. Find $f \cap g$ and $f \cup g$ and decide whether either of those relation is a function.

Solution:

Clearly, f is a function from $A = \{1, 3, 4\}$ to $B = \{2, 5\}$ while g is a function from $C = \{1, 3, 5\}$ to $D = \{2, 6, -10\}$. So,

- $f \cap g = \{(1, 2)\}$ which is clearly a function from $\text{Dom}(f \cap g) = \{1\}$ to $\{2\}$.
- $f \cup g = \{(1, 2), (3, 5), (4, 2), (3, 6), (5, -10)\}$ which is not a function (by the definition) since 3 maps to two different values, namely 5 and 6.

Section 4.3: Functions That are Onto; One-to-One Functions

Definition 4.3.1

A function $f : A \to B$ is **onto (surjective mapping)** B iff $\text{Rng}(f) = B$. Also, f is called a **surjection**. In that case, we write $f : A \xrightarrow{onto} B$.

Remark 4.3.1

Since $\text{Rng}(f) \subseteq B$ is always true, f is a surjection iff $B \subseteq \text{Rng}(f)$. Thus,

$$f : A \xrightarrow{onto} B \iff (\forall b \in B)(\exists a \in A)(f(a) = b).$$

Example 4.3.1

Let $f(x) = x + 2$ and $g(x) = x^2 + 1$ for all $x \in \mathbb{R}$. Determine whether f and g are onto $\mathbb{R}$.

Solution:

- f is onto: Let $y \in \mathbb{R}$ (in the range of f), then there exists $x \in \mathbb{R}$ such that $y = x + 2$ or $x = y - 2$. Thus, $f(x) = f(y - 2) = (y - 2) + 2 = y$. Thus, f is onto $\mathbb{R}$.
- g is not onto: Let $y \in \mathbb{R}$, then $y = x^2 + 1$ so $x = \pm\sqrt{y - 1}$. So, y must be greater than or equal to 1. If we choose $y = 0$, then $x \notin \mathbb{R}$ and hence g is not onto $\mathbb{R}$.

Example 4.3.2

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function defined by $f(m, n) = 2^{m-1}(2n - 1)$. Show that f is onto $\mathbb{N}$.

Solution:

We show that $\mathbb{N} \subseteq \text{Rng}(f)$. That is, for all $s \in \mathbb{N}$, there exists $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $f(m, n) = s$. We consider the following two cases of s.

(*i*) if s is even: s can be written as $2^k t$, where $k \geq 1$ and t is odd. Since t is odd, $t = 2n - 1$ or $n = \frac{t+1}{2}$ for some $n \in \mathbb{N}$. Choosing $m = k + 1$, we have

$$f(m, n) = 2^{m-1}(2n - 1) = 2^k t = s.$$

Thus, $\mathbb{N} \subseteq \text{Rng}(f)$.

(*ii*) if s is odd: $s = 2n-1$ for some $n \in \mathbb{N}$. Choosing $m = 1$, we have $f(m,n) = 2^0(2n-1) = s$. Thus, $\mathbb{N} \subseteq \text{Rng}(f)$.

Therefore, f is onto $\mathbb{N}$.

Theorem 4.3.1

Let A, B, and C be three sets. Then,

1. If $f : A \xrightarrow{onto} B$ and $g : B \xrightarrow{onto} C$, then $g \circ f : A \xrightarrow{onto} C$. That is, the composite of surjective functions is a surjection.

2. If $f : A \to B$, $g : B \to C$, and $g \circ f : A \xrightarrow{onto} C$, then g is onto C.

Proof:

1. We show that for every $c \in C$, $c \in \text{Rng}(g \circ f)$. Since g is onto C, there exists $b \in B$ such that $g(b) = c$. but since f is onto B, there exists $a \in A$ such that $f(a) = b$. Thus, $(g \circ f)(a) = g(f(a)) = g(b) = c$. Thus, $c \in \text{Rng}(g \circ f)$.

2. We show that again $C \subseteq \text{Rng}(g \circ f)$. Let $c \in C$. Since $g \circ f$ is onto C, there exists $a \in A$ such that $(g \circ f)(a) = c$. Let $b = f(a) \in B$. Then, $(g \circ f)(a) = g(f(a)) = g(b) = c$. Thus, there exists $b \in B$ such that $g(b) = c$ and hence g is onto.

Definition 4.3.2

A function $f : A \to B$ is said to be "**one-to-one**" (**injective mapping**) iff $(a_1, b) \in f$ and $(a_2, b) \in f$ imply that $a_1 = a_2$. Also, f is called an **injection**. In that case, we write $f : A \xrightarrow{1-1} B$.

Remark 4.3.2

A function $f : A \xrightarrow{1-1} B$ is one-to-one if and only if

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \quad \text{or equivalently} \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2).$$

Example 4.3.3

Let $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 5x - 1$. Show that f is one-to-one.

Solution:

Assume that $f(a) = f(b)$, then $5a - 1 = 5b - 1 \Rightarrow 5a = 5b \Rightarrow a = b$. Thus, f is 1-1.

Example 4.3.4

Determine whether $f : \mathbb{R} \to \mathbb{R}$ is one-to-one, where $f(x) = \dfrac{1}{x^2 + 1}$.

Solution:

Assume that $f(a) = f(b)$, then

$$\frac{1}{a^2+1} = \frac{1}{b^2+1} \Rightarrow a^2 + 1 = b^2 + 1 \Rightarrow a^2 = b^2 \Rightarrow a = \pm b.$$

Therefore, f is not 1-1. For instance, $f(1) = f(-1)$ while $1 \neq -1$.

Example 4.3.5

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(m, n) = 2^{m-1}(2n - 1)$. Show that f is one-to-one.

Solution:

Assume that $f(a, b) = f(x, y)$ for $(a, b), (x, y) \in \mathbb{N} \times \mathbb{N}$. Then, $2^{a-1}(2b - 1) = 2^{x-1}(2y - 1)$. Consider the following cases:

1. if $a > x$: $2^{a-1}(2b-1) = 2^{x-1}(2y-1) \Rightarrow \underbrace{2^{a-x}(2b-1)}_{\text{even}} = \underbrace{(2y-1)}_{\text{odd}}$ which is impossible.
2. if $a < x$: $2^{a-1}(2b-1) = 2^{x-1}(2y-1) \Rightarrow \underbrace{(2b-1)}_{\text{odd}} = \underbrace{2^{x-a}(2y-1)}_{\text{even}}$ which is impossible.
3. if $a = x$: $2^{a-1}(2b-1) = 2^{x-1}(2y-1) \Rightarrow (2b-1) = (2y-1) \Rightarrow b = y$.

Thus, the only possible case is the third case which suggests that $(a, b) = (x, y)$. Therefore, f is 1-1.

Theorem 4.3.2

Let A, B, and C be three sets. Then,

1. If $f : A \xrightarrow{1-1} B$ and $g : B \xrightarrow{1-1} C$, then $g \circ f : A \xrightarrow{1-1} C$.
2. If $f : A \to B$ and $g : B \to C$, and $g \circ f : A \xrightarrow{1-1} C$, then $f : A \xrightarrow{1-1} B$.

Proof:

1. Assume that $(g \circ f)(x) = (g \circ f)(y)$ for some $x, y \in A$. Then, $g(f(x)) = g(f(y))$. Since, g is 1-1, $f(x) = f(y)$, and since f is 1-1 as well, $x = y$. Therefore, $g \circ f$ is 1-1.
2. Assume that $f(x) = f(y)$ for $x, y \in A$. Then $g(f(x)) = g(f(y))$ implies that $(g \circ f)(x) = (g \circ f)(y)$. Since $g \circ f$ is 1-1, $x = y$. Thus, f is 1-1.

Remark 4.3.3

Horizontal Line Test: Let $f : A \to B$ be a given function. Then,

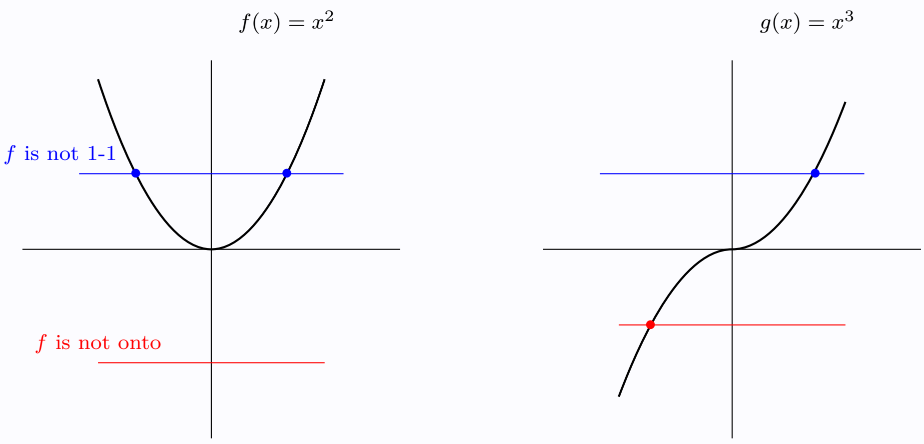
1. f is onto B iff for all $b \in B$, the horizontal line $y = b$ intersects the graph of f at least once.
2. f is one-to-one iff for all $b \in B$, the horizontal line $y = b$ intersects the graph of f at most once.

Example 4.3.6

Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be two function. Use the Horizontal line test to decide whether $f(x) = x^2$ and $g(x) = x^3$ are onto, one-to-one, or neither.

Solution:

We apply the horizontal line test on both f and g. In f, we see that on one place the line crosses the curve in two points, so f is not one-to-one, and it does not cross the curve in another place so it is not onto. However, in g, the line crosses the curve exactly once in any place, so it is one-to-one and onto.



Definition 4.3.3

Let $f : A \to B$ be a function. If the **inverse relation** f^{-1} of f is a function, then we say that f^{-1} is the **inverse function** of f. In particular, if f^{-1} is a function, then $f^{-1} : B \to A$ is defined by

$$f^{-1} = \{(y, x) : (x, y) \in f\}.$$

Example 4.3.7

Let $f = \{(1, 2), (4, 2)\}$ be a function. Decide whether f^{-1} is a function.

Solution:

No. Since $f^{-1} = \{(2, 1), (2, 4)\}$ where 2 is mapped to two distinct elements.

Theorem 4.3.3

Let $f : A \to B$ and $g : B \to A$. Then, $g = f^{-1}$ iff $f \circ g = I_B$ and $g \circ f = I_A$, where $I_A : A \to A$ is the **identity function** defined by $I_A(x) = x$ for all $x \in A$.

Example 4.3.8

Let $f(x) = 2x + 1$ and let $g(x) = \dfrac{x-1}{2}$. Show that $g = f^{-1}$.

Solution:

For all $x \in \mathbb{R}$, $(f \circ g)(x) = f(g(x)) = f(\frac{x-1}{2}) = 2\frac{x-1}{2} + 1 = x - 1 + 1 = x = I_{\mathbb{R}}$. Therefore, $g = f^{-1}$.

Theorem 4.3.4

Let $f : A \to B$ be a function. Then,

1. f^{-1} is a function from $\mathrm{Rng}(f)$ to A iff f is one-to-one.
2. If f^{-1} is a function, then f^{-1} is one-to-one.

Proof:

1. " $\Rightarrow$ ": Assume that f^{-1} is a function. Let $f(x) = f(y) = z$, then $(x, z), (y, z) \in f$. Thus, $(z, x), (z, y) \in f^{-1}$. Since f^{-1} is a function, $x = y$. Therefore, f is 1-1.
   " $\Leftarrow$ ": Assume that f is 1-1. Let $(x, y), (x, z) \in f^{-1}$ (we need to show that $y = z$). Then, $(y, x), (z, x) \in f$. Since f is 1-1, $y = z$. Thus, f^{-1} is a function. By Definition 3.1.6, $\mathrm{Dom}(f^{-1}) = \mathrm{Rng}(f)$ and $\mathrm{Rng}(f^{-1}) = \mathrm{Dom}(f)$.
2. Assume that f^{-1} is a function. Let $f^{-1}(x) = f^{-1}(y) = z$, then $(x, z), (y, z) \in f^{-1}$. Thus, $(z, x), (z, y) \in f$ and since f is a function, $x = y$. Therefore, f^{-1} is 1-1.

Definition 4.3.4

A function $f : A \to B$ is called a **1-1 corresponding** or a **bijection** if it is both 1-1 and onto B. In that case, we write $f : A \xrightarrow[onto]{1-1} B$.

Theorem 4.3.5

Let $f : A \xrightarrow[onto]{1-1} B$ and $g : B \xrightarrow[onto]{1-1} C$. Then,

1. $g \circ f : A \xrightarrow[onto]{1-1} C$ is a bijection.
2. $f^{-1} : B \xrightarrow[onto]{1-1} A$ is a bijection.

Proof:

1. By Theorem 4.3.1 and Theorem 4.3.2, if f and g are one-to-one and onto, the composite function $g \circ f$ is also one-to-one and onto.
2. By Theorem 4.3.4, if f is one-to-one, then f^{-1} is a function and hence it is a one-to-one

function. To show that f^{-1} is onto A, let $a \in A$. Then, $f(a) = b \in B$. Thus, $(a, b) \in f$ and hence $(b, a) \in f^{-1}$ and therefore $f^{-1}(b) = a$.

Section 4.4: Images of Sets

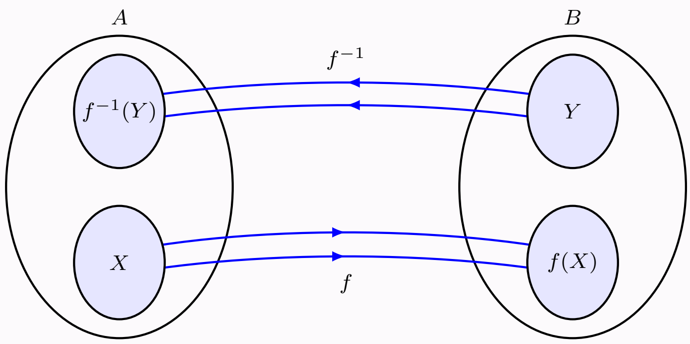
Definition 4.4.1

Let $f : A \to B$. If $X \subseteq A$, the **image of** X or image set of X is

$$f(X) = \{y \in B : y = f(x) \text{ for some } x \in X\}.$$

If $Y \subseteq B$, then the **inverse image of** Y is

$$f^{-1}(Y) = \{x \in A : f(x) = y \text{ for some } y \in Y\}.$$

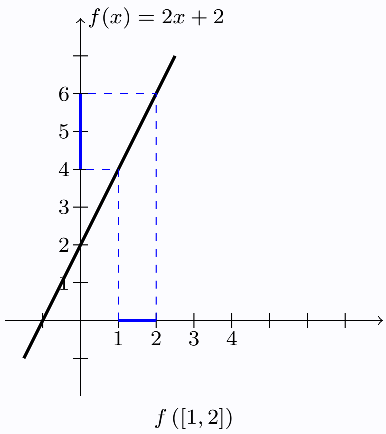


Example 4.4.1

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 2$. Find $f(\{1, 4\})$, $f([1, 2])$, $f(\mathbb{N})$, $f^{-1}(\{2, 3\})$, and $f^{-1}([2, 4])$.

Solution:

- $f(\{1, 4\}) = \{4, 10\}$.
- $f([1, 2]) = [4, 6]$.
- $f(\mathbb{N}) = \{4, 6, 8, 10, 12, \cdots\}$.
- $f^{-1}(\{2, 3\}) = \{0, \frac{1}{2}\}$.
- $f^{-1}([2, 4]) = [0, 1]$.



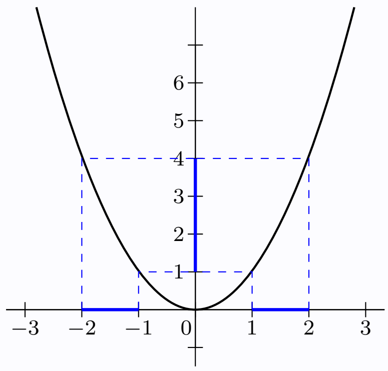
Example 4.4.2

Let $f(x) = x^2$ be a function from $\mathbb{R}$ to $\mathbb{R}$. Find $f([1,2])$, $f([0,1])$, $f(\{2\})$, $f([-2,-1]\cup[1,2])$, and $f^{-1}([1,4])$.

Solution:

- $f([1,2]) = [1,4]$.
- $f([0,1]) = [0,1]$.
- $f(\{2\}) = f(\{2,-2\}) = \{4\}$.
- $f([-2,-1]\cup[1,2]) = [1,4]$.
- $f^{-1}([1,4]) = [-2,-1]\cup[1,2]$.

$f(x) = x^2$



$f([-2,-1]\cup[1,2])$ and $f^{-1}([1,4])$

Example 4.4.3

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. If $X = [-2,-1]$ and $Y = [1,2]$, find $f(X\cap Y)$, $f(X)\cap f(Y)$, $f(X\cup Y)$, and $f(X)\cup f(Y)$.

Solution:

Note that $X\cap Y = \phi$. Thus, $f(X\cap Y) = \phi$. However, $f(X) = [1,4] = f(Y)$ and thus $f(X)\cap f(Y) = [1,4]$. Therefore, $f(X\cap Y) \neq f(X)\cap f(Y)$.

On the other hand, $f(X\cup Y) = [1,4] = f(X)\cup f(Y)$.

Theorem 4.4.1

Let $f : A \to B$ and let $\left\{X_i : i \in \mathcal{I}\right\} \subseteq A$ and $\left\{Y_i : i \in \mathcal{I}\right\} \subseteq B$. Then,

1. $f\left(\bigcap_{i\in\mathcal{I}} X_i\right) \subseteq \bigcap_{i\in\mathcal{I}} f(X_i)$.

2. $f\left(\bigcup_{i\in\mathcal{I}} X_i\right) = \bigcup_{i\in\mathcal{I}} f(X_i)$.

3. $f^{-1}\left(\bigcap_{i\in\mathcal{I}} Y_i\right) = \bigcap_{i\in\mathcal{I}} f^{-1}(Y_i)$.

4. $f^{-1}\left(\bigcup_{i\in\mathcal{I}} Y_i\right) = \bigcup_{i\in\mathcal{I}} f^{-1}(Y_i)$.

Proof:

Proof of (1): Let $b \in f\left(\bigcap_{i\in\mathcal{I}} X_i\right)$, then $b = f(a)$ for some $a \in \bigcap_{i\in\mathcal{I}} X_i$. Thus, $a \in X_i$ for every $i \in \mathcal{I}$ so that $b = f(a)$. Hence, for every $i \in \mathcal{I}$, $b \in f(X_i)$. Therefore, $b \in \bigcap_{i\in\mathcal{I}} f(X_i)$.

Proof of (2):

$$\begin{aligned}
\text{Let } b \in f\left(\bigcup_{i\in\mathcal{I}} X_i\right) &\Leftrightarrow b = f(a) \text{ for some } a \in \bigcup_{i\in\mathcal{I}} X_i \\
&\Leftrightarrow b = f(a) \text{ for some } a \in X_i \text{ for some } i \in \mathcal{I} \\
&\Leftrightarrow b \in f(X_i) \text{ for some } i \in \mathcal{I} \\
&\Leftrightarrow b \in \bigcup_{i\in\mathcal{I}} f(X_i).
\end{aligned}$$

Proof of (3):

$$\begin{aligned}
\text{Let } a \in f^{-1}\left(\bigcap_{i\in\mathcal{I}} Y_i\right) &\Leftrightarrow a = f^{-1}(b) \text{ for some } b \in \bigcap_{i\in\mathcal{I}} Y_i \\
&\Leftrightarrow a = f^{-1}(b) \text{ for some } b \in Y_i \text{ for every } i \in \mathcal{I} \\
&\Leftrightarrow a \in f^{-1}(Y_i) \text{ for every } i \in \mathcal{I} \\
&\Leftrightarrow a \in \bigcap_{i\in\mathcal{I}} f^{-1}(Y_i).
\end{aligned}$$

Example 4.4.4

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $f(m,n) = 2^{m-1}(2n-1)$, and let $Y = \{3, 10\}$. Find the inverse image of Y.

Solution:

By Theorem 4.4.1, $f^{-1}(Y) = f^{-1}(\{3\} \cup \{10\}) = f^{-1}(\{3\}) \cup f(\{10\})$. Then,

- $f^{-1}(\{3\}) = (m,n)$ such that $3 = f(m,n) = 2^{m-1}(2n-1)$. Since $2 \nmid 3$, $2^{m-1} = 1$. Then $m-1 = 0$ or $m = 1$. In that case, $3 = 2n-1$ and hence $n = 2$. Therefore, $f^{-1}(\{3\}) = (m,n) = (1,2)$.

- $f^{-1}(\{10\}) = (m, n)$ such that $10 = f(m, n) = 2^{m-1}(2n - 1)$. After factoring 10, we get $10 = 2^1 \cdot 5$. Thus, $2 \mid 10$ and hence $2^{m-1} = 2^1$. Then, $m - 1 = 1$ and so $m = 2$. As a result of that, $10 = 2^{2-1}(2n-1)$. Thus, $10 = 2(2n-1)$ which implies $n = 3$. Therefore, $f^{-1}(\{10\}) = (2, 3)$.

Therefore, $f^{-1}(\{3, 10\}) = \{(1, 2), (2, 3)\}$.

Example 4.4.5

Let $f : A \to B$ and let $X, Y \subseteq A$. Show that f is 1-1 if and only if $f(X) \cap f(Y) = f(X \cap Y)$.

Solution:

„ $\Rightarrow$ ": Assume that f is 1-1. By Theorem 4.4.1, we have $f(X \cap Y) \subseteq f(X) \cap f(Y)$. So, we only show that $f(X) \cap f(Y) \subseteq f(X \cap Y)$. Assume that $b \in f(X) \cap f(Y)$, then $b \in f(X)$ and $b \in f(Y)$. Thus, $b = f(a_1)$ for some $a_1 \in X$ and $b = f(a_2)$ for some $a_2 \in Y$. Since f is 1-1, $b = f(a_1) = f(a_2)$ implies $a_1 = a_2 =: a$. Thus, $b = f(a)$ for some $a \in X \cap Y$. Therefore, $b \in f(X \cap Y)$ and hence $f(X) \cap f(Y) \subseteq f(X \cap Y)$. Thereforem $f(X) \cap f(Y) = f(X \cap Y)$.
„ $\Leftarrow$ ": Let $x, y \in A$ with $x \neq y$. Then, $\{x\} \cap \{y\} = \phi$. Thus, $f(\{x\} \cap \{y\}) = \phi$ which implies that $f(\{x\}) \cap f(\{y\}) = \phi$.
That is, $\{f(x)\} \cap \{f(y)\} = \phi$ and hence $f(x) \neq f(y)$. Therefore, f is 1-1.

Example 4.4.6

Let $f : A \xrightarrow{1-1} B$. Prove that if $X \subseteq A$, then $f(A - X) = f(A) - f(X)$.

Solution:

„ $\subseteq$ ": Let $y \in f(A - X)$, then there exists $x \in A - X$ such that $y = f(x)$. That is, $x \in A$ and $x \notin X$. Thus, $f(x) \in f(A)$ and $f(x) \notin f(X)$ (since f is 1-1). Therefore, $f(x) \in f(A) - f(X)$ and hence $y \in f(A) - f(X)$.
„ $\supseteq$ ": Let $y \in f(A) - f(X)$. Then, $y \in f(A)$ and $y \notin f(X)$. Thus, there exists $x \in A$ such that $y = f(x)$ and $x \notin X$ (since if $x \in X$, then $f(x) \in f(X)$ which is not the case). Thus, $x \in A - X$ and thus $f(x) \in f(A - X)$ which implies $y \in f(A - X)$.

Exercise 4.4.1

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Find $f(\{-2, 2\})$; $f([1, 2])$; $f([-1, 2])$; and $f^{-1}(\{4, 16\})$.

Exercise 4.4.2

Let $f : A \to B$ be a function and let $Y \subseteq B$. Show that $f\left(f^{-1}(Y)\right) \subseteq Y$. If moreover f is onto B, then $f\left(f^{-1}(Y)\right) = Y$.

Chapter

5 Cardinality

Section 5.1: Equivalent Sets; Finite Sets

Definition 5.1.1

Two sets A and B are **equivalent**, denoted by $A \approx B$, if and only if there exists a bijection $f : A \to B$. Otherwise, $A \not\approx B$.

Example 5.1.1

Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. Show that $A \approx B$.

Solution:

To show that $A \approx B$, we have to find a bijection $f : A \to B$. Let $f : A \to B$ defined by $f(1) = a$, $f(2) = b$, and $f(3) = c$. Thus, f is a bijection from A to B and hence $A \approx B$.

Theorem 5.1.1: The Pigeonhole Principle

Let $h, k \in \mathbb{N}$. If $f : \mathbb{N}_h \to \mathbb{N}_k$ and $h > k$, then f is not a one-to-one function.

Example 5.1.2

Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Is $A \approx B$? Explain.

Solution:

The answer is NO. By the Pigeonhole Principle, there is no one-to-one function from A to B, and hence $A \not\approx B$.

Example 5.1.3

Let $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$. Show that the open intervals $(a, b) \approx (c, d)$.

Solution:

Let $f : (a, b) \to (c, d)$ defined by

$$f(x) = \frac{d-c}{b-a}(x-a) + c.$$

You should show that f is a bijection to get the desired result.

Theorem 5.1.2

The relation "$\approx$" is an equivalence relation on the class of all sets.

Proof:

<u>Reflexive</u>: Clearly, the identity function $I_A : A \to A$ defined by $I_A(x) = x$ for all $x \in A$ is a bijection. Thus, $A \approx A$.

<u>Symmetric</u>: Assume that $A \approx B$. That is, there is a bijection $f : A \to B$. By Theorem 4.3.5, $f^{-1} : B \to A$ is also a bijection. Thus, $B \approx A$.

<u>Transitive</u>: Assume that $A \approx B$ and $B \approx C$. Then, there are two bijective mappings $f : A \to B$ and $g : B \to C$. By Theorem 4.3.5, $g \circ f : A \to C$ is a bijection as well. Thus, $A \approx C$.

Therefore, "$\approx$" is an equivalence relation on the class of all sets.

Theorem 5.1.3

Let $A \approx C$ and $B \approx D$. Show that

1. $A \times B \approx C \times D$,
2. If $A \cap B = \phi$ and $C \cap D = \phi$, then $A \cup B \approx C \cup D$.

Proof:

Assume that $A \approx C$ and $B \approx D$. Then, there exist $f : A \xrightarrow[onto]{1-1} C$ and $g : B \xrightarrow[onto]{1-1} D$. Then,

1. Let $h : A \times B \to C \times D$ given by $h(a, b) = (f(a), g(b))$. We show that h is a bijection:
   - <u>1-1</u>: Assume $h(a_1, b_1) = h(a_2, b_2)$, then $(f(a_1), g(b_1)) = (f(a_2), g(b_2))$. Then, $f(a_1) = f(a_2)$ and $g(b_1) = g(b_2)$. Since f and g are both 1-1, we have $a_1 = a_2$ and $b_1 = b_2$. Thus, $(a_1, b_1) = (a_2, b_2)$ and hence h is 1-1.
   - <u>onto</u>: Let $(c, d) \in C \times D$, then $c \in C$ and $d \in D$. Since f and g are both onto functions, $\exists a \in A$ such that $f(a) = c$ and $\exists b \in B$ such that $g(b) = d$. Thus,

$h(a,b) = (f(a), g(b)) = (c,d) \in C \times D$. Thus, h is onto.

Since h is 1-1 and onto, $h : A \times B \to C \times D$ is a bijection. Therefore, $A \times B \approx C \times D$.

2. Let $h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B \end{cases}$. We show that h is a bijection:

- Assume that $h(x_1) = h(x_2)$, then if $x_1 \in A$ and $x_2 \in B$, then $h(x_1) = h(x_2)$ which implies $f(x_1) = g(x_1)$ but this is not possible since $C \cap D = \phi$. Thus, either $x_1, x_2 \in A$ or $x_1, x_2 \in B$. With out loss of generality, assume that $x_1, x_2 \in A$. Then, $h(x_1) = h(x_2)$ implies $f(x_1) = f(x_2)$. Since f is 1-1, $x_1 = x_2$ and thus h is 1-1.
- Let $y \in C \cup D$, then $y \in C$ or $y \in D$ (but not in both). Without loss of generality, assume that $y \in C$. Thus $\exists a \in A$ such that $f(a) = y$ (f is onto C), then $h(a) = f(a) = y$. Thus, h is onto $C \cup D$.

Since h is 1-1 and onto, $h : A \cup B \to C \cup D$ is a bijection.

Definition 5.1.2

Let $\mathbb{N}_k = \{1, 2, 3, \cdots, k\} \subseteq \mathbb{N}$ with $k \in \mathbb{N}$ and the **cardinality** of $\mathbb{N}_k$ is k, denoted by $\overline{\overline{\mathbb{N}_k}} = k$. In addition, we might say that $\mathbb{N}_k$ has **cardinal number** k.

Definition 5.1.3

A set A is **finite** if and only if $A = \phi$ or $A \approx \mathbb{N}_k$. If $A = \phi$, then $\overline{\overline{A}} = 0$. Otherwise, $A \approx \mathbb{N}_k$ and $\overline{\overline{A}} = k$. The set A is **infinite** if it is not finite.

Theorem 5.1.4

If A is a finite set and $B \approx A$, then B is finite.

Proof:

Suppose A is finite and $A \approx B$. If $A = \phi$, then clearly $B = \phi$ since there is a bijection between A and B. Otherwise, $A \approx \mathbb{N}_k$ for some natural number k, then $B \approx \mathbb{N}_k$ by transitivity of $\approx$. In either cases, B is finite.

Theorem 5.1.5

Every subset of a finite set is finite.

Theorem 5.1.6

If A is a finite set with $\overline{\overline{A}} = k \geq 0$ and $x \notin A$, then $A \cup \{x\}$ is finite and has cardinality $k+1$.

Proof:

If $A = \phi$, then $\overline{\overline{A}} = 0$ and hence $A \cup \{x\} = \{x\}$ is finite as it is equivalent to $\mathbb{N}_1$. In this case, $\overline{\overline{A \cup \{x\}}} = 1$.

If $A \neq \phi$, then $A \approx \mathbb{N}_k$ for some natural number k. Also, $\{x\} \approx \{k+1\}$. Therefore, by Theorem 5.1.3, $A \cup \{x\} \approx \mathbb{N}_k \cup \{k+1\} = \mathbb{N}_{k+1}$. Thus $A \cup \{k+1\}$, and $\overline{\overline{A \cup \{k+1\}}} = k+1$.

Another way: Since A is finite and $|A| = k$, then $A \approx \mathbb{N}_k$. Then there is a bijection function $f : A \to \mathbb{N}_k$. Let $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ defined by $g(t) = \begin{cases} f(t) & \text{if } t \in A, \\ k+1 & \text{if } t = x \end{cases}$. Note that $f(t) \neq k+1$ for all $t \in A$.

Can you show that g is a bijection!? $A \cup \{x\}$ has cardinality $k+1$.

Theorem 5.1.7

If A and B are two finite sets, then $A \cup B$ is finite.

Proof:

Assume first that $A \cap B = \phi$. Note that if either A or B is empty, then the proof is trivial. So, we may assume that neither sets is finite.

Since A and B are finite, then there are bijections $(A \approx \mathbb{N}_m)$ $f : A \to \mathbb{N}_m$ and $(B \approx \mathbb{N}_n)$ $g : B \to \mathbb{N}_n$. Let $H = \{m+1, m+2, \cdots, m+n\}$ and let $h : \mathbb{N}_n \to H$ be defined by $h(x) = m + x$. Clearly, h is a bijection and hence $H \approx \mathbb{N}_n$. Thus, $H \approx B$ (This is because $\approx$ is transitive). Therefore, Theorem 5.1.3 implies

$$A \cup B \approx \mathbb{N}_m \cup H = \mathbb{N}_{m+n}.$$

Hence, $A \cup B$ is finite.

Now assume that $A \cap B \neq \phi$, then clearly $B - A \subseteq B$ which is finite. Thus, $A \cup B = (B - A) \cup A$, where $(B - A)$ and A are disjoint finite sets. Thus $A \cup B$ is finite.

Theorem 5.1.8

For any $n \in \mathbb{N}$, if $A_1, A_2, \cdots, A_n$ are finite sets, then $A_1 \cup A_2 \cup \cdots \cup A_n$ is a finite set.

Theorem 5.1.9

Let A and B be two finite sets. Then

1. If $A \cap B = \phi$, then $|A \cup B| = |A| + |B|$.
2. If $A \cap B \neq \phi$, then $|A \cup B| = |A| + |B| - |A \cap B|$.
3. $A \times B$ is finite and $|A \times B| = |A| \cdot |B|$.

Section 5.2: Infinite Sets

Theorem 5.2.1

The set $\mathbb{N}$ is an infinite set.

Proof:

Assume that $\mathbb{N}$ is finite. Clearly $\mathbb{N} \neq \phi$. Then $\mathbb{N} \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$. Thus, $\exists f : \mathbb{N}_k \xrightarrow[onto]{1-1} \mathbb{N}$. Let $n = f(1) + f(2) + \cdots + f(k) + 1$. Thus, $n > f(i)$ for all $i \in \mathbb{N}_k$ and hence $n \neq f(i)$ for any $i = 1, 2, \cdots, k$. Hence $n \in \mathbb{N}$ and $n \notin \text{Rng}(f)$. Therefore, f is not onto $\mathbb{N}$, contradiction. Thus $\mathbb{N} \not\approx \mathbb{N}_k$ for any $k \in \mathbb{N}$. Therefore, $\mathbb{N}$ is infinite.

Definition 5.2.1

A set S is called **denumerable** if and only if $S \approx \mathbb{N}$. If S is denumerable, then S has cardinal number τ_0. That is, $\overline{\overline{S}} = \tau_0$.

Definition 5.2.2

A set S is called **countable** if and only if S is finite or denumerable. Otherwise, S is said to be **uncountable**.

Theorem 5.2.2

The set of integers $\mathbb{Z}$ is denumerable. In particular, $\overline{\overline{\mathbb{Z}}} = \tau_0$.

Proof:

We show that there is a bijection mapping from $\mathbb{N}$ to $\mathbb{Z}$. That is, $\mathbb{N} \approx \mathbb{Z}$. Let $f : \mathbb{N} \to \mathbb{Z}$ be given by

$$f(x) = \begin{cases} \dfrac{x}{2} & \text{if } x \text{ is even,} \\[2ex] \dfrac{1-x}{2} & \text{if } x \text{ is odd.} \end{cases}$$

That is, we are considering the following mapping:

$$\begin{array}{cccccccccc} \mathbb{N}: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ \mathbb{Z}: & 0 & 1 & -1 & 2 & -2 & 3 & -3 & \cdots \end{array}$$

- f is 1-1: Let $f(x) = f(y)$ for $x, y \in \mathbb{N}$. We consider the following three cases.

  1. x and y are both even. Thus, $f(x) = f(y)$ implies that $\frac{x}{2} = \frac{y}{2}$ which leads to $x = y$.
  2. x and y are both odd. Thus, $f(x) = f(y)$ implies that $\frac{1-x}{2} = \frac{1-y}{2}$. Then $1-x = 1-y$ which implies that $x = y$.
  3. One of them, say x, is even and the other, say y, is odd. Then by the definition of f, we have $f(x) \neq f(y)$.

  Therefore, whenever $f(x) = f(y)$, we get $x = y$. Thus, f is 1-1.

- f is onto: Let $y \in \mathbb{Z}$. If $y > 0$, then $2y$ is an even number in $\mathbb{N}$ and thus $f(2y) = \frac{2y}{2} = y$. On the other hand, if $y \leq 0$, then $1 - 2y$ is an odd number in $\mathbb{N}$ and thus $f(1-2y) = \frac{1-(1-2y)}{2} = \frac{2y}{2} = y$. Thus, in either cases of y, f is onto $\mathbb{Z}$.

Therefore, f is a bijection and $\mathbb{Z}$ is denumerable with cardinal number τ_0.

Example 5.2.1

Show that $A = \left\{\frac{1}{2k} : k \in \mathbb{N}\right\}$ is a denumerable set.

Solution:

We show that $A \approx \mathbb{N}$. That is, we show that $f : \mathbb{N} \to A$ where $f(x) = \frac{1}{2x}$ is a bijection.

- f is 1-1: Let $f(x) = f(y)$, then $\frac{1}{2x} = \frac{1}{2y}$. Thus, $x = y$ and f is 1-1.

- f is onto: Let $y \in A$, then $\frac{1}{2y} \in \mathbb{N}$ and hence $f(\frac{1}{2y}) = \frac{1}{2\frac{1}{2y}} = y$. Thus, f is onto A.

Therefore, A is denumerable.

Exercise 5.2.1

Show that $A = \left\{\frac{1}{2k+1} : k \in \mathbb{N}\right\}$ is a denumerable set.

Example 5.2.2

Show that $\mathbb{N} \times \mathbb{N}$ is denumerable. That is $\overline{\overline{\mathbb{N} \times \mathbb{N}}} = \tau_0$.

Solution:

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $f(m,n) = 2^{m-1}(2n-1)$. Thus, f is 1-1 by Example 4.3.5 and it is onto $\mathbb{N}$ by Example 4.3.2. Therefore, f is a bijection and hence $\mathbb{N} \times \mathbb{N}$ is denumerable.

Theorem 5.2.3

If A and B are denumerable sets, then $A \times B$ is denumerable as well.

Proof:

Since $A \approx \mathbb{N}$ and $B \approx \mathbb{N}$. By Theorem 5.1.3, $A \times B \approx \mathbb{N} \times \mathbb{N}$. By Example 5.2.2, $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$. Therefore, $A \times B \approx \mathbb{N}$. Thus, $A \times B$ is denumerable.

Theorem 5.2.4

The interval $(0,1)$ is uncountable and its cardinal number is $\mathbf{c}$ (continuum).

Proof:

Assume that $(0,1)$ is not uncountable. Then it is countable and so it is either finite or denumerable. Since $(0,1)$ is not finite (for instance it contains the infinite set $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\}$), it is denumerable. Thus, $(0,1) \approx \mathbb{N}$. Suppose that $\exists f : \mathbb{N} \to (0,1)$, which is a bijection. What we will do is to contradict with f is not onto $(0,1)$. Let

$$\begin{aligned} f(1) &= 0.a_{11}a_{12}a_{13}a_{14}a_{15}\cdots \\ f(2) &= 0.a_{21}a_{22}a_{23}a_{24}a_{25}\cdots \\ \vdots &= \quad \vdots \\ f(n) &= 0.a_{n1}a_{n2}a_{n3}a_{n4}a_{n5}\cdots \\ \vdots &= \quad \vdots \end{aligned}$$

Now let $x = 0.b_1b_2b_3b_4b_5\cdots \in (0,1)$, where $b_i = \begin{cases} 5 & \text{if } a_{ii} \neq 5, \\ 1 & \text{if } a_{ii} = 5 \end{cases}$. Thus, $x \neq f(i)$ for each $i \in \mathbb{N}$. Then, there is no element in $\mathbb{N}$ so that $f(n) = x$ since x is different from $f(n)$ in the n^{th} decimal place. Thus, f is not onto, contradiction. Hence $(0,1)$ is **not** denumerable and it is uncountable with cardinal number $\mathbf{c}$.

Theorem 5.2.5

For any $a, b \in \mathbb{R}$ with $a < b$, $(a, b) \approx (0, 1)$ and (a, b) is uncountable set with cardinality **c**. In particular, any (open or closed) interval (not a point) in $\mathbb{R}$ is uncountable.

Proof:

We recall here the definition we use for a function f in Example 5.1.3. Let $f : (0, 1) \to (a, b)$ with $f(x) = (b - a)x + a$ for all $x \in (0, 1)$.

- f is 1-1: Let $f(x) = f(y)$, then $(b - a)x + a = (b - a)y + a$ and that implies $x = y$. Thus, f is 1-1.
- f is onto: Let $y \in (a, b)$. Since $0 < y - a < b - a$, we have $0 < \frac{y-a}{b-a} < 1$. Thus,

$$f(\frac{y-a}{b-a}) = (b - a)\frac{y-a}{b-a} + a = y.$$

  Thus f is 1-1.

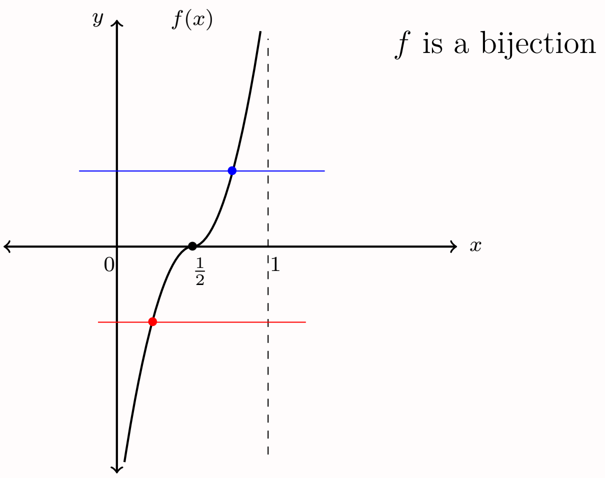
Therefore, f is a bijection and thus, (a, b) is uncountable with cardinality **c**.

Theorem 5.2.6

The set of real numbers $\mathbb{R}$ is uncountable, and $(0, 1) \approx \mathbb{R}$. The cardinality of $\mathbb{R}$ is **c**.

Proof:

Let $f : (0, 1) \to \mathbb{R}$ be defined by $f(x) = \tan(\pi x - \frac{\pi}{2})$. Thus, we can show that f is a bijection by using the horizontal line test.



Example 5.2.3

Let $A = (3,4) \cup [5,6)$. Show that $A \approx (0,1)$ (similarly show that A has cardinal number $\mathbf{c}$).

Solution:

Let $f : (0,1) \to A$ be given by $f(x) = \begin{cases} 2x+3 & \text{if } 0 < x < \frac{1}{2}, \\ 2x+4 & \text{if } \frac{1}{2} \le x < 1. \end{cases}$

- f is 1-1: Assume that $f(x) = f(y)$, we consider the following three cases:

  1. $x, y \in (0, \frac{1}{2})$. Since $f(x) = f(y)$, $2x+3 = 2y+3$ which implies that $x = y$.
  2. $x, y \in [\frac{1}{2}, 1)$. Since $f(x) = f(y)$, $2x+4 = 2y+4$. Thus, $x = y$.
  3. $x \in (0, \frac{1}{2})$ and $y \in [\frac{1}{2}, 1)$. In this case, $f(x) \neq f(y)$.

  Thus, whenever $f(x) = f(y)$, we have $x = y$. Thus, f is 1-1.

- f is onto: We consider the following two cases:

  1. if $y \in (3,4)$, then $0 < \frac{y-3}{2} < \frac{1}{2}$, and thus $f(\frac{y-3}{2}) = 2\frac{y-3}{2} + 3 = y$.
  2. if $y \in [5,6)$, then $\frac{1}{2} \le \frac{y-4}{2} < 1$, and thus $f(\frac{y-4}{2}) = 2\frac{y-4}{2} + 4 = y$.

  Thus, f is onto $(3,4) \cup [5,6)$.

Therefore, f is a bijection and $A \approx (0,1)$. That is $\overline{\overline{(3,4) \cup [5,6)}} = \mathbf{c}$.

Section 5.3: Countable Sets

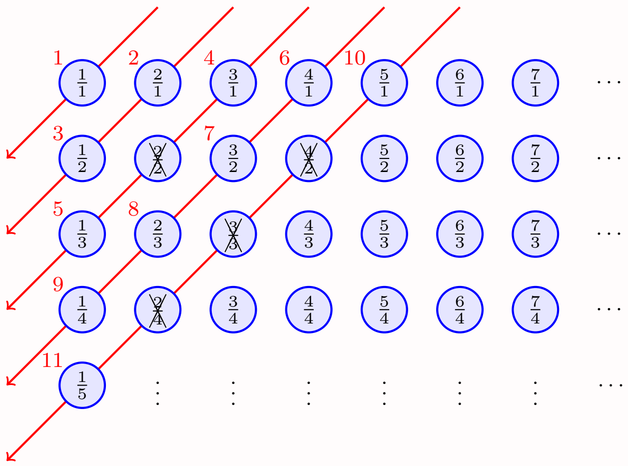
Theorem 5.3.1

The set $\mathbb{Q}^+$ of positive rational numbers is denumerable.

Proof:

One can prove this theorem by considering the following mapping:

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ 1 & 2 & \frac{1}{2} & 3 & \frac{1}{3} & 4 & \frac{3}{2} & \frac{2}{3} & \frac{1}{4} & \cdots \end{array}$$



Theorem 5.3.2

If A is denumerable, then $A \cup \{x\}$ is denumerable.

Proof:

If $x \in A$, then there is nothing to prove. So, assume that $x \notin A$. Since A is denumerable, $A \approx \mathbb{N}$ and thus $\exists$ a bijection $f : \mathbb{N} \to A$. Define $g : \mathbb{N} \to A \cup \{x\}$ by

$$g(n) = \begin{cases} x & \text{if } n = 1, \\ f(n-1) & \text{if } n > 1. \end{cases}.$$

Thus, g is a bijection (show it!). Therefore, $A \cup \{x\}$ is denumerable.

Theorem 5.3.3

If A is denumerable and B is finite, then $A \cup B$ is denumerable.

Proof:

By using an induction on $A \cup \{x\}$ for each $x \in B$ using Theorem 5.3.2.

Theorem 5.3.4

If A and B are disjoint denumerable sets, then $A \cup B$ is denumerable set.

Proof:

Since A and B are denumerable sets, then there are $f : \mathbb{N} \xrightarrow[onto]{1-1} A$ and $g : \mathbb{N} \xrightarrow[onto]{1-1} B$. Define $h : \mathbb{N} \to A \cup B$ by

$$h(n) = \begin{cases} f(\frac{n+1}{2}) & \text{if } n \text{ is odd,} \\ g(\frac{n}{2}) & \text{if } n \text{ is even.} \end{cases}.$$

The function h is a bijection (show it!). Thus, $A \cup B$ is denumerable.

Theorem 5.3.5

The set of all rational numbers $\mathbb{Q}$ is denumerable.

Proof:

Note that $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$. Using Theorem 5.3.2 and Theorem 5.3.4, we can easily show the desired result.

Exercise 5.3.1

Show that $\mathbb{Q} \approx \mathbb{Z} \times \mathbb{N}$. You can use $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$, defined by $f(\frac{p}{q}) = (p, q)$.

The Index