MATH 248
Methods of Proof in Mathematics

Joshua Abel

June 17, 2017

Contents

Chapter 1

Set Theory

A set is a collection of objects together with a rule for deciding whether a given object is a member of one set or not.

Sets are usually denoted by capital letters $A, B, C, ...$

If an object x is a member of the set A we write $x \in A$ "x is an element of A."
If x is not a member of A we write $x \notin A$ "x is not a member of A."

Sets are typically described using curly brackets {(elements go here)}.

Example 1.1.

$A = \{1, 2, 3\}$

$B = \{2, 4, 6, \ \ldots \ , 20\}$

$C = \{5, 6, 7, \ \ldots\}$

$D = \{ \ \ldots \ , -2, -1, 0, 1, 2, \ \ldots\}$

In most cases we will need to be more specific when defining our sets: $\{elements \mid rule\}$. This set notation is standard. The middle line"|" reads as "such that".

Standard Sets

Natural Numbers $\mathbb{N} = \{1, 2, 3, 4, \ \ldots\}$

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

Rational Numbers $\mathbb{Q} = \{\frac{p}{q} \mid \ p, q \in \mathbb{Z},\ q \neq 0\}$

Real Numbers $\mathbb{R}$

Complex Numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i = \sqrt{-1}\}$

Empty Set $\emptyset = \{\}$

Example 1.2. $A = \{x \in \mathbb{Z} \mid x \geq 5\} = \{5, 6, 7, \dots\}$.

Example 1.3. $B = \{2x \mid x \in \mathbb{Z}\} = \{\dots -4, -2, 0, 2, 4, \dots\}$. (Even integers).

Example 1.4. $C = \{x \in \mathbb{R} \mid x > 3 \text{ and } x < 0\} = \emptyset$.

Example 1.5. From the previous examples (1.2-1.4)
$3 \notin A \quad 3 \notin B \quad 3 \notin C \quad 6 \in A \quad 6 \in B \quad 6 \notin C$.

If A has a finite number of elements, we use $|A|$ to denote the number of elements in A.

Example 1.6. If $A = \{2, 5, 7\}$, then $|A| = 3$.

Example 1.7. $|\emptyset| = 0$.

Example 1.8. If $B = \{3, \{2, 3\}, \emptyset, 4, \{1, 5\}\}$, then $|B| = 5$.

Example 1.9. $|\{\emptyset\}| = 1$.

Example 1.10. If $C = \{1, 3, 7, 3\} = \{1, 3, 7\}$, then $|C| = 3$.

Definition 1.11. Let A, B be sets. If every element of A is an element of B, then we say that A is a *subset* of B.
Notation: $A \subseteq B$ "A is a subset of B".

Example 1.12. $\{1, 2, 3\} \subseteq \mathbb{Z}$.

Example 1.13. $\{-1, 1\} \subseteq \mathbb{Z}$.

Example 1.14. $\{-1, 1\}\mathbb{N}$

Example 1.15. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Example 1.16.
$\{1\} \subseteq \{1, \{1\}\}$.
$\{1\} \in \{1, \{1\}\}$.

Example 1.17.
$\{1, \{2\}\} \nsubseteq \{\{1\}, 2\}$.
$\{1, \{2\}\} \nsupseteq \{\{1\}, 2\}$.

*Note: If there exists some $x \in A$ such that $x \notin B$, then $A \nsubseteq B$. As a consequence, if A is any set, $\emptyset \subseteq A$.
Reason: If $\emptyset \nsubseteq A$, there would be some $x \in \emptyset$ such that $x \notin A$. Also if A is any set,then $A \subseteq A$.

When discussing sets, we will often restrict our attention to subsets of a given set $\mathcal{U}$, called *the universe of discourse.* $\mathcal{U}$ may be spelled out explicitly, in other cases the universe will be clear from context.

Intervals $(\mathcal{U} = \mathbb{R})$
$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$
$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$
$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$
$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$
$(a, \infty) = \{x \in \mathbb{R} \mid x > a\}$
$(-\infty, a) = \{x \in \mathbb{R} \mid x < a\}$
$[a, \infty) = \{x \in \mathbb{R} \mid x \geq a\}$
$(-\infty, a] = \{x \in \mathbb{R} \mid x \leq a\}$
$(-\infty, \infty) = \mathbb{R}$

Definition 1.18. Sets A and B are *equal* if they have exactly the same members.

*Note: $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Definition 1.19. If $A \subseteq B$ and $A \neq B$, then A is a *proper subset* of B.
Notation: $A \subset B$ or $A \subsetneq B$.

Example 1.20. $\{1, 2\}$ is a proper subset of $\{1, 2, 3\}$ but $\{1, 2, 3\}$ is not a proper subset of $\{1, 2, 3\}$.

Definition 1.21. Let A be a set. The *power set* of A is the set $\wp(A)$ consisting of all subsets of A.

Example 1.22.
$A = \{x, y\}$
$\wp(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

Example 1.23.
$B = \{2, \{2, 5\}, 7\}$
$\wp(B) = \{\emptyset, \{2\}, \{\{2, 5\}\}, \{7\}, \{2, \{2, 5\}\}, \{2, 7\}, \{\{2, 5\}, 7\}, B\}$.

Example 1.24. $\wp(\emptyset) = \{\emptyset\}$.

Example 1.25. $\wp(x) = \{\emptyset, \{x\}\}$.

We will see that if $|A| = n$ then $|\wp(A)| = 2^n$.

It can be useful to represent a set diagrammatically by a Venn diagram.

- Elements are represented by points.
- $D \subseteq B, D \nsubseteq A, x \in A, x \notin B$.
- Box represents $\mathcal{U}$.
- Subsets of $\mathcal{U}$ are represented by circles.

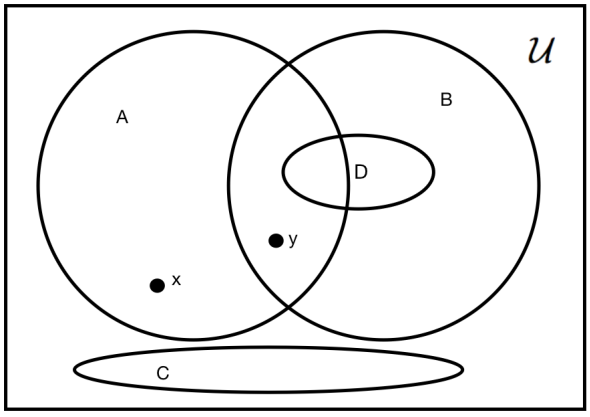


Figure 1.1: The diagram.

Set Operations

Definition 1.26. Let A and B be sets. The *union* of A and B is noted as $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
The union lies in A or B or both.
*Note: In math, "or" is used **inclusively**.

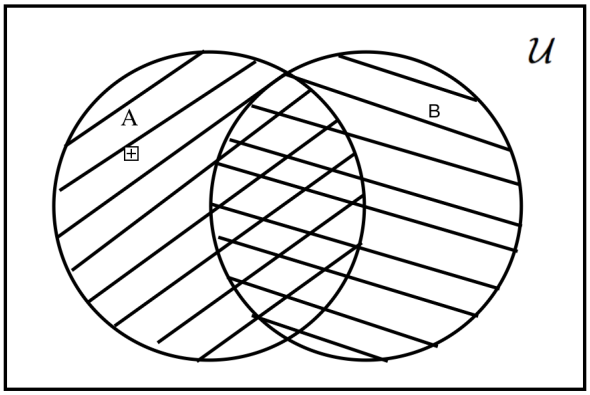


Figure 1.2: The union of two sets A and B.

Example 1.27.
$A = \{-1, 0, 1\}$ and $B = \{1, 2, 3\}$.
$A \cup B = \{-1, 0, 1, 2, 3\}$.

Example 1.28.
$A = \{1, 2\}$ and $B = \{0, 1, 2, 3\}$.
$A \cup B = \{0, 1, 2, 3\}$.

Example 1.29. For any set A, $A \cup \emptyset = A$ and $A \cup A = A$.

Example 1.30.
$A = [1, 2]$ and $B = [2, 3]$.
$A \cup B = [1, 3)$.

Definition 1.31. Let A and B be sets. The *intersection* of A and B is the set $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

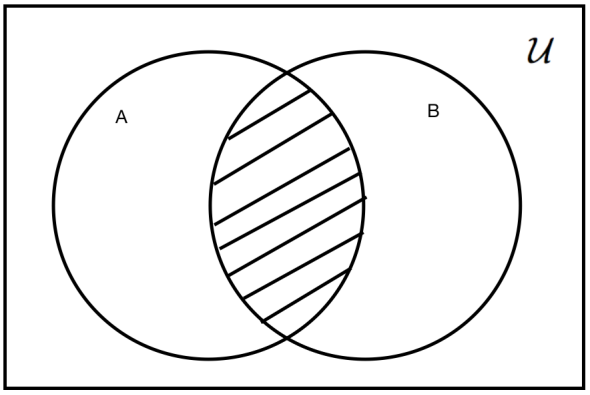


Figure 1.3: The intersection of two sets A and B.

Example 1.32.
$A = \{-1, 0, 1\}$ and $B = \{1, 2, 3\}$.
$A \cap B = \{1\}$.

Example 1.33.
$A = \{1, 2\}$ and $B = \{0, 1, 2, 3\}$.
$A \cap B = \{1, 2\}$.

Example 1.34. For any set A, $A \cap \emptyset = \emptyset$ and $A \cap A = A$.

Example 1.35.
$A = [1, 2]$ and $B = [2, 3]$.
$A \cap B = \{2\}$.

Definition 1.36. Let A and B be sets. The difference of A with B is $A - B = \{x \mid x \in A \text{ and } x \notin B\}$.

Example 1.37.
$A = \{-1, 0, 1\}$ and $B = \{1, 2, 3\}$.
$A - B = \{-1, 0\}$ and $B - A = \{2, 3\}$.

Example 1.38.
$A = \{1, 2\}$ and $B = \{0, 1, 2, 3\}$.
$A - B = \emptyset$ and $B - A = \{0, 3\}$.

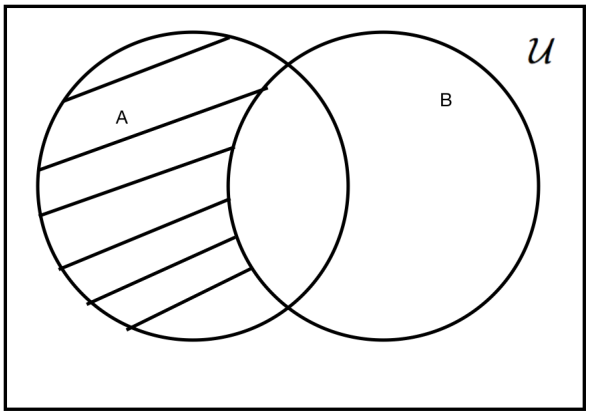


Figure 1.4: The difference of A with B.

Example 1.39. If A is any set, then $A - \emptyset = A$, $\emptyset - A = \emptyset$ and $A - A = \emptyset$.

Example 1.40.
$[1, 2] - [2, 3) = [1, 2)$.
$[2, 3) - [1, 2] = (2, 3)$.

Definition 1.41. Let A be a set in the universe $\mathcal{U}$. The *compliment* of A is $\overline{A} = \mathcal{U} - A$.

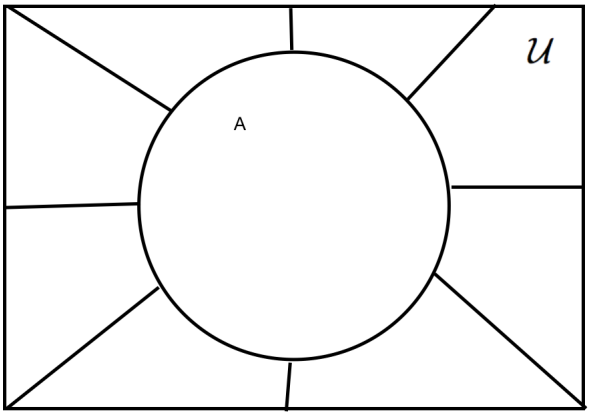


Figure 1.5: The compliment of A.

Example 1.42.
$\mathcal{U} = \mathbb{Z}$ and $A = \mathbb{N}$.
$\overline{A} = \{\ldots, -2, -1, 0\}$.

Example 1.43.
$\mathcal{U} = \mathbb{R}$ and $A = [-1, 1]$.
$\overline{A} = (-\infty, -1) \cup (1, \infty)$.

Example 1.44.
$\mathcal{U} = \mathbb{R}$ and $A = \mathbb{Q}$.
$\overline{A} = \mathbb{R} - \mathbb{Q}$ (irrational numbers).

Example 1.45. $\overline{\mathcal{U}} = \emptyset$.

Example 1.46. $\overline{\emptyset} = \mathcal{U}$.

Example 1.47. $\overline{\overline{A}} = A$.

Unions and intersections are not limited to two sets. If $A_1, \ldots, A_n$ are sets we define their *union*
$\bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for some } 1 \leq i \leq n\}$
and their *intersection*
$\bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for all } 1 \leq i \leq n\}$.

Example 1.48.
$A_1 = \{0\}, A_2 = \{0, \{0, 1\}\}, A_3 = \{0, 1\}, A_4 = \{0, \emptyset\}, A_5 = \{0, \{0, \emptyset\}\}$.
$\bigcup_{i=1}^{5} A_i = \{0, \{0, 1\}, 1, \emptyset, \{0, \emptyset\}\}$.
$\bigcap_{i=1}^{5} A_i = \{0\}$.

Example 1.49.
For $i = 1, 2, \ldots, 10$, define $A_i = [-i, i]$.
$\bigcup_{i=1}^{10} A_i = [-10, 10]$.
$\bigcap_{i=1}^{10} A_i = [-1, 1]$.

Unions and intersections are not limited to finite collections of sets. If $A_1, A_2, A_3, \ldots$ are sets, we define
the union $\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ for some } i \in \mathbb{N}\}$
and intersection $\bigcap_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ for all } i \in \mathbb{N}\}$.

Example 1.50.
For $i \in \mathbb{N}$, define $A_i = \{i, i+1\}$.
$\bigcup_{i=1}^{\infty} A_i = \mathbb{N}$.
$\bigcap_{i=1}^{\infty} A_i = \emptyset$.

Example 1.51.
For each $i \in \mathbb{N}$, define $A_i = [-\frac{1}{i}, \frac{1}{i}]$.
$\bigcup_{i=1}^{\infty} A_i = [-1, 1]$.
$\bigcap_{i=1}^{\infty} A_i = \{0\}$.

Let I be a nonempty set, and for each $\alpha \in I$, let S_α be a set. We can define the set $\{S_\alpha\}_{\alpha \in I}$ consisting of all S_α's. I is called the *indexing set* and $\{S_\alpha\}_{\alpha \in I}$ is an *indexed family* of sets of an *indexed collection of sets*.

Example 1.52.
For each $n \in \mathbb{Z}$, let $S_n = \mathbb{Z} - \{n\}$. ($\mathbb{Z}$ is the index).

Example 1.53.
For each $r \in \mathbb{Q}$ with $r > 0$, define $S_r = [0, r)$.

Given an indexed family of sets $\{S_\alpha\}_{\alpha \in I}$, define the
union $\bigcup_{\alpha \in I} S_\alpha = \{x \mid x \in S_\alpha \text{ for some } \alpha \in I\}$
and their intersection $\bigcap_{\alpha \in I} S_\alpha = \{x \mid x \in S_\alpha \text{ for all } \alpha \in I\}$.

Example 1.54.
For each $\alpha \in \mathbb{Z}$, let $S_\alpha = \mathbb{Z} - \{-\alpha, \alpha\}$.

$\bigcup_{\alpha\in\mathbb{Z}} S_\alpha = \mathbb{Z}$ and $\bigcap_{\alpha\in\mathbb{Z}} S_\alpha = \emptyset$.

Example 1.55.
For each $\theta \in [0, 2\pi]$, define $S_\theta = \{(\cos\theta, \sin\theta)\}$.
$\bigcup_{\theta\in[0,2\pi]} S_\theta = \{(x, y) \mid x^2 + y^2 = 1\}$ (unit circle).
$\bigcap_{\theta\in[0,2\pi]} S_\theta = \emptyset$.

Definition 1.56. An indexed family $\{S_\alpha\}_{\alpha\in I}$ is *pairwise disjoint (mutually disjoint)* $S_\alpha \cap S_\beta = \emptyset$ whenever $\alpha \neq \beta$.
When $A \cap B = \emptyset$ we say that A and B are disjoint.

Definition 1.57. Let A and B be sets. Their *cartesian product* is the set $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

Example 1.58.
$A = \{0, 1\}$ and $B = \{1, 2, 3\}$.
$A \times B = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3)\}$.

Example 1.59. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$.

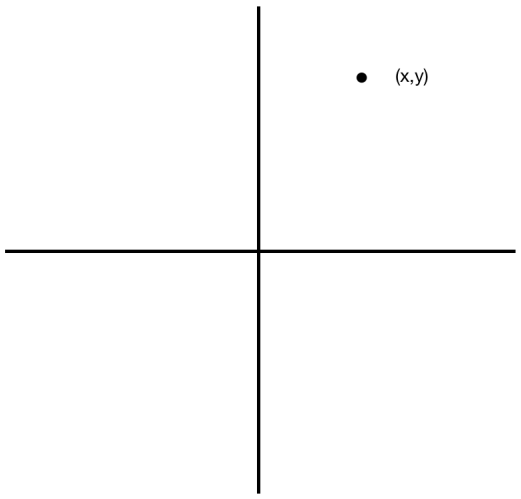


Figure 1.6: Representation of $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$ graphically.

Fact: If A and B are both finite then $|A \times B| = |A||B|$.

Chapter 2

Logic

A *statement* is a declarative sentence that is either true or false.

Example 2.1.
George Washington was the first U.S. President. George Washington was the best U.S. President.
The first sentence is a statement.
The second sentence is an opinion.

Example 2.2.
The integer 6 is prime. (Statement)
The integer 17 is prime. (Statement)
Is 12 an even number? (Question, not a statement)
Compute the derivative of $f(x) = x^2$. (Command, not a statement)

Every statement has a truth value: true T or false F.

It is typical to use capital letters to represent statements:
$P, Q, R, \ldots$ or $P_1, P_2, P_3, \ldots$.

Example 2.3.
P: The number $\sqrt{2}$ is rational.
Q: The integer $2^{11} - 1$ is prime.

Definition 2.4. An *open sentence* is a declarative sentence with one or more variables, where each variable lies in a given set. The

set is called the *domain* of the variable, which becomes a statement when specific elements are substituted for each variable.

Example 2.5. Let $\mathbb{Z}$ be the domain of x.
$x > 3$.
x is irrational.
$x^2 = 4$.

We typically use symbols such as $P(x)$, $Q(x)$, etcetera to represent open sentences in a single variable. More generally, $P(x, y)$ or even $Q(x, y, z)$.

Example 2.6. $P(x) : x^2 \leq 4$, over the domain $\mathbb{Z}$.
$P(x)$ is true for $x \in \{-2, -1, 0, 1, 2\}$ and is false otherwise.

Example 2.7. Let $S = \{-1, 0, 1\}$ be the domain of x and
$T = \{1, 2, 3\}$ be the domain of y.
$P(x, y) : |x| + |y| = 2$.
$P(-1, 1), P(1, 1), P(0, 2)$ are true and $P(x, y)$ is false for all other $(x, y) \in S \times T$.

Truth Tables

The possible combinations of truth values for a collection of statements can be arranged in a truth table.

P
T
F

P	Q
T	T
T	F
F	T
F	F

P	Q	R
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

The integers are equipped with operations; $+, \cdot$ (multiply), $-$ (negate). The operations conform to certain rules (commutativity, associativity, distributivity). $\mathbb{Z}$ forms an "algebraic system". Same for $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Sets are equipped with operations: $\cup, \cap, \overline{(\text{some set})}$. We will see they conform to analogous rules. We will develop a form of "arithmetic" for statements: called *propositional calculus*.

Let P be a statement. The *negation* of P is the statement $\neg P$ "not P" which is true whenever P is false and is false whenever P is true.

P	$\neg P$
T	F
F	T

$\neg P$ can always be expressed as: It is not the case that P. But usually $\neg P$ can be expressed better. Use correct grammar and common sense.

Example 2.8.
P : The real number $\sqrt{5}$ is rational.
$\neg P$: It is not the case that the real number $\sqrt{5}$ is rational.

Or

$\neg P$: The real number $\sqrt{5}$ is not rational.

Or

$\neg P$: The real number $\sqrt{5}$ is irrational.

Example 2.9.
Q : The integer $2^{11} - 1$ is prime.
$\neg Q$: The integer $2^{11} - 1$ is not prime (composite).

Definition 2.10. Let P and Q be statements. The statement "P or Q" is the *disjunction* of P with Q, denoted as $P \vee Q$.
It is true when P is true or Q is true (or both are true) and is false otherwise.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 2.11.
P : The real number $\sqrt{2}$ is irrational. (True)
Q : The real number 7 is irrational. (False)
$P \vee Q$: The real number $\sqrt{2}$ is irrational or the real number 7 is irrational. (True)

Definition 2.12. Let P and Q be statements. The statement "P and Q" is the *conjunction* of P with Q, denoted as $P \wedge Q$.
It is true when both P and Q are true and is false otherwise.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 2.13.
P : The real number $\sqrt{2}$ is irrational. (True)
Q : The real number 7 is irrational. (False)
$P \wedge Q$: The real number $\sqrt{2}$ is irrational and the real number 7 is irrational. (False)

Example 2.14.
P : You get an A on the final.
Q : You get an A in the class.
If both P and Q are true then, 'if P, then Q' is true. If both P and Q are false then, 'if P, then Q' is true. If P is false and Q is true then, 'if P then, Q is' true. If P is true and Q is false then, 'if P, then Q' is false.

Definition 2.15. Let P and Q be statements. The statement "if

P, then Q" is called a *conditional*, denoted $P \Rightarrow Q$. The conditional is false when P is true and Q is false, and is true otherwise.

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

In an if then statement $P \Rightarrow Q$, P is the *hypothesis* or *premise* and Q is the *conclusion*. $P \Rightarrow Q$ is also read/written
"P implies Q", "Q if P", "P only if Q", "P is sufficient for Q", "Q is necessary for P.

Recall the following statement from calculus: If f is differentiable, then f is confinuous.
This is really an open sentence where the domain of f is the set of all functions from $\mathbb{R}$ to $\mathbb{R}$.
$P(f)$: f is differentiable.
$Q(f)$: f is continuous.
$P(f) \Rightarrow Q(f)$ is an open sentence that is true for every f in the domain.
The point: we can operate on open sentences using $\neg, \vee, \wedge, \Rightarrow$ just as with statements.

Example 2.16.
Consider the following open sentences over $\mathbb{R}$.
$P(x) : x^2 > 5$.
$Q(x) : |x| > 2$.

$\neg P(x) : x^2 \leq 5$.
$P(x) \vee Q(x) : x^2 > 5$ or $|x| > 2$.
$P(x) \wedge Q(x) : x^2 > 5$ and $|x| > 2$.
$P(x) \Rightarrow Q(x) :$ If $x^2 > 5,$ then $|x| > 2$.
$Q(x) \Rightarrow P(x) :$ If $|x| > 2,$ then $x^2 > 5$.

*Note: $Q(2.1) \Rightarrow P(2.1)$ is false.

Definition 2.17. The statement $Q \Rightarrow P$ is the *converse* of $P \Rightarrow Q$.

Definition 2.18. Let P and Q be statements. The statement "P if and only if Q" is called a *biconditional*, denoted $P \Leftrightarrow Q$ and is defined as $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

$P \Leftrightarrow Q$ is also read/written "P is equivalent to Q", "P is necessary and sufficient for Q".

The symbols $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ are called *logical connectives*. Statements constructed using logical connectives are *compound statements*.

Definition 2.19. A compound statement is
(a) a *tautology* if it is always true.
(b) a *contradiction* if it is always false.

Example 2.20. $P \vee (\neg P)$ is a tautology.

Example 2.21. $P \wedge (\neg P)$ is a contradiction.

Definition 2.22. Let R and S be compound statements formed using logical connectives on the statements $P_1, P_2, \ldots, P_n$. We say that R and S are *logically equivalent*, denoted $R \equiv S$ if R and S have the same truth values for all combinations of truth values assigned to $P_1, \ldots, P_n$.
Equivalently: $R \equiv S$ whenever $R \Leftrightarrow S$ is tautology.

Example 2.23.

P	Q	$\neg P$	$P \Rightarrow Q$	$(\neg P) \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Conclusion: $P \Rightarrow Q \equiv (\neg P) \vee Q$.

Theorem 2.24. Let P, Q and R be statements. Then the following equivalences hold.

(a) Commutative laws.
(i) $P \vee Q \equiv Q \vee P$.
(ii) $P \wedge Q \equiv Q \wedge P$.

(b) Associative laws.
(i) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$.
(ii) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$.

(c) Distributive laws.
(i) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.
(ii) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

(d) Demorgan's laws.
(i) $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$.
(ii) $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$.

Quantifiers

Recall:

$P(f)$: f is differentiable.
$Q(f)$: f is continuous.

Where f is a variable of the domain of functions from $\mathbb{R}$ to $\mathbb{R}$. Then $P(f) \Rightarrow Q(f)$ is an open sentence that has been shown to be true for every choice of function f from $\mathbb{R}$ to $\mathbb{R}$.

Example 2.25. Consider the open sentence $P(n) : 2^n - 1$ is prime over the domain $\mathbb{N}$. (Not a statement)

There exists $n \in \mathbb{N}$ such that $2^n - 1$ is prime. (statement)

In each example, the open sentence was converted to a statement by "quantification".

Definition 2.26. Let $P(x)$ be an open sentence over the domain S. The statement "for every $x \in S, P(x)$" is denoted $\forall x \in S, P(x)$. It is true if $P(s)$ is true whenever $s \in S$. It is false if $P(t)$ is false for at least one $t \in S$. The phrase "for every" (or "for all") is the *universal quantifier*.

Example 2.27.
$P(n) : 4n + 1$ is odd
We get a statement by using the universal quantifier, $\forall n \in \mathbb{N}, 4n+1$ is odd.

Definition 2.28. Let $P(x)$ be an open sentence over the domain S. The statement "there exists $x \in S$ such that $P(x)$" is denoted $\exists x \in S, P(x)$. It is true if $P(s)$ is true for at least one $s \in S$, and is false if $P(t)$ is false for all $t \in S$. The phrase "there exists" is called the *existential quantifier*.

Example 2.29.
Let $A = \{1, 2, 3\}$. Write each statement in English and then determine its truth value.

$\exists x \in \wp(A), |x \cap A| = 1$.
"There exists $x \in \wp(A)$ such that $|x \cap A| = 1$".
Letting x = $\{1\}$ we see that $|\{1\} \cap A| = |\{1\}| = 1$, thus the statement is true.

$\forall x \in A, x^2 - 1 > 4$.
"For every $x \in A$, $x^2 - 1 > 4$".
Since $1^2 - 1 \not> 4$, the statement is false.

$\forall x \in \wp(A), A - x \subseteq A$.
For all $x \in \wp(A), A - x \subseteq A$.
Since $A - x = \{y \mid y \in A \text{ and } y \notin x\}, A - x \subseteq A$ for every choice of $x \in \wp(A)$.
Thus, the statement is true.

$\exists x \in A, \{x\} \cap A = \emptyset$.
There exists $x \in A$ such that $\{x\} \cap A = \emptyset$.
*Note:
$\{1\} \cap A = \{1\} \neq \emptyset$.
$\{2\} \cap A = \{2\} \neq \emptyset$.
$\{3\} \cap A = \{3\} \neq \emptyset$.
Thus, the statement is false.

Wording: $\forall$: For every, for all. $\exists$: there exists, for some.

For open sentences with 2 variables, 2 quantifiers are required. Possibilities,
$\forall x \in S, \forall y \in T, P(x, y)$.
$\forall x \in S, \exists y \in T, P(x, y)$.
$\exists x \in S, \forall y \in T, P(x, y)$.
$\exists x \in S, \exists y \in T, P(x, y)$.

Example 2.30.
$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^2 + y^2 > 0$. False, reason: when $x = y = 0$.
$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^2 + y^2 > 0$. True, reason: given any $x \in \mathbb{R}$, let $y = 1$.
$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^2 + y^2 > 0$. True, reason: If $x = 1$, then $1^2 + y^2 > 0$ for every choice of $y \in \mathbb{R}$.
$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x^2 + y^2 > 0$. True, reason: Let $x = y = 1$.

Example 2.31.
Let $A = \{1, 2, 3\}$.
$\forall x \in A, \forall y \in \wp(A), \{x\} - y = \emptyset$. False, reason: choosing $x = 1$, $y = \{\emptyset\}$ we have $\{x\} - y = \{1\} \neq \emptyset$.
$\forall x \in A, \exists y \in \wp(A), \{x\} - y = \emptyset$. True, reason: given $x \in A$, let $y = \{x\}$ then $\{x\} - y = \emptyset$.
$\exists x \in A, \forall y \in \wp(A), \{x\} - y = \emptyset$. False, reason: no matter which $x \in A$ we are given, when $y = \emptyset$ we have $\{x\} - y = \{x\} \neq \emptyset$.
$\exists x \in A, \exists y \in \wp(A), \{x\} - y = \emptyset$. True, reason: choose $x = 1$ and $y = \{1\}$, then $\{x\} - y = \emptyset$.

Example 2.32.
$\forall x \in \mathbb{N}, \forall y \in \mathbb{Z}, \frac{y}{x} \in \mathbb{Z}$. False, reason: when $x = 2$ and $y = 1$, $\frac{y}{x} = \frac{1}{2} \notin \mathbb{Z}$.
$\forall x \in \mathbb{N}, \exists y \in \mathbb{Z}, \frac{y}{x} \in \mathbb{Z}$. True, reason: given $x \in \mathbb{N}$, let $y = x$, then

$\frac{y}{x} = \frac{x}{x} = 1 \in \mathbb{Z}$.
$\exists x \in \mathbb{N}, \forall y \in \mathbb{Z}, \frac{y}{x} \in \mathbb{Z}$. True, reason: for $x = 1$, the fraction $\frac{y}{1} \in \mathbb{Z}$ for every choice of $y \in \mathbb{Z}$.
$\exists x \in \mathbb{N}, \exists y \in \mathbb{Z}, \frac{y}{x} \in \mathbb{Z}$. True, reason: choose $x = 1, y = 3$, then $\frac{y}{x} = \frac{3}{1} = 3 \in \mathbb{Z}$.

Negating quantified statements

$\forall x \in S, P(x)$ is a statement that is true when $P(x)$ is true for every $x \in S$ and is false if $P(s)$ is false for at least one $s \in S$. As a consequence, $\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$.

$\exists x \in S, P(x)$ is a statement that is true when $P(s)$ is true for at least one $s \in S$ and is false if $P(x)$ is never true when $x \in S$. As a consequence $\neg(\exists x \in S, P(x)) \equiv \forall x \in S, \neg P(x)$.

Example 2.33.
The square of every real number is positive.

$\forall x \in \mathbb{R}, x^2 > 0$.

Negation: $\neg(\forall x \in \mathbb{R}, x^2 > 0) \equiv \exists x \in \mathbb{R}, x^2 < 0$.

In English: There exists a real number whose square is not positive.

Since $0^2 = 0$ which is not positive, the negation of the original is true. Consequently, the original statement is false.

Example 2.34.
Every P-series is convergent.

$\forall p \in \mathbb{R}, \sum_{n=1}^{\infty} \frac{1}{n^p} < \infty$.

Negation: $\exists p \in \mathbb{R}, \sum_{n=1}^{\infty} \frac{1}{n^p} = \infty$.

In English: There exists a divergent P-series.

With $p = 1$, the series $\sum_{n=1}^{\infty} \frac{1}{n^p}$ diverges and so the negation is true

which implies that the original is false.

Negating statements with multiple quantifiers

$\neg(\forall x \in S, \forall y \in T, P(x,y))$
$\equiv \exists x \in S, \neg(\forall y \in T, P(x,y))$
$\equiv \exists x \in S, \exists y \in T, \neg P(x,y).$

Example 2.35.
Negate: for every positive real number ε, there exists a natural number N such that $\frac{1}{N} < \varepsilon$.

Symbolically: $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \frac{1}{N} < \varepsilon$.

Negation $\exists \varepsilon > 0, \forall N \in \mathbb{N}, \frac{1}{N} \geq \varepsilon$.

In English: There exists a positive real number ε such that for all natural numbers N, $\frac{1}{N} \geq \varepsilon$.

Example 2.36.
$A = \{1, 2, 3\}$.
Negate: $\exists x \in A, \forall y \in \wp(A), |y - \{x\}| > 2$ and determine the truth value.

Negation: $\forall x \in A, \exists y \in \wp(A), |y - \{x\}| \leq 2$.

The negation is true, because given $x \in A$, choose $y = \{x\}$. Then $|y - \{x\}| = |\{x\} - \{x\}| = |\emptyset| = 0 \leq 2$.
Conclusion: The original is false.

Example 2.37.
For every positive real number ε there exists a natural number N such that $N^2 < \varepsilon$, then $\frac{N^3}{4} \in \mathbb{Q}$.

$\forall \varepsilon > 0, \exists N \in \mathbb{N}, N^2 < \varepsilon \Rightarrow \frac{N^3}{4} \in \mathbb{Q}$.

Negation: $\exists \varepsilon > 0, \forall N \in \mathbb{N}, \neg(N^2 < \varepsilon \ (P) \Rightarrow \frac{N^3}{4} \in \mathbb{Q} \ (Q))$.

($\downarrow$ Logically equivalent $\downarrow$)

$\equiv \exists \varepsilon > 0, \forall N \in \mathbb{N}, \neg(N^2 \geq \varepsilon\ (P) \vee \frac{N^3}{4} \in \mathbb{Q}\ (Q))$.

($\downarrow$ Demorgan's laws $\downarrow$)

$\equiv \exists \varepsilon > 0, \forall N \in \mathbb{N}, N^2 < \varepsilon\ (P) \wedge \frac{N^3}{4} \notin \mathbb{Q}\ (Q)$.

Chapter 3

Methods of Proof

Terminology:
Axiom: A true statement whose truth is expected without proof (defined to be true).
Theorem (or proposition): A true statement whose truth can be verified.
Corollary: A true statement whose truth follows easily from previously established results.
Lemma: A result that is useful in proving a theorem.

Most theorems are stated as implications usually as quantified statements in one or more variables.

In the statement $\forall x \in S, P(x) \Rightarrow Q(x)$ the wording is typically along the lines
For $x \in S$, if $P(x)$ then $Q(x)$.
Let $x \in S$, if $P(x)$ then $Q(x)$.
Given $x \in S$, if $P(x)$ then $Q(x)$.

The trivial proof: If one can demonstrate that $Q(x)$ is true for all $x \in S$, then $\forall x \in S, P(x) \Rightarrow Q(x)$ is *trivially true*.

The vacuous proof: If one can demonstrate that $P(x)$ is false for all $x \in S$, then the statement $\forall x \in S, P(x) \Rightarrow Q(x)$ is *vacuously true*.

*Note: Both the trivial proof and the vacuous proof are not good methods of proof to use.

Example 3.1.
Let $x \in \mathbb{R}$, if $x > 0$ then $x^2 + 1 > 0$.
Since $x^2 + 1 > 0$ regardless of the value of x, then the statement is trivially true.

Example 3.2.
Let $n \in \mathbb{N}$, if $n < 0$ then $n^2 + 1$ is even.
Since $n < 0$ is false for $n \in \mathbb{N}$ then, the statement is vacuously true.

The Direct Proof

Suppose we wish to prove the statement $\forall x \in S, P(x) \Rightarrow Q(x)$ (which is neither trivially true nor vacuously true).

Steps of direct proof:

1. Choose an arbitrary $x \in S$ for which $P(x)$ is true.
2. Verify that $Q(x)$ is true for the chosen x.

Many of our early examples will involve $\mathbb{Z}$. We will use the standard properties of $\mathbb{Z}$.

Definition 3.3. An integer x is *even* if there exists some $n \in \mathbb{Z}$ such that $x = 2n$.

Definition 3.4. An integer x is *odd* if there exists some $n \in \mathbb{Z}$ such that $x = 2n + 1$.

Example 3.5.
Prove: If n is an even integer,then $5n + 3$ is odd.

Proof: Let n be an even integer. Then there exists some $k \in \mathbb{Z}$ such that $n = 2k$. Now, $5n+3 = 5(2k)+3 = 5(2k)+2+1 = 2(5k+1)+1$. Since $5k + 1 \in \mathbb{Z}$, we conclude that $5n + 3$ is odd. $\square$

Example 3.6.
If $n \in \mathbb{Z}$ is odd, then n^2 is odd.

Proof: Let $n \in \mathbb{Z}$ be odd. Then there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. Now, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$,

which is odd. □

Definition 3.7. Given statements P and Q, the statement $\neg Q \Rightarrow \neg P$ is the *contrapositive* of $P \Rightarrow Q$.

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

From the truth table we see that $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

Proof by Contrapositive

To prove $\forall x \in S, P(x) \Rightarrow Q(x)$
complete a direct proof of
$\forall x \in S, \neg Q(x) \Rightarrow \neg P(x)$.

Example 3.8.
Prove: If $5x - 7$ is an even integer, then x is odd.
Proof: (Contrapositive) Let $x \in \mathbb{Z}$ be even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Now $5x - 7 = 5(2k) - 7 = 5(2k) - 8 + 1 = 2(5k - 4) + 1$, which is odd. □

Proving a Biconditional

$$P \Rightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

To prove $\forall x \in S, P(x) \Leftrightarrow Q(x)$ we proceed in two steps:

1. Prove $\forall x \in S, P(x) \Rightarrow Q(x)$ by any method.
2. Prove $\forall x \in S, Q(x) \Rightarrow P(x)$ by any method.

Theorem 3.9. Let $n \in \mathbb{Z}$. Then n^2 is even if and only if n is even.

Proof: ($\Rightarrow$)(Contrapositive) Let $n \in \mathbb{Z}$ be odd. Then, $n = 2k+1$ for some $k \in \mathbb{Z}$. Now, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.
($\Leftarrow$) Let $n \in \mathbb{Z}$ be even. Then, there exists $k \in \mathbb{Z}$ such that $n = 2k$.

Now, $n^2 = 4k^2 = 2(2k^2)$, which is even. $\square$.

Corollary 3.10. Let $n \in \mathbb{Z}$. Then n^2 is odd if and only if n is odd.

Theorem 3.11. The product of two integers a and b is even if and only if a is even or b is even.

Proof:($\Rightarrow$)(Contrapositive) Let $a, b \in \mathbb{Z}$ be odd. Then, there exists $k, m \in \mathbb{Z}$ such that $a = 2k + 1$ and $b = 2m + 1$. Now, $ab = (2k+1)(2m+1) = 4km + 2k + 2m + 1 = 2(2km + k + m) + 1$, which is odd.
($\Leftarrow$) Let $a, b \in \mathbb{Z}$ and assume without loss of generality that a is even. Then $a = 2k$ for some $k \in \mathbb{Z}$. Now, $ab = (2k)(b) = 2(kb)$, which is even. $\square$

Definition 3.12. Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a *divides* b if there exists $n \in \mathbb{Z}$ such that $b = an$.
Notation: $a \mid b$.

Definition 3.13. We say that integers a and b have the *same parity* if either both a and b are even or both a and b are odd.

Definition 3.14. Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. Then a *is congruent to* b *modulo* m if m divides $a - b$.
Notation $a \equiv b \bmod m$.

Example 3.15.
$3 \equiv 7 \bmod 2$.
$5 \not\equiv 20 \bmod 4$.
$100 \equiv 50 \bmod 10$.

Theorem 3.16. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Assume that $a \mid b$ and $b \mid c$. Then there exists $m, n \in \mathbb{Z}$ such that $b = am$ and $c = bn$. Now $c = (am)n = a(mn)$ and so $a \mid c$. $\square$

Example 3.17.
Let $x, y \in \mathbb{Z}$. Then $4 \mid x^2 - y^2$ if and only if x and y have the same parity.

Proof:($\Rightarrow$)(Contrapositive) Suppose $x, y \in \mathbb{Z}$ have different parity. If x is even and y is odd, then there exists $k, m \in \mathbb{Z}$ such that $x = 2k$ and $y = 2m + 1$. Now, $x^2 - y^2 = (2k)^2 - (2m + 1)^2 = 4k^2 - (4m^2 + 4m + 1) = 4(k^2 - m^2 - m) - 1$, which is not a multiple of 4 and so $4 \nmid x^2 - y^2$. The case where x is odd and y is even is similar.
($\Leftarrow$) We consider two cases.

1. If x and y are even, then there exists $k, m \in \mathbb{Z}$ such that $x = 2k$ and $y = 2m$. Now, $x^2 - y^2 = 4(k^2 - m^2)$ and so $4 \mid x^2 - y^2$.

2. If x and y are odd, then $x = 2k + 1$ and $y = 2m + 1$ for some $k, m \in \mathbb{Z}$. Now, $x^2 - y^2 = (4k^2 + 4k + 1) - (4m^2 + 4m + 1) = 4(k^2 + k - m^2 - m)$ and so $4 \mid x^2 - y^2$. $\square$

Theorem 3.18. Let $a, b, c, d, k, m \in \mathbb{Z}$ with $m \geq 2$.
(a) If $a \equiv b \bmod m$, then $ka \equiv kb \bmod m$.
(b) If $a \equiv c \bmod m$ and $b \equiv d \bmod m$, then $a + b \equiv c + d \bmod m$.
(c)If $a \equiv c \bmod m$ and $b \equiv d \bmod m$, then $ab \equiv cd \bmod m$.

Proof: (a) If $a \equiv b \bmod m$, then $m \mid a-b$ and so $a-b = mn$ for some $n \in \mathbb{Z}$. Multiplying this equation by k we have $ka - kb = m(nk)$ and so $m \mid ka - kb$. Thus, $ka \equiv kb \bmod m$.

(b) Let $a \equiv c \bmod m$ and $b \equiv d \bmod m$. Then $m \mid a-c$ and $m \mid b-d$. It follows that there exists an $x, y \in \mathbb{Z}$ such that $a - c = xm$ and $b - d = ym$. If $a - c = xm$ and $b - d = ym$ are added
together, then their sum is (a - c) + (b - d) = (xm) + (ym). Thus, $(a + b) + (-c - d) = m(x + y)$ and so (a + b) - (c + d) = m(x + y). Since $m \mid (a + b) - (c + d)$, $a + b \equiv c + d \bmod m$.

(c) Let $a \equiv c \bmod m$ and $b \equiv d \bmod m$. Then, $m \mid a-c$ and $m \mid b-d$ and so there exists $x, y \in \mathbb{Z}$ such that $a - c = xm$ and $b - d = ym$. By multiplying b through $a - c = xm$ we get $ab - cb = bxm$, and by multiplying c through $b - d = ym$ we get $cb - cd = cym$. If $ab - cb = bxm$ and $cb - cd = cym$ are added together, their sum is $ab - cb + cb - cd = mbx + mcy$. Then with simplification, we get

$ab - cd = m(bx + cy)$ and so $m \mid ab - cd$. Thus, $ab \equiv cd \bmod m$. $\square$

Recall:

$$|x| = \begin{cases} \text{x} & \text{if } x \geq 0 \\ \text{-x} & \text{if } x < 0. \end{cases}$$

Theorem 3.19. (Triangle Inequality Theorem)
For any real numbers x and y, $|x + y| \leq |x| + |y|$.

Proof: We consider several cases.

1. If $x = 0$, then we have $|0 + y| = |y| = |0| + |y|$. similarly if $y = 0$.
2. If $x, y < 0$, then $|x + y| = -|x + y| = -x - y = |x| + |y|$.
3. If $x, y > 0$, then $|x + y| = x + y = |x| + |y|$.
4. If $x > 0$ and $y < 0$, we consider two subcases:
   (a) If $x + y \geq 0$ then $|x + y| = x + y = |x| - |y| < |x| + |y|$.
   (b) If $x + y < 0$ then $|x + y| = -(x + y) = -x + -y = -|x| + |y|$ and so $|x + y| < |x| + |y|$.$\square$

Recall: $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$.

To show $A \subseteq B$, there is a standard format *(Containment proof)*.

1. Let $x \in A$.
2. Show $x \in B$.
3. Conclude $A \subseteq B$.

Example 3.20. For any sets A and B, $A - B = A \cap \overline{B}$.

Proof: ($\subseteq$) Let $x \in A - B$. Then, $x \in A$ and $x \notin B$. It follows that $x \in A$ and $x \in \overline{B}$ and so $x \in A \cap \overline{B}$. Thus, $A - B \subseteq A \cap \overline{B}$.
($\supseteq$) Let $x \in A \cap \overline{B}$. Then, $x \in A$ and $x \in \overline{B}$. From this we see that $x \in A$ and $x \notin B$ and so $x \in A - B$. Thus, $A \cap \overline{B} \subseteq A - B$.
Conclusion: $A - B = A \cap \overline{B}$. $\square$

So far we have proved statements of the form $\forall x \in S, P(x)$.

We now consider statements of the form $\exists x \in S, P(x)$.
Such statements can arise in one of two ways:
(i) Directly: The statements given in this form.
(ii) Indirectly: As the negation of a "for all" statement.

To prove $\exists x \in S, P(x)$, produce $s \in S$ such that P(s) is true. To disprove $\forall x \in S, P(x)$ it is equivalent to showing that $\exists x \in S, \neg P(x)$ is true. If $s \in S$ is such that $\neg P(s)$ is true, then s is called a *counter example*.

Example 3.21. Show that the statement, for every $n \in \mathbb{N}$ if $4 \mid n^2 - 1$, then $4 \mid n - 1$ is false.
Letting $n = 3$ we have that $4 \mid 3^2 - 1$ but $4 \nmid 3 - 1$ thus the statement is false.

Proof by Contradiction

Let P be a true statement and suppose you want to show that the statement R is true. In the method of proof by contradiction we assume that R is false. If this leads us to deduce that P is false, then we have a *contradiction*. From this we conclude R is true.

Example 3.22. Prove that the sum of a rational number and an irrational number is irrational.

Proof: (Contradiction) Suppose there exists $x \in \mathbb{Q}$ and $y \in \mathbb{R} - \mathbb{Q}$ such that $x + y \in \mathbb{Q}$. Then, there exists $a, b, c, d \in \mathbb{Z}$ where $b, d \neq 0$ such that $x = \frac{a}{b}$ and $x + y = \frac{c}{d}$. Now, $y = \frac{c}{d} - x = \frac{c}{d} - \frac{a}{b} = \frac{cb-ad}{bd} \in \mathbb{Q}$. This is a contradiction ($\Rightarrow\Leftarrow$). This completes the proof. $\square$

Theorem 3.23. The real number $\sqrt{2}$ is irrational.

Proof: (Contradiction) Suppose $\sqrt{2} \in \mathbb{Q}$. Then there exists $a, b \in \mathbb{Z}$ such that $\sqrt{2} = \frac{a}{b}$, with $b \neq 0$. We may assume that this fraction is reduced. It follows that $2 = \frac{a^2}{b^2}$ and so $a^2 = 2b^2$. This implies that a^2 is even; by Theorem 3.9 we conclude a is even. Then, there exists $m \in \mathbb{Z}$ such that $a = 2m$. Substituting, we have $4m^2 = 2b^2$

and so $b^2 = 2m^2$. It follows that b^2 is even and (again by Theorem 3.9) we conclude that b is even. This means $\frac{a}{b}$ is not reduced $\Rightarrow\Leftarrow$. In conclusion $\sqrt{2}$ is irrational. $\square$

Theorem 3.24. (Properties of Set Operations) Let A, B, C be sets in $\mathcal{U}$

1. Commutativity
   (a) $A \cup B = B \cup A$.
   (b) $A \cap B = B \cap A$.

2. Associativity
   (a) $A \cup (B \cup C) = (A \cup B) \cup C$.
   (b) $A \cap (B \cap C) = (A \cap B) \cap C$.

3. Distributivity
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

4. Demorgan's Laws
   (a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
   (b) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof of 3b:($\subseteq$) Let $x \in A \cap (B \cup C)$. Then, $x \in A$ and $x \in B \cup C$. If $x \in B$, then $x \in A \cap B$, if $x \in C$, then $x \in A \cap C$. Thus, $x \in (A \cap B) \cup (A \cap C)$ and so $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
($\supseteq$) Let $x \in (A \cap B) \cup (A \cap C)$. If $x \in A \cap B$, then $x \in A$ and $x \in B \cup C$. If $x \in A \cap C$, then $x \in A$ and $x \in B \cap C$. Thus, $x \in A \cap (B \cup C)$ and so $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
In conclusion, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. $\square$

Example 3.25. Let A, B, C be sets. Then
$A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof: ($\subseteq$) Let $(x, y) \in A \times (B \cup C)$. Now, we have $x \in A$ and $y \in B$ or $y \in C$. In the first case $(x, y) \in A \times B$; in the second case $(x, y) \in A \times C$. Thus, $(x, y) \in (A \times B) \cup (A \times C)$ and so $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.
($\supseteq$) Let $(x, y) \in (A \times B) \cup (A \times C)$. If $(x, y) \in A \times B$, then $x \in A$ and $y \in B \cup C$. If $(x, y) \in A \times C$, then $x \in A$ and $y \in B \cup C$. As a consequence $(x, y) \in A \times (B \cup C)$ and so $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.

In conclusion, $A \times (B \cup C) = (A \times B) \cup (A \times C)$. $\square$

Chapter 4

Mathematical Induction

Definition 4.1. Let $\emptyset \neq A \subseteq \mathbb{R}$. A real number $m \in A$ is a *least element* of A if $x \geq m$ for all $x \in A$.

Example 4.2.
$A = [1, 2]$. (The) least element of A is 1.

Proof: Let $x \in A$. Then $1 \leq x \leq 2$ as desired. $\square$

Example 4.3. $B = (1, 2)$.
Claim: B has no least element.

Proof: (Contradiction) Suppose $m \in B$ is a least element. Define $m' = \frac{1+m}{2}$ (midpoint between 1 and m). Since $1 < m < 2$ we have $1 = \frac{1+1}{2} < \frac{1+m}{2}$(this is m') $< \frac{1+2}{2} = \frac{3}{2} < 2$ and so $m' \in B$. Also, since $m > 1$, we have $m' = \frac{m+1}{2} < \frac{m+m}{2} = m$. This contradicts our assumption that m is a least element of B. Thus, B has no least element. $\square$

Example 4.4. $A = \{\frac{1}{n} \mid n \in \mathbb{N}\}$.
Claim: A has no least element.

Proof: (Contradiction) Suppose $m \in A$ is a least element. Then $m = \frac{1}{N}$ for some $N \in \mathbb{N}$. Now, $\frac{1}{N+1} < \frac{1}{N}$ and $\frac{1}{N+1} \in A$ contradicting our assumption that m is a least element. Therefore, A has no least element. $\square$

Theorem 4.5. Let $\emptyset \neq A \subseteq \mathbb{R}$. If A has a least element, then this element is unique.

Proof: Suppose $m, m' \in A$ are least elements. Since m is a least element and $m' \in A$. We conclude that $m \leq m'$. Similarly $m' \leq m$. It follows that $m = m'$. $\square$

Definition 4.6. A nonempty set $A \subseteq \mathbb{R}$ is *well-ordered* if every nonempty subset of A has a least element.

Example 4.7. $(1, 2)$ is not well-ordered because it does not have a least element.

Example 4.8. $[1, 2]$ is not well-ordered because the subset $(1, 2)$ has no least element.
More generally if $a < b$ then (a, b) has no least element. As a consequence no interval is well-ordered.

Example 4.9. If $\{a_1, a_2, a_3, \ldots, a_n\} \subseteq \mathbb{R}$ then this set is well-ordered.

Axiom 4.10. (Well Ordering Principle (WOP)) $\mathbb{N}$ is well-ordered

Theorem 4.11. (Principle of Mathematical Induction) Let $P(n)$ be an open sentence over $\mathbb{N}$. If (a) $P(1)$ is true (b) the conditional $P(k) \Rightarrow P(k+1)$ is true for all $k \in \mathbb{N}$. Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof: (Contradiction) Suppose not, then (a) and (b) are true but the set $S = \{n \in \mathbb{N} \mid P(n) \text{ is false}\}$ is nonempty. Since $S \subseteq \mathbb{N}$, by the WOP, S has a least element s. So $P(s)$ is false and if $n \in \mathbb{N}$ is such that $n < s$, then $P(n)$ is true. Since $P(1)$ is true, we conclude that $s \geq 2$. It follows that $s - 1 \in \mathbb{N}$ and, since $s - 1 < s$, we have that $P(s-1)$ is true. By (b) we conclude that $P(s)$ is true $\Rightarrow\Leftarrow$.$\square$

Structure of Proof by Induction

Given $P(n)$ over $\mathbb{N}$.

1. Show that $P(1)$ is true. (Base step)
2. Choose $k \in \mathbb{N}$ arbitrarily and show that $P(k) \Rightarrow P(k+1)$ is true for this k. (Inductive step)
3. Conclude that $P(n)$ is true for all $n \in \mathbb{N}$.

*Note: $P(k)$ is called the inductive hypothesis.

Theorem 4.12. For any $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Proof: (Induction)
(Base step): If $n = 1$, we have the equation $1 = \frac{1(2)}{2}$ which is true.
(Inductive step): Let $k \in \mathbb{N}$ such that $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$.
It follows that

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \text{ as desired.} \end{aligned}$$

By induction the formula holds for all $n \in \mathbb{N}$. $\square$

Alternate proof by Gauss:

$$\begin{aligned} S_n &= 1 + 2 + \cdots + n \\ + S_n &= n + (n-1) + \cdots + 1 \\ (\Updownarrow) & \\ 2S_n &= (n+1) + (n+1) + \cdots + (n+1) \\ &= n(n+1) \end{aligned}$$

Therefore $S_n = \dfrac{n(n+1)}{2}$.

Example 4.13. Prove: For all $n \in \mathbb{N}$

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{(n+1)(n+2)} = \frac{n}{2n+4}.$$

Proof: (Induction)
(Base step): If $n = 1$, we have $\frac{1}{(2)(3)} = \frac{1}{6} = \frac{1}{2(1)+4}$.
(Inductive step): Let $k \in \mathbb{N}$, with

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{(k+1)(k+2)} = \frac{k}{2k+4}.$$

Then,

$$\begin{aligned}
\frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+2)(k+3)} &= \frac{k}{2k+4} + \frac{1}{(k+2)(k+3)} \\
&= \frac{k}{2(k+2)} + \frac{1}{(k+2)(k+3)} \\
&= \frac{k(k+3)}{2(k+2)(k+3)} + \frac{2}{2(k+2)(k+3)} \\
&= \frac{k^2+3k+2}{2(k+2)(k+3)} \\
&= \frac{(k+1)(k+2)}{2(k+2)(k+3)} \\
&= \frac{k+1}{2k+6} \\
&= \frac{k+1}{2(k+1)+4} \text{ as desired.}
\end{aligned}$$

By induction the formula holds for all $n \in \mathbb{N}$.□

Example 4.14. Prove: For all $n \in \mathbb{N}$, 8 divides $5^{2n} - 1$.

Proof: (Induction)
(Base step): When $n = 1$, we have $5^{2(1)} - 1 = 24$, which is divisible by 8.
(Inductive step): Let $k \in \mathbb{N}$ and assume that $8 \mid 5^{2k} - 1$. Then there

exists $m \in \mathbb{Z}$ such that $5^{2k} - 1 = 8m$. Now,

$$\begin{aligned} 5^{2(k+1)} - 1 &= 5^{2k+2} - 1 \\ &= (25)(5^{2k}) - 1 \\ &= (24+1)(5^{2k}) - 1 \\ &= 24 \cdot 5^{2k} + 5^{2k} - 1 \\ &= 8(3 \cdot 5^{2k}) + 8m \\ &= 8(3 \cdot 5^{2k} + m), \text{and so } 8 \mid 5^{2k+1} - 1 \text{ as desired.} \end{aligned}$$

By induction $8 \mid 5^{2n} - 1$ for all $n \in \mathbb{N}$. $\square$

Example 4.15. For each $n \in \mathbb{N}$, let $A_n = \{1, 2, \ldots, n\}$. Prove that $|\wp(A_n)| = 2^n$.

Proof:(Induction)
(Base step): When $n = 1$, we have $\wp(A_1) = \wp(\{1\}) = \{\emptyset, \{1\}\}$ which has 2^1 elements.
(Inductive step): Let $k \in \mathbb{N}$ and assume that $|\wp(A_k)| = 2^k$. Note that $\wp(A_{k+1}) = \wp(A_k) \cup \{B \cup \{k+1\} \mid B \in \wp(A_k)\}$ and the sets on the right are disjoint. It follows that

$$\begin{aligned} |\wp(A_{k+1})| &= |\wp(A_k)| + |\{B \cup \{k+1\} \mid B \in \wp(A_k)\}| \\ &= |\wp(A_k)| + |\wp(A_k)| \\ &= 2^k + 2^k \\ &= 2(2^k) \\ &= 2^{k+1} \text{ as desired.} \end{aligned}$$

By induction for all $n \in \mathbb{N}, |\wp(A_n)| = 2^n$.$\square$

Theorem 4.16. Let $m \in \mathbb{Z}$, then the set $S = \{i \in \mathbb{Z} \mid i \geq m\}$ is well-ordered.

Proof: Let $\emptyset \neq T \subseteq S$. If $T \subseteq \mathbb{N}$, then T has a least element by WOP. If not then $m \leq 0$ and $T - \mathbb{N} \subseteq \{m, m+1, \ldots, 0\}$. Since $T - \mathbb{N}$ is a finite, nonempty set, there exists a least element t in $T - \mathbb{N}$.

Claim: t is the least element of T.
Proof of claim: Choose $u \in T$. If $u \in \mathbb{N}$, then $t < u$ (because $t \leq 0$). If $u \in T - \mathbb{N}$, then $t \leq u$ (because t is a least element of $T - \mathbb{N}$). Claim done.
Since T has a least element, we conclude that S is well-ordered. □

Theorem 4.17. (Generalized Principle of Mathematical Induction) Fix the integer m and let $S = \{i \in \mathbb{Z} \mid i \geq m\}$. For the open sentence $P(n)$ over S, if

1. $P(m)$ is true.
2. $P(k) \Rightarrow P(k+1)$ is true for all $k \in S$, then $P(n)$ is true for all $n \in S$.

Proof: Same as proof for Principle of Mathematical Induction (PMI), but replacing 1 with m.

Example 4.18. Prove that $n! > 2^n$ for all integers n with $n \geq 4$.

Proof:(Induction)
(Base step): When $n = 4$ we have $4! = 24 > 16 = 2^4$.
(Inductive step): Let $k \in \mathbb{Z}$ with $k \geq 4$ and assume that $k! > 2^k$. then

$$\begin{aligned}(k+1)! &= (k+1)(k)! \\ &> (k+1) \cdot 2^k \\ &\geq 5 \cdot 2^k (\text{Reason } k \geq 4) \\ &> 2 \cdot 2^k \\ &= 2^{k+1}.\end{aligned}$$

Therefore $(k+1)! > 2^{k+1}$ as desired.
By induction the inequality holds for all $n \geq 4$.□

Example 4.19. Prove that if $A_1, A_2, \ldots, A_n$ are sets and $n \geq 2$ then $\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$.

Proof: (Induction)
(Base step): When $n = 2$, we have that $\overline{A_1 \cup A_2} = \overline{A_1} \cap \overline{A_2}$ by

DeMorgan.
(Inductive step): Let $k \geq 2$ and assume that $\overline{A_1 \cup A_2 \cup \cdots \cup A_k} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k}$. Then

$$\begin{aligned}\overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}} &= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup (A_{k+1})} \\ &= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k)} \cap \overline{A_{k+1}} \text{ (follows from base step)} \\ &= \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k} \cap \overline{A_{k+1}}\end{aligned}$$

By induction the result holds for all $n \geq 2$. $\square$

Corollary 4.20. (Principle of Strong Induction) Fix $m \in \mathbb{Z}$ and let $S = \{i \in \mathbb{Z} \mid i \geq m\}$. For the open sentence $P(n)$ over S, if

1. $P(m)$ is true.
2. For any $k \in S$, $P(m) \wedge P(m+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$ is true,
   then $P(n)$ is true for all $n \in S$.

Example 4.21. Define the sequence a_n as follows:
$a_1 = 1, a_2 = 3, a_n = 2a_{n-1} - a_{n-2}$ for $n \geq 3$. So
$a_3 = 2(a_2) - a_1 = 2(3) - 1 = 5$ and $a_4 = 2(5) - 3 = 7$.
Prove that $a_n = 2n - 1$ for all $n \in \mathbb{N}$.

Proof:(Strong induction)
(Base step): When $n = 1$ we have $a_1 = 1 = 2(1) - 1$ and for $n = 2$ we have $a_2 = 3 = 2(2) - 1$.
(Inductive step): Let $k \in \mathbb{N}$ and $k \geq 3$ and assume that $a_i = 2i - 1$ for all $i \leq k$. Then

$$\begin{aligned}a_{k+1} &= 2a_k - a_{k-1} \\ &= 2(2k-1) - (2(k-1) - 1) \\ &= 4k - 2 - 2k + 2 + 1 \\ &= 2k + 1 \\ &= 2(k+1) - 1 \text{ as desired.}\end{aligned}$$

By induction the result holds for all $n \in \mathbb{N}$.$\square$

Example 4.22. Define a sequence f_n by $f_1 = 1, f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$ when $n \geq 3$. (Fibonacci sequence).
Prove $2 \mid f_n$ if and only if $3 \mid n$.

Proof:(Strong Induction)
(Base step): Note that $2 \mid f_1 \Leftrightarrow 3 \mid 1$ and $2 \mid f_2 \Leftrightarrow 3 \mid 2$ are true.
*Note: both are true since both sides of each case is false.
(Inductive step): Let $k \in \mathbb{N}$ with $k \geq 3$ and assume that $2 \mid f_i \Leftrightarrow 3 \mid i$ is true for all $i \leq k$.
($\Rightarrow$) Assume $2 \mid f_{k+1}$. Since $f_{k+1} = f_k + f_{k-1}$ is even, f_k and f_{k-1} are both even or are both odd. If f_k and f_{k-1} are both even, then $3 \mid k$ and $3 \mid k-1$, which is impossible. In the case where f_k and f_{k-1} are both odd, by the inductive hypothesis, $3 \nmid k$ and $3 \nmid k-1$. It follows that $k - 1 = 3m + 1$ and $k = 3m + 2$ for some $m \in \mathbb{Z}$. Thus $k + 1 = 3m + 3$, which is divisible by 3.
($\Leftarrow$)(Contrapositive) Assume that $2 \nmid f_{k+1}$. Since $f_{k+1} = f_k + f_{k-1}$ is odd, we conclude that f_k and f_{k-1} have different parity. In the case that f_k is even and f_{k-1} is odd, we have that $3 \mid k$ and $3 \nmid k-1$. Letting $k = 3m$ for some $m \in \mathbb{Z}$ we see that $k + 1 = 3m + 1$ and so $3 \nmid k + 1$. In the case that f_k is odd and f_{k-1} is even, we have $3 \nmid k$ and $3 \mid k-1$. Letting $k - 1 = 3m$ for some $m \in \mathbb{Z}$ we see that $k + 1 = 3m + 2$ and so $3 \nmid k + 1$.
By induction the result holds for all $n \in \mathbb{N}$.$\square$

Chapter 5

Relations

Definition 5.1. Let A and B be nonempty sets. A subset $R \subseteq A \times B$ is a *relation* from A to B.

If $(x, y) \in R$ we typically write ${}_xR_y$ and say that x is related to y.

Example 5.2. $A = \{1, 2\}$ and $B = \wp(\{1, 4\})$

$$R_1 = \{(1, \{1\}), (1, \{1, 4\}), (2, \emptyset)\}.$$
$$R_2 = \{(1, \{4\}), (2, \{1\})\}.$$
$$R_3 = \emptyset.$$
$$R_4 = A \times B.$$

*Note: Each R_i is a relation from A to B.

Definition 5.3. Let R be a relation from A to B.

1. The *domain* of R is the set $dom(R) = \{a \in A \mid (a, b) \in R \text{ for some } b \in B\}$.
2. The *range* of R is the set $rng(R) = \{b \in B \mid (a, b) \in R \text{ for some } a \in A\}$.

Example 5.4. Define the relation R on $\mathbb{Z} \times \mathbb{Z}$ by ${}_xR_y$ if and only if $x \equiv y \bmod 5$.
${}_5R_{20}$ is true since $5 \equiv 20 \bmod 5$.
${}_4R_3$ is false since $4 \not\equiv 3 \bmod 5$.

${}_{100}R_{(-50)}$ is true since $100 \equiv -50 \bmod 5$.
Given $n \in \mathbb{Z}$, note that ${}_nR_{(5+n)}$ and so $n \in dom(R)$. It follows that $\mathbb{Z} \subseteq dom(R)$. The reverse inclusion always holds. Therefore $dom(R) = \mathbb{Z}$. A similar argument shows that $rng(R) = \mathbb{Z}$.

Definition 5.5. A relation $R \subseteq A \times A$ is a *relation on A*.

Example 5.6. Define the relation R on $\mathbb{R}$ by ${}_xR_y$ if and only if $0 < x - y \leq 1$.
${}_5R_4$ is true since $0 < 5 - 4 \leq 1$, but ${}_4 \not R_5$.
Claim: $dom(R) = \mathbb{R}$

Proof: Let $z \in \mathbb{R}$. Then note ${}_zR_{(z-\frac{1}{2})}$ and so $z \in dom(R)$. Thus $\mathbb{R} \subseteq dom(R)$. That $dom(R) \subseteq \mathbb{R}$ is automatic. Therefore
$dom(R) = \mathbb{R}$. Showing that $rng(R) = \mathbb{R}$ is left as an exercise to the reader.

Definition 5.7. A relation R on A is
(a) *reflexive* if for all $a \in A$, ${}_aR_a$
(b) *symmetric* if for all $a, b \in A$, ${}_bR_a$ whenever ${}_aR_b$
(c) *transitive* if for all $a, b, c \in A$, ${}_aR_c$ whenever ${}_aR_b$ and ${}_bR_c$.

Example 5.8. With R as in the previous example.
Is it reflexive? Since $1 - 1 = 0$ we see ${}_1 \not R_1$ and so R is not reflexive.
Is it symmetric? Since ${}_5R_4$ but ${}_4 \not R_5$, R is not symmetric.
Is it transitive? Since ${}_5R_4$ and ${}_4R_3$ but ${}_5 \not R_3$, R is not transitive.

Example 5.9. Define the relation R on $\wp(\mathbb{N})$ by ${}_AR_B$ if and only if $A \subseteq B$.
Reflexive: Let $A \in \wp(\mathbb{N})$. Since $A \subseteq A$ we have ${}_AR_A$ and so R is reflexive.
Symmetric: Note that $\{1, 2\} \subseteq \{1, 2, 3\}$ but $\{1, 2, 3\} \not\subseteq \{1, 2\}$ and so R is not symmetric.
Transitive: Let $A, B, C \in \wp(\mathbb{N})$ such that $A \subseteq B$ and $B \subseteq C$. Let $a \in A$. Then $a \in B$ (because $A \subseteq B$) and so $a \in C$ (because $B \subseteq C$). Therefore $A \subseteq C$. As a consequence we conclude that R is transitive.

Example 5.10. Let $m \geq 2$. Define the relation R on $\mathbb{Z}$ by ${}_aR_b$ if

and only if $a \equiv b \bmod m$.
Reflexive: Given $a \in \mathbb{Z}$, note that $m \mid 0 = a - a$ and so $a \equiv a \bmod m$. Thus ${}_aR_a$ and we have that R is reflexive.
Symmetric: Let $a, b \in \mathbb{Z}$ with ${}_aR_b$. Then $a \equiv b \bmod m$ and so there exists a $k \in \mathbb{Z}$ such that $a - b = mk$. Then $b - a = m(-k)$ and so $b \equiv a \bmod m$. This implies that ${}_bR_a$ and so R is symmetric.
Transitive: Let $a, b, c \in \mathbb{Z}$ ${}_aR_b$ and ${}_bR_c$. Then $a \equiv b \bmod m$ and $b \equiv c \bmod m$ and so there exists $s, t \in \mathbb{Z}$ such that $a - b = ms$ and $b - c = mt$. It follows that $a - c = m(s + t)$. Therefore $a \equiv c \bmod m$. Thus, ${}_aR_c$ and so R is transitive.

General format (example above)(for relation R on A)

Reflexive: $a \in A$ show ${}_aR_a$.
Symmetric: Let $a, b \in A$ with ${}_aR_b$. Show ${}_bR_a$.
Transitive Let $a, b, c \in A$ with ${}_aR_b$ and ${}_bR_c$. Show ${}_aR_c$.

Definition 5.11. A relation R on A is an *equivalence relation* if R is reflexive, symmetric, and transitive.

Example 5.12. In example 5.10 we showed that R defined by ${}_aR_b$ if and only if $a \equiv b \bmod m$ is an equivalence relation.

Typically equivalence relations are denoted $\sim$. We write $a \sim b$ and say "a is equivalent to b".

Example 5.13. Define a relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ if and only if $a - b \in \mathbb{Z}$.
Reflexive: For $a \in \mathbb{Z}$, since $a - a = 0 \in \mathbb{Z}$, we see that $\sim$ is reflexive.
Symmetric: Let $a, b \in \mathbb{Z}$ with $a \sim b$. Then $a - b \in \mathbb{Z}$ which implies that $b - a \in \mathbb{Z}$. Thus, $\sim$ is symmetric.
Transitive: Let $a, b, c \in \mathbb{Z}$ with $a \sim b$ and $b \sim c$. Then $a - b = m$ and $b - c = n$ for some $m, n \in \mathbb{Z}$. It follows (by addition) that $a - c = m + n \in \mathbb{Z}$ and so $a \sim c$. Therefore $\sim$ is transitive.
Conclusion: $\sim$ is an equivalence relation.

Describe $\{x \in \mathbb{R} \mid x \sim \frac{1}{2}\} = \{n + \frac{1}{2} \mid n \in \mathbb{Z}\}$.
Describe $\{x \in \mathbb{R} \mid x \sim 2\} = \mathbb{Z}$.

Definition 5.14. Let $\sim$ be an equivalence relation on A, and let $a \in A$. The *equivalence class of* a is $[a] = \{x \in A \mid x \sim a\}$. The set $A/\sim = \{[a] \mid a \in A\}$ is the set of *equivalence classes of* A *modulo* $\sim$.

Example 5.15
Define $\sim$ on $\mathbb{R} \times \mathbb{R}$ by $(x, y) \sim (s, t) \Leftrightarrow x^2 + y^2 = s^2 + t^2$ (check that $\sim$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$).
Describe $[(1, 1)]$
$[(1, 1)] = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x, y) \sim (1, 1)\}$
$= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2\}$ (circle of radius $\sqrt{2}$)
Describe $[(0, 0)]$
$[(0, 0)] = \{(0, 0)\}$
Describe $\mathbb{R} \times \mathbb{R}/\sim$
$\mathbb{R} \times \mathbb{R}/\sim = [0, \infty)$

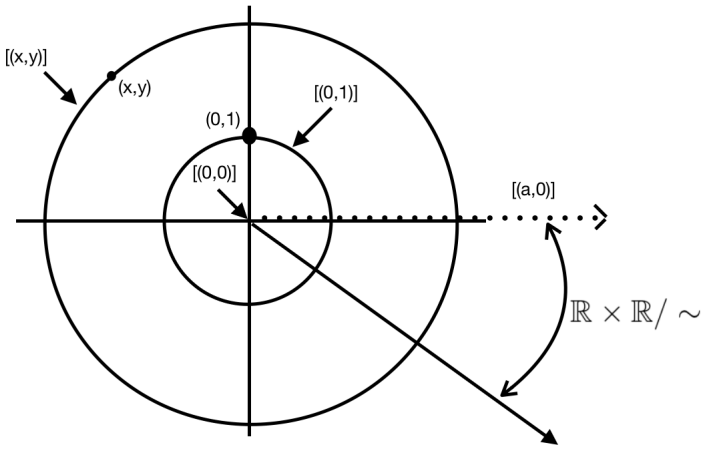
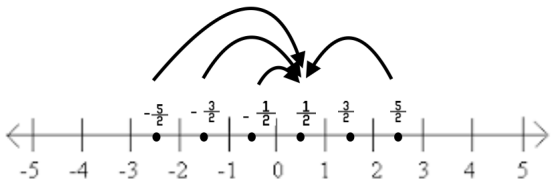


Figure 5.1: $\sim$ on $\mathbb{R} \times \mathbb{R}$ by $(x, y) \sim (s, t) \Leftrightarrow x^2 + y^2 = s^2 + t^2$.

Example 5.16.
Recall $\sim$ on $\mathbb{R}$ defined by $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$.
$[0] = \mathbb{Z} = [1] = [-1] = \ldots$
$[\frac{1}{2}] = [\frac{3}{2}] = [\frac{-1}{2}] = [\frac{-3}{2}] = \ldots$



*Note: If $x \in \mathbb{R}$, then $x = a.b_1b_2b_3\ldots$ where $a \in \mathbb{Z}$ and each $b_i \in \{0, 1, 2, \ldots, 9\}$. It follows that $x \sim 0.b_1b_2b_3\cdots \in [0, 1]$

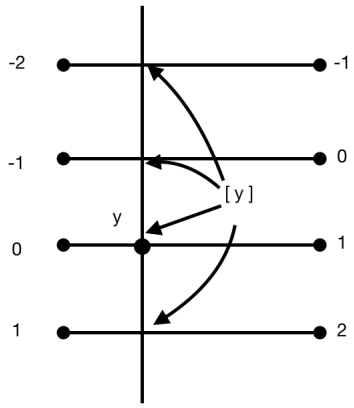


Figure 5.2: Anyone along the vertical line is equivalent.

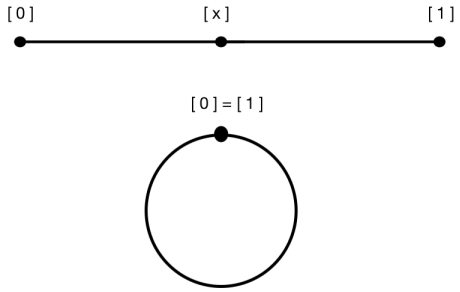


Figure 5.3: $\mathbb{R}/\sim$ is a circle.

Lemma 5.17. Let $\sim$ be an equivalence relation on A, and let $x, y \in A$. Then $[x] \cap [y] \neq \emptyset$ if and only if $[x] = [y]$.

Proof: ($\Rightarrow$) Suppose $[x] \cap [y] \neq \emptyset$. Choose $z \in [x] \cap [y]$. Pick $a \in [x]$. Then $a \sim x$. Since $z \in [x]$, we have that $z \sim x$. By symmetry, $x \sim z$, by transitivity $a \sim z$. Since $z \in [y], z \sim y$, by transitivity $a \sim y$. Therefore $a \in [y]$, and we conclude that $[x] \subseteq [y]$. Similarly $[y] \subseteq [x]$.
($\Leftarrow$) Obvious. (Sets that are equal have to have nonempty intersections). $\square$

Lemma 5.18. (Division Algorithm) Let $a, m \in \mathbb{Z}$ with $m \geq 1$. Then there exists unique $q, r \in \mathbb{Z}$ such that $a = qm + r$ and $0 \leq r < m$.

Proof: (Existence) Let $S = \{a - km \mid k \in \mathbb{Z}, a - km \geq 0\}$. If $0 \in S$, then $m \mid a$ and the result holds by setting $q = \frac{a}{m}$ and $r = 0$. In the case that $0 \notin S$, it follows that $a = a - 0(m) \neq 0$. From this we have that $a > 0$ or $a < 0$. When $a > 0$, note that $a = a - 0(m) \in S$. When $a < 0$ note that $a - (2a)m = a(1 - 2m) \in S$ (note that on the right side of the equation, a and $(1 - 2m)$ are both negative so multiplying the two quantities together gives us a positive quantity). As a consequence, S is a nonempty subset of $\mathbb{N}$; by WOP, S has a least element, r. Thus r can be expressed as $r = a - qm$ for some $q \in \mathbb{Z}$. We have $a = qm + r$ where $r \geq 0$. It remains to show that $r < m$. (By contradiction) Suppose $r \geq m$. Then $a - (q + 1)m = a - qm - m = r - m \geq 0$. It follows that $a - (q + 1)m \in S$, but $a - (q + 1)m < a - qm$, contradicting the fact that r is the least element of S. Therefore $r < m$.
(Uniqueness) Suppose there exists $q', r' \in \mathbb{Z}$ with $0 \leq r' < m$ such that $a = q'm + r'$. We may assume without loss of generality that $r \geq r'$. Then $qm + r = q'm + r'$ and so $r - r' = q'm + qm = m(q' - q)$. So it follows $m \mid r - r'$. But $0 \leq r - r' \leq r < m$, which leads us to conclude that $r - r' = 0 \Leftrightarrow r = r'$. From the previous equation we see that $q' - q = 0 \Leftrightarrow q = q'$ as well. $\square$

Theorem 5.19. Let $m \in \mathbb{Z}$ with $m \geq 2$ and let $\sim$ denote the relation on $\mathbb{Z}$ defined by $x \sim y$ if and only if $x \equiv y \bmod m$. Then $\sim$ is an equivalence relation. Moreover, $\mathbb{Z}/\sim = \{[0], [1], \ldots, [m - 1]\}$

(note that this is what we are proving).

Proof: We proved earlier that $\sim$ is an equivalence relation in example 5.10. Let $x \in \mathbb{Z}$; (we must show that $[x] \in \{[0], [1], \ldots, [m-1]\}$.) By the division algorithm, there exists (unique) $q, r \in \mathbb{Z}$ with $0 \leq r \leq m-1$ such that $x = qm+r$. Since $x-r = qm$ we have that $m \mid x-r$ and so $x \equiv r \bmod m$. This implies that $x \sim r$. By lemma 5.17 we conclude $[x] = [r] \in \{[0], \ldots, [m-1]\}$. We have shown that $\mathbb{Z}/\sim \subseteq \{[0], \ldots, [m-1]\}$. The reverse inclusion is immediate. $\square$

Example 5.20. With $m = 6$

$$
\begin{aligned}
[0] &= \{\ldots, -12, -6, 0, 6, 12, \ldots\} \\
[1] &= \{\ldots, -11, -5, 1, 7, 13, \ldots\} \\
[2] &= \{\ldots, -10, -4, 2, 8, 14, \ldots\} \\
[3] &= \{\ldots, -9, -3, 3, 9, 15, \ldots\} \\
[4] &= \{\ldots, -8, -2, 4, 10, 16, \ldots\} \\
[5] &= \{\ldots, -7, -1, 5, 11, 17, \ldots\}
\end{aligned}
$$

Sets A and B are disjoint if $A \cap B = \emptyset$. More generally, the family of sets $\{A_\alpha\}_{\alpha \in I}$ is pairwise disjoint if $A_\alpha \cap A_\beta = \emptyset$ whenever $\alpha \neq \beta$.

Definition 5.21. Let X be a set. A family $\{A_\alpha\}_{\alpha \in I}$ is a *partition* of X if
(a) $\{A_\alpha\}_{\alpha \in I}$ is pairwise disjoint.
(b) $\bigcup_{\alpha \in I} A_\alpha = X$.

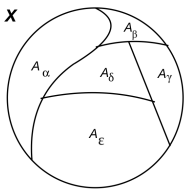


Figure 5.4: The partition of X.

Example 5.22. Consider $\{[i, i+1), i \in \mathbb{Z}\}$
Note: If $i \neq j$, then $[i, i+1) \cap [j, j+1) = \emptyset$
and $\bigcup_{i \in \mathbb{Z}} [i, i+1) = \mathbb{R}$.
So this family is a partition of $\mathbb{R}$.

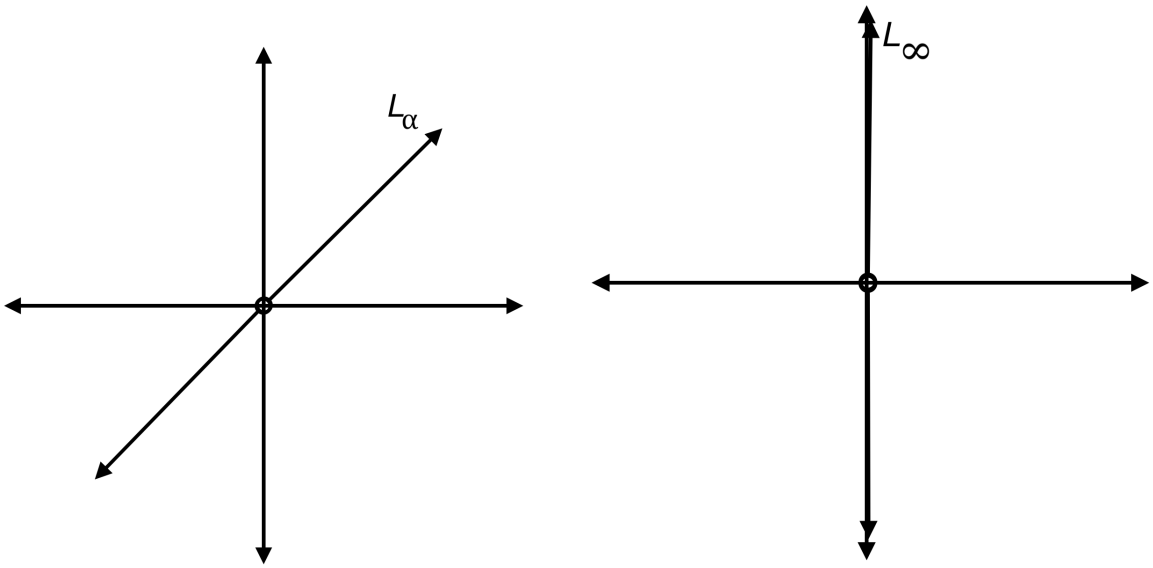
Example 5.23. Fix $m \in \mathbb{Z}$ with $m \geq 2$ and for each $i \in \{0, 1, \ldots, m-1\}$ define $A_i = \{mk + i \mid k \in \mathbb{Z}\}$
Check: If $i \neq j$, then $A_i \cap A_j = \emptyset$
and $\bigcup_{i=0}^{m-1} A_i = \mathbb{Z}$.
Conclusion $\{A_i\}_{i=0}^{m-1}$ is a partition on $\mathbb{Z}$.

Theorem 5.24. Let $\{A_\alpha\}_{\alpha \in I}$ be a partition on X. Then the relation $\sim$ defined by $x \sim y$ if and only if there exists $\alpha \in I$ such that $x \in A_\alpha$ and $y \in A_\alpha$ is an equivalence relation on X.

Proof: To see that $\sim$ is reflexive let $x \in X$. Since $X = \bigcup_{\alpha \in I} A_\alpha$ there exists $\alpha \in I$ such that $x \in A_\alpha$. It follows that $x \in A_\alpha$ and $x \in A_\alpha$ and so $x \sim x$.
To see that $\sim$ is symmetric, let $x, y \in X$ with $x \sim y$. Then there exists $\alpha \in I$ such that $x \in A_\alpha$ and $y \in A_\alpha$. It follows that $y \in A_\alpha$ and $x \in A_\alpha$ and so $y \sim x$.
To see that $\sim$ is transitive let $x, y, z \in X$ with $x \sim y$ and $y \sim z$. Then there exists $\alpha, \beta \in I$ such that $x \in A_\alpha$ and $y \in A_\alpha$ and $y \in A_\beta$ and $z \in A_\beta$. Since $y \in A_\alpha \cap A_\beta$, we conclude that $\alpha = \beta$ ($\{A_\alpha\}_{\alpha \in I}$ is pairwise disjoint) and so $x \in A_\alpha$ and $z \in A_\alpha$. Therefore $x \sim z$. □

$\sim$ in the theorem is the equivalence relation *induced* by the partition.

Example 5.25.
Let $X = \mathbb{R}^2 - \{(0, 0)\}$. For each $\alpha \in \mathbb{R}$
let $L_\alpha = \{(x, y) \in X \mid y = \alpha x\}$. Also, define
$L_\infty = \{(0, y) \mid y \in \mathbb{R} - \{0\}$.



Letting $I = \mathbb{R} \cup \{\infty\}$ we show that $\{L_\alpha\}_{\alpha \in I}$ is a partition of X. Let $(x, y) \in X$. If $x = 0$, then $(x, y) \in L_\infty$. If $x \neq 0$ then $(x, y) \in L_{\frac{y}{x}}$. It follows that $(x, y) \in \bigcup_{\alpha \in I} L_\alpha$. Therefore $X \subseteq \bigcup_{\alpha \in I} L_\alpha$. Since each $L_\alpha \subseteq X$, we conclude that $\bigcup_{\alpha \in I} L_\alpha \subseteq X$. Now let $\alpha, \beta \in I$ and suppose that $L_\alpha \cap L_\beta \neq \emptyset$. Then there exists $(a, b) \in L_\alpha \cap L_\beta$. If $a = 0$, then $b \neq 0$. Since there is no $\alpha \in \mathbb{R}$ such that $0 \neq b = \alpha a = 0$, we conclude that $\alpha = \infty$. Same argument shows that $\beta = \infty$. If $a \neq 0$, the $\alpha a = b = \beta a$ and so $\alpha = \beta$. The equivalence relation on X induced by $\{L_\alpha\}_{\alpha \in I}$ is defined by $(x, y) \sim (z, w)$ if and only if $x \neq 0, z \neq 0$ and $\frac{y}{x} = \frac{w}{z}$ or $x = z = 0$.

So far we know a partition sort of implies an equivalence relation.

Theorem 5.26. Let $\sim$ be an equivalence relation on X. Then $X/\sim$ is a partition of X.

Proof: Note that our goal is to show that $X/\sim = \{[x] \mid x \in X\}$. Let $x \in X$. Then $x \in [x]$ and so $x \in \bigcup_{[y] \in X/\sim} [y]$. Thus $X \subseteq \bigcup_{[y] \in X/\sim} [y]$. The reverse inclusion is automatic (each $[y]$ is in X). Now choose $[x], [y] \in X/\sim$. If $[x] \cap [y] \neq \emptyset$, then $[x] = [y]$ by lemma 5.1. $\square$

Example 5.27. Consider the relation $\leq$ on $\mathbb{N}$.
Reflexive: Since $n \leq n$ for any $n \in \mathbb{N}$, $\leq$ is reflexive.
Symmetric: $\leq$ is clearly no symmetric.
Transitive: Given $a, b, c \in \mathbb{N}$ with $a \leq b$ and $b \leq c$ we can conclude that $a \leq c$, and so $\leq$ is transitive
*Note: $a \leq b$ and $b \leq a$ if and only if $a = b$.

Example 5.28. Let X be a set and consider the relation $\subseteq$ on $\wp(X)$. Check that $\subseteq$ is reflexive, and transitive, but not symmetric. Also note that $A \subseteq B$ and $B \subseteq A$ is true if and only if $A = B$.

Definition 5.29. A relation R on the set X is *antisymmetric* if for all $x, y \in X$, ${}_xR_y$ and ${}_yR_x$ if and only if $x = y$.

Example 5.30.
Define a relation R on $\mathbb{R} \times \mathbb{R}$ by ${}_{(a,b)}R_{(c,d)}$ if and only if $a \leq c$ and $b \leq d$. Reflexive: Easy.
Antisymmetric: Suppose ${}_{(a,b)}R_{(c,d)}$ and ${}_{(c,d)}R_{(a,b)}$. Then $a \leq b$, $b \leq d$ and $c \leq a$, $d \leq b$. Thus $a = c$ and $b = d$. It is Antisymmetric.
Transitive: Easy.

Definition 5.31. A relation $\preceq$ on a set X is a *partial ordering* on X if it is reflexive, antisymmetric, and transitive. When $\preceq$ is a partial ordering on X, then $(X, \preceq)$ is a *partially ordered* set or a *poset*.

Definition 5.32. If $(X, \preceq)$ is a poset, then $x, y \in X$ are *comparable* if $x \preceq y$ or $y \preceq x$.

Example 5.33.
If $X = \{1, 2, 3\}$, then in $(\wp(X), \subseteq)$ $\{1\}$ and $\{1,2\}$ are comparable since $\{1\} \subseteq \{1, 2\}$ but $\{1, 3\}$ and $\{1, 2\}$ are not.

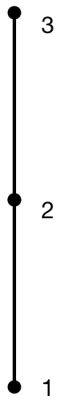
Definition 5.34. A partial ordering on a set X is a *total ordering* (or *linear ordering*) if all elements are comparable.

Example 5.35.
$\preceq$ is a total ordering on $\mathbb{R}$.
$\subseteq$ is not a total ordering on $\wp(\{1, 2, 3\})$.

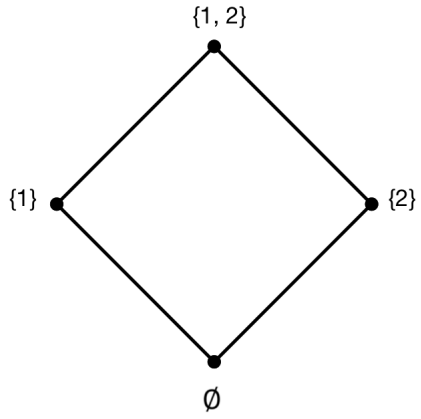
Definition 5.36. Let $(X, \leq)$ be a poset, and let $x, y \in X$. Then y *covers* x if $x \neq y$ and whenever $z \in X$ such that $x \preceq z \preceq y$, $x = z$ or $z = y$. When y covers x, x is an *immediate predecessor* of y and y is an *immediate successor* of x.

A poset $(A, \preceq)$ can be represented by a *hasse diagram*. Elements of A corresponding to vertices; a and b are joined by an edge extending upward from a to b whenever b covers a.

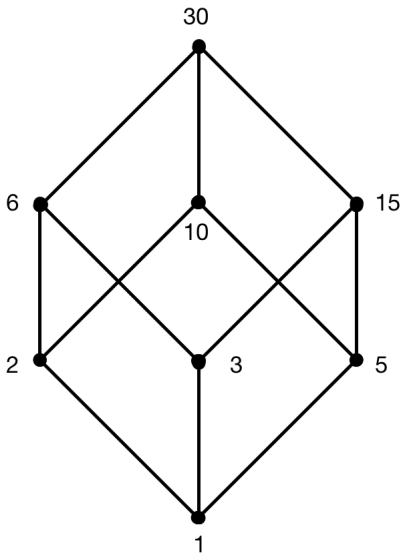
Example 5.37. Let $A = \{1, 2, 3\}$ partially ordered by $\leq$.



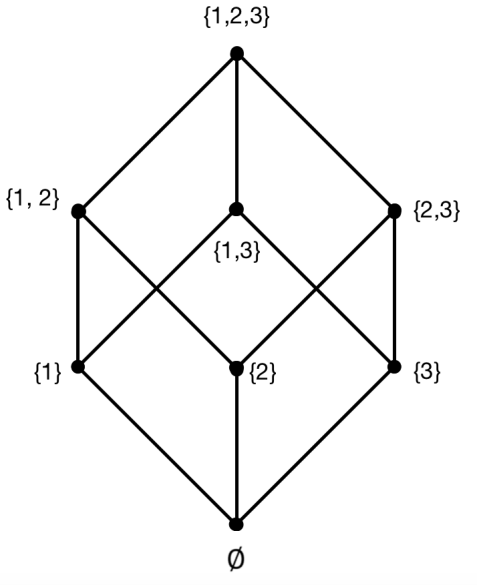
Example 5.38.
$(\wp(\{1,2\}), \subseteq)$. $\wp(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.



Example 5.39.
Let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ (A consists of all divisors of 30). The relation "divides" defines a partial ordering on A: ${}_aR_b$ if and only if $a \mid b$.



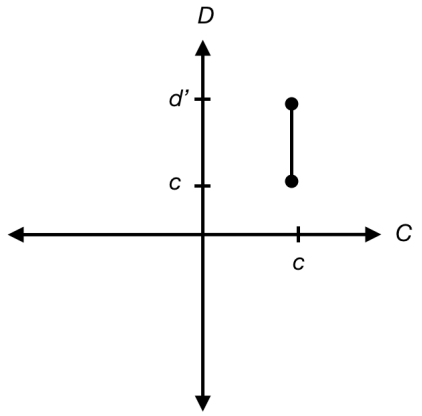
Example 5.40.
$(\wp(\{1,2,3\}), \subseteq)$. $\wp(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$.



Chapter 6

Functions

Definition 6.1. Let C, D be nonempty sets. *A rule of assignment* is a relation $r \subseteq C \times D$ satisfying the following property if $(c, d) \in r$ and $(c, d') \in r$ then $d = d'$. (Vertical line test).



Example 6.2. $C = \{1, 2, 3, 4, 5\}$ and $D = \{s, t, u\}$.
$r_1 = \{(1, t), (2, s), (5, s)\}$ is a rule of assignment.
$r_2 = \{(1, t), (2, s), (2, t), (3, t), (4, u), (5, u)\}$ is not a rule of assignment because of $(2, s)$ and $(2, t)$.

Example 6.3.
$r_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y = 1\}$.
$r_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$.
Claim: r_1 is a rule of assignment.

Proof: Suppose $(x, y), (x, y') \in r_1$. Then $x^2 + y = 1 = x^2 + y'$ and so $y = y'$.$\square$
Claim: r_2 is not a rule of assignment.
Proof: $(0, 1), (0, -1) \in r_2$.

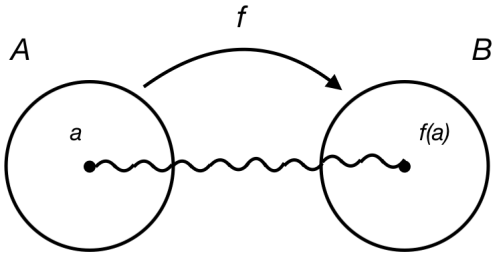
Definition 6.4. Let $r \subseteq C \times D$ be a rule of assignment.
The *Domain* of r is $dom(r) = \{c \in C \mid (c, d) \in r \text{ for some } d \in D\}$.
The *range* of r (or *image*) is
$rng(r) = \{d \in D \mid (c, d) \in r \text{ for some } c \in C\}$.

In example 6.2 the domain of r_1 is $\{1, 2, 3, 4, 5\}$ and the range of r_1 is $\{s, t, u\}$.
In example 6.3 $dom(r_1) = \mathbb{R},\ rng(r_1) = (-\infty, 1]$.

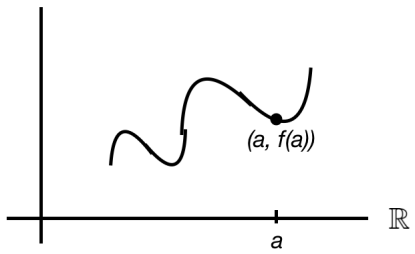
Definition 6.5. A *function* is a rule of assignment r together with a set B that contains the $rng(r)$.
Unused notation: $f = (r, b)$.
The domain of r is the *domin* of f.
The range of r is the *image* of f.
The set B is the *codomain* of f.

If f is a function with domain A and codomain B we write $f : A \to B$ read as "f is a function from A to B" (to can be "into") or "f is a mapping from A to B".

If $f : A \to B$ with rule of assignment r, then for each $a \in A$ there is a unique element $f(a)$ such that $(a, f(a)) \in r$. $f(a)$ is the *image* of a under f.



The *graph* of f is the set $\{(a, f(a)) \in A \times B \mid a \in A\}$.



Example 6.6. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$.
The $dom(f) = \mathbb{R}$ and the $codom(f) = \mathbb{R}$, the $Im(f) = [0, \infty)$, and the graph is $\{(a, f(a)) \mid a \in \mathbb{R}\} = \{(a, a^2) \mid a \in \mathbb{R}\}$.

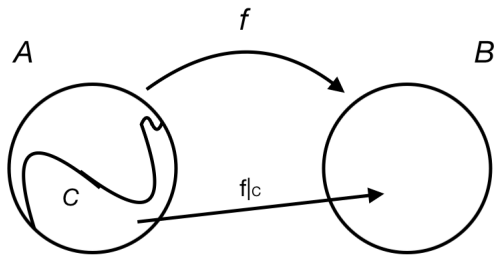
Example 6.7. $f : \mathbb{R} \to \mathbb{R}^2$ defined by $f(t) = (\cos(t), \sin(t))$.
The $dom(f) = \mathbb{R}$, the $codom(f) = \mathbb{R}^2$, the
$Im(f) = \{(x, y) \mid x^2 + y^2 = 1\}$ and the graph is
$\{(t, (\cos(t), \sin(t))) \mid t \in \mathbb{R}\}$.

Example 6.8. $f : \mathbb{N} \to \wp(\mathbb{N})$ defined by $f(n) = \{1, 2, \ldots, n\}$.
The $dom(f) = \mathbb{N}$, the $codom(f) = \wp(\mathbb{N})$, the
$Im(f) = \{\{1, 2, \ldots, n\} \mid n \in \mathbb{N}\}$. The graph is
$\{(n, \{1, 2, \ldots, n\} \mid n \in \mathbb{N}\}$.

Example 6.9.
Let $\sim$ be an equivalence relation on A. Define $\pi : A \to A/\sim$ by $\pi(a) = [a]$. π is the *natural projection* of A onto $A/\sim$.

Example 6.10.
Let A, B be sets. Define $\pi_A : A \times B \to A$ by $\pi_A(a, b) = a$. π_A is *the projection onto the first factor*. There is also π_B which is the projection onto the second factor.

Example 6.11.
Let $f : A \to B$ and let $C \subseteq A$. The function $f|_C : C \to B$ defined by $f|_C(c) = f(c)$ for all $c \in C$ the *restriction* of f to C.



Example 6.12.
Let $A \subseteq B$. The function $i : A \to B$ defined by $i(a) = a$ for all $a \in A$ is the *inclusion mapping*.

Functions and Equivalence Classes

Let $\sim$ be an equivalence relation on X. Given $x \in X$ any element of $[x]$ is called a representative of $[x]$. (Note: If $y \in [x]$, then $[x] = [y]$). When constructing a function with domain $X/\sim$ we have to be careful: $f([x])$ must not depend on the choice of representative of $[x]$.
*If $x \sim y$, then $f([x]) = f([y])$, and when this is satisfied we say that f is *well-defined*.
Notation: For $m \geq 2$ ($m \in \mathbb{Z}$). Let $\sim_m$ denote the equivalence relation on $\mathbb{Z}$ defined by $x \sim_m y$ if and only if $x \equiv y \bmod m$. Also, for $x \in \mathbb{Z}$, $[x]_m$ denotes the equivalence of x under $\sim_m$.

Example 6.13. Define $f : \mathbb{Z}/\sim_5 \to \mathbb{Z}$ by $f([n]_5) = n$.
Since $0 \sim_5 5$ but $f([0]_5) = 0$ while $f([5]_5) = 5$, f is not well-defined.

It is good to note that in general $[x]_m = [y]_m$ if and only if $x \sim_m y$ if and only if $x \equiv y \bmod m$.

Example 6.14. Define $f : \mathbb{Z}/\sim_8 \to \mathbb{Z}/\sim_4$ by $f([n]_8) = [n]_4$.
Let $m, n \in \mathbb{Z}$ with $m \sim_8 n$. Then $m \equiv n \bmod 8$ and so $m - n = 8k$ for some $k \in \mathbb{Z}$. Now $f([m]_8) = [m]_4 = [n + 8k]_4 = [n]_4 = f([n]_8)$.

Therefore, f is well-defined.
The reason we are allowed to do $[n+8k]_4 = [n]_4$ is because $(n+8k) - n = 8k$ is a multiple of 4.

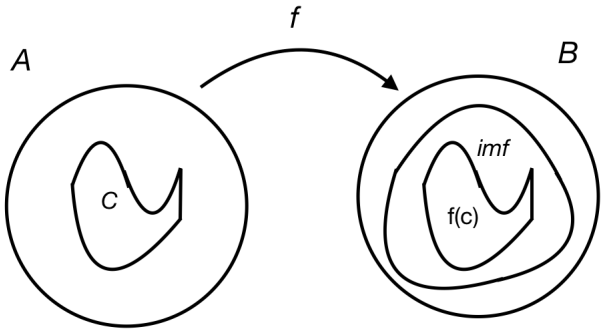
Example 6.15. Define $f : \mathbb{Z}/\sim_4 \to \mathbb{Z}/\sim_8$ by $f([m]_4) = [m]_8$.
Since $[3]_4 = [7]_4$, but $f([3]_4) = [3]_8 \neq [7]_8 = f([7]_4)$, f is not well-defined.

Example 6.16. Define $f : \mathbb{Z}/\sim_{12} \to \mathbb{Z}/\sim_3$ by $f([n]_{12}) = [n^2]_3$.
Let $m, n \in \mathbb{Z}$ with $m \sim_{12} n$. Then $m = n + 12k$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} \text{Now, } f([m]_{12}) &= [m^2]_3 \\ &= [(n+12k)^2]_3 \\ &= [n^2 + 24kn + 144k^2]_3 \\ &= [n^2 + 3(8nk + 48k^2)]_3 \\ &= [n^2]_3 \\ &= f([n]_{12}) \text{ and so } f \text{ is well-defined.} \end{aligned}$$

We can do $[n^2 + 3(8nk + 48k^2)]_3 = [n^2]_3$ because
$n^2 + 3(8nk + 48k^2) - n^2 = 3(8nk + 48k^2)$ is divisible by 3.

Definition 6.17. Let $f : A \to B$ and $C \subseteq A$. The set $f(C) = \{f(c) \mid c \in C\}$ is the *image* of C under f. Note $imf = f(A)$ are used interchangeably.



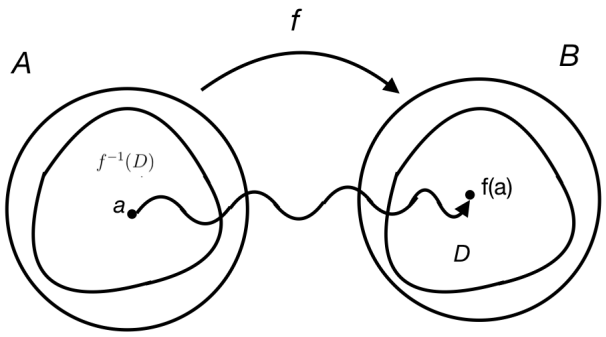
Example 6.18. Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(n) = n^2$ and $C = \{-3, 2, 4\}$.
$f(C) = \{9, 4, 16\}$ and $f(\mathbb{Z}) = \{0, 1, 4, 9, 16, \dots\}$.

Example 6.19. Define $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} 0 & \text{if } x \in \mathbb{Q} \\ 1 & \text{if } x \in \mathbb{R} - \mathbb{Q}. \end{cases}$$

If $C = [-1, 1]$, then $f(C) = \{0, 1\}$. $f(\mathbb{Q}) = \{0\}$ and $f(\mathbb{R}) = \{0, 1\}$.

Definition 6.20. Let $f : A \to B$ and $D \subseteq B$. The *inverse image* D *under* f is the set $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$.
Warning: Using the notation $f^{-1}(D)$ does not imply that the inverse function f^{-1} exists.
Note: $f^{-1}(\{b\})$ (single element) is usually written $f^{-1}(b)$.



Example 6.21. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.
$f^{-1}([0, 1]) = [-1, 1]$ (some set in our domain that if you square it you get $[0, 1]$).
$f^{-1}([-3, -2]) = \emptyset$.
$f^{-1}(9) = \{-3, 3\}$.

Example 6.22. Deifine $\pi_1 : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by $\pi_1(x, y) = x$.
$\pi_1^{-1}([0, 1]) = \{(x, y) \mid 0 \leq x \leq 1\}$.
$\pi_1^{-1}(-2) = \{(-2, y) \mid y \in \mathbb{R}\}$.
What does π_1 do?

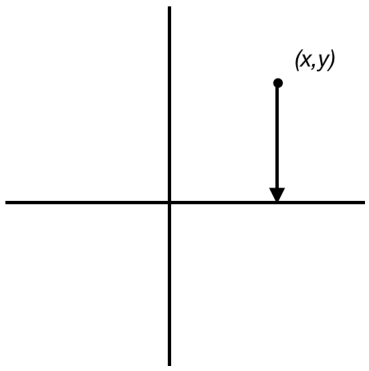


Figure 6.1: π_1 takes a point and smashes it down to the x-axis

Theorem 6.23.
Let $f : A \to B$ and let $A_1, A_2 \subseteq A$ and $B_1, B_2 \subseteq B$. Then,

- (a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
- (b) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.
- (c) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
- (d) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

Proof:(a)($\subseteq$) Let $x \in f(A_1 \cup A_2)$. Then $x = f(a)$ for some $a \in A_1 \cup A_2$. If $a \in A_1$, then $x = f(a) \in f(A_1)$. If $a \in A_2$, then $x = f(a) \in f(A_2)$. Thus, $x \in f(A_1) \cup f(A_2)$ and so $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$.
($\supseteq$) Let $x \in f(A_1) \cup f(A_2)$. If $x \in f(A_1)$, then $x = f(a)$ for some $a \in A_1$. If $x \in f(A_2)$, then $x = f(a)$ for some $a \in A_2$. Thus, $x = f(a)$ for some $a \in A_1 \cup A_2$ and so $x \in f(A_1 \cup A_2)$. As a result, $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$.
In conclusion $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Let $x \in f(A_1 \cap A_2)$. Then $x = f(a)$ for some $a \in A_1 \cap A_2$ and so $a \in A_1$ and $a \in A_2$. It follows that $f(a) \in f(A_1)$ and $f(a) \in f(A_2)$. Therefore, $x \in f(A_1)$ and $x \in f(A_2)$. Thus, $x \in f(A_1) \cap f(A_2)$ and so $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

(c) ($\subseteq$) Let $x \in f^{-1}(B_1 \cup B_2)$. Then $f(x) \in B_1 \cup B_2$ and so $f(x) \in B_1$ or $f(x) \in B_2$. Now, $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$ and so

$x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Thus, $f^{-1}(B_1 \cup B_2) \subseteq f^{-1}(B_1) \cup f^{-1}(B_2)$.
($\supseteq$) Let $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Then $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$ and so $f(x) \in B_1$ or $f(x) \in B_2$. Now $f(x) \in B_1 \cup B_2$ and so $x \in f^{-1}(B_1 \cup B_2)$. Thus, $f^{-1}(B_1) \cup f^{-1}(B_2) \subseteq f^{-1}(B_1 \cup B_2)$.
In conclusion $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

(d) ($\subseteq$) Let $x \in f^{-1}(B_1 \cap B_2)$. Then $f(x) \in B_1 \cap B_2$. Since $f(x) \in B_1$, we have $x \in f^{-1}(B_1)$. Since $f(x) \in B_2$, we have that $x \in f^{-1}(B_2)$. Therefore $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$ and so $f^{-1}(B_1 \cap B_2) \subseteq f^{-1}(B_1) \cap f^{-1}(B_2)$.
($\supseteq$) Let $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$. Since $x \in f^{-1}(B_1)$ we have that $f(x) \in B_1$, similarly $f(x) \in B_2$ and so $f(x) \in B_1 \cap B_2$. Thus $x \in f^{-1}(B_1 \cap B_2)$ and so $f^{-1}(B_1) \cap f^{-1}(B_2) \subseteq f^{-1}(B_1 \cap B_2)$.
In conclusion $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$. $\square$

Definition 6.24. A function $f : A \to B$ is *injective* (or *one-to-one*) if $a = a'$ whenever $f(a) = f(a')$. "A distinct input gives a distinct output."

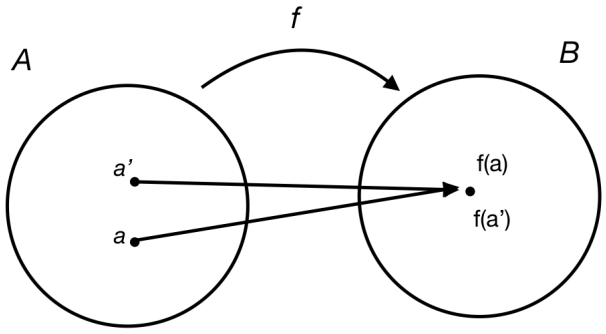
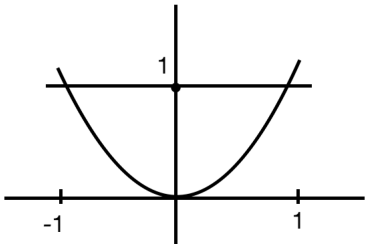


Figure 6.2: This is an example of a function that is not injective.

Example 6.25. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.
Not injective because, $f(-1) = 1 = f(1)$.



Example 6.26. $g : [0, \infty) \to \mathbb{R}$ defined by $g(x) = x^2$.
Claim: g is injective.
Reason: Suppose $g(x) = g(y)$ for some $x, y \in [0, \infty)$. Then $x^2 = y^2$ and so $x = \pm y$ but since $x, y \in [0, \infty)$ we conclude that $x = y$.
Note: $g = f\,|_{[0,\infty)}$ (where f is from the previous example).

Example 6.27. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x, y) = x + 2y$.
Since $f(0, 0) = 0 = f(-2, 1)$, f is not injectve.

Structures of an Injective Proof:

Given $f : A \to B$, let $x, y \in A$ such that $f(x) = f(y)$. Then show that $x = y$ to conclude that f is injective.
*Note: To show that the function is not injective, find a specific $x, y \in A$ with $x \neq y$ such that $f(x) = f(y)$.

Example 6.28. $f : \mathbb{Z}/\sim_{12} \to \mathbb{Z}/\sim_3$ defined by $f([n]_{12}) = [n^2]_3$.
*Note: $\mathbb{Z}/\sim_{12}$ has 12 elements while $\mathbb{Z}/\sim_3$ has only 3 elements. All 12 need to match with all 3. Since the only way for this to be possible is if two or more elements have the same output, the function can not be injective.
Our counter example: Since $f([1]_{12}) = f([2]_{12})$, f is not injective.

Example 6.29. $f : \mathbb{Z}/\sim_4 \to \mathbb{Z}/\sim_8$ defined by $f([n]_4) = [2n]_8$.
We can not guarantee the function is one-to-one, because 4 elements can match with some of the 8 elements but it is still possible to have overlap.
We first show that f is well-defined.

Let $m, n \in \mathbb{Z}$ with $m \sim_4 n$. Then $m = n + 4k$ for some $k \in \mathbb{Z}$. Now,

$$\begin{aligned} f([m]_4) &= [2m]_8 \\ &= [2(n+4k)]_8 \\ &= [2n+8k]_8 \\ &= [2n]_8 = f([n]_4) \end{aligned}$$

and so f is well-defined.
To see that f is injective use the procedure. Let $m, n \in \mathbb{Z}$ such that $f([m]_4) = f([n]_4)$. Then $[2m]_8 = [2n]_8$ and so $2m - 2n = 8k$ for some $k \in \mathbb{Z}$. It follows that $m - n = 4k$ and so $[m]_4 = [n]_4$. Therefore f is injective.

Definition 6.30. A function $f : A \to B$ is *surjective* (or *onto*) if $imf = B$.
*Note: Because $imf \subseteq B$ is automatic we only need to show that $B \subseteq imf$.

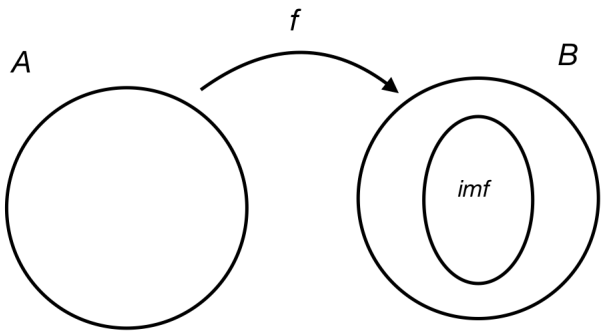


Figure 6.3: This function is not surjective.

Example 6.31. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.
Since $imf = [0, \infty) \neq \mathbb{R}$, f is not surjective.

Example 6.32. $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $f(x, y) = x + 2y$.
Let $z \in \mathbb{R}$. Then $f(-z, z) = -z + 2z = z$ and so $z \in imf$. Thus $\mathbb{R} \subseteq imf$ and so f is surjective.

Structures of a Surjective Proof:

Given $f : A \to B$ let $b \in B$. Find $a \in A$ such that $f(a) = b$. Conclude that $B \subseteq imf$ and so f is surjective.
To show that f is not surjective, produce $b \in B$ such that $f(a) \neq b$ for all $a \in A$.

Example 6.33. $f : \mathbb{Z}/\sim_{12} \to \mathbb{Z}/\sim_3$ defined by $f([n]_{12}) = [n^2]_3$.
Claim: $[2]_3 \notin imf$.
Proof: This can be done with a brute force.
$f([0]_{12}) = [0^2]_3 = [0]_3$.
$f([1]_{12}) = [1^2]_3 = [1]_3$.
$f([2]_{12}) = [2^2]_3 = [4]_3$.
$f([3]_{12}) = [3^2]_3 = [9]_3 = [0]_3$
and so on until $n = 12$. As we can see $[2]_3$ does not exist and so f is not surjective.

Definition 6.34. A function $f : A \to B$ is a *bijection* if f is both injective and surjective. (Also called a *one-to-one correspondence*).

Example 6.35. $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n + 1$.
f is injective: Let $m, n \in \mathbb{N}$ with $f(m) = f(n)$. Then $m + 1 = n + 1$ and so $m = n$. Thus f is injective.

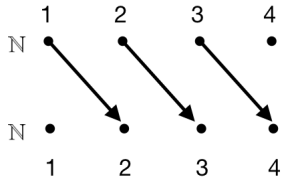
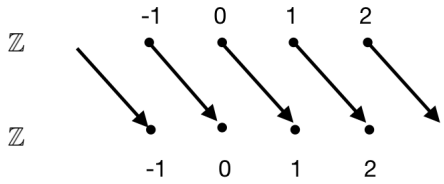


Figure 6.4: Trying to show that the function is not surjective.

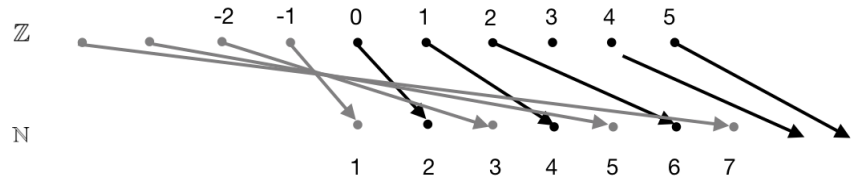
f is not surjective: Note that $f(n) = 1$ is impossible. $n + 1 = 1$ implies that $n = 0 \notin \mathbb{N}$.

Example 6.36. $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n + 1$
f is injective by the same argument as in the previous example.



To see that f is surjective, let $n \in \mathbb{Z}$. Then $f(n-1) = (n-1)+1 = n$ and $((n-1) \in \mathbb{Z})$. Thus f is surjective.

Example 6.37.



Find a formula that does what the arrows do.
Define $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2n+2 & \text{if } n \geq 0 \\ -2n-1 & \text{if } n < 0. \end{cases}$$

Claim: f is a bijection.

Proof: Let $m, n \in \mathbb{Z}$ with $f(m) = f(n)$. If $m, n \geq 0$, then $2m+2 = 2n+2$ and so $m = n$. If $m, n < 0$, then $-1-2m = -1-2n$ and so $m = n$. If m or n is positive and the other is negative, then they are different numbers. Therefore, if $m \geq 0$ and $n < 0$, then $2m+2 = -1-2n$ and so $2(m+n) = -3$, which is impossible because there is an even integer on the left side of the equation and an odd integer on the right. Thus, f is injective.
Now, let $n \in \mathbb{N}$. If n is even, then $n = 2k$ for some $k \in \mathbb{Z}$ and so $f(k-1) = 2k = n$. How do we get $k-1$? We are trying to find which expression in terms of k gives us n. In other words 2(something in terms of k) $+ 2 = 2k = n$. We can say that this something is n and so $2n+2 = 2k$ and solving for n we get $n = k-1$.
If n is odd, then $n = 2k+1$ for some $k \in \mathbb{Z}$ and so
$f(-(k+1)) = 2k+1 = n$. Getting $-(k+1)$ has a similar process

and what we get from the process is that $-2n-1 = 2k+1$ and solving for n we get $n = -(k+1)$. Thus, f is surjective.
In conclusion f is a bijection.

Example 6.38. $f : \mathbb{Z}/\sim_4 \to \mathbb{Z}/\sim_4$ given by $f([n]_4) = [3n+1]_4$.
Exercise: Show that f is well defined.
$f([0]_4) = [1]_4$.
$f([1]_4) = [0]_4$.
$f([2]_4) = [3]_4$.
$f([3]_4) = [2]_4$.
By inspection, f is a bijection.

Example 6.39.
For an interval $I \subseteq \mathbb{R}$ and a nonnegative integer k, let $C^k(I)$ be the set of all functions $f : I \to \mathbb{R}$ such that for all $0 \leq i \leq k$, $f^{(i)}$ exists and $f^{(k)}$ is continuous. So, $C^{(2)}(-1,1)$ is the set of all functions $f : (-1,1) \to \mathbb{R}$ such that f'' is continuous. $C^0([0,1])$ is the set of continuous functions $[0,1] \to \mathbb{R}$. If $f : (-1,1) \to \mathbb{R}$ is given by $f(x) = x^{\frac{2}{3}}$. Since f is continuous $f \in C^0(-1,1)$. But
$f'(x) = \frac{2}{3}x^{\frac{-1}{3}} = \frac{2}{3x^{\frac{1}{3}}}$, so f is not in $C^1(-1,1)$ because there is a hole at $x = 0$. Define $A : C^0[0,1] \to \mathbb{R}$ by $A(f) = \int_0^1 f(x)\,dx$. Note that if $f : [0,1] \to \mathbb{R}$ and $g : [0,1] \to \mathbb{R}$ are given by $f(x) = x^2$ and $g(x) = \frac{2}{3}x$ we have $A(f) = \frac{1}{3} = A(g)$ and so A is not one-to-one. Given $r \in \mathbb{R}$, define $f : [0,1] \to \mathbb{R}$ by $f(x) = r$, then $A(f) = r$ and so A is onto.

Example 6.40. Define $D : C^1[0,1] \to C^0[0,1]$ by $D(f) = f'$. Since $D(2) = 0 = D(1)$ in which $f(x) = 2$ and $g(x) = 1$, D is not one-to-one.
Given $f \in C^0[0,1]$, let $g(x) = \int_0^x f(t)\,dt$. By the fundamental theorem of calculus, $D(g) = f$ and so D is onto.

Definition 6.41. Let $f : A \to B$ and $g : B \to C$. The *composition* of f with g is $g \circ f : A \to C$ defined by $g \circ f(a) = g(f(a))$.

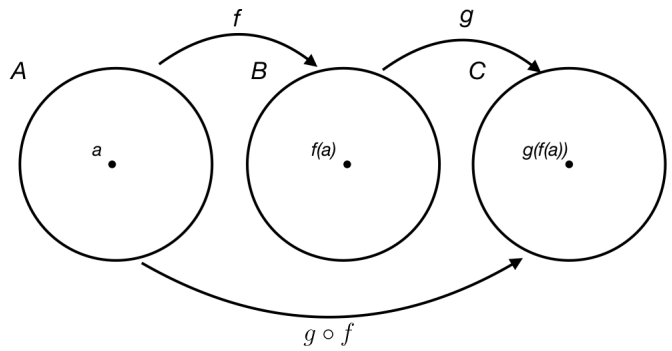


Figure 6.5: This is a composition function.

Example 6.42.
$f : \mathbb{Z} \to \mathbb{Z}/\sim_8$ defined by $f(n) = [n]_8$.
$g : \mathbb{Z}/\sim_8 \to \mathbb{Z}/\sim_4$ defined by $g([n]_8) = [n]_4$.
$g \circ f(n) = [n]_4$.

Theorem 6.43.
Let $f : A \to B$ and $g : B \to C$.
(a) If f and g are injective, then $g \circ f$ is injective.
(b) If f and g are surjective, then $g \circ f$ is surjective.
(c) If $g \circ f$ is injective, then f is injective.
(d) If $g \circ f$ is surjective, then g is surjective.

Proof: (a) Assume f and g are injective and let $a, a' \in A$ be such that $g \circ f(a) = g \circ f(a')$. Then $g(f(a)) = g(f(a'))$ and since g is injective we conclude that $f(a) = f(a')$. Since f is injective, $a = a'$. Therefore $g \circ f$ is injective.

(b) If $c \in C$ then there exists a $b \in B$ such that $g(b) = c$. Also there exists an $a \in A$ such that $f(a) = b$ so $g \circ f(a) = g(f(a)) = g(b) = c$ hence $g \circ f$ is surjective.

(c) Suppose that $g \circ f$ is injective. Then there exists an $a, a' \in A$ such that $f(a) = f(a')$. Then $(g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a')$. But since $g \circ f$ is injective, this implies that $a = a'$. Thus f is injective.

(d) Assume that $g \circ f$ is surjective and let $c \in C$. There exists an $a \in A$ such that $g \circ f(a) = c$. Letting $b = f(a)$ we have $g(b) = g(f(a)) = c$. Therefore, g is surjective. $\square$

Corollary 6.44.
If $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection.

Definition 6.45. Functions $f : A \to B$ and $g : A \to B$ are *equal* if $f(a) = g(a)$ for all $a \in A$. (Same formula, domain and codomain).

Theorem 6.46.
Let $f : A \to B$, $g : B \to C$, and $h : C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$. (Composition is associative).

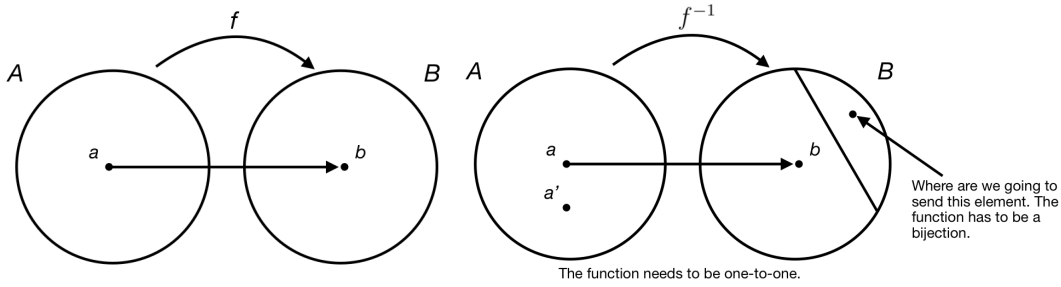
Proof: Note: $dom((h \circ g) \circ f) = A = dom(h \circ (g \circ f))$ and the $codom((h \circ g) \circ f) = D = codom(h \circ (g \circ f))$.
Now let $a \in A$. Then $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$ and $(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$. $\square$

Let $f : A \to B$. If $C \subseteq A$ and $D \subseteq B$, then it is true that
(i) $C \subseteq f^{-1}(f(C))$
(ii) $f(f^{-1}(D)) \subseteq D$.
Equality does not hold in general.

Example 6.47.
$f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$ defined by

$$f(x) = \begin{cases} 1 & \text{if } x \in \{1, 2\} \\ 2 & \text{if } x \in \{3, 4\}. \end{cases}$$

With $C = \{2, 3\}$, we have $f^{-1}(f(c)) = f^{-1}(\{1, 2\}) = \{1, 2, 3, 4\}$.
With $D = \{2, 3\}$, we have $f(f^{-1}(D)) = f(\{3, 4\}) = \{2\}$.
Now suppose that $f : A \to B$ is a bijection. Then,for each $b \in B$ there is a unique $a \in A$ such that $f(a) = b$.



Definition 6.48.
Let $f : A \to B$ be a bijection. The function $f^{-1} : B \to A$ defined by $f^{-1}(b) = a$ if and only if $f(a) = b$ is the *inverse* of f.
Note: $domf^{-1} = codomf$ and $codomf^{-1} = domf$.

Example 6.49.
Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^3$. Then $f^{-1} : \mathbb{R} \to \mathbb{R}$ is given by $f^{-1}(x) = \sqrt[3]{x}$.

Example 6.50.
$f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$. This function is not a bijection. But consider $g : [0, \infty) \to [0, \infty)$ where $g(x) = x^2$. Then $g^{-1} : [0, \infty) \to [0, \infty)$ is given by $g^{-1}(x) = \sqrt{x}$.

Definition 6.51. The function $i_A : A \to A$ defined by $i_A(a) = a$ for all $a \in A$ is the *identity function* on A.
Observation: If $f : A \to B$ is a bijection, then $f^{-1} \circ f(a) = a$ and $f \circ f^{-1}(b) = b$ for all $a \in A$ and $b \in B$. That is $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

Theorem 6.52.
Let $f : A \to B$. Then there exists $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$ if and only if f is a bijection. Moreover, if such a function g exists then $g = f^{-1}$.

Proof: ($\Rightarrow$) If there exists $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$ then observing that i_A and i_B are bijections we see that f is one-to-one by theorem 6.43 part c and f is onto by theorem 6.43 part d.

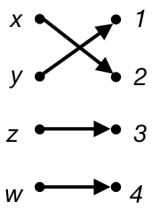
($\Leftarrow$) If f is a bijection, then f^{-1} exists and $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$. Suppose $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$. Then $(g \circ f) \circ f^{-1} = i_A \circ f^{-1}$. For the left-hand side: $(g \circ f) \circ f^{-1} = g \circ (f \circ f^{-1}) = g \circ i_B$. Given $b \in B$, note that $g \circ i_B(b) = g(i_B(b)) = g(b)$. Thus $g \circ i_B = g$. Similarly, for the right-hand side, we have $i_A \circ f^{-1}(b) = i_A(f^{-1}(b)) = f^{-1}(b)$ for all $b \in B$. Therefore $i_A \circ f^{-1} = f^{-1}$.
In conclusion $g = f^{-1}$. $\square$

Chapter 7

Cardinality

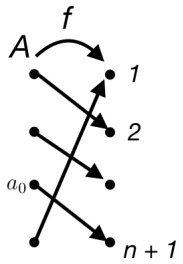
Definition 7.1. A set A is *finite* if $A = \emptyset$ or there exists a bijection $f : A \to \{1, \ldots, n\}$ for some $n \in \mathbb{N}$.
In the first case we write $|A| = 0$ and say that A has a *cardinality* of 0. In the second case we write $|A| = n$ and say that A has a *cardinality* of n.

Example 7.2. $A = \{x, y, z, w\}$ Conclusion: $|A| = 4$.

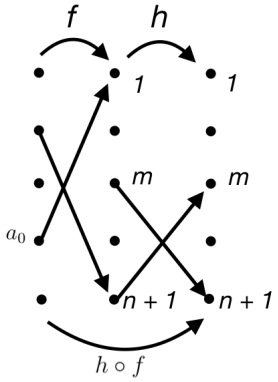


It seems obvious that if $|A| = m$ and $|A| = n$ then $m = n$.

Lemma 7.3.
Let A be a set, $a_0 \in A$ and $n \in \mathbb{N}$. Then there exists a bijection $f : A \to \{1, 2, \ldots, n + 1\}$ if and only if there exists a bijection $g : A - \{a_0\} \to \{1, 2, \ldots, n\}$.



Proof: ($\Rightarrow$) Assume $f : A \to \{1, 2, \ldots, n+1\}$ is a bijection. If $f(a_0) = n+1$, then define $g : A - \{a_0\} \to \{1, 2, \ldots, n\}$ by $g(a) = f(a)$ for all $a \in A - \{a_0\}$. If $a, a' \in A - \{a_0\}$ such that $g(a) = g(a')$, then $f(a) = f(a')$. Since f is injective we have that $a = a'$ and conclude that g is injective. Let $m \in \{1, 2, \ldots, n\}$. Note that $f^{-1}(m) \in A - \{a_0\}$ and so $g(f^{-1}(m)) = f(f^{-1}(m)) = m$. Thus g is surjective. If $f(a_0) = n + 1$ then we have a bijection $g : A - \{a_0\} \to \{1, 2, \ldots, n\}$.

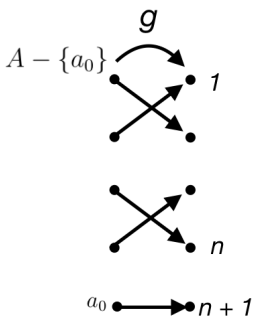


Otherwise, let $m \in \{1, \ldots, n\}$ be such that $f(a_0) = m$ and let $a_1 \in A$ be such that $f(a_1) = n+1$. Define $h : \{1, \ldots, n+1\} \to \{1, \ldots, n+1\}$ by

$$h(i) = \begin{cases} \text{i} & \text{if } i \in \{m, n+1\} \\ \text{n + 1} & \text{if } i = m \\ \text{m} & \text{if } i = n+1. \end{cases}$$

Check that h is a bijection. By corollary 6.44, $h \circ f : A \to \{1, \ldots, n+1\}$ is a bijection. Note that $h \circ f(a_0) = h(f(a_0)) = h(m) = n+1$. From our work on the previous

case, there exists a bijection $g : A - \{a_0\} \to \{1, \ldots, n\}$.
($\Leftarrow$)



Assume there is a bijection $g : A - \{a_0\} \to \{1, \ldots, n\}$. Check: The function $f : A \to \{1, \ldots, n+1\}$ defined by

$$f(a) = \begin{cases} \text{g(a)} & \text{if } a \neq a_0 \\ \text{n + 1} & \text{if } a = a_0 \end{cases}$$

is a bijection. □

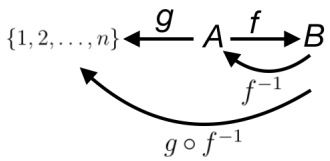
Theorem 7.4.
Let A be a set with $|A| = n > 0$. If B is a proper subset of A, then
(a) $|B| \neq n$
(b) there exists $0 \leq m < n$ such that $|B| = m$.

Proof: If $B = \emptyset$, then $|B| = 0$ (so part (b) is true). Note: If $f : \emptyset \to \{1, \ldots, n\}$, then f cannot be surjective. That is, there is no bijection $B \to \{1, \ldots, n\}$ and so $|B| \neq n$. We now proceed by induction on $|A| = n$. In the case that $n = 1$, we have $B = \emptyset$ and so the result holds by the previous discussion. Now let $k \in \mathbb{N}$ and assume that the result holds for k. Consider the case that $|A| = k+1$. Then there exists a bijection $f : A \to \{1, \ldots, k+1\}$. Let $B \subseteq A$ be a proper non empty subset. We may choose $a_0 \in B$ and $a_1 \in A - B$. By lemma 7.3, there exists a bijection $g : A - \{a_0\} \to \{1, \ldots, k\}$. This means $|A - \{a_0\}| = k$. Since $a_1 \in (A - \{a_0\}) - (B - \{a_0\})$, $B - \{a_0\}$ is a proper subset of $A - \{a_0\}$. By the inductive hypothesis, $|B - \{a_0\}| \neq k$ and there exists $0 \leq p < k$ such that $|B - \{a_0\}| = p$. This means (1) there is no bijection $B - \{a_0\} \to \{1, \ldots, k\}$ and (2)

$B - \{a_0\} = \emptyset$ or there is a bijection $B - \{a_0\} \to \{1, \ldots, p\}$. Since $|B - \{a_0\}| \neq k$, by lemma 7.3 we conclude that $|B| \neq k + 1$. By induction, part (a) holds for all $n \in \mathbb{N}$. In the case that $B - \{a_0\} = \emptyset$, then there is a bijection $B : \{a_0\} \to \{1\}$ and so $|B| = 1$. In the case that there is a bijection $B - \{a_0\} \to \{1, \ldots, p\}$, by lemma 7.3, there exists a bijection $B \to \{1, \ldots, p + 1\}$. Since $p < k$, we have $p + 1 < k + 1$ and so $|B| = p + 1 < k + 1$. By induction, part (b) holds for all $n \in \mathbb{N}$. □

Corollary 7.5.
If A is finite and $B \subsetneqq A$, then there is no bijection $A \to B$.

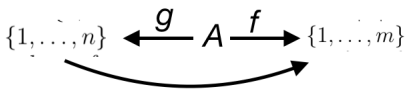
Proof: Suppose $f : A \to B$ is a bijection. Since A is finite, there exists a bijection $g : A \to \{1, \ldots, n\}$ for some $n \in \mathbb{N}$.



Then $g \circ f^{-1} : B \to \{1, \ldots, n\}$ is a bijection and so $|B| = n$. This contradicts theorem 7.4 part (a). □

Corollary 7.6.
If A is a finite set, then there exists a unique integer $n \geq 0$ such that $|A| = n$.

Proof: Suppose $|A| = m$ and $|A| = n$, where $m < n$. Then we have bijections $f : A \to \{1, \ldots, m\}$ and $g : A \to \{1, \ldots, n\}$.



It follows that $f \circ g^{-1} : \{1, \ldots, n\} \to \{1, \ldots, m\}$ is a bijection. Since $\{1, \ldots, m\}$ is a proper subset of $\{1, \ldots, n\}$, this contradicts corollary 7.5. □

Corollary 7.7.
If A is a finite set and $B \subseteq A$, then B is finite. Moreover, if $B \subsetneqq A$,

then $|B| < |A|$.

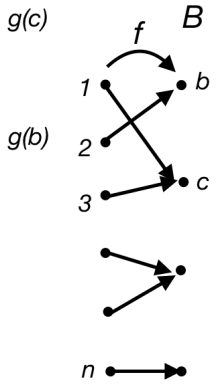
Corollary 7.8. (Pigeonhole Principle)
If A and B are finite sets, $|A| > |B|$ then there is no injective function $A \to B$.

Corollary 7.9.
The set $\mathbb{N}$ is not finite.

Proof: The function $f : \mathbb{N} \to \mathbb{N} - \{1\}$ defined by $f(n) = n + 1$ is a bijection from $\mathbb{N}$ to a proper subset of $\mathbb{N}$. If $\mathbb{N}$ was finite, this would contradict corollary 7.5. □

Theorem 7.10.
Let $B \neq \emptyset$ and $n \in \mathbb{N}$. The following statements are equivalent.
(a) There is a surjection $f : \{1, \ldots, n\} \to B$.
(b) There is an injection $g : B \to \{1, \ldots, n\}$.
(c) $|B| \leq n$.

Proof: (a) ⇒ (b)



Assume $f : \{1, \ldots, n\} \to B$ is onto. For each $b \in B$,
$f^{-1}(b) \subseteq \{1, \ldots, n\}$, and so $f^{-1}(b)$ has a unique least element. Define $g : B \to \{1, \ldots, n\}$ by $g(b) = min(f^{-1}(b))$. Suppose $b, b' \in B$ such that $g(b) = g(b')$. If $b \neq b'$, then we have
$min(f^{-1}(b)) = min(f^{-1}(b'))$ and so $f^{-1}(b) \cap f^{-1}(b') \neq \emptyset$. But $f^{-1}(b) \cap f^{-1}(b') = f^{-1}(\{b\} \cap \{b'\}) = f^{-1}(\emptyset) = \emptyset$ by theorem 6.43

part (d). There is a contradiction $\Rightarrow\Leftarrow$. Therefore g is injective.

(b) $\Rightarrow$ (c) Assume we have a one-to-one function $g : B \to \{1, \ldots, n\}$. Then $g(B) \subseteq \{1, \ldots, n\}$ and so $g(B)$ is finite by corollary 7.7. Then there exists a bijection $h : g(B) \to \{1, \ldots, p\}$, where $p \leq n$. Letting $g' : B \to g(B)$ be defined by $g'(b) = g(b)$ for all $b \in B$ we have a bijection $h \circ g' : B \to \{1, \ldots, p\}$ and so $|B| = p \leq n$.

(c) $\Rightarrow$ (a) We write $|B| = m \leq n$. Then there is a bijection $h : \{1, \ldots, m\} \to B$. Define $f : \{1, \ldots, n\} \to B$ by

$$f(i) = \begin{cases} \text{h(i)} & \text{if } 1 \leq i \leq m \\ \text{h(1)} & \text{if } m+1 \leq i \leq m. \end{cases}$$

f is surjective because h is surjective. $\square$

Corollary 7.11.
If $A_1, \ldots, A_n$ are finite sets, then $\bigcup_{i=1}^{n} A_i$ and $A_1 \times \cdots \times A_n$ are finite.
Proof: Exercise.

Definition 7.12. A set A is *infinite* if it is not finite. A set A is *countably infinite* (or *denumerable*) if there is a bijection $f : A \to \mathbb{N}$. A set A is *countable* if A is finite or countably infinite.
Notation: If A is countably infinite we write $|A| = \aleph_0$.

Example 7.13. $|\mathbb{Z}| = \aleph_0$

Proof: In example 6.37 we showed that there is a bijection $\mathbb{Z} \to \mathbb{N}$. $\square$

Theorem 7.14.
If A is countable and $B \subseteq A$ then B is countable.

Proof: If A is finite, then so is B by corollary 7.7. If A is countably infinite and B is finite, there is nothing to prove. Thus we may assume that B is an infinite subset of the countably infinite set A. Let $f : \mathbb{N} \to A$ be a bijection. Define $S = f^{-1}(B)$. Since $\emptyset \neq S \subseteq \mathbb{N}$, S has a least element s_1. Since $\emptyset \neq S - \{s_1\} \subseteq \mathbb{N}$, $S - \{s_1\}$ has a least

element s_2. Repeating this process we have s_{k+1} is the least element of $S - \{s_1, s_2, \ldots, s_k\}$. Now we have the subset $\{s_1, s_2, s_3, \ldots\} \subseteq S$ with $s_1 < s_2 < s_3 < \ldots$. Suppose $S - \{s_1, s_2, \ldots\} \neq \emptyset$. Then there exists $m \in S - \{s_1, s_2, \ldots\}$. Note that $m < s_{m+1}$ and so s_{m+1} is not the least element of $S - \{s_1, \ldots, s_m\}$. This contradiction forces us to conclude that $S = \{s_1, s_2, s_3, \ldots\}$.
Observations: (1) $g : S \to \mathbb{N}$ defined by $g(s_i) = i$ is a bijection.
(2) $f\,|_s$: $S \to B$ is a bijection.
Thus $g \circ (f\,|_s) : B \to \mathbb{N}$ is a bijection and so B is countable. □

Definition 7.15. Let A and B be sets.
(a) $|A| = |B|$ if there exists a bijection from $A \to B$.
(b) $|A| \leq |B|$ if there exists an injection from $A \to B$.
(c) $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$.

Applying theorem 7.10: To show that a set B is countably infinite, one can show that $B \subseteq A$ where $|A| = \aleph_0$. More generally, to show that $|B| = \aleph_0$, produce an injection $f : B \to A$ where A is known to be countably infinite.

Example 7.16. Show that $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Proof 1: Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m, n) = 2^m 3^n$. Suppose $f(m, n) = f(p, q)$. Then $2^m 3^n = 2^p 3^q$. If $m < p$, then $3^n = 2^{p-m} 3^q$, which implies that 3^n is even $\Rightarrow\Leftarrow$. There is a similar contradiction if $m > p$. Thus $m = p$. From this we have that $3^n = 3^q$ and so $n = q$. Therefore f is injective. □

Proof 2:

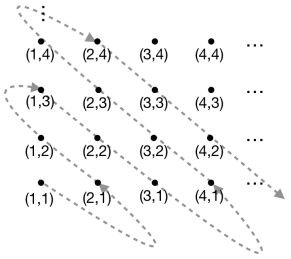
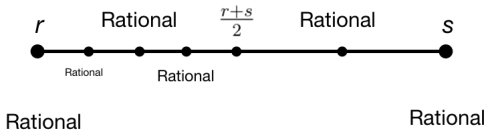


Figure 7.1: The zig-zag defines a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that is bijective.

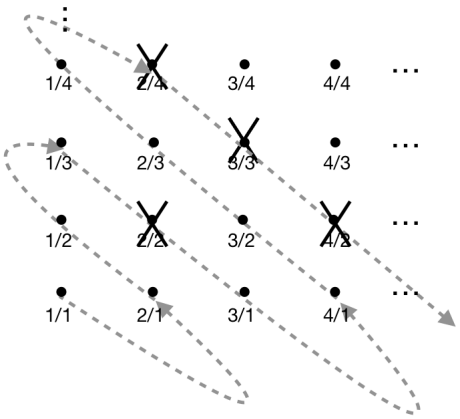
Question: Is $\mathbb{Q}$ countable?
$\mathbb{Q}$ is tricky: between any rationals r and s there are an infinite number of rationals.



Let $\mathbb{Q}^+ = \mathbb{Q} \cap (0, \infty)$ (positive rationals).

Theorem 7.17. (Cantor, 1872) The set $\mathbb{Q}^+$ is countable.

Proof:



□

Theorem 7.18.
Let A, B be countable.
(a) Then $A \cup B$ is countable.
(b) $A \times B$ is countable.

Proof (a): We first show that the result holds for $A \cap B = \emptyset$.
(Case 1) If A and B are finite, say $|A| = m$ and $|B| = n$, then there exist bijections $f : A \to \{1, 2, \ldots, m\}$ and $g : B \to \{1, 2, \ldots, n\}$.

Define $h : A \cup B \to \{1, 2, \ldots, m+n\}$ by

$$h(x) = \begin{cases} \text{f(x)} & \text{if } x \in A \\ \text{g(x)} + \text{m} & \text{if } x \in B. \end{cases}$$

Since $A \cap B = \emptyset$, h is well-defined. Now check that h is a bijection and conclude that $|A \cup B| = m + n$.
(Case 2) If A is finite and B is infinite, then there exist bijections $f : A \to \{1, 2, \ldots, m\}$ and $g : B \to \mathbb{N}$. Define $h : A \cup B \to \mathbb{N}$ by

$$h(x) = \begin{cases} \text{f(x)} & \text{if } x \in A \\ \text{g(x)} + \text{m} & \text{if } x \in B. \end{cases}$$

As above h is well-defined, and we can check that h is a bijection. Thus $|A \cup B| = \aleph_0$.
(Case 3) If both A and B are infinite, then there exist bijections $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$. Define $h : A \cup B \to \mathbb{Z}$ by

$$h(x) = \begin{cases} \text{f(x)} & \text{if } x \in A \\ \text{-g(x)} & \text{if } x \in B. \end{cases}$$

As above h is well-defined. One can check that h is injective and so $|A \cup B| \leq |\mathbb{Z}|$. Since $A \cup B$ is infinite (it contains the infinite subset A), $|A \cup B| = |\mathbb{Z}| = \aleph_0$.
The general result no follows from the following observations: If A and B are any sets, then $A \cup B = (A - B) \cup B$ and $(A - B) \cap B = \emptyset$. $\square$

Proof (b): We make two observations:
(1) For each $a \in A$, $|\{a\} \times B| = |B|$ (under the obvious bijection).
(2) $A \times B = \bigcup_{a \in A} \{a\} \times B$. $\square$

Corollary 7.19.
If $A_1, \ldots, A_n$ are countable,
(a) then $\bigcup_{i=1}^{n} A_i$
(b) $A_1 \times \cdots \times A_n$ are countable.

Proof (a): (Induction) Base step: Theorem 7.19 part (a).
Inductive step: Let $k \in \mathbb{N}$ and assume that $A_1 \cup A_2 \cup \cdots \cup A_k$ is countable. We know that A_{k+1} is countable. Now, let $B = (A_1 \cup \cdots \cup A_k)$.

Then B is countable. As shown in theorem 7.19 part (a), the union of two countable sets is countable. Now $B \cup A_{k+1}$ must be countable. In conclusion $\bigcup_{i=1}^{n} A_i$ is countable. $\square$

Proof (b):Base step: (Induction) Theorem 7.19 part (b).
Inductive step: Let $k \in \mathbb{N}$ and assume that $A_1 \times A_2 \times \cdots \times A_k$ is countable. We know that A_{k+1} is countable. Now, let
$B = (A_1 \times \cdots \times A_k)$. Then B is countable. As shown in theorem 7.19 part (b), the cartesian product of two countable sets is countable. Now $B \times A_{k+1}$ must be countable. In conclusion $A_1 \times \cdots \times A_n$ is countable. $\square$

Corollary 7.20. $\mathbb{Q}$ is countable.

Proof: $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$ is a union of countable sets. Now by corollary 7.19 $\mathbb{Q}$ is countable. $\square$

Definition 7.21. Let A be a set. If A is not countable, then A is *uncountable*.

Theorem 7.22. (Cantor's Theorem, 1891) For any set A, $|A| < |\wp(A)|$. (Injective, no bijection).

Proof:(Contradiction) The function $f : A \to \wp(A)$ defined by
$f(a) = \{a\}$ is injective and so $|A| \leq |\wp(A)|$. Suppose there exists a bijection $g : A \to \wp(A)$. Define the set $B = \{a \in A \mid a \notin g(a)\}$. Note that $B \subseteq A$. Since g is surjective, there exists $z \in A$ such that $g(z) = B$. There are two possibilities:
(1) If $z \notin B = g(z)$ then $z \in B$.
(2) If $z \in B = g(z)$ then $z \notin B$.
It follows that no such z exists and so g is not onto $\Rightarrow\Leftarrow$. Thus, no bijection $A \to \wp(A)$ exists and so $|A| < |\wp(A)|$. $\square$

Corollary 7.23.
There exists an uncountable set.

Proof: By theorem 7.22, $|\mathbb{N}| < |\wp(\mathbb{N})|$.

If $x \in (0, 1)$ then x has a decimal expansion of the form

$x = 0.x_1x_2x_3\ldots$ where each $x_i \in \{0, 1, 2, \ldots, 9\}$.

Theorem 7.24. (Cantor's Theorem, 1873)
The interval $(0, 1)$ is uncountable.

Proof: (Contradiction): Suppose we have a bijection $f : \mathbb{N} \to (0, 1)$. Then
$f(1) = 0.a_{11}a_{12}a_{13}\ldots$
$f(2) = 0.a_{21}a_{22}a_{23}\ldots$
$f(3) = 0.a_{31}a_{32}a_{33}\ldots$
In general $f(n) = 0.a_{n1}a_{n2}a_{n3}\ldots$
Define $b = 0.b_1b_2b_3\ldots$ where

$$b_i = \begin{cases} 1 & \text{if } a_{ii} \neq 1 \\ 2 & \text{if } a_{ii} = 1. \end{cases}$$

Note that $b_i \neq a_{ii}$ for all $i \in \mathbb{N}$ and so $b \notin imf$. Thus no such bijection exists $\Rightarrow\Leftarrow$. $\square$

Notation: A set A has *cardinality* $\vec{c}$ if $|A| = |(0, 1)|$.

Theorem 7.25. $|\mathbb{R}| = \vec{c}$

Proof: The function $f : (0, 1) \to \mathbb{R}$ given by $f(x) = \tan(\pi x - \frac{\pi}{2})$ is a bijection. (We know that the tangent function has an inverse). $\square$

Continuum Hypothesis (conjured by Cantor, 1878)
There is no set X such that $\aleph_0 < |X| < \vec{c}$.

Gödel (1940): The Continuum Hypothesis cannot be disproved.
Cohen (1962): The Continuum Hypothesis cannot be proved.

Recall: $p \in \mathbb{N}$ is <u>prime</u> if $p > 1$ and has 1 and p as divisors.

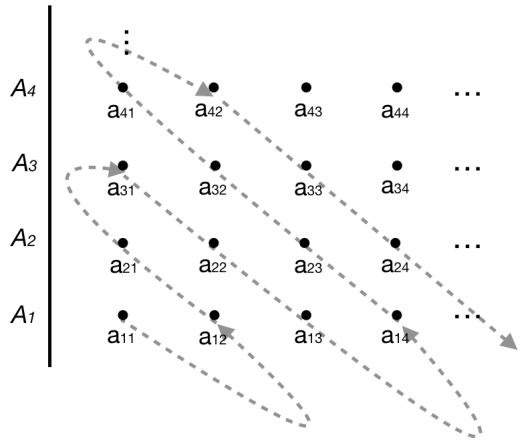
Theorem 7.26. (Euclid $\approx$ 300 BC)
There are infinitely many primes.

Proof: (Contradiction) Let $P \subseteq \mathbb{N}$ be the set of primes. Suppose P is finite. Then $P = \{p_1, p_2, p_3, \ldots, p_n\}$. Consider $z = 1 + p_1p_2\ldots p_n$.

Since $z > p_i$ for each $1 \leq i \leq n$, $z \notin P$. It follows that p_j divides z for some $1 \leq j \leq n$. Also note that $p_j \mid p_1 p_2 \dots p_n$. This implies that $p_j \mid z - p_1 p_2 \dots p_n = 1 \Rightarrow\Leftarrow$. Therefore P cannot be finite. □

Theorem 7.27. A countable union of countable sets is countable.

Proof: For each $i \in \mathbb{N}$, let A_i be a countable set. We can write $A_i = \{a_{i1}, a_{i2}, a_{i3}, \dots\}$. Then we can arrange $\{A_i\}_{i \in \mathbb{N}}$ as



Using Cantor's "zig-zag" we have that $\bigcup_{i=1}^{\infty} A_i$ is countable. □

Definition 7.28. A real number r is *algebraic* if there exists a non-zero polynomial $p(x) = a_0 + a_1 x + \dots + a_n x^n$ where each $a_i \in \mathbb{Q}$ such that p(r) = 0.

Example 7.29.
4 is algebraic because $p(x) = x - 4$.
$\sqrt{2}$ is algebraic because $p(x) = x^2 - 2$.
$\sqrt{2} + \sqrt{3}$ is algebraic because $p(x) = x^4 - 10x^2 + 1$.

Definition 7.30. A real number that is not algebraic is *transcendental*.

Example 7.31.
e is transcendental (Hermite 1873).

π is transcendental (Lindenmann 1882).

Corollary 7.32.
The set of algebraic numbers is countable.

Proof: Let P be the set of polynomials with rational coefficients. For each $f \in P$, let R_f be the set of roots of f. Then the set of algebraic numbers equals $\bigcup_{f \in P} R_f$. Since each R_f is finite, by theorem 7.27 it suffices to show that P is countable. Define $P_n = \{f \in P \mid deg(f) = n\}$. Then $P = \bigcup_{n=0}^{\infty} P_n \cup \{0\}$. Define $h : P_n \to \mathbb{Q}^{n+1}$ by $h(a_0 + a_1 x + \cdots + a_n x^n) = (a_0, a_1, \ldots, a_n)$. Check that h is injective to conclude that $|P_n| \leq |\mathbb{Q}^{n+1}|$. Since $\mathbb{Q}$ is countable, so is $\mathbb{Q}^{n+1}$ by corollary 7.19. It now follows that P is countable by theorem 7.27. $\square$

Corollary 7.33.
The set of transcendental numbers is uncountable.

Proof: $A \cup T = \mathbb{R}$. Basically the set of algebraic numbers "A" union the set of transcendental numbers "T" is the real numbers which is not countable. And we already proved that the set of algebraic numbers is countable and so the other set, the set of transcendental numbers must not be countable. $\square$