Contents

Chapter 1

Proofs

Mathematical Statements

A *mathematical statement* is an English statement that has a truth value.

Types of Statements Compound statements, Implications, Double implications, Converse of an Implications, Negations, and Quantifiers.

Compound Statement (P and Q)

A *compound statement* is a statement constructed from two statements joined be the words "and" or "or".

Example 1.1 (Compound Statement)**.** Let x be a real number.

P : Then number x is greater than 3.

Q : Then number x is even.

P and Q : The number x is greater than 3 **and** x is even.

P and Q : The number x is greater than 3 **or** x is even.

Question: What are the truth values of P and Q and P and Q?

1. If $x = 6$? P and Q, P or Q are true.
2. If $x = 5$? P and Q is false. P or Q is true.
3. If $x < 3$? P and Q is false. , P or Q depends on the value of x.

Implication ($P \to Q$)

The mathematical statement "P implies Q" is an implication where P is the hypothesis and Q is the conclusion. Other forms of an implication are "If P then Q.", "$P \to Q$", and "$P \Rightarrow Q$".

Example 1.2. If x is greater than 0, then x^2 is greater than 0. Here "x is greater than 0" is the hypothesis and "x^2 is greater than 0" is the conclusion.

Converse of an implication ($Q \to P$)

The converse of " P implies Q" is " Q implies P".

Example 1.3. Converse of previous example

If x^2 is greater than 0, then x is greater than 0.

Double implication ($Q \leftrightarrow P$)

The statement "'"P implies Q" and "Q implies P"' is a double implication. Other forms of a double implication are " $P \leftrightarrow Q$", "$P \Leftrightarrow Q$", "P iff Q", where 'iff' means 'if and only if'.

Example 1.4. (Double implication) The value of x is greater than 0 if and only if x^2 is greater than 0.

Negation ($\neg P$)

The negation of P is not P. The notation for the negation of P is denoted by $\neg P$

Example 1.5. (Negation) Let P : The value of x is greater than 0. Then $\neg P$: The value of x is less than or equal to 0.

Contrapositive ($\neg Q \to \neg P$)

The contrapositive of an implication $P \to Q$ is an equivalent statement of the following form $\neg Q \to \neg P$.

Example 1.6. The following statement is the contrapositive of the statement from example Example 1.2. If x^2 is less than or equal to 0 then x is less than or equal to 0.

Problem 1.7. *Is the statement "Let x be a real number." a mathematical statement?*

Solution 1.8. This is not a mathematical statement because it does not have a truth value. Statements similar to the statement "Let x be a real number." are *commands* and are typically used to define variables.

Quantifiers

Expressions that quantify statements. Common quantifiers are "for all" and "there exists" denoted by $\forall$ and $\exists$ respectively.

Example 1.9. (Quantifiers)

- For all integers x, $x^2 \geq 0$. Here the expression "For all" quantifies for which integers the statement $x^2 \geq 0$ is true.
- There exists an integer x such that $x^2 - 1 = 0$.
- For all x there exists y such that x is less than y.

Truth Tables

Truth tables help us determine the validity of a statement. Truth tables give us a way to construct equivalent statements.

Let P and Q be mathematical statements. A table listing the possible truth values of each statement is called a truth table. For simplicity, instead of writing the word "and"("or") to join to statements we will used the symbols $\wedge(\vee)$ respectively.

Example 1.10. The following is a truth table which can be used to determine the value of the statement $P \wedge Q$.

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

Example 1.11. Below are the truth values of some frequently used statements.

P	Q	$\neg P$	$P \vee Q$	$P \to Q$
T	T	F	T	T
T	F	F	T	F
F	T	T	T	T
F	F	T	F	T

Consider the more complexed statement $\neg Q \to \neg P$ which is the contrapositive of $P \to Q$. A truth table can be used to show that the two statements are actually equivalent. To do this we must show that the two statements have the exact same true values which are independent of the values of P and Q.

Example 1.12. The statements $\neg Q \to \neg P$ and $P \to Q$ are equivalent statements because they have the same values in their columns.

P	Q	$\neg P$	$\neg Q$	$P \to Q$	$\neg Q \to \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

In some cases, proving an equivalent statements may be easier than proving the actual statement.

Problem 1.13. *Use a truth table to show that* $(P \to Q) \wedge (Q \to R) \to (P \to R)$.

Review

1. The product of nonzero real numbers is nonzero. For example, if $xy \neq 0$ then $x \neq 0$ and $y \neq 0$.
2. If x is a nonzero real number then $x^2 > 0$.
3. If x is an even integer then $x = 2k$ for some integer k.
4. If x is an odd integer then $x = 2k + 1$ for some integer k.
5. If x and y are integers then xy is an integer.
6. If x and y are even integers, then xy is an even integer.

Proofs in Mathematics

Proofs should consist of English statements. That is, mathematical expression should be written as complete English sentences. Proofs should not have statements that begin with mathematical symbols.

Example 1.14. The statement "x is even." should not be used in a proof. However, using the previous statement as a hypothesis is fine.

If x is even, then x^2 is even.

Types of proofs:

1. Direct Proof - sequence of implications
2. Proof by Cases - a list of proofs that cover all possible values
3. Proof by Contrapositive - proving a equivalent implication
4. Proof by Contradiction - showing the negation is false
5. Counterexamples - using an example to disprove a statement

Direct Proof ($P_1 \to P_2 \to \cdots \to P_n$)

Direct proof can be thought of as sequence of implications used to show that the hypothesis of the first implication in the sequence implies the last hypothesis in the sequence. Typically, the hypothesises are omitted from the proof for a more elegant proof.

Theorem 1.15. *If x is even then x^2 is even.*

To prove the previous theorem we must show that the value of the implication is true. This means whenever "x is even" (the hypothesis) is a true statement then " x^2 is even" (the conclusion) is a true statement. Whenever the hypothesis is a false the implication is true no matter the value of conclusion. So we need only to consider the case when the hypothesis is a true statement.

Proof. Assume x is even. Then $x = 2k$ for some integer k. Hence $x^2 = x{\cdot}x = 2k{\cdot}2k = 2(2k^2)$. Since $x^2 = 2(2k^2)$ and $2k^2$ is an integer it follows that x^2 is even. □

Notice that after the first sentence which is a command (not a mathematical statement) each of the following statements imply the next. Which leads to the less attractive proof.

Proof. If x is even then $x = 2k$ for some integer k. If $x = 2k$ for some integer k then $x^2 = x \cdot x = 2k \cdot 2k = 2(2k^2)$. If $x^2 = 2(2k^2)$ then x^2 is even. Therefore, if x is even then x^2 is even. □

Problem 1.16. *Prove that if x is odd then x^2 is odd.*

Cases

Proof by cases is useful when it is easier to use different proof techniques for different values of the hypothesis.

Theorem 1.17. *For all integers x, $x^2 + x$ is even.*

The following theorem is a quantified statement which is an indication that proof by cases might be useful.

Proof. For consistency write the quantified statement as an implication. If x is an integer then $x^2 + x$ is even.

Case 1: (x is even)

Assume x is even. Then $x = 2k$ for some integer k. Hence $x^2+x = (2k)^2+(2k) = 2(2k^2+k)$. Therefore, $x^2 + x$ is even.

Case 2: (x is odd)

Assume x is odd. Then $x = 2k+1$ for some integer k. Hence $x^2+x = (2k+1)^2+(2k+1) = 2(2k^2 + 3k + 1)$. Therefore, $x^2 + x$ is even. □

Problem 1.18. *Let x be an integer. Prove that $x^2 - 3x + 9$ is odd.*

Contrapositive

Recall that the contrapositive of the implication $P \to Q$ is $\neg Q \to \neg P$.

Theorem 1.19. *Let x be an integer. If $5x - 7$ is even, then x is odd.*

A direct proof might be the first proof in mind. However $x = \frac{2k-7}{5}$ for some integer k is not a useful form of x when considering it's parity.

Proof. Consider the contrapositive, if x is even then $5x - 7$ is odd. Assume x is even. Then $x = 2k$ for some integer k. Hence $5x - 7 = 5(2k) - 7 = 2(5k) - 2(4) + 1 = 2(5k - 4) + 1$. Therefore, $5x - 7$ is odd. □

The first statement of the proof is a tip to the reader that proof by contrapositive is used.

Problem 1.20. *Prove that if x^2 is even then x is even.*

Contradiction

Proof by way of contradiction is a proof that uses the negation of the original statement to prove the validity of the original statement. For example, let suppose P is a statement that is to be proven. One way to use a proof by contradiction is to disprove $\neg P$ constructing an implication $\neg P \to Q$ and showing that the value of Q is always false. This implies that $\neg P$ must be false to guarantee that $\neg P \to Q$ is a true statement.

Theorem 1.21. *The real number $\sqrt{2}$ is irrational.*

To prove the following theorem we will show that the negation, "The real number $\sqrt{2}$ is rational" is false.

Idea of proof: Let P : The real number $\sqrt{2}$ is irrational., $\neg P$: The real number $\sqrt{2}$ is rational., and Q : There exists integers m and n such that $\sqrt{2} = \frac{m}{n}$ where $n \neq 0$ and m and n have no common factors. If $\neg P$ is false then P is true. Assume $\neg P$ is true. Then Q is true. However in the proof Q is shown to be false. Therefore $\neg P$ must be false which implies that P is true.

Proof. Assume $\sqrt{2}$ is rational. Then there exists integers m and n such that $\sqrt{2} = \frac{m}{n}$ where $n \neq 0$ and m and n have no common factors. Since m and n have no common factors we know that $\frac{m}{n}$ is in lowest terms so both m and n can not be even. We have $\sqrt{2} = \frac{m}{n}$ implies $2 = \frac{m^2}{n^2}$ which implies $2n^2 = m^2$. Since m^2 is even it must be the case that m is even. Hence $m = 2k$ for some integer k. Moreover, $2n^2 = m^2 = (2k)^2$ which implies $n^2 = 2k^2$. This contradicts that both m and n are not even. Therefore, $\sqrt{2}$ is irrational. □

Problem 1.22. *Prove that no odd integer can be expressed as the sum of three even integers.*

Counter Example

Counter examples are examples which show that a statement is false. For instance, $x = 3$ is a counter example to the statement "For all integer x, x^2 is even." Evaluation of the example suffices when showing that the statement is false. For instance, "For all integer x, x^2 is even." is false, since $3^2 = 9$ is odd.

Problem 1.23. *Disprove the following statement. For all positive integers x, if $\frac{x(x+1)}{2}$ is odd then $\frac{(x+1)(x+2)}{2}$ is odd.*

Chapter 2

Sets

Sets

A *set* is a collection of elements. Sets are typically represented by a left curly brace before the first element of the list and a right curly brace after the last element of the list. A definition for the elements of a set can also be used to describe a set. The *empty set* is a set with no elements. The empty set can be denoted by $\emptyset$ or $\{\}$.

Example 2.1. The following are sets.

$$\{1,2,3\} \quad \{\{1,w\},\pi,x^2+x,\text{'proofs'}\} \quad \{x|x^2-1=0\}$$

The symbols $\in$ can be used to indicate that the element x is in the set A. Write $x \in A$. If the element x is not in the set A write, $x \notin A$. The symbols $\setminus$ can be used to construct a set which is the difference between two set. For instance, the set containing elements in the set A which are not in the set B can be represented by $A \setminus B$.

Example 2.2. Let $A = \{1,2,3\}$ and $B = \{\{\},2,\{1,2,3\}\}$. Then $1 \in A$ and $A \in B$. Moreover $B \setminus A = \{\emptyset, A\}$.

Problem 2.3. *Write out the elements of the following sets.*

1. $\{x|x^2+2x-3=0\}$
2. $\{\{\},1,\{1,2,3\}\}$

Common Sets

- The natural numbers (denoted by $\mathbb{N}$) $= \{1,2,3,\dots\}$

- The integers (denoted by $\mathbb{Z}$) $= \{\dots, -2, -1, 0, 1, 2, \dots\}$
- The rational numbers (denoted by $\mathbb{Q}$) $= \{\frac{m}{n} | m, n \in \mathbb{Z}$ and $n \neq 0\}$
- The real numbers (denoted by $\mathbb{R}$) is the set of all numbers
- The irrational numbers (denoted by $\mathbb{I}$) $= \mathbb{R} \setminus \mathbb{Q}$

Subsets

A set A is a *subset* of the set B, denoted by $A \subseteq B$, if and only if every element in A is an element in B. In this case, the set B is called *superset* of the set A. If A is not a subset of B write $A \nsubseteq B$.

Example 2.4. The set $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$ and $\{\} \subseteq \{1, 2\}$.

Some of the common sets are subsets of each other.

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

Problem 2.5. *Which of the common sets are supersets of* $\mathbb{I}$*? Which of the common sets are subsets of* $\mathbb{I}$*?*

The *power set* of the set A, denoted by $\mathcal{P}(A)$, is the set of all subsets of A.

Example 2.6. Let $A = \{1, 2, 3\}$. Then

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

Since the empty set and the set A are subsets of A they are listed in $\mathcal{P}(A)$.

Problem 2.7. *Write the power set for the set* $\{\{1, 2\}, 3, \{\}\}$.

Problem 2.8. *How many elements are in the power set of a set containing exactly three elements?*

To show that a set A is a subset of the set B is suffices to show that every element in A is in B. One way to do this is to pick an arbitrary element in A, say x, and show that $x \in B$. Since x is an arbitrary element in A it is the case that all elements of A are elements of B.

Theorem 2.9. *For any set* A*,* $A \subseteq A$ *and* $\{\} \subseteq A$.

Proof. Direct Proof

For every $x \in A$ it is the case that $x \in A$. Therefore, by definition of subsets, $A \subseteq A$.

Proof by Contradiction

Suppose $\{\} \nsubseteq A$. By definition, there exists $x \in \{\}$ such that $x \notin A$. However, this contradicts that the empty set has no elements. This shows that $\{\} \nsubseteq A$ is false which implies that $\{\} \subseteq A$ is true. □

The set A and B are equal, denote by $A = B$, whenever every element of A is in B and every element of B is in A. A common technique to prove that two sets are equal is to show that they are subsets of each other.

Theorem 2.10. *Let A and B be sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Since Theorem 2.10 is a double implication it is necessary to prove two implications. While this can be done in a linear fashion(The proof only uses double implications.), it is not always easy to construct a proof which only uses double implications.

Proof. This proof breaks the double implication into two implications and prove them individually.

($\Rightarrow$) We want to show, if $A = B$ then $A \subseteq B$ and $B \subseteq A$.

Direct Proof

Suppose $A = B$. Let $x \in A$. Then $x \in B$ since $A = B$. By definition $A \subseteq B$. Now let $x \in B$. Then $x \in A$ since $A = B$. Therefore $B \subseteq A$.

($\Leftarrow$) We want to show, if $A \subseteq B$ and $B \subseteq A$ then $A = B$.

Direct Proof

Suppose $A \subseteq B$ and $B \subseteq A$. Then every element in A is in B and every element in B is in A. By definition, $A = B$. □

Problem 2.11. *Let A, B, and C be sets such that $A \in B$. Prove that if $B \subseteq C$ then $A \in C$.*

Operations on Sets

The *union* of two sets A and B, denoted by $A \cup B$, is the set containing elements from A or B. The *intersection* of two sets A and B, denoted by $A \cap B$, is the set of elements which are in A and B.

Example 2.12.

$$A = \{1, 2, 4, 6\} \quad B = \{1, 3, 5, 6\}$$

$$A \cap B = \{1, 6\} \quad A \cup B = \{1, 2, 3, 4, 5, 6\}$$

Problem 2.13. *Let $A = \{a, b, c\}$ and $B = \{A, b, 3\}$. Find $A \cup B$ and $A \cap B$.*

The union of multiple sets can be generalized in the following way.

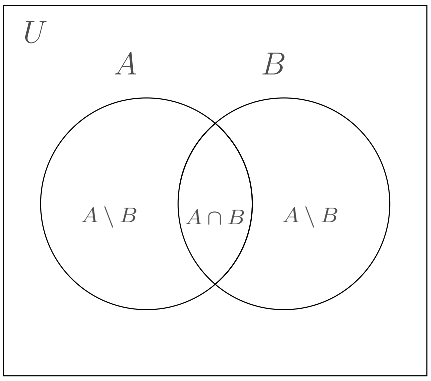
Notation

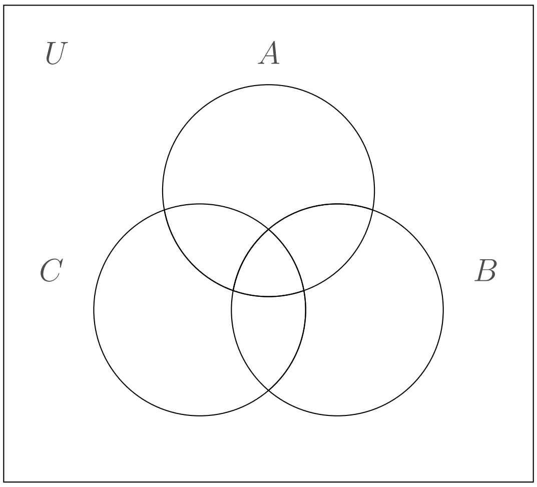
Union of n Sets	Intersection of n Sets
$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$	$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$

The *complement* of a set A with respect to the superset U, denoted by A^c, is the set containing all elements of U which are not in A.

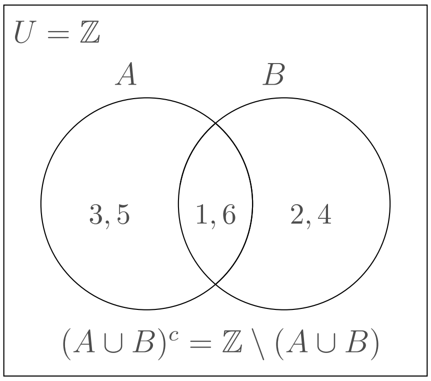
Venn Diagram

A *Venn diagram* is a diagram which shows the relationship between an element x in a set A with another set B.





Example 2.14. Consider the following set define in Example 2.12. The following Venn diagram show lists all elements from all set.



Problem 2.15. *Make a Venn diagram for the sets $A = \{1, 2, 3\}$, $B = \{1, 4, 5\}$, and $C = \{2, 5, 7\}$.*

The *Cartesian product* of the set A and B, denoted by $A \times B$, is the set

$$\{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Note that the Cartesian product of two sets is a set of order pairs. Hence $(a, b) \in A \times B$ does not imply that $(b, a) \in A \times B$. Also,

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}} = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A\,, i \in \{1, 2, \ldots, n\}\}.$$

Example 2.16. Consider the sets $A = \{1, 2\}$ and $B = \{x, y, z\}$. Then the Cartesian product $A \times B$ is

$$\{(1, x), (1, y), (1, z), (2, x), (2, y)(2, z)\}$$

and

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

Problem 2.17. *Let A and B be the sets defined in Example 2.16. Find $B \times A$ and B^2.*

Theorem 2.18. *For any sets A and B,*

$$(A \cup B)^c = A^c \cap B^c$$

Proof. We want to show that $(A \cup B)^c \subseteq A^c \cap B^c$ and $A^c \cap B^c \subseteq (A \cup B)^c$.

1. $(A \cup B)^c \subseteq A^c \cap B^c$

Let $x \in (A \cup B)^c$. Then $x \notin A$ and $x \notin B$. Hence $x \in A^c$ and $x \in B^c$. Thus $x \in A^c \cap B^c$. Therefore $(A \cup B)^c \subseteq A^c \cap B^c$.

Notice that this proof is nice and boring but it gets the job done.

2. $A^c \cap B^c \subseteq (A \cup B)^c$

Let $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$ which implies $x \notin A$ and $x \notin \cap B$. Hence $x \notin A \cap B$ and it follows that $x \in (A \cap B)^c$. Therefore $A^c \cap B^c \subseteq (A \cup B)^c$.

This proof has a little more flavor than the former but it is still kept simple.

□

Problem 2.19. *Prove that for any set A and B, $(A \cap B)^c = A^c \cup B^c$.*

Chapter 3

Functions

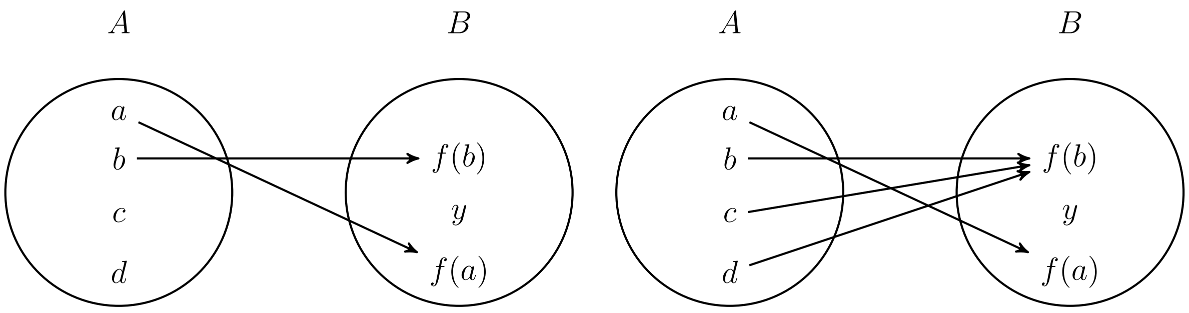
Basic Terminology

Let A and B be sets. A *binary relation* from A to B is a subset of $A \times B$. A *function* (or *map*) from a set A to a set B is a binary relation, called f, from A to B with the property that

$$\forall a \in A \text{ there is exactly one } b \in B \text{ such that } (a, b) \in A \times B.$$

Write $f : A \to B$ to indication that the function f is being mapped from the set A to the set B. This notation should not be used if f is not a function. Write $f : a \mapsto b$ whenever $f(a) = b$.

The following diagram show a relation R which is not a function from A to B since all elements in A are not being mapped to B. Whereas, the relation f is a function from A to B even though multiple elements of A are being mapped to $f(b)$.



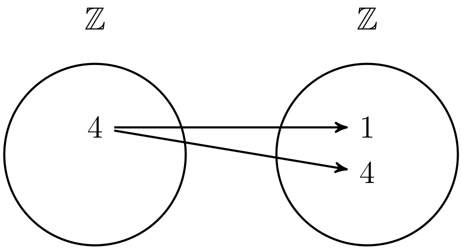
Relation and not a function

$R = \{(a, f(a)), (b, f(b)\}$

Relation and a function

$f = \{(a, f(a)), (b, f(b), (b, f(b), (b, f(b)\}$

Example 3.1. The set $\{(a, b) \mid a, b \in \mathbb{N}, a/b \in \mathbb{Z}\}$ is a binary relation from $\mathbb{N}$ to $\mathbb{N}$.



Note that the binary relation in Example 3.1 is not a function since both $(4,1),(4,4)$ are in the relation.

Example 3.2. The set $\{(x_1,x_2)\,|\,x_1,x_2 \in \mathbb{Z}, x_1^2 = x_2\} = f$ is a function. The function f could also be represented by $f(x) = x^2$ for $x \in \mathbb{Z}$.

Problem 3.3. *Let $A = \{1,2,3\}$ and $B = \{a,b,c,d\}$. Give an example of a relation from A to B containing exactly three elements such that the relation is not a function from A to B.*

Let f be a function from A to B.

1. The *domain* of f is A which is denoted by $\operatorname{dom} f$.

2. The *range* of f, denoted by $\operatorname{rng} f$, is the set
$$\{b \in B\,|\,f(a) = b \text{ for some } a \in A\}.$$
Note that $\operatorname{rng} f$ may not contain all elements of B.

3. The function f is *one-to-one* if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$. Equivalently, f is one-to-one if $f(x_1) = f(x_2)$ then $x_1 = x_2$.

4. The function f is *onto* if $\operatorname{rng} f = B$. In other words, $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

5. The function f is *bijective* if it is one-to-one and onto. The function is also called a *bijection.*

Example 3.4. The domain of the function $\{(x_1,x_2)\,|\,x_1,x_2 \in \mathbb{Z}, x_1^2 = x_2\}$ is $\mathbb{Z}$. The range of f is $\{x^2\,|\,x \in \mathbb{Z}\}$. Since $\operatorname{rng} f \neq \mathbb{Z}$ the function f is not onto. It is left a problem to show that f is one-to-one.

Problem 3.5. *Let $A = \{a,b,c,d\}$ and $B = \{x,y,z\}$. Then $f\{(a,y),(b,z),(c,y),(d,z)\}$ is a function from A to B. Determine $\operatorname{dom} f$ and $\operatorname{rng} f$.*

Problem 3.6. *Let $A = \{w,x,y,z\}$ and $B = \{r,s,t\}$. Give an example of a function $f : A \to B$ that is neither one-to-one nor onto.*

Theorem 3.7. *Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined as $f(x) = 3x^3 - x$.*

1. *The function f is one-to-one.*
2. *The function f is not bijective.*

Proof. 1. Proof by Contradiction

We want to show that f is not one-to-one is false.

Let $x_1, x_2 \in \mathbb{Z}$ such that $x_1 \neq x_2$. Suppose $f(x_1) = f(x_2)$. Then

$$\begin{aligned} 3x_1^3 - x_1 = 3x_2^3 - x_2 &\Rightarrow 3x_1^3 - 3x_2^3 = x_1 - x_2 \\ &\Rightarrow 3(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = x_1 - x_2 \\ &\Rightarrow x_1^2 + x_1x_2 + x_2^2 = \frac{1}{3}. \end{aligned}$$

However, this contradicts that $x_1^2 + x_1x_2 + x_2^2 \in \mathbb{Z}$ which must be the case since $x_1, x_2 \in \mathbb{Z}$. Therefore, f is one-to-one.

2. Direct Proof

We want to show that f is not onto which implies that f is not bijective.

Since $x \in \mathbb{Z}$, $3x^3$ and x are of the same parity. Hence $3x^3 - x$ is always even. Thus there does not exists $x \in \mathbb{Z}$ such that $f(x) = 1$. This shows that f is not onto. Therefore f is not bijective.

□

Problem 3.8. *Show that the function $\{(x_1, x_2) \mid x_1, x_2 \in \mathbb{N}, x_1^2 = x_2\}$ is one-to-one.*

The *absolute value of* x, denoted by $|x|$, is x if $x \geq 0$ and $-x$ otherwise. The *floor of* x, denoted by $\lfloor x \rfloor$, is the greatest integer less than or equal to x. The *ceiling of* x, denoted by $\lceil x \rceil$, is the least integer greater than or equal to x

Example 3.9. It is the case that $|-3| = 3 = |3|$, $\lfloor 2.3 \rfloor = 2$, and $\lceil \pi \rceil = 4$.

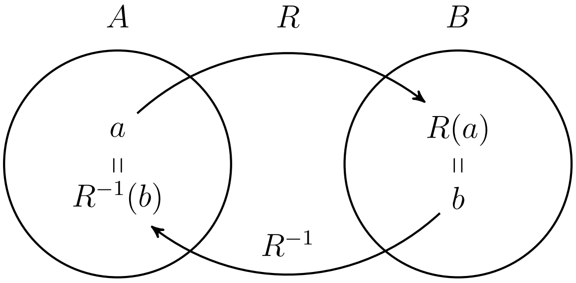
Inverse and Composition

Inverse Relations

Let R be a relation from the set A to the B. The *inverse relation*, denoted by R^{-1}, from B to A is the set

$$\{(b, a) \mid (a, b) \in R\} \subseteq B \times A.$$

Inverse Relation



Example 3.10. Let $R = \{(a,1),(a,3),(c,2),(c,3),(d,1)\}$ be a function from A to B. Then the inverse relation of R is $R^{-1} = \{(1,a),(3,a),(2,c),(3,c),(1,d)\}$.

In Example 3.10, the inverse relation is not a function from B to A because the element 3 gets mapped to two distinct elements, namely a and c. This leads to the question of when is the inverse relation a function from B to A.

Proposition 3.11. *Let $f : A \to B$. Then the inverse relation f^{-1} is a function from B to A if and only if f is a bijection.*

Proof. We want to show f^{-1} is a function from B to A if and only if f is a bijection(one-to-one and onto).

($\Rightarrow$) Assume f^{-1} is a function from B to A.

One-to-one, Proof by Contradiction

Suppose $x_1, x_2 \in A$, $x_1 \neq x_2$, and $f(x_1) = f(x_1)$. Let $f(x_1) = b_1$ and $f(x_2) = b_2$. Then $(x_1, b_1), (x_2, b_2) \in f$ and $b_1 = b_2$. So $(b_1, x_1), (b_2, x_2) \in f^{-1}$ which implies $(b_1, x_1), (b_2, x_2) \in f^{-1}$ since $b_1 = b_2$. This contradicts that f^{-1} is a function. Therefore f is one-to-one.

Onto, Direct Proof

Since f^{-1} is a function from B to A, $\forall b \in B$ there exists $a \in A$ such that $(b,a) \in f^{-1}$. Since f^{-1} is the inverse relation of f it is the case that $(a,b) \in f$. Hence $\forall b \in B$ there exists $a \in A$ such that $(a,b) \in f$ which implies that f is onto.

This shows that f is bijective.

($\Leftarrow$) Assume f is bijective.

The inverse relation maps B to A.

Since f is onto, for every $b \in B$ there exists $a \in A$ such that $(a,b) \in f$. Hence, for every $b \in B$ there exists $a \in A$ such that $(b,a) \in f^{-1}$. Therefore f^{-1} maps B to A.

The inverse relation of f is a function, Proof by Contradiction

Suppose $(b, y_1), (b, y_2) \in f^{-1}$ where $y_1 \neq y_2$. Then $(y_1, b), (y_2, b) \in f$. However this contradicts that f is one-to-one.

□

The inverse relation f^{-1} is called the *inverse of f* if f is a bijection. Hence an inverse of a function is an inverse relation but an inverse relation need not be an inverse. Also, f^{-1} should not be confused with $\frac{1}{f}$.

In each step of the proof we start with the definitions of the variables in the hypothesis. Then we create implications assuming the original hypothesis is true to show that the conclusion must be true.

Composition

Let $f : A \to B$ and $g : B \to C$. The function $g \circ f$ from A to C is the composition of g and f. The function is defined in the following way, $(g \circ f)(a) = g(f(a))$ where $a \in A$.

Problem 3.12. *Using the definition of function composition, verify that $g \circ f$ is a function from A to C.*

Example 3.13. Let $f = \{(1, a), (2, b), (3, c)\}$ and $g = \{(a, x), (b, y), (c, z)\}$. Then $g \circ f = \{(1, x), (2, y), (3, z)\}$.

Problem 3.14. *Let $A = \{1, 2, 3, 4\}, B = \{a, b, c, d\}$ and $C = \{r, s, t, u, v\}$ and define the functions $f : A \to B$ and $g : B \to C$ by*

$$f = \{(1, b), (2, d), (3, a), (4, a)\} \text{ and } g = \{(a, u), (b, r), (c, r), (d, s)\}.$$

Determine $g \circ f$ and $(g \circ f)(1)$.

Theorem 3.15. *The functions $f : A \to B$ and $g : B \to A$ are inverses of each other if and only if*

$$(g \circ f)(a) = a \text{ and } (f \circ g)(b) = b$$

for all $a \in A$ and for all $b \in B$.

One-to-One Correspondence and the Cardinality of Sets

A *one-to-one correspondence* is a function that is both one-to-one and onto. Sets A and B have the *same cardinality* if and only if there exists a one-to-one correspondence from A to

B. This is denoted by $|A| = |B|$. The *cardinality* of a set A, denoted by $|A|$, is the number of elements in A.

If $|A|$ is a natural number then A is a finite set. Otherwise A in an infinite set.

Example 3.16. Let $A = \{1, 2\}$ and $B = \{a, b\}$. Then $f = \{(1, a), (2, b)\}$ is a one-to-one correspondence from the set A to B. This shows that $|A| = |B|$.

In Example 3.16, counting the number of elements in B is easy. However, it is possible to determine the number of elements in B by counting the number of elements in A. This is the case since there is an one-to-one correspondence from A to B. In the next example it might not seem obvious that the two set have the same cardinality.

Example 3.17. Consider the two set $\mathbb{N}$ and $\mathbb{N} \cup \{0\}$. Define the function f to be a function from $\mathbb{N}$ to $\mathbb{N}$ such that $f : a \mapsto a - 1$. Then f^{-1} defined by $f^{-1} : a \mapsto a + 1$ is a function from $\mathbb{N} \to \mathbb{N} \cup \{0\}$. Therefore f is a bijection which implies that f is one-to-one correspondence from $\mathbb{N} \to \mathbb{N} \cup \{0\}$. This shows that $|\mathbb{N}| = |\mathbb{N} \cup \{0\}|$.

Theorem 3.18. *Let X, Y, and Z be sets. Then $|(X \times Y) \times Z| = |X \times (Y \times Z)|$.*

Problem 3.19. *Suppose f is a one-to-one and onto function from $\mathbb{N} \to \mathbb{Z}$. Prove that the function g from $\mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{Z}$ defined by $g : (m, n) \mapsto (m, f(n))$ is one-to-one and onto.*

Chapter 4

Integers

The Division Algorithm

Let $\emptyset \neq A \subseteq \mathbb{R}$ and $x \in A$. Then x is the *least element* of A if $x \leq b$, for all $b \in A$.

Let $S \subseteq A$ where $S \neq \emptyset$. Then A is *well-ordered* if every S has a least element.

(Well-Ordering Principle) The set of natural numbers is well-ordered. In other words, any nonempty subset of $\mathbb{N}$ contains a least element.

Lemma 4.1. *Let $a, b \in \mathbb{N}$. Then there are unique nonnegative integers q and r with $0 \leq r < b$ such that*

$$a = qb + r.$$

Example 4.2. Consider the integers 11 and 5. Then $11 = 2(5) + 1$. Here $a = 11$, $b = 5$, $q = 2$, and $r = 1$. Notice that $0 \leq r < b$.

Problem 4.3. *Find integers q and r as in Lemma 4.1 for the integers $a = 51$ and $b = 7$.*

Proof. (Proof of Lemma 4.1)

Proof of existence

Let $a, b \in \mathbb{N}$. Consider the set

$$B = \{kb \,|\, k \in \{0, 1, 2, \dots\}\}.$$

Then $B \subseteq \mathbb{N}$. Also $0 \in B$ so $\emptyset \neq B$. Moreover, there exists $q \in \mathbb{Z}$ such that $qb \in B$ and $a < qb$ since $a < (a + 1)b \in B$. Let

$$C = \{q \in \mathbb{Z} \,|\, a < qb\}.$$

Then $a + 1 \in C$. Since $C \neq \emptyset$ and $C \subseteq \mathbb{Z}$ it follows that C has a least element, say $q_0 + 1$ by the Well-ordering principle. Hence

$$\begin{aligned} q_0 b \leq a < (q_0 + 1)b &\Rightarrow q_0 b \leq a < q_0 b + b \\ &\Rightarrow 0 \leq a - q_0 b < b. \end{aligned}$$

By letting $r = a - q_0 b$ we get that $a = q_0 b + r$ and $0 \leq r < b$ as desired.

Proof of Uniqueness

Assume $a = q_1 b + r_1$ and $a = q_2 b + r_2$ where $0 \leq r_1, r_2 < b$. Then $q_1 b + r_1 = q_2 b + r_2$ which implies $(q_1 - q_2)b = r_2 - r_1$. Since $r_2 - r_1$ is a multiple of b and $r_2 - r_1 < b$ it must be the case that $r_2 - r_1 = 0$ which implies $q_1 - q_2 = 0$. Therefore $r_1 = r_2$ and $q_1 = q_2$.

□

Lemma 4.1 can be extended to all integers as in Problem 4.4. In both cases, a common mistake made when finding q and r it to pick r to be negative. This happens exactly when the q chosen is too large. If the q chosen is too small then the r will be too large.

Problem 4.4 (The Division Algorithm). *Let $a, b \in \mathbb{Z}, b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$ such that $a = qb + r$.*

Hint: Try using proof by cases.

Case 1: $a = 0, b \neq 0$.

Case 2: $a, b > 0$.

Case 3: $a > 0, b < 0$.

Case 4: $a < 0, b > 0$.

Case 5: $a < 0, b < 0$.

It is worth noting that some books label Lemma 4.1 as the Division Algorithm. In the Division Algorithm q is the *quotient* and r is the *remainder* when a is divided by b.

Example 4.5. Find integers q and r, with $0 \leq r < 20$ such that $2,345 = -20q + r$.

Divisibility and Euclidean Algorithm

Let a and b be integers such that $b \neq 0$. The a is *divisible* by b, denoted $b \mid a$, if and only if there exists integer k such that $a = bk$. In this case, b *divides* a.

Example 4.6. The integer 24 is divisible by 4 since 24 can be written as 4(6).

Example 4.7. Let $a \in \mathbb{Z}$ such that $a \neq 0$. Then $a^2 \mid a^5$ since $a^5 = a^2(a^3)$.

Theorem 4.8. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$, then $a \mid (-b)$ and $(-a) \mid b$.*

Proof. Suppose that $a \mid b$. By definition, there is an integer k such than $b = ak$. Hence $b = a(-1)(-k)$. Dividing by side by -1 gives $-b = a(-k)$. Therefore $a \mid -b$.

Now suppose $a \mid b$. Then for some integer k it is the case that $b = ak$. Hence $b = (-a)(-k)$. Therefore $b \mid -a$. □

Theorem 4.9. *For every integer n, $3|(n^3 - n)$.*

First note that $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. Since $n-1$, n, and $n+1$ are consecutive integers 3 must divide one of them.

Proof. By the Division Algorithm, $n = 3q + r$ where $0 \leq r < 3$. Hence $r \in \{0, 1, 2\}$. If $r = 0$ then we are done. If $r = 1$ then $n - 1 = 3q$. This shows that $3 \mid n - 1$. Similarly if $r = 2$, then $n + 1 = 3q$ which shows that $3 \mid n + 1$. □

Problem 4.10. *Suppose a, b, and c are integers such that $c \mid a$ and $c \mid b$. Show that $c \mid (ax + yb)$ for any integers x and y.*

Let $a, b \in \mathbb{Z}$ with $b \neq 0$ The *greatest common divisor*, denoted by $\gcd(a, b)$, is the largest common divisor of a and b.

Problem 4.11. *What is the greatest common divisor of* 4 *and* 16*?*

Example 4.12. The greatest common divisor of 4 and 16 is 4, since $4 \mid 4$, $4 \mid 16$, and if $c \mid 4$ and $c \mid 16$ then $c \leq 4$. Hence $\gcd(4, 16) = 4$.

Problem 4.13. *What is the greatest common divisor of* 70 *and* 42*?*

Theorem 4.14. *Euclidean Algorithm Let a and b be natural numbers with $b < a$. To find the greatest common divisor of a and b, write*

$$a = q_1 b + r_1 \qquad \textit{with} \qquad 0 < r_1 < b$$

then $b = q_2 r_1 + r_2$ and repeat until $r_{k+1} = 0$. Then $r_k = \gcd(a, b)$.

Note that the Euclidean Algorithm uses the Division Algorithm.

Example 4.15. Find $\gcd(630, 196)$. Using the Euclidean Algorithm we get

$$\begin{aligned} 630 &= 3(196) + 42 \\ 196 &= 4(42) + 28 \\ 42 &= 1(28) + 14 \\ 28 &= 2(14) + 0. \end{aligned}$$

Problem 4.16. *Use the Euclidean Algorithm to find the greatest common divisor of* 70 *and* 42*.*

If the greatest common divisor of a and b is 1, then a and b are *relatively prime.*

Theorem 4.17. *Let $a, b \in \mathbb{Z}$. Then there exists integers m and n such that* $\gcd(a, b) = ma + nb$*.*

Example 4.18. Find m and n such that $630m + 196n = \gcd(630, 196)$. In Example 4.15 it was shown that $\gcd(630, 196) = 14$. Hence,

$$\begin{aligned} 630 &= 3(196) + 42 \\ 196 &= 4(42) + 28 \\ 42 &= 1(28) + 14 \\ 28 &= 2(14) + 0. \end{aligned}$$

Rewriting the previous equations we get,

$$\begin{aligned} 630 - 3(196) &= 42 \\ 196 - 4(42) &= 28 \\ 42 - 1(28) &= 14. \end{aligned}$$

Now use backwards substitution to get,

$$\begin{aligned} 42 - 1(196 - 4(42)) &= 14 && \text{plug in expression} \\ 5(42) - 1(196) &= 14 && \text{simplify} \\ 5(630 - 3(196)) - 1(196) &= 14 && \text{plug in expression} \\ 5(630) - 4(196) &= 14 && \text{simplify} \end{aligned}$$

Therefore $m = 5$ and $n = -4$. It is important to write $m = 5$ and not -4 and $n = -4$ and not $n = 4$.

Problem 4.19. *Find integers m and n such that $-19m + 119n = 1$.*

Prime Numbers

A natural number $a > 1$ is prime if the only numbers which divides a are 1 and a. So a is prime if $a \mid a$, $1 \mid a$, and if $c \mid a$ then $c = a$ or $c = 1$. The integer a is said to be composite if a is not prime. Hence there exists a positive integer $c \neq a$ and $c \neq 1$ such that $c \mid a$

Lemma 4.20. *Given any natural number $n > 1$, there exists a prime p such that $p \mid n$.*

Proof. Proof by contradiction

Suppose there is no prime which divides n. Let C be the set of integers greater than 1 which are not divisible by a prime number. Since $n \in C$ we know that C is not the empty set. Hence by the Well Order Principle, C has a least element, say k. Now, k can not be prime because $k \mid k$ and $k \in C$. Since k is not prime there exist a such that $1 < a < k$ and $a \mid k$. If there exists a prime, p that divides a then $p \mid k$ as $a \mid k$. Otherwise $a \in C$ which contradicts that m is the least element in C.

□

Theorem 4.21. *There are an infinite number of primes.*

Proof. Proof by contradiction

Assume that there are an finite number of primes, say $p_1, p_2, \ldots, p_k$. Consider the integer $n = (p_1 p_2 \cdots p_k) + 1$. By Lemma 4.20 there exists a prime $p_i \in \{p_1, p_2, \ldots, p_k\}$ which divides n. Moreover $p_i \mid p_1, p_2, \ldots, p_k$ which implies that $p_i \mid n - p_1 p_2 \cdots p_k = 1$. This means $p_i = 1$ which contradicts that p_i is prime.

□

Theorem 4.22. *Every integer n greater than 1 can be written as*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$$

where p_i are distinct primes and k_i are integers.

In Theorem 4.22 $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$ is the *prime factorization/decomposition* of n.

Example 4.23. Write the factorization of 2088. To write prime factorization of 2088 find small prime which divide it and write the number. Since $2 \mid 2088$ we have $2088 = 2 \cdot 1044$. Similarly, $2 \mid 1044$ which implies $2088 = 2 \cdot 2 \cdot 522 = 2^2 \cdot 522$. Continuing this process we get

$$\begin{aligned} 2088 &= 2^2 \cdot 522 \\ &= 2^3 \cdot 261 \\ &= 2^3 \cdot 3 \cdot 87 \\ &= 2^3 \cdot 3^2 \cdot 29. \end{aligned}$$

Since $2, 3, 29$ are all prime we know that $2^3 \cdot 3^2 \cdot 29^1$ is the prime factorization 2088.

Problem 4.24. *Write the prime factorization of* 127*.*

Problem 4.25. *Let x, a and b be integers such that $x \mid ab$. If x and a are relatively prime prove that $x \mid b$.*

Congruence

Let $n \in \mathbb{N} \setminus \{1\}$ and $a \in \mathbb{Z}$. Then a modulo n, denoted by $a \bmod n$, is r such that

$$a = nq + r$$

where $0 \leq r < n$ and $q \in \mathbb{Z}$.

Example 4.26. $49 \bmod 7 = 0$ since $49 = 7(7) + 0$.

Problem 4.27. *Determine* $63 \bmod 6$*.*

The integers a and b are congruent modulo n, denoted by $a \equiv b \bmod n$, if and only if $a - nq_1 = b - nq_2 = r$ where $r, q_1, q_2 \in \mathbb{Z}$ and $r < n$. In other words, $a \equiv b \bmod n$ if and only if $n \mid a - b$. To see that the definitions are equivalent let us use the Division Algorithm to write $a = nq_a + r_a$ and $b = nq_b + r_b$ where $0 \leq r_a, r_b < n$. Since $n \mid (a - b)$ implies there exists $q \in \mathbb{Z}$ such that $a - b = nq$ we have

$$\begin{aligned} n|(a-b) &\Rightarrow a - b = nq \\ &\Rightarrow a = nq + b \\ &\Rightarrow a = nq + nq_b + r_b \quad \text{where} \quad 0 \leq r_b < n \\ &\Rightarrow a = n(q + q_b) + r_b \quad \text{where} \quad 0 \leq r_b < n. \end{aligned}$$

Therefore $r_b = r_a$ as desired. For the converse, $a - nq_1 = b - nq_2$ implies $a - b = n(q_1 - q_2)$ and it follows that $n \mid a - b$.

Example 4.28. Determine if 6 is congruent to 2 modulo 4. First note that $6 = 1(4) + 2$ and $4 = 1(2) + 2$. Hence $6 \equiv 2 \bmod 4$.

Theorem 4.29. *If $a \equiv b \mod n$ and $c \equiv d \bmod n$ then $a + c \equiv b + d \mod n$.*

Proof. Suppose $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then $n \mid a - b$ and $n \mid c - d$. Hence there exists k and ℓ such that $a - b = nk$ and $c - d = n\ell$. Thus $(a + c) - (b + d) = n(k + \ell)$ which implies $a + c \equiv b + d \bmod n$. □

Problem 4.30. *Show that if $a \equiv b \mod n$ and $c \equiv d \bmod n$ then $ac \equiv bd \mod n$.*

The converse of Problem 4.30 need not be true. For example, $4 \cdot 7 \equiv 2 \cdot 2 \bmod 12$. However 7 is not congruent to 2 modulo 12.

Theorem 4.31. *Let $a, b \in \mathbb{Z}$. Then $a \equiv b \bmod 3$ if and only if $2a + b \equiv 0 \bmod 3$.*

Proof. Suppose $a \equiv b \bmod 3$. Then there exists $k \in \mathbb{Z}$ such that $(a - b) = 3k$ which implies $2(a-b) = 6k$. Moreover, $2a - 2b + 3b = 6k + 3b$ which implies $2a + b = 6k + 3b = 3(2k + b)$. It follows that $2a + b \equiv 0 \bmod 3$. Conversely, suppose $2a + b \equiv 0 \bmod 3$. Then there exists $k \in \mathbb{Z}$ such that $2a + b = 3k$. Hence $b = 3k - 2a$. Now

$$a - b = a - (3k - 2a) = 3a - 3k = 3(a - k).$$

Therefore $a \equiv b \bmod 3$. □

Theorem 4.32. *(Fermat's Little Theorem) Let p be a prime and $c \in \mathbb{Z}$. If c is not divisible by p then $c^p \equiv c \bmod p$.*

Problem 4.33. *Determine $5^{17} \bmod 17$.*

Chapter 5

Mathematical Induction

Mathematical Induction

Proposition 5.1. *Prove that for any integer $n \geq 1$ the sum of the odd integers from 1 to $2n-1$ is n^2.*

Proposition 5.1 is an example of a statement that can be proved using Mathematical Induction. Mathematical Induction is used to prove a statement is true for an infinite list of consecutive integers which contains a least element.

Theorem 5.2. *(Principle of Mathematical Induction)*

Given a statement $P(n)$ concerning the integer n, suppose

(1) $P(n_0)$ is a true statement for some integer n_0, and

(2) if k is an arbitrary integer greater than n_0 and $P(k)$ is true, then $P(k+1)$ is true.

Then the statement $P(n)$ is true for all integers n such that $n_0 \leq n$.

Proof. Proof of Proposition 5.1

Proof by induction on n

Base step:

For $n = 1$, $2n-1 = 2(1)-1 = 1$. The sum of odd integers from 1 to 1 is 1. Also $n^2 = 1^2 = 1$. Therefore the statement is true for $n = 1$.

Induction step:

Assume that the statement is true for some integer $k > 1$. Then $1 + 3 + \cdots + 2k - 1 = k^2$. Now,

$$\begin{aligned} 1 + 3 + \cdots + (2(k+1) - 1) &= [1 + 3 + \cdots + (2k+1)] + (2(k+1) - 1) \\ &= k^2 + 2(k+1) - 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2. \end{aligned}$$

Therefore by the Principle of Mathematical Induction the statement is true. □

Proof. Proof of Theorem 5.2

Proof by contradiction

Suppose (1) and (2) are true and $P(n)$ is false for some positive integer. Let $Q = \{t \mid P(t) \text{ is false }\}$. We can assume $Q \neq \emptyset$ and $1 \notin Q$. Since $Q \subseteq \mathbb{N}$, Q contains a least element k. Hence $1, 2, \ldots, k \notin Q$ which implies $P(1), \ldots, P(k-1)$ are true. Thus by assumption $P(k)$ is true for arbitrary k. This contradicts that $k \in Q$. □

Theorem 5.3. *Principle of Mathematical Induction implies the Well Ordering Principle.*

Proof. Let P be an nonempty subset of natural numbers. Suppose P has no least element. Let Q be the set of elements of $\mathbb{N}$ which are not in P. Then $1, 2, \ldots, k, k+1 \in Q$ for an arbitrary $k \in \mathbb{N}$.

Base Step: $1 \in Q$.

Induction Step: Assume $1, 2, \ldots, k \in Q$. If $k + 1 \in P$ then $k + 1$ is a least element. Hence $k + 1 \in Q$. By the Principle of Mathematical Induction $\mathbb{N} \subseteq Q$. This contradicts that $P \neq \emptyset$. □

The summation of the statement $P(i)$ from k to n, denoted by $\sum\limits_{i=k}^{n} P(i)$, is

$$P(k) + P(k+1) + P(k+2) + \cdots + P(k+n).$$

Example 5.4. Let $P(i) = 2^i$. Then $\sum\limits_{i=1}^{4} P(i) = \sum\limits_{i=1}^{4} 2^i = 2^1 + 2^2 + 2^3 + 2^4$.

Problem 5.5. *Compute* $\sum\limits_{i=0}^{3} 2i + 1$ *and* $\sum\limits_{i=0}^{3} 1$.

Problem 5.6. *Prove that* $\sum_{i=1}^{n}(i+1)2^i = n2^{n+1}$ *for* $n \in \mathbb{N}$.