MHF3203
Notes

Oliver Deng

April 9, 2025

Contents

0.1 Introduction

The point of this class is to set a unified way of writing "stuff." In a sense, it is the grammar class of mathematics.

Chapter 1

Sets

1.1 Introduction to Sets

Definition 1.1.1: Sets

Sets are collections of "things" or "**elements**." For example,

$$\{1, 2, 3, 4\}$$

is a set, which is different from

$$\{\{1\}, 2, 3, 4\}$$

Note

The curly braces specify that it is a set.

Note

Sets are typically denoted by capital letters, like A.

We can say that an element is or isn't part of a set using the $\in$ or $\notin$ symbols.

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$
$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
$$\mathbb{Q} = \{x : x = \frac{m}{n}, m, n \in \mathbb{Z}, n \neq 0\}$$
$$\mathbb{R} = \text{Real numbers}$$

Note

In this course, the natural numbers do NOT include 0.

Note

Your first instinct when given a definition should be to break it.

Definition 1.1.2: Set-Builder Notation

$$\{x : \text{Properties of } x\}$$

For example,

$$\{x : x \in \mathbb{Z}, |x| < 2\}$$

This is going to be the most rigorous way of writing a set.

Definition 1.1.3: Cardinality

The cardinality of a set is notated by $|A|$ or $\text{card}(A)$, which is the number of elements in a finite set.

Definition 1.1.4: Empty Set

This is the set with nothing in it:

$$\{\} = \varnothing$$

Note

$$|\varnothing| = 0$$
$$\varnothing \neq 0$$
$$\{\varnothing\} = \{\{\}\}$$

1.2 The Cartesian Product

Definition 1.2.1: Ordered Pairs

$$(x, y)$$

for x and y. This can be extended to any n-tuple.

Definition 1.2.2: Cartesian Product

Let A, B be sets. Then the Cartesian Product

$$A \times B := \{(x, y) : x \in A, y \in B\}$$

Note

The $:=$ operator indicates a definition, not just equality.

Note

$A \times B$ does not necessarily equal $B \times A$.

For bigger tuples, we just extend this definition.

$$A \times B \times C = \{(x, y, z) : x \in A, y \in B, z \in C\} \tag{1.2.1}$$

This raises a question:

$$X \times Y \stackrel{?}{=} A \times B \times C$$

where $X = A$ and $Y = B \times C$. We first look at

$$\begin{aligned}(X \times Y) &\stackrel{?}{=} A \times (B \times C)\\ A \times (B \times C) &= A \times \{(b, c) : b \in B, c \in C\}\\ &= \{(a, (b, c)) : a \in A, (b, c) \in B \times C\}\end{aligned}$$

which is equal. However, this is different from the definition in eq.(1.2.1), and thus they are not equal.

1.2.1 Cartesian Products with the Empty Set

Example 1.2.1 ($A = \{1,2\}, B = \{1,3\}$)

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

Note

$$A \neq \{(1,),(2,)\}$$

Basically, if there are no elements to take (since it's the empty set) you cannot create ordered pairs, and thus create the empty set again. Anything crossed with the empty set creates an empty set; this is what we call an **annihilator**.

Note

In a finite list, the order of elements in a set does not matter. In an infinite list, you have to consistently make clear what's in the set.

1.3 Subsets

Definition 1.3.1: Subsets

For sets A, B, if every element of B is also an element of A, we say B is a subset of A, and we denote that with

$$B \subseteq A$$

Also, if $A \neq B$, we say that B is a proper subset

$$B \subsetneq A \quad \text{or} \quad B \subset A$$

Example 1.3.1

$$\{1,2\} \subseteq \{1,2,3\}$$
$$\{1,2\} \subsetneq \{1,2,3\}$$
$$\{1,2,3\} \subseteq \{1,2,3\}$$
$$\{1,2,3\} \subset \{1,2,3\} \text{ IS WRONG}$$

Note

Going the other way, we have **supersets**, denoted by $\supset$.

Note

Given the set $\{\{1\}\}$, $\{1\} \in \{\{1\}\}$, but $\{1\} \not\subseteq \{\{1\}\}$.

Example 1.3.2 (Write the subsets of $\{1, \varnothing\}$)

$$\varnothing, \{1\}, \{\varnothing\}, \{1, \varnothing\}$$

1.4 Power Sets

In general, given a set A with n elements (i.e. $|A| = n$), then there are 2^n subsets.

Definition 1.4.1: Power Sets

Given a set A, then the set of all subsets possible subsets of A is called a power set of A, and is denoted by

$$\mathcal{P}(A)$$

Example 1.4.1

The power set of $\{1, 2\}$ is

$$\{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$$

Example 1.4.2

The standard Cartesian plane is $\mathbb{R}^2$. $\mathcal{P}(\mathbb{R}^2)$ gives the entire representation of anything on $\mathbb{R}^2$.

Note

The power sets of finite sets are typically easy to think about. The power sets of infinite sets, however, are much more complicated to think about.

1.5 Binary Operations On Sets

Definition 1.5.1: Binary Operations

These are operations that take in two things and return one.

Note

In math, when we say "or," we typically mean "or," not "xor."

Definition 1.5.2: Union

Let A, B be sets. We can write the union of A and B as

$$A \cup B := \{x : x \in A \textbf{ or } x \in B\}$$

Definition 1.5.3: Intersection

Let A, B be sets. We can write the intersection of A and B as

$$A \cap B := \{x : x \in A \textbf{ and } x \in B\}$$

Definition 1.5.4: Difference

$$A - B = \{x : x \in A, x \notin B\} = A \setminus B \text{ (using the "set minus" symbol)}$$

Example 1.5.1 ($A = \{1, 2, 3, 5, 8\}, B = \{2, 4, 6, 8\}$)

$$A \cup B = \{1, 2, 3, 4, 5, 6, 8\}$$
$$B \cup A = \{1, 2, 3, 4, 5, 6, 8\}$$
$$A \cap B = \{2, 8\}$$
$$B \cap A = \{2, 8\}$$
$$A \setminus B = \{1, 3, 5\}$$
$$B \setminus A = \{4, 6\}$$

Example 1.5.2 ($A = \{1, 2\}, B = \{2, 3\}, C = \{1, 3\}$)

$$A \cup B \cup C = \{1, 2, 3\}$$
$$A \cap B \cap C = \varnothing$$
$$A \cup B \cap C = \{1, 3\}*$$
$$A \cap B \cup C = \varnothing*$$

Note

*When looking at set operations, you must **always** have parentheses, since the operations do not actually have a hierarchy. So, in fact, the last two questions are **nonsense**.

1.6 Complements

Definition 1.6.1: Complement

The complement of a set A is the universal set U minus A, or

$$\overline{A} = A^c := U \setminus A$$

Note

The universal set should always be explicitly clear.

Example 1.6.1 ($U = \{x : x \in \mathbb{N}, x > 7\}$)

$$A = \{8\} \subsetneq U$$
$$\overline{A} = \{9, 10, 11, \ldots\} = \{x \in \mathbb{N} : x \geq 9\}$$

Note

$A = B$ as sets if $x \in A \iff x \in B$. That is, $A \subseteq B$ and $B \subseteq A$.

Example 1.6.2 ($A = \{1, 2\}$)

1. In $\mathbb{N}$, $\overline{A} = \{x \in \mathbb{N} : x \neq 1, x \neq 2\} = \{x \in \mathbb{N} : x > 2\}$
2. In $\mathbb{Z}$, $\overline{A} = \{x \in \mathbb{Z} : x \neq 1, x \neq 2\}$

3. In $\mathbb{R}$, $\overline{A} = \{x \in \mathbb{R} : x \neq 1, x \neq 2\} = (-\infty, 1) \cup (1, 2) \cup (2, \infty)$
4. In $\mathbb{Q}$, $\overline{A} = \{x \in \mathbb{Q} : x \neq 1, x \neq 2\} = \{x \in \mathbb{Q} : x \notin \{1, 2\}\}$

What is $\overline{U}$?

$$\overline{U} = U \setminus U = \varnothing$$

1.7 Venn Diagrams

Please tell me you know what a Venn diagram is.

Note

One thing of note is that if you want to represent the universal set, just draw a box around everything.

Note

Also, these are not considered rigorous.

1.8 Well-Ordering Principle

If a set and all of its subsets have a least element, it is well-ordered.

1.9 Indexed Sets

If we have a lot of sets $A_1, A_2, A_3, \ldots, A_N$, we can find the intersection or union via

$$\bigcup_{i=1}^{N} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_N := \{x : x \text{ is in } \textbf{at least} \text{ one } A_i\}$$

or

$$\bigcap_{i=1}^{N} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_N := \{x : x \text{ is in } \textbf{every } A_i\}$$

We can actually push this kind of notation. For example, we can have it go to infinity. But what if we wanted sets indexed with something like the prime numbers?

Example 1.9.1

Let P be the set of prime numbers. Then

$$\bigcup_{i \in P} A_i := A_2 \cup A_3 \cup A_5 \cup A_7 \cup \ldots$$

Note

Always be careful when your sets are indexed from an infinite set.

Example 1.9.2 (Let $A_n = [-\frac{1}{n}, \frac{1}{n}]$, which is also called a nesting sequence.)

$$\bigcup_{n\in\mathbb{Z}\setminus\{0\}} A_n = [-1, 1]$$
$$\bigcap_{n\in\mathbb{Z}\setminus\{0\}} A_n = \{0\}$$

Example 1.9.3 (Let $B_n = \bigcup_{k=1}^{\infty}[k - \frac{1}{n}, k + \frac{1}{n}]$.)

$$\bigcup_{n\in\mathbb{Z}\setminus\{0\}} B_n = \bigcup_{n=1}^{\infty}\left(\bigcup_{k=1}^{\infty}[k - \frac{1}{n}, k + \frac{1}{n}]\right) = [0, \infty)$$
$$\bigcap_{n\in\mathbb{Z}\setminus\{0\}} B_n = \bigcap_{n=1}^{\infty}\left(\bigcup_{k=1}^{\infty}[k - \frac{1}{n}, k + \frac{1}{n}]\right) = \mathbb{N}$$

Definition 1.9.1: Nesting Sequence

A decreasing nested sequence is where $A_n \subset A_{n+1}$.
An increasing nested sequence is where $A_n \supset A_{n+1}$

Chapter 2

Logic

Note

If you're using this as review, most of this has already been covered in COT3100 (Applications of Discrete Structures) at a less intense level, so most of these notes are usually more interesting things that we learn in lecture.

2.1 Statements

Definition 2.1.1: Statement

Something that can be described as correct or incorrect. The convention we use to denote statements are the capital letters P, Q, R, S.

Note

We do not necessarily know if the statement is actually true or not, which is called an open statement, but we do know that it really is one or the other.

2.2 And, Or, and Not

Definition 2.2.1: And

$\wedge$

Definition 2.2.2: Or

$\vee$

Definition 2.2.3: Not

$\neg$ or $\sim$

Example 2.2.1 (I have a cat and a dog, but not a turtle.)

Let $P =$ I have a cat. Let $Q =$ I have a dog. Let $R =$ I have a turtle.

Note

We can let $R =$ I don't have a turtle, but having negations in the statement makes everything annoyingly complicated.

This can be represented as

$$(P \wedge Q) \wedge (\neg R)$$

Note

$\neg$ is a unary operator, and $\wedge$ and $\vee$ are binary operators.

2.3 Truth Tables

You can create tables based on different cases for statements.

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

2.4 Conditionals and Biconditionals

Note

Division does not exist.

The conditional is, informally, the "if-then" statement. If we say we have P and Q as statements, we say that "P implies Q " (most of the time), and denote this with

$$P \implies Q$$

If P is a sufficient condition, then $P \implies Q$. If P is a necessary condition, then $Q \implies P$. If you have a necessary and sufficient condition, then we have the biconditional

$$P \iff Q$$

Note

When writing proofs, you must go **both ways**!

Note

(Almost) All definitions are (secretly) iff statements. Also, we can say that P and Q are **equivalent** (not equal).

2.4.1 DeMorgan's Laws

$$\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \iff (\wedge P) \vee (\wedge Q)$$

2.4.2 Distributive Law

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$$

2.4.3 Contrapositive

$$(P \implies Q) \iff ((\neg Q) \implies (\neg P))$$

Note

You **cannot** use the converse for proofs:

$$Q \implies P$$

2.5 Quantifiers

There are 2 approaches when considering a proposition about a set: either talk about the set as a whole, or talk about each individual element in the set. This is where quantifiers come in.

Definition 2.5.1: Universal Quantifier

"For all" or "for each" or "every":

$$\forall$$

This quantifier is more useful when considering properties of a set.

Note

This is the "default" implicit quantifier.

Definition 2.5.2: Existential Quantifier

"There exists" or "is/are" or "some":

$$\exists$$

This quantifier is more useful when considering specific examples or a "useful element."

Note

There's a subtext of "at least 1"

Note

Don't forget $\exists!$ for "there exists a **unique**"

2.5.1 Negating Quantifiers

$$\neg\forall x P(x) \iff \exists x \neg P(x)$$
$$\neg\exists x P(x) \iff \forall x \neg P(x)$$

2.5.2 Quantifier Order

$$\forall x \exists y \neq \exists x \forall y$$

Chapter 3

Proofs

3.1 Terms and Definitions

Definition 3.1.1: Definition

Precise and exact explanation in the mathematical use of a word.

Note

Definitions are in fact biconditionals, even though they are almost always written as conditionals.

Definition 3.1.2: Theorem

Theorems are conditional statements that are major results or are of some sort of universal interest.

Definition 3.1.3: Corollary

Consequences of a theorem.

Definition 3.1.4: Lemma

Used to prove something else.

Definition 3.1.5: Proposition

These are lesser versions of theorems. They are interesting in context.

Definition 3.1.6: Conjecture

Things we believe are true but are unable to prove.

Definition 3.1.7: Proof

Steps by which you actually demonstrate that something is true.

3.2 Proof by Direct Proof

Direct proof is this idea that we suppose P is true, do some work, and then conclude that Q **must** be true.

Example 3.2.1

Note

Do not beg the question! You cannot suppose that the conclusion is true and then say that the conclusion is true.

Proposition 3.2.1 Prove that 8 is an even number.

If we want to prove something obvious like this, which is a statement, then we need to consider that what we can suppose is what an even number is in the first place, and then show that 8 is one of those.

Proof: Suppose n is an even number if $\exists a \in \mathbb{Z}$ s.t. $n = 2a$.
Consider $n = 8$ and let $a = 4$.

Note

Use "consider" when we want to instantiate or generate an example. "Let" isn't a claim that something is true, but rather a hint that you will demonstrate something.

Notice, $a \in \mathbb{Z}$, and $8 = 2(4)$.
Hence 8 is an even number by the definition of even numbers.

Note

Be careful of saying "by definition" because it needs to literally be by definition.

Proposition 3.2.2 Prove that 8 is not an odd number.

Proof: Suppose n is odd if $\exists a \in \mathbb{Z}$ s.t. $n = 2a + 1$. 

We actually cannot prove this with a direct proof!

Note

In the $P \implies Q$ relationship, if P is always false, then the implication is **vacuously** true, and if Q is always true, then the implication is **trivially** true.

Example 3.2.2

Proposition 3.2.3 For any $n \in \mathbb{N}$, the value $5^{2n} - 1$ is divisible by 4.

Plugging in some starting values, we convince ourselves that this proposition is true.

Lemma 3.2.1 For any $n \in \mathbb{N}, 5^n - 1 = (1 + 5 + 5^2 + \ldots + 5^{n-1})(5 - 1)$

Proof: Fix $n \in \mathbb{N}$ arbitrarily (arbitrarily is unnecessary but useful in this case).

Note

This creates n and makes sure it doesn't vary, since it's considered variable unless we fix it.

Observe (or alternatively, "by a calculation"/"BaC"): $5(1+5+5^2+\ldots+5^{n-1}) = 5+5^2+\ldots+5^n$ and $-1(1 + 5 + 5^2 + \ldots + 5^{n-1}) = -1 - 5 - 5^2 - \ldots - 5^{n-1}$.
So by distribution, $(1+5+5^2+\ldots+5^{n-1})(5-1) = 5+5^2+\ldots+5^n-(1+5+5^2+\ldots+5^{n-1}) = 5^n - 1$.
By choice of n arbitrary our conclusion follows. ☺

Proof: Fix $n \in \mathbb{N}$.

Note

"ift" means "if follows that."

By lemma 3.2.1 we have

$$5^{2n} - 1 = (5^n - 1)(5^n + 1) = (1 + 5 + 5^2 + \ldots + 5^{n-1})(5 - 1)(5^n + 1) \tag{3.2.1}$$

Note

We don't **need** to justify the difference of squares step because it is a simple calculation, and only the lemma step needs to be justified. However, you **can** say it to ere on the side of caution.

Notice, since the product and sum of integers is an integer, there is $a \in \mathbb{Z}$ s.t. $a = (1 + 5 + 5^2 + \ldots + 5^{n-1})(1 + 5^n)$.
So by equation 3.2.1,

$$5^{2n} - 1 = (5 - 1)(1 + 5 + 5^2 + 5 \ldots + 5^{n-1})(1 + 5^n) = 4a.$$

Since $a \in \mathbb{Z}$, $5^{2n} - 1$ is divisible by 4 by definition. ☺

3.3 Proof By Cases

Example 3.3.1

Proposition 3.3.1 Product preserves parity.

Let $a, b \in \mathbb{Z}$.

Case 1: Suppose a, b are even.

Then there are integers n, m s.t. $a = 2n, b = 2m$.

Thus $ab = (2n)(2m) = 2(2nm)$.

So ab is even by definition.

Note

Within cases, it is best practice not to reuse variables.

Case 2: Suppose a, b are odd.

Then there exists $n_1, m_1 \in \mathbb{Z}$ s.t. $a = 2n_1 + 1, b = 2m_1 + 1$.

So $(ab) = (2n_1 + 1)(2m_1 + 1) = 4n_1m_1 + 2n_1 + 2m_1 + 1 = 2(2n_1m_1 + n_1 + m_1) + 1$.

Since $2n_1m_1 + n_1 + m_1 \in \mathbb{Z}$ by product and sum of integers, ab is odd by definition.

Case 3: Without loss of generality (WLOG), suppose a is even and b is odd.

(The rest of this case is similar to the previous ones, and for the sake of time was not finished.)

Note

Using WLOG is often wrong! Most mathematical papers also don't use it.

Case 4: An alternative to using WLOG is to say this: "Case 4 is similar to case 3."

3.4 Proof by Contrapositive

$$\neg Q \implies \neg P$$

Example 3.4.1

Proposition 3.4.1

Let $p \in \mathbb{Z}$ be prime, and $a, b, \in \mathbb{Z}$.
If $p \nmid ab$, then $p \nmid a$ and $p \nmid b$.

Proof: Suppose by way of contrapositive that $p \mid a$ or $p \mid b$.

Case 1: $p \mid a$

Suppose there exists $c \in \mathbb{Z}$ s.t. $a = cp$.

So $ab = cpb = (cb)p$.

Notice $(cb) \in \mathbb{Z}$.

So $p \mid ab$ by the definition of p divides ab.

Case 2: $p \mid b$

By switching a and b, case 2 is similar to case 1 (or you can say "case 2 follows by case 1").

Since cases 1 and 2 are exhaustive, $p \mid ab$. 😊

Definition 3.4.1: Congruence of Integers

Let $a, b, n \in \mathbb{Z}$. We say "a is congruent modulo n to b" or "a is equal to b mod n" or "a is congruent to b, modulo n" if $\exists m \in \mathbb{Z}$ s.t. $(a - b) = nm$, i.e. $a = b + nm$. We denote this by $a \equiv b \pmod{n}$ or by $a \equiv_n b$.

Example 3.4.2

Proposition 3.4.2

Let $P > 3$ be prime.
Then $P \equiv_6 1$ or $P \equiv_6 5$.

Proof: Suppose $P \equiv_6 0$, $P \equiv_6 2$, $P \equiv_6 3$, or $P \equiv_6 4$.

Case 1: $P \equiv_6 2$

Suppose $\exists a \in \mathbb{Z}$ s.t. $p = a * 6 + 2 = 2(3a + 1)$.

So, letting $b = 3a + 1$, $P = 2b$, i.e. $2 \mid P$.

Observe, since $P > 3$, $P \neq 2$, so there is a divisor of P that is neither 1 nor P.

Thus, P is not prime by the definition of a prime number.

Notice, by subtracting or adding 1 to b in case 1, we see that the cases $P \equiv_6 0$, and $P \equiv_6 4$ (respectively) are similar to case 1.

Case 2: $P \equiv_6 3$

Suppose $\exists c \in \mathbb{Z}$ s.t. $P = c * 6 + 3 = 3(2c + 1)$.

Letting $d = 2c + 1$, $P = 3d$, i.e. $3 \mid P$.

Hence $3 \mid P$, and since $P > 3$, $P \neq 3$, there is a divisor of P that is neither 1 nor P.

Thus, P is not prime by the definition of a prime number.

Since our cases are exhaustive, $P \equiv_6 1$ or $P \equiv_6 5$. ☺

3.5 Proof by Contradiction

If $\neg P$ "leads to nonsense" (i.e. generates a "$C \wedge (\neg C)$ " statement), then $\neg P$ is false, hence P is true.

Instead of taking the contrapositive, we instead negate the implication itself $P \implies Q$ to get $P \wedge \neg Q$ and show that this is not possible and thus the original claim must be true.

Example 3.5.1 (Prove: If $a, b, \in \mathbb{Z}$, then $3a + 9b \neq 2$.)

Proof: Suppose (by way of contradiction) that there exists $a, b \in \mathbb{Z}$ s.t. $3a + 9b = 2$.
Notice: $3a + 9b = 3(a + 3b)$, and let $a + 3b = c$.
Since the sum and product of integers is an integer, $c \in \mathbb{Z}$.

Case 1: $c = 0$

Observe that $2 = 3 * c = 3(0) = 0$, which is a contradiction.

Case 2: $c < 0$

Observe that $2 = 3(c) < 3(0) = 0$, which is a contradiction.

Case 3: $c \geq 1$

Observe that $2 = 3(c) \geq 3(1) = 3$, which is a contradiction.

Note

Most of the time, here we would see "Thus our claim is proved." For clarity, though, we expand the rest of the proof.

Hence, for any $c \in \mathbb{Z}$ we have a contradiction.
So the statement "$\exists a, b \in \mathbb{Z}$ s.t. $3a + 9b = 2$" is false. ☺

Theorem 3.5.1 There are infinitely many prime numbers.

Proof: Suppose there are finitely many prime numbers, i.e. $\exists n \in \mathbb{N}$ s.t. the set P of prime numbers can be denoted by $P = \{p_1, p_2, p_3, \ldots, p_n\}$.
Consider the number $q = p_1 * p_2 * p_3 * \ldots * p_n + 1$.
Fix $p_i \in P$ arbitrarily.
Notice $p_i \mid p_1 * p_2 * p_3 * \ldots * p_n$, and $p_i > 1$.
So, by the division algorithm, $q = p_i * a + r$ where $a, r \in \mathbb{Z}$, then a, r are unique.
Since $q = p_i * (p_1 * p_2 * \ldots * p_{i-1} * p_{i+1} * \ldots * p_n) + 1$, we have $p_i \nmid q$.
By choice of p_i arbitrary, for all $1 \leq i \leq n$, $p_i \nmid q$.
Thus by the Fundamental Theorem of Algebra, q is prime. Since $q \notin P$, our claim is proved. 😄

3.6 Proof by Induction

Induction is a rigorous way to do the "..." part of a proof. There are two fundamental ideas to induction: something starts, and then it keeps working after that.

Practically, this means we need a base case and

Example 3.6.1

Proposition 3.6.1 If $x \in \mathbb{Z}$ is odd, x^n is odd for any $n \in \mathbb{N}$.

Proof: **Base Case:** Let $n = 1$.
$x^n = x^1 = x$ is odd by supposition. So we have our base case.
Inductive Hypothesis: Suppose for $k \in \mathbb{N}$, if x is odd, x^k is odd (this is the inductive hypothesis).

Note

We want to show that x^{k+1} is odd.

Inductive Step: Consider x^{k+1}. Notice $x^{k+1} = x^k x$.
By the inductive hypothesis, there is $m \in \mathbb{N}$ s.t. $x^k = 2m + 1$, i.e. x^k is odd.
Thus $x^{k+1} = x^k x$ is the product of two odd integers, and thus is odd.
So the claim is proven by induction on n. 😄

Note

Induction does not cross the barrier from arbitrarily large finite numbers to infinity; you cannot use "go to infinity."

Example 3.6.2

Proposition 3.6.2 For any $n \in \mathbb{N}$, $2^n \leq 2^{n+1} - 2^{n-1} - 1$.

Proof: **Base Case:** Observe $2^1 = 4 - 1 - 1 = 2^2 - 2^0 - 1 \leq 2^{1+1} - 2^{1-1} - 1$.
So our claim is satisfied for $n = 1$, and thus we have our base case.
Inductive Hypothesis: Suppose for $k \in \mathbb{N}$, $2^k \leq 2^{k+1} - 2^{k-1} - 1$.
Inductive Step: Since $k \in \mathbb{N}$, $2^k \leq 2^{k+1} - 2^{k-1} - 1\, 2^{k+1} \leq 2^{k+2} - 2^k - 2$.
Thus $2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1$.
Therefore, by induction, $2^n \leq 2^{n+1} - 2^{n-1} - 1$ for any $n \in \mathbb{N}$. 😄

Theorem 3.6.1 Fundamental Theorem of Arithmetic

For any natural number $n \geq 2$, there exists a sequence of primes $a_1, a_2, a_3, \ldots, a_k$ s.t. $n = a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_k$. Moreover, this sequence of primes is unique **up to** permutation.

Note

"Up to" can be used as a hint for what to use to prove uniqueness, but we do not yet have the language for permutations.

Proof: We start by showing that for any $n \geq 2$ $n \in \mathbb{N}$, has a prime factorization.

Note

It is kind of silly to prove this first part with a lemma, but it would have no utility outside of this proof since we would just use the actual result if we needed something like it.

For the sake of induction, consider $m = 2$.
Then m is prime and, thus its own (unique) prime factorization.
Suppose there exists $N \in \mathbb{N}$ s.t. for $k \leq N,\ k$ has a prime factorization.
Consider $N + 1$.
Observe, if $N + 1$ is prime, then it is its own prime factorization and we are done.

Note

This could've been done as cases, but if you can do one case in a sentence, then do it like we just did.

So, suppose $N + 1$ is not a prime.
Thus it's composite and there exists some natural numbers a, b with $N + 1 = ab$ and $2 \leq a, b \leq N$.
So, by the inductive hypothesis, there exists prime factorizations of a, b; i.e. $a = a_1 \cdot a_2 \cdot \ldots \cdot a_{j_1}$ and $b = b_1 \cdot b_2 \cdot b_3 \cdot \ldots \cdot b_{j_2}$ for primes a_i $(1 \leq i \leq j_1)$ and b_i $(1 \leq i \leq j_2)$.
Thus $N + 1 = ab = (a_1 \cdot a_2 \cdot \ldots \cdot a_{j_1}) \cdot (b_1 \cdot b_2 \cdot \ldots \cdot b_{j_2})$.
So we have a prime factorization of $N + 1$.
Therefore by induction, for any $n \geq 2,\ n \in \mathbb{N},\ n$ has a prime factorization.
It remains to show that any such factorization is unique up to permutation.
Recall that we know for $n = 2$ there is a unique prime factorization.
Suppose, by way of contradiction, that $k \in \mathbb{N},\ k > 2$ is the smallest number with at least two distinct prime factorizations.
In particular, there exists the prime factorization $a_1, a_2, a_3, \ldots, a_{k_1}$ and $b_1, b_2, \ldots, b_{k_2}$ (which are primes) such that $a_1 \cdot a_2 \cdot \ldots \cdot a_{k_1} = k = b_1 \cdot b_2 \cdot \ldots \cdot b_{k_1}$.
Since $a_1 \cdot a_2 \cdot \ldots \cdot a_{k_1} = b_1 \cdot b_2 \cdot b_{k_2}$, $a_1 \mid b_1 \cdot b_2 \cdot \ldots \cdot b_{k_2}$.
Since a_1 is prime, there exists $i \in \mathbb{N}$ s.t. $a_1 \mid b_i$.
Since b_i is prime, $a_1 = b_i$.
So $a_2 \cdot a_3 \cdot \ldots \cdot a_{k_1} = b_1 \cdot b_2 \cdot \ldots b_{i-1} \cdot b_{i+1} \cdot \ldots \cdot b_{k_2} := \hat{k}$.
So $\hat{k}$ has 2 distinct prime factorizations.
Finally, since $k = a_1 \cdot \hat{k},\ a_1 \geq 2,\ \hat{k} < k$, which is a contradiction. 😄

3.6.1 Proof by Strong Induction

The previous version of induction is known as "weak induction." Strong induction is almost the same, but you assume that every case until where you are is true instead of just the case you're on. These are logically equivalent but are both still used to help with understanding.

3.6.2 Proof by Least Counterexample

This works by finding a contradiction within induction. Specifically, by claiming that you have the smallest example and then finding a smaller example.

Example 3.6.3

Proposition 3.6.3 $4 \mid 5^n - 1$ for any $n \in \mathbb{N}$.

Note

This is actually easier without induction, but we use it in this case to show a very elegant way to combine contradiction and induction: proof by least counterexample.

Proof: **Base Case:** Observe $5^1 - 1 = 4,\ 4 = 1 * 4,\ 4 \mid 4$, so our claim holds for $n = 1$ and we have our base case.

Note

We need the base case to show that we can go back that far with $k - 1$ later.

Suppose by way of contradiction, $4 \nmid 5^n - 1$ for every $n \in \mathbb{N}$.
Thus there exists a smallest $k \in \mathbb{N},\ k > 1$ s.t. $4 \nmid 5^k - 1$ (but $4 \mid 5^m - 1$ for every $m \in \mathbb{N},\ m < k$).
Since $4 \mid 5^{k-1} - 1$, there is $c \in \mathbb{Z}$ s.t. $4c = 5^{k-1} - 1$.
So $20c = 5^k - 5$ and $20c + 4 = 5^k - 1$, i.e. $4(5c + 1) = 5^k - 1$.
Since $5c + 1 \in \mathbb{Z}$ by the sum and product of integers, $4 \mid 5^k - 1$ which is a contradiction. 😄

Chapter 4

Specific Proofs

4.1 Proofs of Biconditionals

We need to prove both directions of $P \implies Q$ and $Q \implies P$.

Example 4.1.1

A triangle is equilateral **iff** all of its sides have the same length.

Example 4.1.2

Proposition 4.1.1 The integer n is odd if and only if n^2 is odd.

Proof: First we show that if n is odd, then n^2 is odd.
Suppose n is odd.
Then $n = 2k + 1$ for some integer k.
So $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1 = 2l$ for some integer l.
Hence, n^2 is odd by definition of an odd number.

Conversely, we aim to prove that if n^2 is odd, then n is odd.
Suppose n is not odd, and then n is even.
We can write $n = 2a$ for some integer a.
Then $n^2 = (2a)^2 = 4a^2 = 2(2a^2) = 2j$, for some integer j.
So n^2 is even by definition of an even number, and hence n is odd by contrapositive.

Note

We can include a concluding sentence for clarity, but it is not strictly necessary.

Since both sides have been proven, the biconditional holds. 😄

Example 4.1.3

Proposition 4.1.2 Suppose a and b are integers. Then $a \equiv b \pmod 6$ if and only if $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.

Proof: First we prove that if $a \equiv b \pmod 6$, then $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.
Suppose $a \equiv b \pmod 6$.
Then $a - b = 6n$ for some $n \in \mathbb{Z}$.
From here, we see that $a - b = 3(2n)$ and $a - b = 2(3n)$.
The former tells us that $a \equiv b \pmod 3$, since $2n$ is an integer, and the latter tells us that $a \equiv b \pmod 2$, since $3n$ is an integer.

Conversely, we aim to show that if $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$, then $a \equiv b \pmod 6$.
Suppose $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.
Then there is some $k \in \mathbb{Z}$ s.t. $a - b = 2k$, and hence $a - b$ is even.
Similarly, there is some $l \in \mathbb{Z}$ s.t. $a - b = 3l$.
Since $a - b$ is even, l must be even (since if l were odd, then $a - b$ would be a product of two odd integers and hence odd.)
So $l = 2j$ for some $j \in \mathbb{Z}$.
Then $a - b = 3l = 3(2m) = 6m$.
Hence $a \equiv b \pmod 6$. 😄

4.2 Proofs of Equivalence Statements

Example 4.2.1

Theorem 4.2.1

Suppose A is an $n \times n$ matrix. The following statements are equivalent (TFAE):

1. A is invertible.
2. The equation $A\vec{x} = \vec{b}$ has a unique solution for every $\vec{b} \in \mathbb{R}^n$.
3. The equation $A\vec{x} = \vec{0}$ has only the trivial solution.
4. The reduced row echelon form of A is in I_n.
5. $\det(A) \neq 0$.
6. The matrix A does not have 0 as an eigenvalue.

Note

Saying that all of these are equivalent is saying that every statement is in a biconditional with every other statement.

The best case scenario is to prove that a bunch of statements are equivalent are to prove the statements in a cycle, i.e. $a \implies b \implies c \implies a$.

4.3 Proofs of Existence Statements

Most theorems are of the form $P \implies Q$. Really, these statements are saying $\forall x P(x) \implies Q(x)$.

There are theorems of the form $\exists x P(x)$. To prove this, one of the most basic ways to do this is to give an example and show that the example satisfies the proposition (there are some proofs where you can prove it without an example, but those only really come up much later). Statements of this form are called "existence statements." Theorems of this form are called "existence theorems."

Note

Often you will use this for counterexamples; do not use it to prove universal quantifiers!

Example 4.3.1

Proposition 4.3.1 There exists an even prime.

Proof: 2 is an even prime. ☺

Example 4.3.2

Proposition 4.3.2 There exists an integer which can be expressed as the sum of cubes in two distinct ways.

Proof: $1729 = 1^3 + 12^3 = 9^3 + 10^3$. ☺

4.3.1 Proofs of Uniqueness Statements

Example 4.3.3

Proposition 4.3.3 Suppose $r \in \mathbb{R}^+$ and $r^2 = 1$. Then $r = 1$.

Proof: Observe, if $r = 1$, then $1^2 = 1$, so we have existence.
Next let $r \neq 1$.

Note

This kind of proof is, at an abstract level, focusing on a place on the real number line and looking at the distance from that place. This is very useful.

Case 1: $r > 1$

There exists $\delta > 0$ so that $r = 1 + \delta$.

Observe, $r^2 = (1 + \delta)^2 = 1 + 2\delta + \delta^2$.

Since $\delta > 0$, $2\delta + \delta^2 > 0$.

So $r^2 = 1 + 2\delta + \delta^2 > 1$, and $r^2 \neq 1$.

Case 2: $0 < r < 1$

There exists $0 < \delta < 1$ so that $r = 1 - \delta$.

$r = 1 - \delta$, and thus $r^2 = 1 - 2\delta + \delta^2$.

Since $1 > \delta > 0$, we have $2\delta > \delta = 1 \cdot \delta > \delta \cdot \delta = \delta^2$.

That is, $-\delta + \delta^2 < 0$, so $r^2 = 1 - 2\delta + \delta^2 < 1$.

So $r^2 \neq 1$.

So, by case 1 and case 2, if $r^2 \neq 1$, then $r \neq 1$.
So we have uniqueness. 😄

4.3.2 Constructive vs. Non-Constructive Proofs

Constructive proofs give a concrete example; non-constructive proof do not.

Example 4.3.4

This is a constructive proof:

Proposition 4.3.4 There is an n s.t. $3^n + 4^n = 5^n$

Proof: Observe $3^2 + 4^2 = 5^2$. 😄

This is a non-constructive proof:

Proposition 4.3.5 There exists $x, y \in \mathbb{R} \setminus \mathbb{Q}$ s.t. $x^y \in \mathbb{Q}$

Proof: Consider $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$.

Case 1: $x \in \mathbb{R} \setminus \mathbb{Q}$

Then $x^y \in \mathbb{Q}$.

Case 2: $x \in \mathbb{Q}$

Then $\sqrt{2}^{\sqrt{2}}$ satisfies our claim.

☺

Example 4.3.5

Let's try the previous example constructively:

Lemma 4.3.1 Suppose $p \in \mathbb{N}$ is prime, and fix $b \in \mathbb{N},\ b > 1,\ p \nmid b$. Then $\log_b(p)$ is irrational.

Proof: Suppose $p \in \mathbb{N}$ is prime, and fix $b \in \mathbb{N},\ b > 1,\ p \nmid b$.
Next by way of contradiction suppose $\log_b(p)$ is rational.
So there exists $n, m \in \mathbb{Z},\ m \neq 0$ s.t. $\log_b(p) = \frac{n}{m}$.
We may assume that the $\text{GCD}(n, m) = 1$.

Note

"We may assume" or "wma" is another trap like "wlog."

Thus, $p^m = b^n$.

Note

This approach, as opposed to something like $p = b^{\frac{n}{m}}$, retains the most information.

Notice, $p \mid p^m$, so $p \mid b^n$.
Since p is prime, $p \mid b$. ☺

Proposition 4.3.6 There exists $x, y \in \mathbb{R} \setminus \mathbb{Q}$ s.t. $x^y \in \mathbb{Q}$.

Proof: Let $x = \sqrt{2}\, y = \log_2(25) = 2\log_2(5)$.
y is irrational by the lemma 3.8.1.
So $x^y = \sqrt{2}^{\log_2(25)} = \sqrt{2}^{2\log_2(5)} = \left(\sqrt{2}^2\right)^{\log_2(5)} = 2^{\log_2(5)} = 5$. ☺

4.4 Proofs with Sets

4.4.1 Proving if Something is an Element

Example 4.4.1 (Let $A = \{1, 2, 3, 4\}$. Prove $3 \in A$.)

Proof: Observe $3 \in A$ by inspection. 😄

Example 4.4.2 (Let $B = \{x \in \mathbb{R} : \exists y \in \mathbb{Z} \text{ s.t. } x = y^2 + 3y\}$. Prove $28 \in B$.)

Proof: Let $y = 4$, note $y \in \mathbb{Z}$.
By a calculation we have $4^2 + 3(4) = 16 + 12 = 28$.
Finally, since $28 \in \mathbb{R},\ 28 \in B$. 😄

Example 4.4.3 (Let $A = \{\ldots, -4, 0, 4, 16, \ldots\}$. Prove or disprove $28 \in A$.)

Proof: Notice $A = \{0 + (-1)^n 2^{\lfloor n \rfloor} : n \in \mathbb{N}, n > 2\}$

Note

We can come up with anything we want! Therefore it's kind of impossible to prove something that's not in set-builder notation.

😄

4.4.2 Proving if Something is a Subset

Example 4.4.4 (Let $B = \{4x : x \in \mathbb{Z}\}, A = \{ax : a \in \mathbb{Z}, x \text{ is any prime}\}$. Prove $B \subseteq A$.)

Proof: Let $b \in B$ arbitrarily.
We want to show (WTS) $b \in A$ so we must show $\exists a \in \mathbb{Z},\ p$ a prime s.t. $b = ap$.
$b \in B$ means there is $k \in \mathbb{Z}$ s.t. $b = 4k$.
So $b = 2(2k)$.
Taking $a = 2k,\ p = 2,\ b \in A$.
Therefore, $B \subseteq A$. 😄

Example 4.4.5

Proposition 4.4.1 Let $S_k := \{ak : a \in \mathbb{N}\}$, and $p \in \mathbb{Z}$ be prime. Define $I_{n,p} := \{x \in \mathbb{N} : 2 \leq x \leq n, x \neq p\}$. Then for any $n \in \mathbb{N}$, $p \in \mathbb{Z} \setminus \left(\bigcup_{k \in I_{n,p}} S_k\right)$.

Proof: Let $S_k, I_{n,p}, p \in \mathbb{Z}$ be as defined in the statement.
Suppose by way of contradiction that $p \notin \mathbb{Z} \setminus \left(\bigcup_{k \in I_{n,p}} S_k\right)$.
Since $p \in \mathbb{Z}$, there exists $2 \leq k \leq n$ s.t. $k \neq p, p \in S_k$.
So there exists $a \in \mathbb{N}$ s.t. $p = ak$.
That is, $p \mid a$ or $p \mid k$ since p is prime.

Case 1: $p \mid a$

So there is $b \in \mathbb{N}$ s.t. $bp = a$.

Notice, $k \geq 2$.

So $p = ak = (bk)p \geq 2bp$.

Since $b \geq 1$, $p \geq 2bp > 2p$ for $p \in \mathbb{N}$.

This is a contradiction.

Case 2: $p \mid k$

So there is $c \in \mathbb{N}$ s.t. $cp = k$.

Since $p \neq k, c \neq 1$, i.e. $c \geq 2$.

Thus $p = ak = (ac)p \geq 2ap \geq 2p$.

This is a contradiction.

Note

The fixed $p \in \mathbb{Z} \setminus \left(\bigcup_{k \in I_{n,p}} S_k\right)$ is called a sieve on p.

4.4.3 Proving Equality of Sets

You must prove that $A \subseteq B$ and $B \subseteq A$.

Chapter 5

Disproof

Claim P is true. Formally, a disproof shows that P is false, or rather that $\neg P$ is true.

5.1 Disproof by Counterexample

In practice, almost all claims of interest are universal qualifiers. Thus negation converts to an existential quantifier.
All this to say, disproof is "usually" "disproof by counterexample."

Example 5.1.1 (Prove or disprove the claim.)

Claim 5.1.1 For every $n \in \mathbb{N}$, $3 \mid 8^n - 5$.

Proof: Suppose $n \in \mathbb{N}$. We claim this doesn't hold, and proceed by counterexample.
Consider $n = 2$. Then $8^n - 5 = 8^2 - 5 = 64 - 5 = 59$.

Note

We can't say "Observe, there is no $a \in \mathbb{Z}$ s.t. $3a = 59$" since there's no way to check that in a finite number of steps. We **could**, as a cheap trick, say "Observe that 59 is prime" and go from there.

Observe, by the division algorithm, $59 = 3 \cdot 19 + 2$.
In particular, $r \neq 0$.
So $3 \nmid 59$, i.e. $3 \nmid 8^2 - 5$. ☺

5.2 Disproof by Contradiction

Example 5.2.1 (Prove or disprove the claim)

Claim 5.2.1 There exists $x \in \mathbb{R}$ s.t. $x^4 < x < x^2$.

We want to prove that $\forall x \in \mathbb{R},\ x^4 \geq x$ or $x \geq x^2$. However, this is annoying, so we use proof by contradiction to disprove the claim. This is weird because it gives us our original claim back, but now you're suppose that it's true and showing that there's a contradiction.

Proof: We claim this is false.
To that end, suppose there exists $x \in \mathbb{R}$ s.t. $x^4 < x < x^2$.
First, for any $y \in \mathbb{R},\ y^4 \geq 0$.
So since $x > x^4,\ x > 0$.
So, canceling x in each term yields $x^3 < 1 < x$ (since $x \neq 0$ and it's positive so it doesn't change the inequality), thus $x^3 - 1 < 0 < x - 1$.
So $(x-1)(x^2+x+1) < 0 < x - 1$. Observe $x - 1 > 0$ (so we've learned something new from what we supposed).
Observe, since $x > 0$ (or $x > 1$, whichever you want), $x^2 > 0$, so $x^2 + x + 1 > 0$.
Also, since $x - 1 > 0$, $x^2 + x + 1 < 0$, which is a contradiction. 😄

Chapter 6

Relations

6.1 Relations

Definition 6.1.1: Relation

A relation on some set A is a subset $R \subseteq A \times A$. We denote for $(x, y) \in R$ that "xRy " or "$x \sim y$" and for $n, m \notin R$ that "$n \not R m$" or " $n \not\sim m$".
Any subset of $A \times A$ is a relation on A. The challenge then is creating useful relations which need to be very exact.

Example 6.1.1

Let $A = \{1, 2, 3, 4\}$.
Two numbers in A are the same parity (i.e. $x \equiv y \pmod 2$) if the ordered pair of them (x, y) is in the set $R = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)\}$.

Note

Since relations are sets, you can do things involving sets with them to give you more information!

Example 6.1.2

For the infinite case of something like $\leq$, we use set-builder notation:

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} | y - x \in \mathbb{N} \cup \{0\}\}$$

6.2 Properties of Relations

These are properties that you can see if a relation has, not necessarily properties that every relation has:

1. Reflexive

   For every $a \in A$, aRa.

2. Symmetric

   Given that aRb, then bRa.

3. Transitive

   Given that aRb and bRc, then aRc.

Note

Equality and congruency have all 3 properties.

Note

The reflexive property is very unique in that it is a statement about every element in the set, but the other two properties are statements about the relation itself. A larger result from this fact is that being transitive and symmetric does not mean it must be reflexive.

Definition 6.2.1: Equivalence Relations

If the relation R on A is reflexive, symmetric, and transitive, then we call R an **equivalence relation**.

6.3 Equivalence Classes

Definition 6.3.1: Equivalence Classes

Suppose R is an equivalence relation on a set A.
Given any element $a \in A$, the "**equivalence class** containing a" is the subset of $R : \{x \in A : xRa\}$.
This is denoted $[a]$.

Note

a is called the "representative."

Example 6.3.1

Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (2, 2), (3, 3)\}$.
R is reflexive, symmetric, and transitive, and so is an equivalence relation.
Also, for any $a \in A$, $[a]$ is the equivalence class containing a.
For example, $[1] = \{(1, 1)\}$.

Note

Remember that an equivalence class is a **set**!

Theorem 6.3.1

If R is an equivalence relation on A, then aRb if and only if $[a] = [b]$.

Proof: Suppose $a, b \in A$ such that aRb.
Consider $c \in [a]$.
So cRa and aRb, and by transitivity, cRb.
Thus $c \in [b]$.
So $[a] \subseteq [b]$.
Now consider $k \in [b]$.
So kRb and aRb.
So by symmetry bRa, and by transitivity, kRa, and $k \in [a]$.
Thus $[a] \subseteq [b] \subseteq [a]$, and $[a] = [b]$.

Conversely, suppose $[a] = [b]$.
First, since R is reflexive, $a \in [a]$.
Since $a \in [a]$, $a \in \{x \in A : xRa\} = [a] = [b] = \{x \in A : xRb\}$.
So aRb. 😊

Definition 6.3.2: Partition

A partition of a set A is a **set** of non-empty subsets of A such that their union is A, and they are pairwise disjoint.
That is, for any $U_1, U_2, U_3, \ldots, U_n \in A$, $\bigcup_{k=1}^{n} U_k = A$ and for **any** $1 \leq j, k \leq n, U_j \cap U_k = \varnothing$.

Theorem 6.3.2

Suppose R is an equivalence relation on A. Then the set $\{[a] : a \in A\}$ is a partition of A.

Proof: We begin by showing that $\bigcup_{a\in A}[a] = A$.
First observe, for each $a \in A$, $a \in [a]$ by the reflexive property.
So $a \in \bigcup_{x\in A}[x]$, so $\bigcup_{x\in A}[x] \supseteq A$.
Next, notice for any $c, x, c \in [x]$, then $c \in A$.
So $\bigcup_{x\in A}[x] \subseteq A$.
So $\bigcup_{x\in A}[x] = A$.
Next, by way of contrapositive, suppose $[a] \cap [b] \neq \varnothing$.
Then, by the previous theorem, observe:
$c \in [a] \cap [b]$, so cRa and cRb, thus by symmetry aRc and so aRb, thus we conclude $[a] = [b]$.
So we have that the set of equivalence classes are pairwise disjoint.
Therefore the set $\{[a] : a \in A\}$ is a partition. 😄

Theorem 6.3.3

Let $n \in \mathbb{N}$. The "integers modulo n" is an equivalence relation on $\mathbb{Z}$, and the set of equivalence classes is denoted $\mathbb{Z}_n$.

Theorem 6.3.4

Let $n \in \mathbb{N}$.
Then for $[a], [b] \in \mathbb{Z}_n$, we have that

1. $[a] + [b] := [a + b]$

   Note

   This gives us $[a] - [b]$ as well.

2. $[a] \cdot [b]] := [ab]$

are well defined.

Chapter 7

Functions

7.1 Functions

We now want to show functions as relations between sets. That is, we have a relation from A to B which is itself a set $R \subset A \times B$.

Example 7.1.1

$$f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$$

We say that "f is a relation from $\mathbb{R}$ to $\mathbb{R}$, i.e. $f \subseteq \mathbb{R} \times \mathbb{R}$ such that $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}, y = x^2\}$."

Given a function $f : A \to B$ (for example, $f(a) = b^2$), the following are defined:

1. Domain: The "inputs," i.e. the set A
2. Codomain: The "type" of output, i.e. the set B

   Note

   Technically a codomain is any set containing the range, so it's not really useful because you can pick any set containing the range. However, it is more useful to consider, like mentioned above, the "type" of the output.

3. Range: The attainable/actual values, i.e. the set $\{b \in B : f(a) = b \text{ for } a \in A\}$ or alternatively, $\{b \in B : (a, b) \in f\}$

   Note

   Using abuse of notation, we can also define it to be written as $f(A)$ which is a set.

Definition 7.1.1: Function

Suppose A and B are sets. A function f from A to B (denoted $f : A \to B$) is a relation $f \subseteq A \times B$ satisfying the property that for each $a \in A$, the relation f contains exactly **one** ordered pair (a, b) for some $b \in B$. Then we denote $(a, b) \in f$ by

$$f(a) = b.$$

Note

Remember that since functions are ultimately sets, proving that functions are equal or not equal involves proofs with sets.

7.2 Graphs of Functions

I can't make graphics yet. Maybe in a future class I will. Graphs aren't rigorous anyways so it's fine.

7.3 Injective, Surjective, and Bijective Functions

Functions are deterministic, so you will always get the same value out when you plug in the same value. The following properties help us to better relate the inputs and outputs.

Definition 7.3.1

Let $f : A \to B$ be a function. We say

1. f is injective (one-to-one) if for $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
2. f is surjective (onto) if for any $b \in B$, there is an $x \in A$ so that $f(x) = b$. This is equivalent to saying that the range is equal to the codomain. So, a function being surjective is more so a commentary on the codomain than the function itself.
3. f is bijective if f is injective **and** surjective.

Note

Use counterexamples to disprove these properties if necessary!

Example 7.3.1 ($f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$. Prove that f is neither injective nor surjective.)

Proof: First we show that it is not injective.
That is, we want to show that there exists $x, y \in \mathbb{R}$ so that $x \neq y$ and that $f(x) = f(y)$.
Observe for $x = 1, y = -1$ that $x \neq y$ but $f(x) = 1 = f(y)$.
Now we show that it is not surjective.
That is, we want to show that there exists $y \in \mathbb{R}$ such that $f(x) \neq y$ for **any** $x \in \mathbb{R}$.
Consider $y = -1$.
Since for any $x \in \mathbb{R}, x^2 \geq 0$, we have that $f(x) = x^2 \geq 0$.
Since $-1 < 0$ and $f(x) \geq 0$ for all $x \in \mathbb{R}$, $-1 \notin f(\mathbb{R})$.
Therefore f is not bijective. 😄

Note

A classic way of proving that a function is injective is by the contrapositive, i.e. supposing $f(x) = f(y)$, show that $x = y$.

Proposition 7.3.1

For any $a < b, c < d \in \mathbb{R}$, there exists a bijection $f : [a, b] \to [c, d]$.

Proof: Let $a < b, c < d \in \mathbb{R}$ be given.
Let $f(x) = \frac{d-c}{b-a}(x - a) + c$.
It remains to show that $f(x)$ is injective and surjective, i.e. bijective.
Note $d - c > 0$, $b - a > 0$.
To show that it is injective, suppose by way of contrapositive that $f(x) = f(y)$ for some $x, y \in [a, b]$.
Then $\frac{d-c}{b-a}(x - a) + c = \frac{d-c}{b-a}(y - a) + c$.
By subtracting c from both sides, then multiplying both sides by $\frac{b-a}{d-c}$ we have $(x - a) = (y - a)$.
Thus $x = y$ and so $f(x)$ is injective.

Note

Mathematicians usually try to be specific by using subscripts, i.e. something like y_0 instead of just y.

To show that it is surjective, let $y_0 \in [c, d]$ be given and denote $y_0 - c = \delta$.
Consider $x_0 = \delta \cdot \frac{b-a}{d-c} + a$.
Observe, since $y_0 \in [c, d], c \leq y_0 \leq d$, so $y_0 - c = \delta \in [0, d - c]$.
Thus $\delta \cdot \frac{b-a}{d-c} + a \leq (d - c) \cdot \frac{b-a}{d-c} = b - a + a = b$, since $\frac{b-a}{d-c} > 0$.
Thus $a \leq x_0 \leq b$, and thus $x_0 \in [a, b]$.

Therefore, f is surjective.
Since f is injective and surjective, it is bijective. 😊

Note

Again, dealing with the distance from a point to something that is better understood is often more useful than looking at the point itself.

Theorem 7.3.1

Let $f : A \to B,\ g : B \to C$ be bijections.
Then $g(f)$ is a bijection.

7.3.1 Pigeonhole Principle

Theorem 7.3.2 Pigeonhole Principle

Let A, B be finite sets and $f : A \to B$ be any function.

1. If $|A| > |B|$ then f is **not** injective.
2. If $|A| < |B|$ then f is **not** surjective.

Note

This means that if f is bijective, then $|A| = |B|$.

Proposition 7.3.2

Let A be a set of ten distinct integers from 1 to 100. Then there are two subsets $X, Y \in A$ s.t. $X \neq Y$ and $\sum_{x\in X} x = \sum_{y\in Y} y$.

Proof: First observe, for any A, $\sum_{a\in A} a < 10 \cdot 100 = 1000$.
Define $f : \mathcal{P}(a) \to [0, 1000] \cap \mathbb{Z}$ by $f(X) = \sum_{x\in X} x$.
Notice, the domain of f has $2^{10} = 1024$ elements and the codomain has 1001 elements.
So by the pigeonhole principle, there exists some $X, Y \in \mathcal{P}(A)$ with $X \neq Y$ with $f(X) = f(Y)$, i.e. $\sum_{x\in X} x = \sum_{y\in Y} y$. 😊

Note

One of the downsides of the pigeonhole principle is that it isn't constructive, so most proofs involving it are non-constructive.

7.4 Other Definitions

Definition 7.4.1

Let R be a relation.
Then we denote the "inverse relation" by

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

Definition 7.4.2

Let $f : A \to B$ be a function.
We denote the "pull back" of y (under f) by

$$f^{\leftarrow}(y) = \{x \in X : f(x) = y\}.$$

Further, if the pull back is a function we call it the "inverse function" and denote it

$$f^{-1} = \{(b, a) : (a, b) \in f\}.$$

Definition 7.4.3

Let $f : A \to B$ be a function.
Fix $X \subseteq A$ and $y \subseteq B$.
Then $f(X) = \{f(x) : x \in X\}$ is called the **image** of X (under f) and $f^{\leftarrow}(Y) = \{x \in A : f(x) \in Y\}$ is called the **preimage**.

7.5 Cardinality of Infinite Sets

Our previous idea of equality of cardinality is no longer adequate for infinite sets, so we now change it to one involving functions:

Definition 7.5.1

Let A, B be (not necessarily finite) sets.
We say $|A| = |B|$ if there exists a bijection from A to B (alternatively, "between A and B).

Theorem 7.5.1 $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| \neq |\mathbb{R}|$

1. $|\mathbb{N}| = |\mathbb{Z}|$

   Proof: Let $f(x) = \begin{cases} \frac{x}{2} & x = 2k,\ k \in \mathbb{N} \\ -\frac{x-1}{2} & x = 2k+1,\ k \in \mathbb{N} \end{cases}$, $f : \mathbb{N} \to \mathbb{Z}$.

   Note

   That it is a bijection remains to be proved.

   😄

2. $|\mathbb{Z}| = |\mathbb{Q}|$

   Idea of Proof: It is sufficient to show that $|\mathbb{N}| = |\mathbb{Q}^+|$.
   Think of the rationals as the xy-plane.
   The integer lattice will give you the rationals.
   Your ordering can then be the diagonals, and we have a bijection. 😄

3. $|\mathbb{N}| \neq |\mathbb{R}|$

   Cantor's Diagonalization Proof: The claim is that there is no bijection between them.
   Look online for the proof. 😄

This gives us the nomenclature for "countable" and "uncountable" infinities.