MAT 2534 Discrete Math

Joe Wells
Virginia Tech

Spring 2024[1]

Last Updated: May 4, 2024

[1]This courses is using Susanna Epp's *Discrete Mathematics with Applications*, 4th Edition. The chapter/section titles have been retained, but otherwise internal numbering of theorems, examples, etc. will likely disagree with the course text.

Contents

Chapter 2

The Logic of Compound Statements

2.1 Logical Form and Logical Equivalence

Definition

A **statement** (or a **proposition**) is a sentence which is either true or false, but not both. The **truth value** of a statement either "true" or "false."

Example 2.1.1

- "$1 + 2 = 3$" is a true statement.
- "$1 + 2 = 4$" is a false statement.
- "$x + 2 = 5$" is neither true nor false; not a statement. Since x is unspecified. Usually when we are solving for x, we are trying to find an x-value that makes the statement true.

To make life simpler when breaking down compound statements, we introduce some logical notation:

Logical Connectives and Order of Operations

symbol	English translation
$\vee$	"or"
$\wedge$	"and"
$\neg$ or $\sim$	"not"

Order of Operations
1. Parentheses ()
2. $\neg$
3. $\wedge$
4. $\vee$

Remark. "not" should be interpreted generally as negating a statement, which is more commonly how one would use it in English.

Example 2.1.2

Let p and q be the following statements.:

p : Trey drinks water.

q : Sandy eats cookies.

Interpret the following statements in plain English.

- $p \vee q$
- $p \wedge q$
- $\neg p \vee q$
- $\neg p \wedge \neg q$

- $p \vee q$ means "Trey drinks water or Sandy eats cookies."
- $p \wedge q$ means "Trey drinks water and Sandy eats cookies."
- $\neg p \vee q$ means "Trey does not drink water or Sandy eats cookies."
- $\neg p \wedge \neg q$ means "Trey does not drink water and Sandy does not eats cookies."

Logical form of common expressions

"Neither a nor b"	means	not a and not b.
"a but not b"	means	a and not b.
"$a \geq 2$"	means	$a > 2$ or $a = 2$.
"$1 \leq b < 5$"	means	$1 \leq b$ and $b < 5$.

2.1.1 Truth Tables

When considering a sentence comprised of several component statements, we want to know if the entire compound sentence is actually a statement (i.e. has a well-defined truth value). In order to do this, we'll need to analyze how the logical symbols (i.e. logical connectives) relate to the validity of the compound statement.

Example 2.1.3

Let x be a fixed real number and consider the sentence "$2 < x < 5$," which we know is

"$x > 2$ and $x < 5$."

Fix a couple of different x-values and record the truth values of the three statements $x > 2$, $x < 5$, and $2 < x < 5$ in a *truth table*.

x-value	$x > 2$	$x < 5$	$2 < x < 5$
-1	F	T	F
3	T	T	T
7	T	F	F

The sentence "$2 < x < 5$" is only true for x-values in which *both of "$2 < x$" and "$x < 5$" are true.*

Definition

If p and q are both statements, then the **conjunction** of p and q is the statement $p \wedge q$. The truth table for conjunctions is below.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 2.1.4

Let x be a fixed real number and consider the sentence "$x \leq 2$," which we know is

"$x < 2$" or "$x = 2$."

Let's fix a couple of different x-values and record the truthfulness of $x < 2$, $x = 2$, and $x \leq 2$ in a *truth table*:

x-value	$x < 2$	$x = 2$	$x \leq 2$
-1	T	F	T
2	F	T	T
7	F	F	F

The sentence "$x \leq 2$" is only true for x-values in which *at least one of "$x < 2$" and "$x = 2$" are true.*

Definition: Disjunction

If p and q are both statements, then the **disjunction** of p and q is the statement $p \vee q$. The truth table for conjunctions is below.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Remark. Common English tends to use an "exclusive or." At a restaurant, when asked "Soup or salad?" we implicitly understand it to mean that you can have either soup or salad, but not both. In logic, disjunction represents an "inclusive or", which would allow for "soup, salad, or both" as valid answers. While this is a bit of a conventional choice, by comparing the final column of the conjunctive and disjunctive truth tables, we see that the inclusivity keeps them similar. Sometimes the symbol $\oplus$ will be used to denote an exclusive or (although we will not use that in these notes).

Definition

If p is any statement, then the **negation** of p is the statement $\neg p$. The truth table for negation is below.

p	$\neg p$
T	F
F	T

Now that we know about the basic logical connectives, let's fill in their truth tables.

Definition

Let p and q be statements. Then **exclusive or**, denoted $p \oplus q$ is true when precisely one of p and q is true. The truth table for $\oplus$ is below.

p	q	$p \vee q$
T	T	F
T	F	T
F	T	T
F	F	F

In plain English, this corresponds to the phrase "either... or..."

Definition

A **compound statement** is a logical statement involving multiple logical connectives.

Example 2.1.5: 3-variable truth table

Complete the following truth table for the statement: $p \wedge \neg(q \vee r)$.

p	q	r	$q \vee r$	$\neg(q \vee r)$	$p \wedge \neg(q \vee r)$
T	T	T	T	F	F
T	T	F	T	F	F
T	F	T	T	F	F
T	F	F	F	T	T
F	T	T	T	F	F
F	T	F	T	F	F
F	F	T	T	F	F
F	F	F	F	T	F

Definition

Two (compound) statements, P and Q, with all of the same truth values are called **logically equivalent**.

Symbolically we write $P \equiv Q$.

Example 2.1.6: Exclusive Or

Let p and q be statements. Show that

$$\Big[p \oplus q\Big] \equiv \Big[(p \vee q) \wedge \neg(p \wedge q)\Big]$$

by filling out a truth table and verifying both statements have the same truth values.

p	q	$p \oplus q$	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
T	T	F	T	T	F	F
T	F	T	T	F	T	T
F	T	T	T	F	T	T
F	F	F	F	F	T	F

This table justifies the interpretation of the exclusive or: "p or q is true, but not both."

Example 2.1.7: Negation is Not Distributive

Show that $\neg(p \vee q) \not\equiv (\neg p) \vee (\neg q)$.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
T	T	T	F	F	F	F
T	F	T	F	F	T	T
F	T	T	F	T	F	T
F	F	F	T	T	T	T

Definition: Tautology and Contradiction

A **tautology** is a statement (call it **t**) that is always true and a **contradiction** is a statement (call it **c**) that is always false.

2.1.2 Table of Logical Equivalences

Theorem 2.1.8: Table of Logical Equivalances

Let p, q, and r be statements, let **t** be a tautology, and let **c** be a contradiction. We then have the following table of equivalences:

Commutative Laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative Laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive Laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity Laws	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
Negation Laws	$p \vee \neg p \equiv \mathbf{t}$	$p \wedge \neg p \equiv \mathbf{c}$
Double Negative Laws	$\neg(\neg p) \equiv p$	
Idempotent Laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound Laws	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
De Morgan's Laws	$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation of $\mathbf{t}$ and $\mathbf{c}$	$\neg\mathbf{t} \equiv \mathbf{c}$	$\neg\mathbf{c} \equiv \mathbf{t}$

Example 2.1.9: Proof of Commutative Laws

Use a truth table to show the Commutative Laws in Theorem 2.1.8.

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

p	q	$p \vee q$	$q \vee p$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Example 2.1.10: Proof of Associative Laws

Use a truth table to show the Associative Laws in Theorem 2.1.8.

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$q \vee r$	$p \vee (q \vee r)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	T	F	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

Example 2.1.11: Proof of Distributive Laws.

Use a truth table to show the Distributive Laws in Theorem 2.1.8.

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Example 2.1.12: Proof of Identity Laws

Use a truth table to show the Identity Laws in Theorem 2.1.8.

p	t	$p \wedge$ t
T	T	T
F	T	F

p	c	$p \vee$ c
T	F	T
F	F	F

Example 2.1.13: Proof of Negation Laws.

Use a truth table to show the Negation Laws in Theorem 2.1.8.

p	$\neg p$	$p \vee \neg p$	t
T	F	T	T
F	T	T	T

p	$\neg p$	$p \wedge \neg p$	c
T	F	F	F
F	T	F	F

Example 2.1.14: Proof of Double Negative Law

Use a truth table to show the Double Negation Law in Theorem 2.1.8.

p	$\neg p$	$\neg(\neg p)$
T	F	T
F	T	F

Example 2.1.15: Proof of Idempotent Laws.

Use a truth table to show the Idempotent Laws in Theorem 2.1.8.

p	$p \wedge p$
T	T
F	F

p	$p \vee p$
T	T
F	F

Example 2.1.16: Proof of Universal Bound Laws

Use a truth table to show the Universal Bound Laws in Theorem 2.1.8.

p	t	$p \vee$ t
T	T	T
F	T	T

p	c	$p \wedge$ c
T	F	F
F	F	F

Example 2.1.17: Proof of De Morgan's Laws

Use a truth table to show the De Morgan's Laws in Theorem 2.1.8.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Example 2.1.18: Proof of Absorption Laws

Use a truth table to show the Absorption Laws in Theorem 2.1.8.

p	q	$p \wedge q$	$p \vee (p \vee q)$
T	T	T	T
T	F	F	T
F	T	F	F
F	F	F	F

p	q	$p \vee q$	$p \wedge (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	F

Example 2.1.19: Proof of Negation of t and c

Use a truth table to show the Negation of **t** and **c** in Theorem 2.1.8.

t	c	$\neg$t
T	F	F

t	c	$\neg$c
T	F	F

2.2 Conditional Statements

Consider the following promise made by your instructor to his broccoli-averse child.

If you eat your dinner, then I will give you cookies for dessert.

If the child eats dinner and your instructor gives the child cookies for dessert, then the promise is upheld.
If the child eats dinner and your instructor does not gives the child cookies for dessert, then the promise is not upheld.
If the child does not eat dinner, then cookies or not, it would be unfair to claim that the instructor did not uphold the promise.

Definition: If p then q

If p and q are statements, then the statement "if p, then q" is called the **conditional** of q by p and is denoted "$p \implies q$." p is called the **hypothesis** and q is called the **conclusion**. The truth table for the conditional is below.

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

When the hypothesis is false, the conditional is called **vacuously true**.

Remark. One could also write $q \impliedby p$, but since English is read left-to-right, we will typically avoid using the left-pointing arrow.

Remark. Your book uses two different arrows, $\to$ and $\implies$, which have different meanings in the realm of formal logic. In this class, we will be a little bit sloppy and always use $\implies$.

Since $p \to q$ is only false when p is true and q is false, then the following observation is immediate.

Example 2.2.1: conditional identity

Let p, q be statements. Use a truth table to show that $(p \Rightarrow q) \equiv (\neg p \vee q)$.

p	q	$p \implies q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Proposition 2.2.2: Negation of a conditional statement

If p, q are statements, then $\neg(p \Rightarrow q) \equiv (p \wedge \neg q)$.

Proof. Using the results of *Example* 2.2.1, this follows immediately from DeMorgan's Law.

$$\begin{aligned} \neg(p \implies q) &\equiv \neg(\neg p \vee q) \\ &\equiv \neg\neg p \wedge \neg q && \text{(DeMorgan's Law)} \\ &\equiv p \wedge \neg q && \text{(double negation law)} \end{aligned}$$

□

Now that we have a new symbol, we revisit the order of operations.

Order of Operations

1. Parentheses ()
2. $\neg$ or $\sim$
3. $\wedge$
4. $\vee$
5. $\implies$ or $\rightarrow$

Remark. Although the order of operations suggests that everything to the left of "$\implies$" implies everything to the right of "$\implies$," it is perfectly reasonable to use parentheses to clarify.

Example 2.2.3: Division Into Cases

Let p, q, r be statements. Show the following logical equivalence

$$\Big[p \vee q \implies r\Big] \equiv \Big[(p \implies r) \wedge (q \implies r)\Big].$$

p	q	r	$p \vee q$	$p \vee q \Rightarrow r$	$p \Rightarrow r$	$q \Rightarrow r$	$(p \Rightarrow r) \wedge (q \Rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

2.2.1 Related Conditionals

Definition: Converse, inverse, contrapositive

Given statements p, q and the conditional statement, $p \implies q$, there are three closely-related conditionals:

- The **converse** is $p \impliedby q$.
- The **inverse** is $\neg p \implies \neg q$.

- The **contrapositive** is $\neg p \iff \neg q$.

Example 2.2.4

Consider the following conditional statement:

If my car is in the repair shop, then I cannot get to class.

Write the converse, inverse, and contrapositive statements.

- [Converse] If I cannot get to class, then my car is in the repair shop.
- [Inverse] If my car is not in the repair shop, then I can get to class.
- [Contrapositive] If I can get to class, then my car is not in the repair shop.

Notice that some of these sound like they could be logically equivalent to one another. The contrapositive, for example, may be logically equivalent to the original statement. The converse, however, doesn't seem like it should be - there may be other reasons that one cannot attend class that are independent of the car needing repairs.

Proposition 2.2.5: Conditional Equivalences

Let S be the conditional statement $p \implies q$. Then
1. S is logically equivalent to the contrapositive of S, and
2. the converse of S is logically equivalent to the inverse of S.

Proof of 1.

$$\begin{aligned} p \implies q &\equiv \neg p \vee q && \text{(Conditional Identity)} \\ &\equiv \neg p \vee \neg(\neg q) && \text{(Double Negative Law)} \\ &\equiv \neg(\neg q) \vee \neg p && \text{(Commutative Law)} \\ &\equiv \neg q \implies \neg p && \text{(Conditional Identity).} \end{aligned}$$

□

Proof of 2.

$$\begin{aligned} q \implies p &\equiv \neg q \vee p && \text{(Conditional Identity)} \\ &\equiv \neg q \vee \neg(\neg p) && \text{(Double Negative Law)} \\ &\equiv \neg(\neg p) \vee \neg q && \text{(Commutative Law)} \\ &\equiv \neg p \implies \neg q && \text{(Conditional Identity).} \end{aligned}$$

□

One may use the phrase that p happens "only if" q happens. In other words, if q doesn't occur, then p doesn't occur. This is now phrased like the contrapositive, so it must be equivalent to $p \Rightarrow q$. We record this and some other typical phrases below

Logical form of common expressions

"p implies q"	means	"$p \implies q$"
"p only if q"	means	"$p \implies q$"
"p if q"	means	"$p \impliedby q$"
"p is a sufficient condition for q"	means	"$p \implies q$"
"p is a necessary condition for q"	means	"$p \impliedby q$"

2.2.2 Biconditional Statements

Definition: biconditional

If p, q are logical statements, then the **biconditional** of p and q, denoted $p \iff q$, is true when p and q have the same truth values, and false when p and q have opposite truth values.

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 2.2.6

Show that that $\Big[p \iff q\Big] \equiv \Big[(p \implies q) \wedge (p \implies q)\Big]$.

p	q	$p \Leftrightarrow q$	$p \Rightarrow q$	$p \Leftarrow q$	$(p \Rightarrow q) \wedge (p \Leftarrow q)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

Because of this connection, we often use the following English phrases to mean "$p \iff q$":

"p if and only if q."
"p iff q."
"p is both necessary and sufficient for q."

Example 2.2.7

For each set of statements below, fill in the blank to correctly identify whether the statement is an "if", "only if", or "if and only if" statement.

Note: Any mathematical statements below were chosen only to provide context for results you *may* have encountered before; none of them is actually mandatory prerequisite knowledge for this class.

It is cloudy	**if**	it is raining.
A polynomial has odd degree	**only if**	it has at least one real root.
The glass is half empty	**if and only if**	the glass is half full.
A matrix is invertible	**if and only if**	its determinant is nonzero.
Lassie is a dog	**only if**	Lassie is a mammal.
A function f has a critical point at $x = a$	**if**	$f'(a) = 0$.

Exercise 2.2.8

Let p, q be statements. What is the relationship between $p \iff q$ and $p \oplus q$?

2.3 Valid and Invalid Arguments

Definition: argument, validity

An **argument** is a sequence of statements. All statements in an argument, except for the final one are called **premises**. The final statement is called the **conclusion**. An argument is said to be **valid** when it satisfies the following criterion: if the premises are all true, then the conclusion is also true.

In logical symbols, an argument is typically written in the following way:

$$\begin{array}{ll} p_1 & \text{(hypothesis 1)} \\ p_2 & \text{(hypothesis 1)} \\ \vdots & \\ p_n & \text{(hypothesis 1)} \\ \hline \therefore\ c & \text{(conclusion)} \end{array}$$

The symbol $\therefore$ is read as "therefore."

Remark. An argument is valid whenever the proposition

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \implies c$$

is a tautology. In this way, it is clear that the order of the premises do not actually matter.

We can check validity of an argument using a truth table by looking for any rows with all true premises (called **critical rows**) and verifying that the conclusion table entry is also true *in every critical row*. If one or more critical rows has a false conclusion, the argument is invalid.

Example 2.3.1

Determine whether the following argument is valid or invalid.

$$\begin{array}{ll} & p \\ & p \implies q \\ \hline \therefore & q \end{array}$$

p	q	Premise 1 p	Premise 2 $p \Rightarrow q$	Conclusion q
T	T	T	T	T
T	F	T	F	
F	T	F		
F	F	F		

There is exactly one row where all hypotheses are true (highlighted), and that row has a true conclusions, so it must be valid.

Example 2.3.2

Determine whether the following argument is valid.

> If we meet the God of Death, then we say "Not today."[a]
> The phrase "not today" was not spoken.
> Therefore, we did not meet death.

[a] *Game of Thrones* Season 1, Episode 6.

The argument above can be simplified with symbols and variables.

$$\begin{array}{rl} & p \implies q \\ & \neg q \\ \therefore & \neg p \end{array}$$

and so we set up a truth table.

p	q	**Premise 1** $p \Rightarrow q$	**Premise 2** $\neg q$	**Conclusion** $\neg p$
T	T	T	F	F
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

There is only one row in the truth table where all premises are true, and that row also has a true conclusion, so it must be valid.

Example 2.3.3

Determine whether the following argument is valid.

$$\begin{array}{rl} & p \implies q \\ & \neg p \\ \hline \therefore & \neg q \end{array}$$

p	q	**Premise 1** $p \Rightarrow q$	**Premise 2** $\neg p$	**Conclusion** $\neg q$
T	T	T	F	
T	F	F		
F	T	T	T	F
F	F	T	T	T

There are two critical rows (highlighted), but one of them has a false conclusion. The argument is invalid.

Example 2.3.4

Determine whether the following argument is valid.

$$\begin{array}{l} p \vee q \\ \neg q \\ \hline \therefore \quad p \end{array}$$

p	q	Premise 1 $p \vee q$	Premise 2 $\neg q$	Conclusion p
T	T	T	F	
T	F	T	T	T
F	T	T	F	
F	F	F		

There is only one row in the truth table where all hypotheses are true (highlighted), and that row also has a true conclusion, so it must be a valid argument.

2.3.1 Rules of Inference

Definition: rule of inference

A **rule of inference** is the form of argument that is valid.

Theorem 2.3.5: Common Rules of Inference

Let p, q, r be propositions. The following are all valid logical argument forms.

(a) **modus ponens** [a]

$$\begin{array}{l} p \implies q \\ p \\ \hline \therefore \quad q \end{array}$$

(b) **modus tollens** [b]

$$\begin{array}{l} p \implies q \\ \neg q \\ \hline \therefore \quad \neg p \end{array}$$

(c) **contradiction rule**

$$\begin{array}{ll} p \implies \mathbf{c} & \text{(a contradiction)} \\ \therefore \quad \neg p & \end{array}$$

(d) **division of cases**

$$\begin{array}{l} p \vee q \\ p \Rightarrow r \\ q \Rightarrow r \\ \hline \therefore \quad r \end{array}$$

(e) **addition**

$$\begin{array}{l} p \\ \hline \therefore \quad p \vee q \end{array}$$

(f) **specialization** (or **simplification**)

$$\begin{array}{l} p \wedge q \\ \hline \therefore \quad p \end{array} \qquad \begin{array}{l} p \wedge q \\ \hline \therefore \quad q \end{array}$$

(g) **conjunction**[c]

$$\begin{array}{l} p \\ q \\ \hline \therefore \quad p \wedge q \end{array}$$

(h) **transitivity** (or **hypothetical syllogism**)

$$\begin{array}{l} p \implies q \\ q \implies r \\ \hline \therefore \quad p \implies r \end{array}$$

(i) **elimination** (or **disjunctive syllogism**) [d]

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore \quad q \end{array} \qquad \begin{array}{l} p \vee q \\ \neg q \\ \hline \therefore \quad p \end{array}$$

(j) **resolution**

$$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore \quad q \vee r \end{array}$$

[a] This is latin for "method of affirming" and was proven in Example 2.3.1.
[b] This is latin for "method of denying" and was proven in Example 2.3.2.
[c] The proof of this trivially follows from the definition of conjunction
[d] This was proven in Example 2.3.4.

Example 2.3.6: Proof of contradiction rule

Use a truth table to prove the contradiction rule in Theorem 2.3.5.

p	Premise 1 $p \Rightarrow c$	Conclusion $\neg p$
T	F	F
F	T	T

Example 2.3.7: Proof of division of cases

Use a truth table to prove the division of cases rule in Theorem 2.3.5.

p	q	r	Premise 1 $p \vee q$	Premise 2 $p \Rightarrow r$	Premise 3 $q \Rightarrow r$	Conclusion r
T	T	T	T	T	T	T
T	T	F	T	F		
T	F	T	T	T	T	T
T	F	F	T	F		
F	T	T	T	T	T	T
F	T	F	T	T	F	
F	F	T	F			
F	F	F	F			

Example 2.3.8: Proof of addition rule

Use a truth table to prove the addition rule in Theorem 2.3.5.

p	q	Premise 1 p	Conclusion $p \vee q$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	F	F

Example 2.3.9: Proof of simplification rule

Use a truth table to prove the simplification rule in Theorem 2.3.5.

p	q	Premise 1 $p \wedge q$	Conclusion p
T	T	T	T
T	F	F	T
F	T	F	
F	F	F	

Example 2.3.10: Proof of transitivity

Use a truth table to prove the transitivity rule in Theorem 2.3.5.

p	q	r	Premise 1 $p \Rightarrow q$	Premise 2 $q \Rightarrow r$	Conclusion $p \Rightarrow r$
T	T	T	T	T	T
T	T	F	T	F	
T	F	T	F		
T	F	F	F		
F	T	T	T	T	T
F	T	F	T	F	
F	F	T	T	T	T
F	F	F	T	T	T

Example 2.3.11: Proof of resolution

Use a truth table to prove the resolution rule in Theorem 2.3.5.

p	q	r	Premise 1 $p \vee q$	$\neg p$	Premise 2 $\neg p \vee r$	Conclusion $q \vee r$
T	T	T	T	F	T	T
T	T	F	T	F	F	
T	F	T	T	F	T	T
T	F	F	T	F	F	
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T		
F	F	F	F	T		

2.3.2 Logical Proofs

Definition: logical proof

A **logical proof** is a method of validating an argument by applying a sequence of rules of inference to deduce the stated conclusion from the hypotheses.

Remark. Logical proofs allow us to avoid truth tables. We note that, although the final proof is recorded in an enumerated list, you will likely think about things nonlinearly.

Remark. When writing down a logical proof, the only rule is that earlier steps cannot follow from later steps, otherwise you have freedom of choice as to when to introduce various statements. The analog in programming are the competing conventions of when to introduce variables – all at the beginning, or only before they are needed.

Example 2.3.12

Write a logical proof demonstrating the validity of the following argument.

$$\begin{array}{l} \neg A \implies (C \wedge D) \\ A \implies B \\ \neg B \\ \hline \therefore \quad C \end{array}$$

$\neg A \implies (C \wedge D)$	(premise 1)
$A \implies B$	(premise 2)
$\neg B$	(premise 3)

Begin by noticing that the last two lines of premises can be combined using modus tollens.

$$\begin{array}{l} A \implies B \\ \neg B \\ \hline \therefore \quad \neg A \end{array}$$

So we can rewrite the original collection of premises

$$\boxed{\begin{array}{l} \neg A \implies (C \wedge D) \\ A \implies B \\ \neg B \end{array}} \longrightarrow \boxed{\begin{array}{l} \neg A \implies (C \wedge D) \\ \neg A \end{array}}$$

Now notice that we can apply modus ponens

$$\begin{array}{l} \neg A \implies (C \wedge D) \\ \neg A \\ \hline \therefore \quad C \wedge D \end{array}$$

and our premises become

$$\boxed{\begin{array}{l} \neg A \implies (C \wedge D) \\ \neg A \end{array}} \longrightarrow \boxed{C \wedge D}$$

Finally, we can apply simplification to get

$$\begin{array}{l} C \wedge D \\ \hline \therefore \quad C \end{array}$$

which is precisely the conclusion we wanted to reach.
Now let's collect this all in a single procedural list.

1. $A \implies B$ (Hypothesis)
2. $\neg B$ (Hypothesis)
3. $\neg A$ (Modus Tollens, Steps 1 and 2)
4. $\neg A \implies (C \wedge D)$ (Hypothesis)
5. $C \wedge D$ (Modus Ponens, Steps 3 and 4)
6. C (Simplification in Step 6)

Example 2.3.13: Proof by Contradiction

Write down a logical proof demonstrating the validity of the following argument.

$$\begin{array}{ll} & P \implies R \\ & P \implies \neg R \\ \hline \therefore & \neg P \end{array}$$

First we apply the conditional identity to both of our premises. Begin by noticing that we can apply conjunction to our first two hypotheses

$$\begin{array}{ll} & P \implies R \\ \therefore & (\neg P \vee R) \end{array} \qquad \begin{array}{ll} & P \implies \neg R \\ \therefore & (\neg P \vee \neg R) \end{array}$$

so we rewrite the original collection of premises

$$\boxed{\begin{array}{l} P \implies R \\ P \implies \neg R \end{array}} \longrightarrow \boxed{\begin{array}{l} \neg P \vee R \\ \neg P \vee \neg R \end{array}}$$

We can now apply conjunction to get

$$\begin{array}{ll} & \neg P \vee R \\ & \neg P \vee \neg R \\ \therefore & (\neg P \vee R) \wedge (\neg P \vee \neg R) \end{array}$$

so we rewrite the premises

$$\boxed{\begin{array}{l} \neg P \vee R \\ \neg P \vee \neg R \end{array}} \longrightarrow \boxed{(\neg P \vee R) \wedge (\neg P \vee \neg R)}$$

Using the distributive property, we rewrite the premises again

$$\boxed{(\neg P \vee R) \wedge (\neg P \vee \neg R)} \longrightarrow \boxed{\neg P \vee (R \wedge \neg R)}$$

Applying the conditional identity

$$\boxed{\neg P \vee (R \wedge \neg R)} \longrightarrow \boxed{P \implies (R \wedge \neg R)}$$

The complement law yields

$$\boxed{P \implies (R \wedge \neg R)} \longrightarrow \boxed{P \implies \mathbf{c}}$$

and finally the contradiction rule gives

$$\boxed{P \implies \mathbf{c}} \longrightarrow \boxed{\neg P}$$

Now let's collect this all in a single procedural list.

1. $P \implies R$ (hypothesis)
2. $\neg P \vee R$ (conditional identity, 1)
3. $P \implies \neg R$ (hypothesis)
4. $\neg P \vee \neg R$ (conditional identity,3)
5. $(\neg P \vee R) \wedge (\neg P \vee \neg R)$ (conjunction,2 and 4)
6. $\neg P \vee (R \wedge \neg R)$ (distributive law, 5)
7. $P \implies (R \wedge \neg R)$ (conditional identity, 6)
8. $P \implies \mathbf{c}$ (complement law, 7)
9. $\neg P$ (contradiction rule)

2.3.3 Fallacies

Definition: fallacy

A **fallacy** is an error in reasoning that results in an invalid argument.

Remark. An argument is invalid precisely when all premises are true, but the conclusion is false.

Example 2.3.14: Ambiguous Premises

Ambiguous premises can arise in many ways. For example, using words with multiple meanings and equivocating them.

	6 is an odd number of legs for a horse.
	Odd numbers cannot be divided by 2.
Therefore	6 cannot be divided by 2.

The word "odd" in line 1 is a synonym for "unusual" and in line 2 it is being used to describe a number not divisible by 2.

Example 2.3.15: Ambiguous Premises

Ambiguous premises can arise in many ways. For example, using words that cannot be quantified:

	If you have a good understanding of Discrete Math, then you will do well on the exam.
	You have a good understanding of Discrete Math.
Therefore	you get an "A" on the exam.

"Doing well" on a test is ambiguous – arguably a grade of "B" or "C+" would be considered "doing well" to most.

Example 2.3.16: Circular Reasoning

Circular reasoning occurs when you use the conclusion as a premise.

You can't give me a "C" – I'm an "A" student!

You cannot claim to be an "A" student until you receive an "A" grade.

Example 2.3.17: Jumping to the Conclusion

Jumping to the conclusion happens when some premises are missing.

	Drake and Rihanna have been seen together in public.
Therefore	Drake and Rihanna are dating.

Example 2.3.18: Converse Error

Show that the following argument is invalid.

	If Zeke is a cheater, then Zeke sits in the back of the classroom.
	Zeke is sitting in the back of the classroom.
Therefore	Zeke is a cheater.

Let's assign some variables b, c to the above statements

c : "Zeke is a cheater"
b : "Zeke sits in the back"

Then we have the following truth table

		Premise 1	Premise 2	Conclusion
c	b	$c \Rightarrow b$	b	c
T	T	T	T	T
T	F	F		
F	T	T	T	**F**
F	F	T	F	

This is called the "converse error" beause it implicitly assumes that $q \Rightarrow p$ is logically equivalent to $p \Rightarrow q$, which is not the case.

Example 2.3.19: Inverse Error

Show that the following argument is invalid.

If this polygon $\mathcal{P}$ is a square, then it has four sides.
$\mathcal{P}$ is not a square.
Therefore $\mathcal{P}$ does not have four sides.

There are plenty of 4-sided polygons that are not squares, so already this argument seems problematic. Let's assign some variables s, f to the above statements

s : "$\mathcal{P}$ is a square"
f : "$\mathcal{P}$ has four sides"

Then we have the following truth table

		Premise 1	Premise 2	Conclusion
s	f	$s \Rightarrow f$	$\neg s$	$\neg f$
T	T	T	F	
T	F	F		
F	T	T	F	
F	F	T	T	**F**

This is called the "inverse error" because it implicitly assumes that $\neg p \Rightarrow \neg q$ is logically equivalent to $p \Rightarrow q$, which is not the case.

2.3.4 Sound Arguments

Definition

An argument is called **sound** if is it valid *and* the premises are all actually true. An argument is **unsound** otherwise.

The above is more of a philosophical distinction than one detectable in a truth table. For example, consider the two following arguments

If an animal is a fluffy god, then it has fur.
An animal does not have fur.
Therefore it is not a dog.

If a potato is green, then it is from Mars.
A potato is not from Mars.
Therefore that is not green.

Both of the above arguments are examples of *modus tollens* and are thusly valid. However, the one on the left is sound (ignore the pedantry of "hair vs. fur", but the one on the right is not – any discussion of Martian potatoes is pretty outlandish and absurd at present.

Remark. Don't eat green potatoes. Not only are they almost certainly not from Mars, they carry a high risk of solanine poisoning.

Chapter 3

The Logic of Quantified Statements

3.1 Predicates and Quantified Statements I

Definition: predicate, domain

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The **domain** of a predicate is the collection of values that may be substituted in place of the variable(s).

Example 3.1.1

Let $P(x)$ be the predicate $x^2 > x$ and let D be the domain $\mathbb{R}$ - the set of real numbers. Assess the truth values of the following statements: $P(-1), P(1), P(10)$.

$$\begin{array}{rll} P(-1): & (-1)^2 = 1 > -1 & \text{True} \\ P(1): & (1)^2 = 1 \not> 1 & \text{False} \\ P(10): & (10)^2 = 100 > 10 & \text{True} \end{array}$$

Example 3.1.2

Let $P(x, y)$ be the predicate $y \geq x$ and let D be the domain $\mathbb{R} \times \mathbb{R}$ (that is, x and y are both real numbers). Assess the truth values of the following statements: $P(0, 1)$, $P(1, 1)$, $P(1, 0.9)$.

$$\begin{array}{rll} P(0,1): & 1 \geq 0 & \text{True} \\ P(1,1): & 1 \geq 1 & \text{True} \\ P(1,0.9): & 0.9 \geq 1 & \text{False} \end{array}$$

Definition: truth set

If $P(x)$ is a predicate and x has domain D, then the **truth set** of $P(x)$ is the set of all elements of D that make $P(x)$ true when they are substituted for x. The truth set of $P(x)$ is denoted

$$\{x \in D \mid P(x)\}.$$

The symbol $\in$ is short for "in" in English.

Definition

The following short-hand notation is used for some commonly-occuring sets.

$\mathbb{N}$	The natural numbers: $0, 1, 2, 3, \ldots$
$\mathbb{Z}$	The integers: $\ldots, -2, -1, 0, 1, 2, \ldots$
$\mathbb{Z}^+$	The positive integers: $1, 2, 3, 4, \ldots$
$\mathbb{Q}$	The rational numbers (i.e. all possible fractions)
$\mathbb{R}$	The real numbers

Remark. Some people take the convention that 0 is not a natural number, and some take the convention that that 0 is a positive integer. These competing conventions are commonplace, and it's not often a big deal in practice if an author doesn't make their particular conventions explicit at the onset. Nevertheless, mathematicians are human and need something to argue about, so your instructor will staunchy insist that anyone who doesn't adhere to his conventions is patently wrong.

Example 3.1.3

Let $P(x)$ be the predicate $x^2 < 10$. Find the truth set for P when the domain D is ...

a. ... $\mathbb{N}$.

b. ... $\mathbb{Z}$.

c. ... $\mathbb{Z}^+$.

d. ... $\mathbb{R}$.

a. The natural numbers x which make $P(x)$ true are $\{0, 1, 2, 3\}$

b. The integers x which make $P(x)$ true are $\{-3, -2, -1, 0, 1, 2, 3\}$

c. The positive integers $\mathbb{Z}^+$ which make $P(x)$ true are $\{1, 2, 3\}$

d. The real numbers $\mathbb{R}$ which make $P(x)$ true are $\{x \in \mathbb{R} \mid -3 < x < 3\}$

3.1.1 The Universal Quantifier: $\forall$

Definition: universal statement, counterexample

Let $P(x)$ be a predicate and let D be the domain of x. A **universal statement** is a statement of the form

$$\text{For every } x \text{ in } D,\ P(x) \text{ is true. (In symbols, } \forall x \in D, P(x))$$

The universal statement $\forall x \in D, P(x)$ is true if and only if it is true for every x in D. The universal statement is false if there is at least one x' in D where $P(x')$ is false. Such an x' is called a **counterexample**.

Example 3.1.4

Let $P(x)$ be the predicate $x^2 \geq x$. Determine whether or not the universal statements are true or false.

1. $\forall x \in \mathbb{Z}, P(x)$
2. $\forall x \in \mathbb{R}, P(x)$

1. This is true.
2. This is false. When $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \not\geq x$, so $x = \frac{1}{2}$ is a counterexample. In fact, any x in the interval $0 < x < 1$ will be a counter-example.

Example 3.1.5: Method of Exhaustion

Let D be the following set of prime numbers

$$D = \{29, 41, 47, 53, 59\}$$

and let $P(x)$ be the predicate "x divided by 6 has a remainder of 5." Is the universal statement $\forall x \in D, P(x)$ true?

Statements about prime numbers are often nontrivial, but since we only have a few, we can check them all explicitly:

$$\begin{aligned} 29 &= 4(6) + 5 \\ 41 &= 6(6) + 5 \\ 47 &= 7(6) + 5 \\ 53 &= 8(6) + 5 \\ 59 &= 9(6) + 5 \end{aligned}$$

so the universal statement is true.

3.1.2 The Existential Quantifier: $\exists$

Definition: existential statement

Let $P(x)$ be a predicate and let D be the domain of x. An **existential statement** is a statement of the form

There exists some x in D for which $P(x)$ is true. (In symbols, $\exists x \in D, P(x)$)

The existential statement $\exists x \in D, P(x)$ is true if and only if it is true for at least one x in D. It is false if and only if it is false for every x in D.

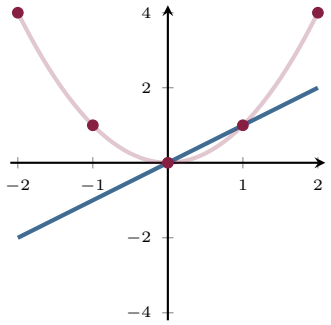
Example 3.1.6

Let $P(x)$ be the predicate $x^2 < x$. Determine whether or not the existential statements are true or false.

1. $\exists x \in \mathbb{R}, P(x)$
2. $\exists x \in \mathbb{Z}, P(x)$

1. This is true. When $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} < \frac{1}{2} = x$.
2. This is false. We don't yet have a means of proving it, but you can be convinced by

comparing the graphs of $y = x$ and $y = x^2$ (where x, y are integers).



In English, of course, there are numerous ways in which we can communicate these quantifiers. Below is an incomplete list of such things.

Quantifiers and common expressions

$\forall$	$\exists$
"for each"	"for some"
"for all"	"there is"
"for arbitrary"	"there exists"
"for any"	"at least one"
"for every"	"can find a"

Remark. It's also worth noting that, in symbolic logic, the quantifiers are always written first, but in English the quantifier may come at the end. For example

$$\text{"}x^2 \geq 0 \text{ for every } x \in \mathbb{R}\text{."}$$

3.1.3 Universal Conditional Statement

Definition: universal conditional statement

Let $P(x)$, $Q(x)$ be predicates with the same domain D. A **universal conditional statement** is a statement of the form

$$\text{For every } x \text{ in } D, \text{ if } P(x) \text{ is true, then } Q(x) \text{ is true.}$$

Symbolically, this is

$$\forall x \in D,\ P(x) \implies Q(x).$$

and it is true if and only if $P(x) \implies Q(x)$ is true *for every* x in the domain D. It is false if and only if it is false for *at least one* x in D (which occurs when $P(x)$ is true and $Q(x)$ is false).

Example 3.1.7

Which of the following conditionals are true for the domain $\mathbb{R}$?

1. $x^2 > 4 \implies x > 2$
2. $x^2 > 4 \iff |x| > 2$

For simplicity we use the following notation:

$$\begin{array}{ll} P(x) & \text{“}x^2 > 4\text{”} \\ Q(x) & \text{“}x > 2\text{”} \\ R(x) & \text{“}|x| > 2\text{”} \end{array}$$

1. $x^2 > 4 \implies x > 2$ is false. This universal conditional has the form

$$\forall x \in \mathbb{R}, P(x) \implies Q(x).$$

But $P(-3)$ is true and $Q(-3)$ is false, so $x = -3$ is a counterexample.

2. $x^2 > 4 \iff |x| > 2$ is true. This universal conditional has the form

$$\forall x \in \mathbb{R}, P(x) \iff R(x).$$

3.1.4 Implicit Quantification

As is often the case, many times the quantifier is not ever stated explicitly, which we refer to as **implicit quantification**. It is up to you, the reader, to correctly determine which quantifier applies here.

Example 3.1.8: Implicit Quantification

“The sum of even integers is even.”

“For all integers x and for all integers y, if x and y are even, then $x + y$ is even.”

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \text{ even} \wedge y \text{ even} \implies (x + y) \text{ even}$$

Example 3.1.9: Sentences: Informal to Formal

For each of the following statements, identify the predicate(s), domain(s), and variable(s). Then rewrite the sentence formally using logical symbols and quantifiers.

1. Whenever an integer is non-zero, its square is positive.
2. Every integer is even if its square is even.
3. $a^2 + 2 = 6$ for some integer a.
4. There's at least one ghost in this classroom right now.

1. *Whenever an integer is non-zero, its square is positive.*

$$\begin{aligned} P(x)&: \quad x \neq 0 \\ Q(x)&: \quad x^2 > 0 \\ D&: \quad \mathbb{Z} \end{aligned}$$

With the above notation, this sentence is written

$$\forall x \in \mathbb{Z},\ P(x) \implies Q(x).$$

. . . . . .

Alternatively, one could take

$$\begin{aligned} P(x)&: \quad x^2 > 0 \\ D&: \quad \text{nonzero integers} \end{aligned}$$

in which case the sentence is written

$$\forall x \in D,\ P(x).$$

---

2. *Every integer is even if its square is even.*

$$\begin{aligned} P(x)&: \quad x \text{ is even} \\ Q(x)&: \quad x^2 \text{ is even} \\ D&: \quad \mathbb{Z} \end{aligned}$$

With the above notation, this sentence can be written

$$\forall x \in \mathbb{Z},\ Q(x) \implies P(x).$$

---

3. $a^2 + 2 = 6$ *for some integer* a.

$$\begin{aligned} P(x)&: \quad x^2 + 2 = 6 \\ D&: \quad \mathbb{Z} \end{aligned}$$

With the above notation, this sentence can be written

$$\exists a \in \mathbb{Z},\ P(x).$$

---

4. *There's at least one ghost in this classroom right now.*

$$\begin{aligned} P(x)&: \quad x \text{ is in this classroom right now} \\ D&: \quad \text{Ghosts} \end{aligned}$$

With the above notation, this sentence can be written

$$\exists a \in D\ P(x).$$

Exercise 3.1.10: Sentences: Informal to Formal

For each of the following statements, identify the predicate(s), domain(s), and variable(s). Then rewrite the sentence formally using logical symbols and quantifiers.

1. Some people have tattoos.
2. Among all basketball players, some are tall.
3. Somebody in your group likes the orange Starburst.
4. There is an even prime number.
5. No Tech student has class on Sundays.
6. Integers are also real numbers.
7. All dogs go to heaven.
8. If a real number is rational, then so is its multiplicative inverse.
9. The sum of even integers is even.
10. Any factor of 4 is also a factor of 8.
11. John likes the taste of every Starburst.
12. For any Starburst flavor, there's someone out there who likes the taste it.

3.1.5 Relationship between $\forall$ and $\wedge$; Relationship between $\exists$ and $\vee$

Suppose $D = \{x_1, x_2, x_3, \ldots, x_n\}$ is a finite domain and $P(x)$ is some predicate. Using the method of exhaustion, one can verify the claim $\forall x \in D, P(x)$ by checking that $P(x_1)$, $P(x_2)$, ..., and $P(x_n)$ are all true. In other words

$$\forall x \in D, P(x) \equiv P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

Similarly, by exhaustion, one can verify the claim $\exists x \in D, P(x)$ by checking that at least one of $P(x_1)$, $P(x_2)$, ..., or $P(x_n)$ is true. In other words

$$\exists x \in D, P(x) \equiv P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

Example 3.1.11

Rewrite the following statements in terms of $\wedge$ and $\vee$.

1. Every integer x with $-1 \leq x \leq 1$ satisfies $x^3 = x$.
2. There is a natural number $x < 4$ for which $x^3 = x$.

In both of these, let $P(x)$ be the statement $x^3 = x$.

1. $\forall x \in \{-1, 0, 1\}, P(x) \equiv P(-1) \wedge P(0) \wedge (P1)$
2. $\exists x \in \{0, 1, 2, 3\}, P(x) \equiv P(0) \vee P(1) \vee P(2) \vee P(3)$

3.2 Predicates and Quantified Statements II

3.2.1 Negating Universal and Existential Statements

Recall that the universal statement statement

$$\forall x \in D, P(x)$$

is false when there is some x in D (that is, one or more) where $P(x)$ is false. Thus, its negation

$$\neg(\forall x \in D, P(x))$$

is true when there is some x in D where $P(x)$ is false. This observation (and the equivalent one when negating an existential statement) yields the following:

Theorem 3.2.1: Negation of Universal/Existential Statements

Let $P(x)$ be a predicate with domain D. Then we have the following:

$$\neg\left(\forall x \in D, P(x)\right) \equiv \exists x \in D, \neg P(x)$$
$$\neg\left(\exists x \in D, P(x)\right) \equiv \forall x \in D, \neg P(x)$$

Example 3.2.2

Negate the following statements.

1. All cats have wings.
2. $y^2 = -7$ for some integer y.
3. $x^2 > 1$ for all real numbers x.
4. No mathematicians are interesting.

1. The universally quantified object is "cats" and the predicate regards the number of wings, so the negation is

   Some cats have no wings.

2. The existentially quantified object is "y" and the predicate is $y^2 = -7$, so the negation is

   $y^2 \neq -7$ for all integers y.

3. The universally quantified object is "x" and the predicate is $x^2 > 1$, so the negation is

   $x^2 \leq 1$ for some real number x.

3.2.2 Conditionals - Related Conditionals and Negations

There are, of course, universal conditionals that are related to the usual universal conditional $\forall x \in D, P(x) \implies Q(x)$.

Definition: Related Universal Conditionals

Let $P(x), Q(x)$ be predicates with domain D and consider the universal conditional statement $\forall x \in D, P(x) \implies Q(x)$. The **contrapositive** is

$$\forall x \in D, \neg Q(x) \implies \neg P(x).$$

The **converse** is

$$\forall x \in D, Q(x) \implies P(x).$$

The **inverse** is

$$\forall x \in D, \neg P(x) \implies \neg Q(x).$$

Example 3.2.3

Write down the contrapositive, converse, and inverse of the following statement:

For all pairs of integers, x and y, if x is even and y is even then $x + y$ is even.

Let $\mathbb{Z}^2$ denote pairs of integers. Define the following predicates

$P(x, y)$: "x is even and y is even."
$Q(x, y)$: "$x + y$ is even."

The statement is then written symbolically as

$$\forall (x, y) \in \mathbb{Z}^2, P(x, y) \implies Q(x, y).$$

Now we have

(Contrapositive). Symbolically the contrapositive is $\forall (x, y) \in \mathbb{Z}^2, \neg Q(x, y) \implies \neg P(x, y)$, which can be written in plain English as

For all pairs of integers, x and y, if $x + y$ is not even then x and y are not both even.

(Converse). Symbolically the converse is $\forall (x, y) \in \mathbb{Z}^2, Q(x, y) \implies P(x, y)$, which can be written in plain English as

For all pairs of integers, x and y, if $x + y$ is even then x and y are both even.

(Inverse). Symbolically the converse is $\forall (x, y) \in \mathbb{Z}^2, Q(x, y) \implies P(x, y)$, which can be written in plain English as

For all pairs of integers, x and y, if x and y are not both even then $x + y$ is not even.

Proposition 3.2.4: Negation of Universal Conditional Statement

Let $P(x), Q(x)$ be predicates with domain D. Then we have the following:

$$\neg\left(\forall x \in D, P(x) \implies Q(x)\right) \equiv \exists x \in D, P(x) \wedge \neg Q(x).$$

Proof.

$$\begin{aligned}
\neg\left(\forall x \in D, P(x) \implies Q(x)\right) &\equiv \exists x \in D, \neg\left(P(x) \implies Q(x)\right) && (??)\\
&\equiv \exists x \in D, \neg\left(\neg P(x) \vee Q(x)\right) && (??)\\
&\equiv \exists x \in D, \neg\neg P(x) \wedge \neg Q(x) && \text{(DeMorgan's Law)}\\
&\equiv \exists x \in D, P(x) \vee \neg Q(x) && \text{(Double Negative Law)}
\end{aligned}$$

□

Example 3.2.5

Negate the following conditional statements:

1. $\forall x,$ if $x < -1,$ then $x^2 > 1$
2. Whenever VT students attend a football game, they sing "Enter Sandman."

1. We first begin by recalling that the negation of $a > b$ is $a \leq b$. Now,

$$\begin{aligned}
\neg\left(\forall x, \text{if } x < -1, \text{ then } x^2 > 1\right) &\equiv \exists x, \neg\left(\text{if } x < -1, \text{ then } x^2 > 1\right)\\
&\equiv \exists x, x < -1 \text{ and } \neg\left(x^2 > 1\right)\\
&\equiv \exists x, x < -1 \text{ and } x^2 \leq 1
\end{aligned}$$

2. First we have to interpret this symbolically to understand the (universal) conditional. This statement is about all VT students (by Hokie Law, you are required to know the lyrics of Enter Sandman...). If any student attends a football game, then they must sing "Enter Sandman". More symbolically, one might write

$$\forall \text{ student} \in \text{VT, student attends football game} \implies \text{student sings "Enter Sandman".}$$

So the negation is

$$\exists \text{ student} \in \text{VT, student attends football game } \textit{land} \text{ student does not sing "Enter Sandman".}$$

Written in plain English, one would probably write something like

There is a VT student who attends a foodball game and doesn not sing "Enter Sandman."

3.3 Statements with Multiple Quantifiers

As is often the case in math, quantified statements may involve multiple variables with multiple quantifiers. Anyone who has already taken a calculus class and has seen the formal definition of a limit has experienced this.

Definition of Limit of a Function

A function f has a limit L at $x = a$ if it has the following property:

$$\forall \varepsilon \in \mathbb{R}^+, \exists \delta \in \mathbb{R}^+, \forall x \in \mathbb{R}, \Big(0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon\Big)$$

Definition: nested quantifiers

A logical statement with multiple variables and multiple quantifiers is said to have **nested quantifiers**.

3.3.1 $\forall\forall$ Statements

Recall that, for a finite domain $D = \{d_1, \ldots, d_n\}$, we have

$$\forall x \in D, P(x) \equiv P(d_1) \wedge P(d_2) \wedge \cdots \wedge P(d_n)$$

Example 3.3.1

Let $D_x = \{x_1, x_2\}$ and $D_y = \{y_1, y_2\}$. Rewrite the following doubly-quantified statements

$$\forall x \in D_x, \forall y \in D_y, P(x, y)$$
$$\forall y \in D_y, \forall x \in D_x, P(x, y)$$

using only logical connectives $\wedge, \vee, \neg$.

$$\begin{aligned}\forall x(\forall y P(x,y)) &\equiv \forall x(P(x,y_1) \wedge P(x,y_2)) \\ &\equiv \Big(P(x_1,y_1) \wedge P(x_1,y_2)\Big) \wedge \Big(P(x_2,y_1) \wedge P(x_2,y_2)\Big)\end{aligned}$$

which by commutativity and associativity can be rewritten as

$$\begin{aligned}&\equiv \Big(P(x_1,y_1) \wedge P(x_2,y_1)\Big) \wedge \Big(P(x_1,y_2) \wedge P(x_2,y_2)\Big) \\ &\equiv \forall x(P(x,y_1) \wedge P(x,y_2)) \\ &\equiv \forall y(\forall x P(x,y))\end{aligned}$$

Example 3.3.2

Write the following sentence formally and rearrange the order of the quantifiers. Then translate this back into plain English.

Every student must do all homework problems.

Symbolically, the above sentence is

$$\forall x \in \{\text{students}\}, \forall y \in \{\text{homework problems}\}, x \text{ must do } y.$$

Changing the order

$$\forall y \in \{\text{homework problems}\}, \forall y \in \{\text{students}\}, y \text{ must do } x$$

which translates to

All homework problems must be done by everyone

and this has the same meaning as the original statement.

Nested Universal Quantifiers

Let $P(x,y)$ be a predicate involving two variables from domains D_x and D_y, respectively.

$$\forall x \in D_x, \forall y \in D_y, P(x,y) \equiv \forall y \in D_y, \forall x \in D_x, P(x,y)$$

3.3.2 $\exists\exists$ Statements

Recall that, for a finite domain $D = \{d_1, \ldots, d_n\}$, we have

$$\exists x \in D, P(x) \equiv P(d_1) \vee P(d_2) \vee \cdots \vee P(d_n)$$

Example 3.3.3

Let $D_x = \{x_1, x_2\}$ and $D_y = \{y_1, y_2\}$. Rewrite the following doubly-quantified statements

$$\exists x \in D_x, \exists y \in D_y, P(x, y)$$
$$\exists y \in D_y, \exists x \in D_x, P(x, y)$$

using only the logical connectives.

$$\begin{aligned}\exists x(\exists y P(x, y)) &\equiv \exists x(P(x, y_1) \vee P(x, y_2)) \\ &\equiv \Big(P(x_1, y_1) \vee P(x_1, y_2)\Big) \vee \Big(P(x_2, y_1) \vee P(x_2, y_2)\Big)\end{aligned}$$

which by commutativity and associativity can be rewritten as

$$\begin{aligned}&\equiv \Big(P(x_1, y_1) \vee P(x_2, y_1)\Big) \vee \Big(P(x_1, y_2) \vee P(x_2, y_2)\Big) \\ &\equiv \exists x(P(x, y_1) \vee P(x, y_2)) \\ &\equiv \exists y(\exists x P(x, y))\end{aligned}$$

Example 3.3.4

Write the following sentence formally and rearrange the order of the quantifiers. Then write the resulting sentence back in plain English.

Some kid is stealing cookies from one of the boxes.

Symbolically, the above sentence is

$$\exists x \in \{\text{kids}\}, \exists y \in \{\text{boxes of cookies}\}, x \text{ stole from } y.$$

Changing the order

$$\exists y \in \{\text{boxes of cookies}\}, \exists y \in \{\text{kids}\}, y \text{ stole from } x.$$

which translates to

There is a box from which some kid stole cookies.

and this has the same meaning as the original statement.

Nested Existential Quantifiers

Let $P(x, y)$ be a predicate involving two variables from domains D_x and D_y, respectively.

$$\exists x \in D_x, \exists y \in D_y, P(x, y) \equiv \exists y \in D_y, \exists x \in D_x, P(x, y)$$

3.3.3 $\forall\exists$ and $\exists\forall$ Statements

Example 3.3.5

Let $D_x = \{x_1, x_2\}$ and $D_y = \{y_1, y_2\}$. Rewrite the following doubly-quantified statements

$$\forall x \in D_x, \exists y \in D_y, P(x, y)$$
$$\exists y \in D_y, \forall x \in D_x, P(x, y)$$

using only the logical connectives. Are these logically equivalent?

$$\forall x(\exists y P(x, y)) \equiv \Big(P(x_1, y_1) \vee P(x_1, y_2)\Big) \wedge \Big(P(x_2, y_1) \vee P(x_2, y_2)\Big)$$
$$\exists y(\forall x P(x, y)) \equiv \Big(P(x_1, y_1) \wedge P(x_2, y_1)\Big) \vee \Big(P(x_1, y_2) \wedge P(x_2, y_2)\Big)$$

They do not appear to be logically equivalent. This can be seen looking at a truth table.

$P(x_1, y_1)$	$P(x_1, y_2)$	$P(x_2, y_1)$	$P(x_2, y_2)$	$\forall x\exists y P(x, y)$	$\exists y\forall x P(x, y)$
⋮	⋮	⋮	⋮	⋮	⋮
T	F	F	T	**T**	**F**
⋮	⋮	⋮	⋮	⋮	⋮

Example 3.3.6

Write the following symbolically, rearrange the quantifiers, and translate it back into plain English. How do the quantifiers change the meaning?

Everybody is good at something.

In symbols, this would read

$$\forall x \in \{\text{people}\}, \exists y \in \{\text{things}\}, x \text{ is good at } y.$$

Switching the order of the quantifiers, we get

$$\exists y \in \{\text{things}\}, \forall x \in \{\text{people}\}, x \text{ is good at } y.$$

which translates to

There is one thing that everyone is good at (i.e., everyone is good at the same thing).

and this sentence is not equivalent to the original sentence.

Nested Quantifiers of Mixed Type

Let $P(x, y)$ be a predicate involving two variables from domains D_x and D_y, respectively.

$$\forall x \in D_x, \exists y \in D_y, P(x, y) \not\equiv \exists y \in D_y, \forall x \in D_x, P(x, y)$$

$$\exists x \in D_x, \forall y \in D_y, P(x, y) \not\equiv \forall y \in D_y, \exists x \in D_x, P(x, y)$$

Remark. To be clear, even switching the placement of the variables results in inequivalent statements. In other words, none of $\forall x \exists y P(x, y)$, $\exists y \forall x P(x, y)$, $\forall y \exists x P(x, y)$, or $\exists x \forall y P(x, y)$ are equivalent. Below is the full truth table using the same domains above.

$P(x_1, y_1)$	$P(x_1, y_2)$	$P(x_2, y_1)$	$P(x_2, y_2)$	$\forall x \exists y$ $P(x, y)$	$\exists y \forall x$ $P(x, y)$	$\forall y \exists x$ $P(x, y)$	$\exists x \forall y$ $P(x, y)$	
T	T	T	T	T	T	T	T	(1)
T	T	T	F	T	T	T	T	(2)
T	T	F	T	T	T	T	T	(3)
T	T	F	F	F	F	T	T	(4)
T	F	T	T	T	T	T	T	(5)
T	F	T	F	T	T	F	F	(6)
T	F	F	T	T	F	T	F	(7)
T	F	F	F	F	F	F	F	(8)
F	T	T	T	T	T	T	T	(9)
F	T	T	F	T	F	T	F	(10)
F	T	F	T	T	T	F	F	(11)
F	T	F	F	F	F	F	F	(12)
F	F	T	T	F	F	T	T	(13)
F	F	T	F	F	F	F	F	(14)
F	F	F	T	F	F	F	F	(15)
F	F	F	F	F	F	F	F	(16)

One then sees that

$\forall x \exists y P(x, y) \not\equiv \exists y \forall x P(x, y)$	by row (7)
$\forall x \exists y P(x, y) \not\equiv \forall y \exists x P(x, y)$	by row (4)
$\forall x \exists y P(x, y) \not\equiv \exists x \forall y P(x, y)$	by row (4)
$\exists y \forall x P(x, y) \not\equiv \forall y \exists x P(x, y)$	by row (4)
$\exists y \forall x P(x, y) \not\equiv \exists x \forall y P(x, y)$	by row (4)
$\forall y \exists x P(x, y) \not\equiv \exists x \forall y P(x, y)$	by row (7)

Example 3.3.7

The following table encodes the truth values of $P(x, y)$ for all ordered pairs of $x = 1, \ldots, 5$ and $y = 1, \ldots, 5$.

$P(x,y)$	$x=1$	$x=2$	$x=3$	$x=4$	$x=5$
$y=1$	T	F	T	F	F
$y=2$	T	F	T	T	T
$y=3$	F	F	T	F	F
$y=4$	T	T	T	T	T
$y=5$	F	T	T	F	T

Determine which of the following are true:

(a) $\forall x, \exists y, P(x,y)$

(b) $\exists x, \forall y, P(x,y)$

(c) $\forall y, \exists x, P(x,y)$

(d) $\exists y, \forall x, P(x,y)$

(a) $\forall x, \exists y, P(x,y)$.
One should think about this statement as a game: If I hand you any x-value, can you find a y-value making $P(x,y)$ true? Yes, for example:

$$P(1,1), \quad P(2,4), \quad P(3,3), \quad P(4,4), \quad P(5,2)$$

(we remark that, for each x, the above choices of y are not unique possible choices). Thus the statement is true.

(b) $\exists x, \forall y, P(x,y)$
One should think about this statement as a game: Can you find a single x-value, so that $P(x,y)$ is always true no matter what y is? Yes, for example:

$$P(3,1), \quad P(3,2), \quad P(3,3), \quad P(3,4), \quad P(3,5)$$

Thus the statment is true.

(c) $\forall y, \exists x, P(x,y)$
One should think about this statement as a game: If I hand you any y-value, can you find a x-value making $P(x,y)$ true? Yes, for example:

$$P(3,1), \quad P(1,2), \quad P(3,3), \quad P(2,4), \quad P(5,5).$$

(we remark that, for each y, the above choices of x are not unique possible choices). Thus the statement is true.

(d) $\exists y, \forall x, P(x,y)$
One should think about this statement as a game: Can you find a single y-value, so that $P(x,y)$ is always true no matter what x is? Yes, for example:

$$P(1,4), \quad P(2,4), \quad P(3,4), \quad P(4,4), \quad P(5,4).$$

Thus the statement is true.

Example 3.3.8

The following table encodes the truth values of $P(x, y)$ and $Q(x, y)$ for all ordered pairs of $x = 1, 2, 3$ and $y = 1, 2, 3$.

$P(x,y)$	$x=1$	$x=2$	$x=3$
$y=1$	T	F	T
$y=2$	F	T	F
$y=3$	T	F	T

$Q(x,y)$	$x=1$	$x=2$	$x=3$
$y=1$	T	F	T
$y=2$	T	T	F
$y=3$	F	T	T

Determine which of the following are true:

(a) $\forall x, \exists y, P(x, y) \implies Q(x, y)$

(b) $\exists x, \forall y, P(x, y) \implies Q(x, y)$

(c) $\forall y, \exists x, P(x, y) \implies Q(x, y)$

(d) $\exists y, \forall x, P(x, y) \implies Q(x, y)$

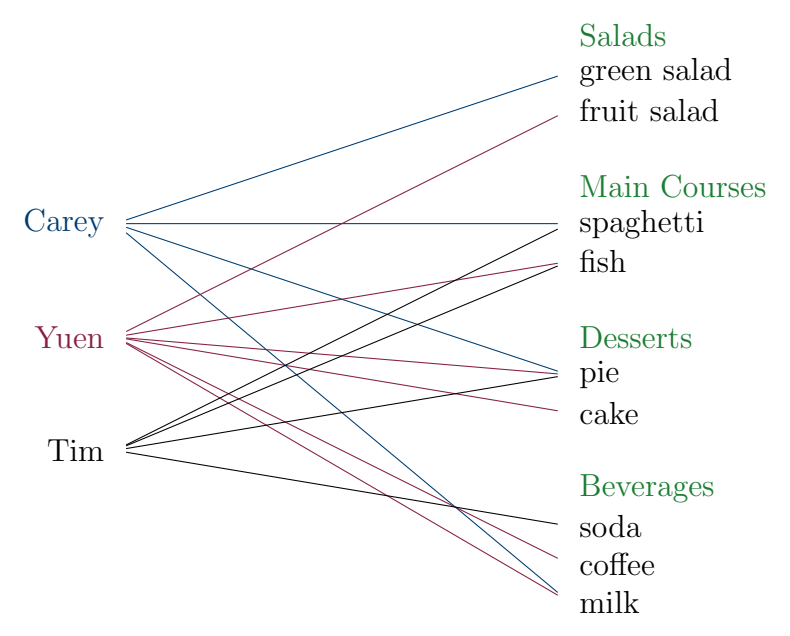
Recall that a conditional statement $p \implies q$ is only false when p is true and q is false. So for simplicity, we begin by making a single table corresponding to the conditional $P(x, y) \implies Q(x, y)$. That is, we look at the conditional $P(x, y) \implies Q(x, y)$ for every possible pair of (x, y).

$P(x,y) \implies Q(x,y)$	$x=1$	$x=2$	$x=3$
$y=1$	T	T	T
$y=2$	T	T	T
$y=3$	F	T	T

And now we've reduced this problem to something like Example 3.3.7 INCOMPLETE

Exercise 3.3.9

Three people, Carey, Yuen, and Tim, are going to eat at a buffet. The buffet has four main areas: salads, main courses, desserts, and beverages. The figure below shows which person (P) selected which item (I) from each area (A).



Rewrite each of the following statements informally and find its truth value.

1. $\exists I, \forall P, P$ chose I.
2. $\exists P, \forall I, P$ chose I.
3. $\exists P, \forall A, \exists I$ in A, P chose I.
4. $\forall P, \forall A, \exists I$ in A, P chose I.

Theorem 3.3.10: Negations of Multiple Quantifiers

Let $P(x, y)$ be a predicate and D_x, D_y the domains for x, y, respectively. Then

$$\neg\left(\forall x \in D_x, \exists y \in D_y, P(x, y)\right) \equiv \exists x \in D_x, \forall y \in D_y, \neg P(x, y)$$
$$\neg\left(\exists x \in D_x, \forall y \in D_y, P(x, y)\right) \equiv \forall x \in D_x, \exists y \in D_y, \neg P(x, y)$$

Example 3.3.11

Negate each of the following statements.

1. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $xy < 0$.
2. $\forall \varepsilon \in \mathbb{R}^+, \exists \delta \in \mathbb{R}^+, \forall x \in \mathbb{R}, \left[0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon\right]$.

1. $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$, $xy \geq 0$.
2. $\exists \varepsilon \in \{\text{positive reals}\}$ such that $\forall \delta \in \{\text{positive reals}\}$, $0 < |x - a| < \delta$ and $|f(x) - L| \geq \varepsilon$.

3.4 Arguments with Quantified Statements

3.4.1 Rules of inference with quantifiers

Definition: arbitrary, particular

An element x of a domain D is called **arbitrary** if it is indistinguishable from all other elements in the domain. x is called **particular** if it has some additional properties not shared by the other elements in the domain.

Remark. In a proof, you will never see the word "particular," but they are usually pretty easy to identify as there are usually other conditions that are satisfied. For example, if the domain is $\mathbb{Z}$, then you might see something like "take $x = 1$" or "Let x be an integer greater than 2."
Arbitrary elements are sometimes labeled as arbitrary, usually with a phrase like "arbitrary" or "fixed, but arbitrary." However, it is often the case that the arbitrary-ness is only communicated implicitly.

Theorem 3.4.1: Quantified Rules of Inference

Let $P(x)$ be a predicate. The following are all valid logical argument forms.

(a) **universal instantiation**

	c is an element (arbitrary or particular)
	$\forall x \in D, P(x)$
$\therefore$	$P(c)$

(b) **universal generalization**

	c is an arbitrary element
	$P(c)$
$\therefore$	$\forall x \in D, P(x)$

(c) **existential instantiation**

	$\exists x \in D, P(x)$
$\therefore$	(c is a particular element) $\wedge P(c)$

(d) **existential generalization**

	c is an element (arbitrary or particular)
	$P(c)$
$\therefore$	$\exists x \in D, P(x)$

Remark. Instantiation allows us remove the quantifiers and focus on a single statement $P(c)$. We can then apply rules of inference to this single statement.
Generalization allows us to add quantifiers to a single statement $P(c)$.

We should be a bit more verbose and explanatory about why each of the above works.

Universal instantiation. If $P(x)$ is true for every x in the domain, then we can pick a single element c from the domain and it follows that $P(c)$ must be true. We may choose c arbitrarily or not – it doesn't matter because c is in the domain and $P(x)$ is true for every x in the domain.

Universal generalization. Since an arbitrary element c is indistinguishable from all other elements, proving $P(c)$ represents the exact same strategy that we would use to prove $P(x)$ for every $x \in D$. Thus we can conclude that our singular proof is enough to conclude $\forall x \in D, P(x)$. Note that c being arbitrary is necessary: if c is particular and satisfies some additional conditions not shared by the rest of the domain, we can't actually conclude that $P(x)$ holds for every x in the domain.

Existential instantiation. If $P(x)$ is true for some x in the domain, then there must be some element c for which $P(c)$ is true. However, such a c is probably pretty special ($P(x)$ may be true for only a handful of domain elements), so c is necessarily particular.

Existential generalization. If we can show that there is an element c (either arbitrary or particular – it doesn't matter) for which $P(c)$ is true, then we can claim there is an element in the domain for which the predicate evaluates to true. Hence $\exists x \in D, P(x)$.

Example 3.4.2: Universal Modus Ponens

Let P and Q be predicates with domain D. Use the Rules of Inference to see that the following argument is valid.

$$\begin{array}{ll} & \forall x \in D, P(x) \implies Q(x) \\ & \exists x \in D, P(x) \\ \hline \therefore & \exists x \in D, Q(x) \end{array}$$

Proof.

1.	$\forall x \in D, P(x) \implies Q(x)$	(Hypothesis)
2.	$\exists x \in D, P(x)$	(Hypothesis)
3.	$c \in D$ is particular	(Existential Instantiation, 2)
4.	$P(c)$	(Existential Instantiation, 2)
5.	$P(c) \implies Q(c)$	(Universal Instantiation, 1 & 3)
6.	$Q(c)$	(Modus Ponens, 4 & 5)
7.	$\exists x \in D, Q(x)$	(Existential Generalization, 3 & 6)

□

Example 3.4.3: Universal Modus Tollens

Let P and Q be predicates with domain D. Use the Rules of Inference to see that the following argument is valid.

$$\begin{array}{ll} & \forall x \in D, P(x) \implies Q(x) \\ & \exists x \in D, \neg Q(x) \\ \hline \therefore & \exists x \in D, \neg P(x) \end{array}$$

Proof.

1.	$\forall x \in D, P(x) \implies Q(x)$	(Hypothesis)
2.	$\exists x \in D, \neg Q(x)$	(Hypothesis)
3.	$c \in D$ is particular	(Existential Instantiation, 2)
4.	$\neg Q(c)$	(Existential Instantiation, 2)
5.	$P(c) \implies Q(c)$	(Universal Instantiation, 1 & 3)
6.	$\neg P(c)$	(Modus Tollens, 4 & 5)
7.	$\exists x \in D, \neg P(x)$	(Existential Generalization, 3 & 6)

□

Example 3.4.4: Proof by Cases

Let P, Q, R be predicates with domain D. Use the Rules of Inference to see that the following argument is valid.

$$\begin{array}{l} \forall x \in D, (P(x) \vee Q(x)) \\ \forall x \in D, (P(x) \implies R(x)) \\ \forall x \in D, (Q(x) \implies R(x)) \\ \hline \therefore \quad \forall x \in D, R(x) \end{array}$$

We begin by applying universal instantiation to each of the premises.

$$\boxed{\begin{array}{l} c \text{ is arbitrary} \\ P(c) \vee Q(c) \\ P(c) \implies R(c) \\ Q(c) \implies R(c) \end{array}}$$

Now, each of $P(c), Q(c), R(c)$ is a *statement* and is definitively true or false. We can apply the conditional identity of Table of Logical Equivalances and rewrite some of the hypotheses.

$$\boxed{\begin{array}{l} c \text{ is arbitrary} \\ P(c) \vee Q(c) \\ \neg P(c) \vee R(c) \\ \neg Q(c) \vee R(c) \end{array}}$$

We combine two of the hypotheses using the resolution rule of inference

$$\boxed{\begin{array}{l} c \text{ is arbitrary} \\ Q(c) \vee R(c) \\ \neg Q(c) \vee R(c) \end{array}}$$

We combine two of the hypotheses using the resolution rule of inference

$$\boxed{\begin{array}{l} c \text{ is arbitrary} \\ R(c) \vee R(c) \end{array}}$$

Now we use the idempotent law to rewrite our premises as

$$\boxed{\begin{array}{l} c \text{ is arbitrary} \\ R(c) \end{array}}$$

And finally some universal generalization to write

$$\boxed{\forall x \in D, R(x)}$$

Now we'll write down this sequence of steps in a logical proof.

Proof.

1.	$\forall x \in D, (P(x) \vee Q(x))$	(Hypothesis)
2.	$\forall x \in D, (P(x) \implies R(x))$	(Hypothesis)
3.	$\forall x \in D, (Q(x) \implies R(x))$	(Hypothesis)
4.	$c \in D$ is arbitrary	(defining an arbitrary variable)
5.	$P(c) \vee Q(c)$	(Universal Instantiation, 1 & 4)
6.	$P(c) \implies R(c)$	(Universal Instantiation, 2 & 4)
7.	$Q(c) \implies R(c)$	(Universal Instantiation, 3 & 4)
8.	$\neg P(c) \vee R(c)$	(Conditional Identity, 6)
9.	$\neq Q(c) \vee R(c)$	(Conditional Identity, 7)
10.	$Q(c) \vee R(c)$	(Resolution, 5 & 8)
11.	$R(c) \vee R(c)$	(Resolution, 9 & 10)
12.	$R(c)$	(Idempotent Law, 11)
13.	$\forall x \in D, R(x)$	(Universal Generalization, 4 & 12)

□

3.4.2 Logical Proofs with Nested Quantifiers

The same rules of inference work for nested quantifiers, applied successively left-to-right. But since order matters, we need to think very carefully about our instantiated variables.

Example 3.4.5: Mixed Type Quantifiers and Instantiation

Explain the subtle (but very important) difference in the proofs below.

1.	$\exists x \forall y, P(x, y)$	(Hypothesis)
2.	c is particular	($\exists$ Inst., 1)
3.	$\forall y, P(c, y)$	($\exists$ Inst., 1)
4.	d is arbitrary	(def. of variable)
5.	$P(c, d)$	($\forall$ Inst., 3 & 4)
⋮		

1.	$\forall y \exists x, P(x, y)$	(Hypothesis)
2.	d is arbitrary	(def. of variable)
3.	$\exists x, P(x, d)$	($\forall$ Inst., 1 & 2)
4.	c is particular	($\exists$ Inst., 3)
5.	$P(c, d)$	($\exists$ Inst., 3)
⋮		

The difference between the two proofs is in the variable c.

- In the proof on the left, c is chosen so that $P(c, y)$ is true, regardless of y. This means that c's definition is independent of d.
- In the proof on the right, c is chosen so that $P(c, d)$ is true, which means that c's definition is *very much dependent upon* d.[a]

[a] Although it would make notation more cumbersome, it would be appropriate to write $c(d)$ to stress the fact that c is a particular function of d. This is actually not uncommon in mathematics literature.

3.4.3 An Actual Math Proof

Let's see a logical proof in context.

Example 3.4.6: "If x is even, then x^2 is even."

For simplicity, all variables below have domain $\mathbb{Z}$.

Let $E(x)$ be the predicate "$\exists k, x = 2k$." Use the rules of inference to see that the following argument is valid.

$\forall x \forall y, [xy \in \mathbb{Z}]$	(closure of multiplication)
$\forall x \forall y \forall z \forall w, [w = x(yz) \implies w = (xy)z]$	(associativity of multiplication)
$\forall x \forall y \forall z, [(x = y) \implies (xz = yz)]$	(multiplicative property of equality)
$\therefore \quad \forall x, E(x) \implies E(x^2)$	

Proof. In what follows, all variables have domain $\mathbb{Z}$.

1.	$\forall x \forall y, [xy \in \mathbb{Z}]$	(hypothesis)
2.	$\forall x \forall y, \forall z \forall w [w = x(yz) \implies w = (xy)z]$	(hypothesis)
3.	$\forall x \forall y \forall z, [(x = y) \implies (xz = yz)]$	(hypothesis)
4.	n is arbitrary integer	(element definition)
5.	k is arbitrary integer	(element definition)
6.	$(n = 2k) \implies \left(n^2 = (2k)n\right)$	(universal instantiation, 3)
7.	$\left(n^2 = (2k)n\right) \implies \left(n^2 = 2(kn)\right)$	(universal instantiation, 2)
8.	$(n = 2k) \implies \left(n^2 = 2(kn)\right)$	(transitivity, 7 & 8)
9.	$kn \in \mathbb{Z}$	(universal instantiation, 1)
10.	$(n = 2k) \implies \exists z \left[n^2 = 2z\right]$	(existential generalization, 9)
11.	$\exists y \left(n = 2y\right) \implies \exists z \left(n^2 = 2z\right)$	(existential generalization, 10)
12.	$\forall x \left[\exists y \left(x = 2y\right) \implies \exists z \left(x^2 = 2z\right)\right]$	(universal generalization, 11)

and this final line is precisely the statement $\forall x, E(x) \implies E(x^2)$. □

Chapter 4

Elementary Number Theory and Methods of Proof

4.1 Direct Proof and Counterexample I: Introduction

4.1.1 Context/Relation to Formal Proofs

Definition: theorems,propositions,lemmas,corollaries

A **theorem** or **proposition** or **lemma** or **corollary** is a statement that requires proof.

Remark. In math, the different naming is really just to convey nome heirarchy as to importance of results. For example

- Theorems – these are the big, important results.
- Propositions – these are big results, but not as important as theorems.
- Lemmas – these are results (usually fairly technical) proven to aid in the proof of Theorems/Propositions.
- Corollaries – these are interesting results that follow immediately from one of the above and usually require almost no proof.

Remark. To avoid confusion with "proposition" as used synonymously with "statement," we will not use that term in this class. In fact, we'll default to "Theorem" for everything we prove.

Most theorems are simply stated as quantified statements of one of the following forms

$$\forall x, P(x) \qquad \forall x, P(x) \implies Q(x) \qquad \exists x, P(x)$$

but are really arguments of the following forms

(hypotheses)
$\therefore \quad \forall x, P(x)$

(hypotheses)
$\therefore \quad \forall x, P(x) \implies Q(x)$

(hypotheses)
$\therefore \quad \exists x, P(x)$

where the hypotheses are things like definitions, rules of arithmetic, etc.
Look again at Example 3.4.6 from the end of last class:

Theorem 4.1.1

For all integers x, if x is even, then x^2 is even.

Letting $E(x)$ be the predicate "x is even," the argument of the proof was more formally

$\forall x \forall y, [xy \in \mathbb{Z}]$	(closure of multiplication)
$\forall x \forall y \forall z \forall w, [w = x(yz) \implies w = (xy)z]$	(associativity of multiplication)
$\forall x \forall y \forall z, [(x = y) \implies (xz = yz)]$	(multiplicative property of equality)
$\therefore \quad \forall x, E(x) \implies E(x^2)$	

and the proof was

Proof. In what follows, all variables have domain $\mathbb{Z}$.

1.	$\forall x \forall y, [xy \in \mathbb{Z}]$	(hypothesis)
2.	$\forall x \forall y, \forall z \forall w [w = x(yz) \implies w = (xy)z]$	(hypothesis)
3.	$\forall x \forall y \forall z, [(x = y) \implies (xz = yz)]$	(hypothesis)
4.	n is arbitrary integer	(element definition)
5.	k is arbitrary integer	(element definition)
6.	$(n = 2k) \implies \left(n^2 = (2k)n\right)$	(universal instantiation, 3)
7.	$\left(n^2 = (2k)n\right) \implies \left(n^2 = 2(kn)\right)$	(universal instantiation, 2)
8.	$(n = 2k) \implies \left(n^2 = 2(kn)\right)$	(transitivity, 7 & 8)
9.	$kn \in \mathbb{Z}$	(universal instantiation, 1)
10.	$(n = 2k) \implies \exists z \left[n^2 = 2z\right]$	(existential generalization, 9)
11.	$\exists y \, (n = 2y) \implies \exists z \left(n^2 = 2z\right)$	(existential generalization, 10)
12.	$\forall x \left[\exists y \, (x = 2y) \implies \exists z \left(x^2 = 2z\right)\right]$	(universal generalization, 11)
12.	$\forall x \left[\exists y \, (x = 2y) \implies \exists z \left(x^2 = 2z\right)\right]$	(universal generalization, 11)
12.	$\forall x, \left[(x = 2y) \implies \exists z \left(x^2 = 2z\right)\right]$	(universal generalization, 11)
13.	$\forall x, \left[E(x) \implies E(x^2)\right]$	(rewriting, 12)

□

Our goal is going to be to write proofs like this in a human-readable way.

4.1.2 Important Hypotheses and Definitions

Generally we'll assume all of the usual rules of arithmetic; see Appendix A of the course textbook. Some specific ones that we'll give names to are the following:

Important Arithmetic Hypotheses

1. The integers are **closed under addition**. (The sum of two integers is again an integer.) Stated formally,
$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, [x + y \in \mathbb{Z}]$$
2. The integers are **closed under multiplication**. (The product of two integers is again an integer.)
$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, [xy \in \mathbb{Z}]$$

Definition: even and odd integers

An integer is said to be **even** precisely when it is twice another integer. An integer is said to be **odd** if and only if it is 1 more than twice another integer. Symbolically,

$$\begin{aligned} n \text{ is even} &\iff \exists k \in \mathbb{Z} \text{ such that } n = 2k. \\ n \text{ is odd} &\iff \exists k \in \mathbb{Z} \text{ such that } n = 2k+1. \end{aligned}$$

Remark. You may freely regard "odd" as meaning "not even."

Since even/oddness is an existential statement, any proof requires only finding a single integer k.

Example 4.1.2

Use the definitions of even and odd to justify the following statements.

1. 0 is even.
2. -401 is odd.
3. If a, b are integers, $6a^2b$ is even.

1. *Proof.* Choosing $k = 0$, we have that $0 = 2(0) = 2k$. Therefore 0 is even. □
2. *Proof.* Choosing $k = -201$, we have that $-401 = 2(-201) + 1 = 2k + 1 =$. Therefore -401 is odd. □
3. Notice that this statement nas multiple quantifiers $\forall a \in \mathbb{Z}, \forall b \in Z, \exists k \in \mathbb{Z}$ such that $6a^2b = k$.

   Proof. Let $a, b \in \mathbb{Z}$ and choose $k = 3a^2b$. As the integers are closed under multiplication, k is an integer. We have that $6a^2b = 2(3a^2b) = 2k$, therefore $6a^2b$ is even. □

Definition: prime and composite numbers

An positive integer p is **prime** if and only if $p > 1$ and for any integers m, n with $p = mn$, then one of m or n is p. An integer is **composite** if and only if $p > 1$ and there are integers $1 < m, n < p$ for which $p = mn$. Symbolically,

$$\begin{aligned} p \text{ is prime} &\iff p > 1 \text{ and } \forall m, n \in Z^+, \text{ if } p = mn \text{ then } m = p \\ &\quad \text{or } n = p. \\ p \text{ is composite} &\iff p > 1 \text{ and } \exists m, n \in Z^+ \text{ such that } 1 < m, n < p \\ &\quad \text{and } p = mn. \end{aligned}$$

Remark. "Composite" and "not prime" are not actually negations of each other. "Not prime" allows for the possibility that $p = 1$.

Remark. You may assume that both the m and n in the definition of prime satisfy $1 \leq m, n \leq p$. We'll prove in a later section that this has to happen.

Example 4.1.3

Use the definitions of prime and composite to justify each of the following statements

1. 1 is not prime.
2. 2468 is composite.
3. 5 is prime.

1.

Proof. By definition, a prime number is strictly greater than 1. Therefore 1 is not prime. □

2.

Proof. Choose $m = 2$ and $n = 1234$, which satisfies $1 < m < n < 2468$. Since $2468 > 1$ and $2468 = 2(1234) = mn$, then 2468 is a composite number. □

3. Using the remark above, we have to show that the only possible integers m and n for which $p = mn$ are $m = 1, n = 5$ or $m = 5, n = 1$. We can do this by checking all possible pairs with $1 \leq m, n \leq p$.

Proof. Look at the following table.

mn	$m = 1$	$m = 2$	$m = 3$	$m = 4$	$m = 5$
$n = 1$	1	2	3	4	5
$n = 2$	2	4	6	8	10
$n = 3$	3	6	9	12	15
$n = 4$	4	8	12	16	20
$n = 5$	5	10	15	20	25

□

4.1.3 Proofs – Scaffolding

You should think of writing a proof as something akin to writing an essay. You need to organize your thoughts and scaffold it into a proof. Here is a simple list.

1. **Restate the theorem symbolically**
   You want to make sure you appropriately parse the theorem to understand the quantifiers, predicates, any conditionals, etc.

2. **State relevant definitions**

3. **State your assumptions and list any variables (are they arbitrary or particular?)**

4. **State your goal (what are you trying to deduce from your assumptions?)**

5. **Scratch work/algebra**

6. **Write the proof**

4.1.4 Proving an Existential Statement

Proving a Existential Statement

1. Express the statement to be proved in the form $\exists x \in D, P(x)$.
2. Let x_0 be a fixed particular element of the domain. This is for you to choose.
3. Show that $P(x_0)$ is true by using definitions and previously established rules.
4. Existential generalization allows us to conclude that the original existential proposition is true.

Example 4.1.4

Prove the following theorem.

Theorem. There is an odd composite number.

Our scratch work

1. **Restate the theorem symbolically**

$$\exists x \in \mathbb{Z}^+, x \text{ is odd} \wedge x \text{ is composite.}$$

2. **State relevant definitions**
   x_0 is "odd" iff that we can find an integer k so that $x_0 = 2k + 1$.
   x_0 is "composite" iff we can find two integers m, n with $x_0 = mn$ and $1 < m, n < x_0$.
3. **State your assumptions and list any variables (are they arbitrary or particular?)**
   Particular integers: $x_0 = 9$, $k = 4$, $m = 3$, $n = 3$.
4. **State your goal (what are you trying to deduce from your assumptions?)**
   Want to show that x_0 is odd using k, and x_0 is composite using m, n above.
5. **Scratch work/algebra**

$$x_0 = 2(4) + 1$$
$$x_0 = (3)(3)$$

Proof. Choose $x_0 = 9$, an integer. Since we can write $x_0 = 2(4) + 1$ and $4 \in \mathbb{Z}$, then 9 is odd. Since we can write $x_0 = 9 = (3)(3)$, and $3 \in Z$ satisfies $1 < 3 < 9$, then x_0 is also composite. □

Definition: Constructive and Nonconstructive Proofs of Existence

A **constructive proof** of existence involves

1. finding an x in our domain for which $Q(x)$ is true or
2. giving an set of directions for finding such an x in the domain.

A **nonconstructive proof** of existence involves showing either:

1. the existence of a value x that makes $Q(x)$ true is guaranteed by an axiom or a previously

proved theorem

2. the assumption that there is no such x leads to a contradiction.

You've probably seen a non-constructive proof before; below is one such proof.

Example 4.1.5: non-constructive proof

Prove the claim:

$$\text{The polynomial } p(x) = x^5 - x + 1 \text{ has a real root.}$$

Proof. Recall from calculus that polynomials are continuous functions. Since $p(-2) = -29$ and $p(1) = 1$ and $-29 < 0 < 1$, then by the Intermediate Value Theorem, there is a real number $x \in (-2, 1)$ for which $p(x) = 0$. □

4.1.5 Disproving Universal Statements

Recall the negation

$$\neg(\forall x, P(x))$$

is logically equivalent to

$$\exists x, \neg P(x).$$

Disproof by Counterexample: $\forall x \in D, P(x)$

1. Pick a particular c in the domain.
2. Verify $P(c)$ is false.(c is a *counterexample*)
3. By existential generalization, conclude $\exists x, \neg P(x)$.
4. By logical equivalence, we conclude that $\forall x, P(x)$ is false.

Recall the negation

$$\neg(\forall x, P(x) \implies Q(x))$$

is logically equivalent to

$$\exists x, P(x) \wedge \neg Q(x).$$

Disproof by Counterexample: $\forall x \in D, P(x) \implies Q(x)$

1. Pick a particular c in the domain.
2. Verify $P(c)$ is true.
3. Verify $Q(c)$ is false.(c is a *counterexample*)
4. By existential generalization, conclude $\exists x, P(x) \wedge \neg Q(x)$.
5. By logical equivalence, we conclude that $\forall x, P(x)$ is false.

Example 4.1.6

Prove or disprove the following claim:

For all real numbers a, b, if $a < b$ then $a^2 < b^2$.

Our scratch work

1. **Restate the theorem symbolically**
   INCOMPLETE
2. **State relevant definitions**
   INCOMPLETE
3. **State your assumptions and list any variables (are they arbitrary or particular?)**
   INCOMPLETE
4. **State your goal (what are you trying to deduce from your assumptions?)**
   INCOMPLETE
5. **Scratch work/algebra**
   INCOMPLETE

Disproof. Let $a = -10$ and $b = 1$. Then $a = -10 < 1 = b$, but $a^2 = 100 \geq 1 = b^2$. □

4.1.6 Proving a Universal Statement

We've already seen the Method of Exhaustion before, which works well for small finite domains. In practice

Direct Proof of Universal Statement $\forall x, P(x)$

1. Let c be a fixed, but arbitrary, element of the domain.
2. Show that $P(c)$ is true by using definitions and previously established rules.
3. By universal generalization, conclude that $\forall x \in D, P(x)$.

Remark. Item 2 is doing *a lot* of heavy lifting here - that's absolutely the hard part and there's no one-size-fits-all strategy for doing it – this is where you, the human, have to think.

Direct Proof of Universal Statement $\forall x, P(x) \implies Q(x)$

1. Let c be a fixed, but arbitrary, element of the domain.
2. Suppose that $P(c)$ is true.
3. Show that the conclusion $Q(c)$ is true by using definitions and previously established rules.
4. By universal generalization, conclude that $\forall x \in D, P(x) \implies Q(x)$.

Remark. If c is arbitrary, it's entirely possible that $P(c)$ is false. This is okay – $P(c) \implies Q(c)$ is vacuously true. As such, we lose nothing in the way of generality by assuming in Item 2 that $P(c)$ is true.

Example 4.1.7

Prove the statement:

The sum of two even integers is even.

Our scratch work

1. **Restate the theorem symbolically**
   INCOMPLETE
2. **State relevant definitions**
   INCOMPLETE
3. **State your assumptions and list any variables (are they arbitrary or particular?)**
   INCOMPLETE
4. **State your goal (what are you trying to deduce from your assumptions?)**
   INCOMPLETE
5. **Scratch work/algebra**
   INCOMPLETE

We first acknowledge that, symbolically, this statement is $\forall x \in Z, \forall y \in Z$ if x is even and y is even, then $x + y$ is even. For scratch work, recalling the definition of even and odd **??**, we know that, if x, y are even, there are integers k, ℓ for which

$$x = 2k \text{ and } y = 2\ell \implies x + y = 2k + 2\ell = 2(k + \ell)$$

and these rearrangement rules give us the clue into the proof.

Proof. Suppose x and y are arbitrary even integers. Then (by definition) there exist integers k and ℓ such that $x = 2k$ and $y = 2\ell$. It follows then that $x + y = 2k + 2\ell = 2(k + \ell)$. Since the integers are closed under addition, $k + \ell$ is an integer, and therefore $x + y$ is an even integer. □

4.1.7 Disproving an Existential Statement

Recall the negation

$$\neg(\exists x, P(x))$$

is logically equivalent to

$$\forall x, \neg P(x)$$

Disproving an Existential: $\exists x \in D, P(x)$

1. Let c be a fixed, but arbitrary, element of D.
2. Prove $\neg P(c)$
3. By universal generalization, conclude that $\forall x, \neg P(x)$.
4. By logical equivalence, conclude $\exists x, P(x)$ is false.

Example 4.1.8

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Our scratch work

1. **Restate the theorem symbolically**
   INCOMPLETE
2. **State relevant definitions**
   INCOMPLETE
3. **State your assumptions and list any variables (are they arbitrary or particular?)**
   INCOMPLETE
4. **State your goal (what are you trying to deduce from your assumptions?)**
   INCOMPLETE
5. **Scratch work/algebra**
   INCOMPLETE

Proving that this statement is false is equivalent to proving that its negation is true. The negation of this statement is

For every positive integer n, $n^2 + 3n + 2$ is composite (i.e. not prime).

We begin with some scratch work. Notice that we can factor this quadratic

$$n^2 + 3n + 2 = (n + 1)(n + 2)$$

and neither of the factors are 1.

Proof. Let n be an arbitrary positive integer. Then

$$n^2 + 3n + 2 = (n + 1)(n + 2)$$

and since $n > 0$ (by definition), then neither $n + 1 = 1$ nor $n + 2 = 1$. Therefore $n^2 + 3n + 2$ cannot be a prime number. □

4.1.8 Proof by Cases

NOTE TO INSTRUCTOR: Proof By Cases is technically handled in Section 4.6, so this entire subsection has been copied there. In future iterations of these notes, delete this subsection.

Recall that

$$\Big[(P(x) \vee Q(x)) \implies R(x)\Big]$$

is logically equivalent to

$$\Big[P(x) \implies R(x)\Big] \wedge \Big[P(x) \implies R(x)\Big].$$

Proof by Cases: $\forall x \in D, [P(x) \vee Q(x) \implies R(x)]$

1. Let c be a fixed, but arbitrary element of D.
2. Case 1:
   (a) Assume $P(c)$ is true.
   (b) Prove $R(c)$ is true.
3. Case 2:
   (a) Assume $Q(c)$ is true.
   (b) Prove $R(c)$ is true.
4. By logical equivalence, conclude $(P(c) \vee Q(c)) \implies R(c)$.
5. By universal generalization, conclude that $\forall x, (P(x) \vee Q(x)) \implies R(x)$.

Remark. $P(x)$ and $Q(x)$ do not have to be distinct/disjoint! If $P(x)$ is "x is prime" and $Q(x)$ is "x is even", then there will be overlap when $x = 2$.

Remark. You may have to come up with $P(x)$ and $Q(x)$ on your own.

Remark. You may have to come up with far more than 2 cases. Famously, Kenneth Appel and Wolfgang Haken proved the *Four Color Theorem* using more than 1500 cases. (Neil Robertson has since proven that 663 cases is sufficient.)

Example 4.1.9

Prove that for all integers n, $n^2 - 3n$ is even.

Our scratch work

1. **Restate the theorem symbolically**
   INCOMPLETE
2. **State relevant definitions**
   INCOMPLETE
3. **State your assumptions and list any variables (are they arbitrary or particular?)**
   INCOMPLETE
4. **State your goal (what are you trying to deduce from your assumptions?)**
   INCOMPLETE
5. **Scratch work/algebra**
   INCOMPLETE

It's not presently clear that $n^2 - 3n$ becomes twice some integer, but maybe if we know more about n we can say more. Let's do some scratch work.

$$\begin{aligned} n = 2k &\implies n^2 - 3n = (2k)^2 - 3(2k) = 2(2k^2 - 3k) \\ n = 2k+1 &\implies n^2 - 3n = (2k+1)^2 - 3(2k+1) = 4k^2 + 4k + 1 - 6k - 3 \\ &\qquad = 4k^2 - 2k - 2 = 2(2k^2 - k - 2) \end{aligned}$$

Proof. Suppose that n is an even integer. Then there exists another integer k for which $n = 2k$.

It follows that

$$n^2 - 3n = 2(2k^2 - 3k).$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $2k^2 - 3k$ is an integer. Therefore $n^2 - 3n$ is even.
Suppose now that n is an odd integer. Then there exists another integer ℓ for which $n = 2\ell$. It follows that

$$n^2 - 3n = 2(2k^2 - k - 2).$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $2k^2 - k - 2$ is an integer. Therefore $n^2 - 3n$ is even.
We conclude that, regardless of the parity of n, $n^2 - 3n$ is an even integer. □

4.1.9 Direct Proof with Nested Quantifiers

Proving a Statement with Nested Quantifiers: $\forall x, \exists y, P(x, y)$

1. Let x_0 be a fixed arbitrary element of the domain D_x.
2. Pick y_0 in the domain D_y. Your choice of y_0 will likely be a function of x_0.
3. Show that the conclusion $P(x_0, y_0)$ is true by using definitions and previously established rules.
4. Existential/Universal generalization allows us to conclude that the original universal statement is true.

Example 4.1.10

Prove the following theorem.

> **Theorem.** For every real number $x \neq 1$, there is some real number y for which $xy = x + y$.

Scratch work.
Symbolically we can write

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}\,[(x \neq 1) \implies (xy = x + y)]$$

although it may be beneficial for the purposes of writing the proof to write

$$\forall x \in \mathbb{R}\,[(x \neq 1) \implies \exists y \in \mathbb{R}(xy = x + y)]$$

We try out some scratch work and manipulate our target equation to see if we can figure out how to choose y.

$$xy = x + y \implies xy - y = x \implies (x - 1)y = x \implies y = \frac{x}{x - 1}$$

From here we probably have enough to write our proof.

Proof. Let x be an arbitrary real number and suppose that $x \neq 1$. Since $x \neq 1$, then $x-1 \neq 0$, so we choose $y = \dfrac{x}{x-1}$. Now we have that

$$xy = \frac{x^2}{x-1}$$

and

$$x + y = x + \frac{x}{x-1} = \frac{x(x-1)}{x-1} + \frac{x}{x-1} = \frac{x(x-1)+x}{x-1} = \frac{x^2-x+x}{x-1} = \frac{x^2}{x-1}$$

therefore $xy = x + y$. □

Exercise 4.1.11

Prove the following theorem.

Theorem. For all positive real numbers a, b, c, if

$$\begin{cases} a+b>c, \\ a+c>b, \text{ and} \\ b+c>a \end{cases}$$

there is a triangle $\triangle ABC$ in the Cartesian plane with side lengths a, b, c.

I don't expect you to prove this, but it's interesting to think about what this problem looks like symbolically and figure out how we might approach this.

$$\forall a \in \mathbb{R}^+, \forall b \in \mathbb{R}^+, \forall c \in R^+ \left[\begin{pmatrix} (a+b>c) \\ \wedge\,(a+c>b) \\ \wedge\,(b+c>a) \end{pmatrix} \implies \exists \triangle ABC \right]$$

So we'll let a, b, c be arbitrary, but fixed, and we'll try to construct $\triangle ABC$. Now, we can always think about rotating and translating the triangle in the plane, so we might as well assume that one vertex is at the origin and another vertex is along the x-axis.

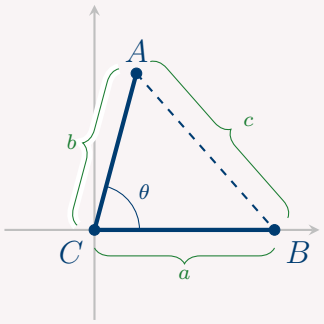


Figure 4.1: The general setup for the triangle we construct

After this setup, it comes down to finding the particular θ so that the distance between A and B has length c. That such a θ exists require some more thought, but this seems like a decent strategy to start with.

Proof. Let a, b, c be arbitrary positive integers, and suppose these numbers satisfy the following inequalities:

$$\begin{cases} a+b>c, \\ a+c>b, \text{ and} \\ b+c>a \end{cases}$$

Without loss of generality, let's assume that $a \geq b$. We place the points $C(0,0)$, $B(a,0)$, and $A(b\cos\theta, b\sin\theta)$ in the plane, where θ is some real number between 0 and π. In this way, the length of $\overline{BC}$ is a, the length of $\overline{AC}$ is b. All that's left is to find the particular θ-value for which $\overline{AB}$ has length c. Notice that the distance between points A and B is given by the distance function

$$d(\theta) = \sqrt{(b-a\cos\theta)^2 + b^2\sin^2\theta}.$$

This function is continuous on the interval $[0,\pi]$. In this interval, d satisfies

$$a-b \leq d(\theta) \leq a+b$$

The first assumed inequality shows that $c < a+b$, and the third assumed inequality rearranges to show that $a-b<c$. Combining these two, we see that

$$a-b<c<a+b$$

so by the Intermediate Value Theorem, there is a value of θ in $(0,\pi)$ for which $d(\theta)=c$, as desired. □

The proof above is kind of interesting because, although we tried to explicitly construct the triangle, the existence of the triangle was actually shown non-explicitly (the IVT does not tell you what the value is; just that it exists.

You could also have used the Law of Cosines to get the value of θ specifically:

$$\theta = \cos^{-1}\left(\frac{c^2-a^2-b^2}{2ab}\right)$$

Proving a Statement with Nested Quantifiers: $\exists x \forall y, P(x,y)$

1. Pick x_0 as a particular element from the domain D_x.
2. Let y_0 be a fixed, but arbitrary, element in the domain D_y. Your choice of y_0 *cannot* depend on x_0.
3. Show that the conclusion $P(x_0, y_0)$ is true by using definitions and previously established rules.
4. Existential/Universal generalization allows us to conclude that the original universal statement is true.

Example 4.1.12

Prove the following claim.

Theorem. $f(x) = \dfrac{1}{x^2+1}$ is a bounded function. That is, there exists some positive real number M so that $|f(x)| \leq M$ for all $x \in \mathbb{R}$.

Scratch work.
Symbolically this statement says

$$\exists M \in \mathbb{R}, \forall x \in \mathbb{R}, \left|\frac{1}{x^2+1}\right| \leq M$$

Proof. Take $M = 1$ and let x be an arbitrary real number. We know that $x^2 \geq 0$, so we have

$$\begin{aligned} x^2 &\geq 0 \\ x^2 + 1 &\geq 1 \\ \frac{1}{x^2+1} &\leq \frac{1}{1} = 1 \end{aligned}$$

We also note that $\frac{1}{x^2+1}$ is always positive, hence is equal to its own absolute value. Therefore, for all x,

$$\left|\frac{1}{x^2+1}\right| \leq M.$$

□

4.2 Direct Proof and Counterexample II: Writing Advice

Guidelines for Writing Proofs

1. Begin by writing the statement which you wish to prove.
2. Identify the domain, hypotheses and conclusion.
3. Clearly mark the beginning of your proof with the word Proof.
4. Make your proof self-contained.
5. Write your proof in complete, grammatically correct sentences. In particular, do not use symbols to replace simple words in sentences
   ("Todd is happy and Tammi is sad" vs. "Todd is happy $\wedge$ Tammi is sad.")
6. Keep your reader informed about the status of each statement in your proof.
7. Give a reason for each assertion in your proof.
8. Include connecting words and phrases to make your argument clear.
9. Display equations and inequalities.
10. Make sure that the conclusion has been explicitly shown.
11. Clearly mark the end of your proof, usually with a symbol like $\square$ or $\blacksquare$.

(Note that if you use LaTeX, then typing `\begin{proof}...\end{proof}` *will handle items 3 and 11 for you.*

Note that the above should not be taken as a rigid set of instructions, but more as a guide line. Professional mathematicians will often skip item 10, for example, when the statement of the theorem immediately precedes the proof.

4.2.1 Common Mistakes in Proof-Writing

Example 4.2.1: Arguing from examples

Prove: The sum of any two even integers is even.

Proof. This is true because if $m = 14$ and $n = 6$, which are both even, then $m + n = 20$, which is also even. $\square$

Example 4.2.2: Using the same letter to mean two different things

Prove: the sum of any two even integers is even.

Proof. Let m and n be fixed, but arbitrary, even integers. Then $m = 2k$ and $n = 2k$ for some integer k.

$\vdots$

$\square$

Example 4.2.3: Jumping to a conclusion

Prove: The sum of any two even integers is even.

Proof. Let m and n be fixed, but arbitrary, even integers. Then by the definition of even, $m = 2k_1$ and $n = 2k_2$ for some integers k_1 and k_2. Thus, $m + n = 2k_1 + 2k_2$. So $m + n$ is even. □

Example 4.2.4: Circular reasoning

Prove: The product of odd integers is odd.

Proof. Suppose m and n are odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd. □

Example 4.2.5: Confusion between what is known and what is still to be shown

Prove: The product of two odd integers is odd.

Proof. Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that $mn = 2s + 1$.
Also by the definition of odd, there exist integers a and b such that $m = 2a + 1$ and $n = 2b + 1$.
Then $mn = (2a + 1)(2b + 1) = 2s + 1$.
So, since s is an integer, mn is odd by definition of odd. □

This following issues are not serious on their own, but each reflects imprecise thinking that sometimes leads to problems later in a proof.

Example 4.2.6: Use of *any* rather than *some*

Prove: The square of any odd integer is odd.

Proof. Suppose m is a fixed, but arbitrary, odd integer. By definition of odd, $m = 2a + 1$ for any integer a.
⋮

□

Example 4.2.7: Use of *if* rather than *because* or *since*

Prove: The square of any odd integer is odd.

Proof. Suppose m is a fixed, but arbitrary, chosen odd integer. If m is odd, $m = 2a + 1$ for any integer a. ⋮

□

4.3 Direct Proof and Counterexample III: Rational Numbers

Definition: rational numbers

A real number r is a **rational number** if and only if, there are integer a, b with $b \neq 0$ such that $r = \frac{a}{b}$.

$$r \text{ is rational} \iff \exists p \in \mathbb{Z} \text{ and } \exists q \in \mathbb{Z} \text{ such that } r = p/q \text{ and } q \neq 0.$$

A real number that is not rational is called **irrational**.

Remark. The set of rational numbers is typically denoted $\mathbb{Q}$, and the irrational numbers are denoted $\mathbb{R} \setminus \mathbb{Q}$ or $\mathbb{R} - \mathbb{Q}$.

Remark. The name rational number comes from the fact that we can write a *ratio*nal number as a *ratio* of integers.

Although this is contained in the properties of real numbers per Appendix A, we'll state it in an attempt to be self-contained:

Zero Product Property

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ have the following property:

If x and y are both nonzero numbers, then xy is nonzero.

The contrapositive of this statement is:

If the product of numbers $xy = 0$, then at least one of x and y is zero.

Example 4.3.1: Properties of $\mathbb{Q}$

Prove the following theorem.

Theorem. $\mathbb{Q}$ has the following properties:

$\mathbb{Q}$ **is closed under addition.** The sum of two rational numbers is a rational number..

$\mathbb{Q}$ **is closed under multiplication.** The product of two rational numbers is a rational number.

Proof. Let x, y be arbitrary rational numbers. By definition, we must have integers a_1, a_2 and nonzero integers b_1, b_2 such that

$$x = \frac{a_1}{b_1} \qquad \text{and} \qquad y = \frac{a_2}{b_2}.$$

$\mathbb{Q}$ **is closed under addition.** Notice that

$$x + y = \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2}{b_1 b_2} + \frac{a_2 b_1}{b_1 b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

Since the integers are closed under addition and multiplication, then $a_1b_2 + a_2b_1$ and b_1b_2 are integers. Since b_1, b_2 are nonzero, then b_1b_2 is also nonzero by the zero product property for $\mathbb{Z}$. Thus $x + y$ is rational.

$\mathbb{Q}$ **is closed under multiplication.** Left as an exercise for the reader.

□

Example 4.3.2

Prove the following theorem.

Theorem. Every integer is a rational number.

In order to prove this, we begin by noting that this statement can be written in logical symbols as

$$\forall z \in \mathbb{Z}, z \text{ is rational.}$$

which again becomes

$$\forall z \in \mathbb{Z}, \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, \text{ such that} z = \frac{a}{b} \text{ and } b \neq 0$$

Now we know that this is a universal statement, so we need to let z be fixed but arbitrary and then show that we can choose a and b appropriately.

Proof. Let x be an arbitrary integer, and choose integers $a = x$ and $b = 1$. Then we have that

$$x = \frac{x}{1} = \frac{a}{b}$$

so x is a rational number, by definition. □

Example 4.3.3

Prove or disprove the following claim.

Claim. Given any rational number x, there is an integer y for which xy is an integer.

Symbolically, this statement is

$$\forall x \in \mathbb{Q}, \exists y \in \mathbb{Q}, \text{ such that } xy \in \mathbb{Z}$$

which means that x is arbitrary and we get to choose y (in a way that probably relies on x).

Proof. Let x be an arbitrary rational number. By definition, we can write $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Choose $y = b$. With this choice, we have that

$$xy = \left(\frac{a}{b}\right)(b) = \frac{a}{1} = a$$

and a is an integer, whence xy is an integer. □

Alternate proof idea.

Proof. Let x be an arbitrary rational number and choose $y = 0$. Then we have that $xy = x(0) = 0$ and since 0 is an integer, xy is an integer. □

Example 4.3.4

Prove or disprove the following claim.

Claim. The irrational numbers are closed under addition.

Symbolically, this statement is

$$\forall x \in \mathbb{R} - \mathbb{Q}, \forall y \in \mathbb{R} - \mathbb{Q}, x - y \in \mathbb{R} - \mathbb{Q}$$

Disproof. Choose $x = \pi$ and $y = -\pi$, two irrational numbers. Then $x + y = \pi - \pi = 0$, an integer, hence we've found a counterexample to the claim. □

4.4 Direct Proof and Counterexample IV: Divisibility

Definition: divides

Let n, d be integers. We say that d **divides** n if $d \neq 0$ and there exists some integer k for which $n = dk$. Notationally, we write this as $d \mid n$.

Other phrases:

- n is **divisible** by d.
- n is a **multiple** of d.
- d is a **divisor** of n.
- d is a **factor** of n.

Remark. Do not confuse the "divides" sign with a fraction. $d \mid n$ is equivalent to saying that $\frac{n}{d}$ is an integer.

Example 4.4.1

Prove or disprove the following claim.

Claim. For all integers a, b, c, if $a|b$ and $a|c$, then $a|(b+c)$.

Proof. Let a, b, c be arbitrary integers and suppose both that $a|b$ and $a|c$. By definition of divisibility, we must have that a is nonzero and that there are integers k, ℓ for which

$$b = ak \quad \text{and} \quad c = a\ell.$$

By routine algebraic manipulation, we see that

$$b + c = ak + a\ell = a(k + \ell)$$

and we note that $k + \ell$ is an integer since $\mathbb{Z}$ is closed under addition. Since $a \neq 0$, then we must have that $a|(b+c)$. □

Example 4.4.2

Prove or disprove the following claim.

Claim. For all integers a, b, c, if $a|(b+c)$, then $a|b$ and $a|c$.

Disproof. Take $a = 4$, $b = 2$ and $c = 6$. □

Example 4.4.3

Prove or disprove the following claim.

Claim. For all integers a, b, c, if $a|b$ and $a|(b+c)$, then $a|c$.

Proof. Suppose $a|b$ and $a|(b+c)$. Then there are integers k and ℓ for which $b = ak$ and $b + c = a\ell$. Combining this information and utilizing our algebra skills

$$b + c = a\ell \implies c = a\ell - b = a\ell - (ak) = a(\ell - k)$$

since the integers are closed under addition and multiplication, $\ell - k$ is an integer. Therefore c is an integer multiple of a, whence $a|c$ as desired. □

Example 4.4.4: Transitivity of Division

Prove or disprove the following claim.

Claim. For all integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

Proof. Let $a, b, c \in \mathbb{Z}$ be arbitrary and suppose that $a|b$ and $b|c$. By definition of division, there exist integers k, ℓ for which $b = ak$ and $c = b\ell$. Combined this gives $c = b(ak) = a(bk)$ (since integer multiplication is commutative). Moreover, by closure integer multiplication, bk is an integer, and therefore $a|c$. □

Example 4.4.5

Prove or disprove the following claim.

Claim. For all integers a, b, c, if $a|bc$, then $a|b$ and $a|c$.

Disproof, sketch. Take $a = 4, b = 2, c = 2$. □

Example 4.4.6

Prove or disprove the following claim.

Claim. For all integers a, b, c, if $a|b$ and $a|bc$, then $a|c$.

Disproof, sketch. Take $a = 2, b = 4, c = 3$. □

Example 4.4.7

Prove or disprove the following claim.

Claim. For all integers a, b, c, d, if $a|b$ and $c|d$, then $ac|(bc + ad)$.

Proof sketch. $b = ak$ and $d = c\ell$, so

$$bc + ad = (ak)c + a(c\ell) = ac(k + \ell)$$

□

Lemma 4.4.8

For any positive integer k, $10^k - 1$ is divisible by 9.

Proof. Notice that

$$10^k - 1 = (10 - 1)(10^{k-1} + 10^{k-2} + \cdots + 10^2 + 10 + 1)$$

and $10 - 1 = 9$. □

Theorem 4.4.9: Easy Test for Division by 9

For all positive integers n, n is divisible by 9 if and only if the sum of n's digits is a multiple of 9.

Proof. Let n be an arbitrary $(k+1)$-digit number "$a_k a_{k-1} \cdots a_2 a_1 a_0$", by which we mean that

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0. \tag{4.1}$$

Through routine algebraic manipulation (which we've tried to color-code for simplicity for the reader) Equation (4.1) can be rewritten as

$$\begin{aligned} n &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \\ &= a_k + a_k(10^k - 1) + a_{k-1} + a_{k-1}(10^{k-1} - 1) + \cdots + a_1 + a_1(10 - 1) + a_0 \\ &= a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \cdots + a_1(10 - 1) + (a_k + a_{k-1} + \cdots + a_1 + a_0) \end{aligned} \tag{4.2}$$

Lemma 4.4.8 guarantees the existence of integers $m_1, \ldots, m_k$ for which Equation (4.2) becomes

$$\begin{aligned} &= a_k(9m_k) + a_{k-1}(9m_{k-1}) + \cdots + a_1(9m_1) + (a_k + a_{k-1} + \cdots + a_1 + a_0) \\ &= 9\,(a_k m_k + a_{k-1} m_{k-1} + \cdots + a_1 m_1) + (a_k + a_{k-1} + \cdots + a_1 + a_0) \end{aligned} \tag{4.3}$$

Case (⇒). Suppose that n is divisible by 9. By Equation (4.3), since

$$n = 9\,(a_k m_k + a_{k-1} m_{k-1} + \cdots + a_1 m_1) + (a_k + a_{k-1} + \cdots + a_1 + a_0)$$

and 9 clearly divides $9\,(a_k m_k + a_{k-1} m_{k-1} + \cdots + a_1 m_1)$, then by Example 4.4.3 9 divides $(a_k + a_{k-1} + \cdots + a_1 + a_0)$.

Case (⇐). Suppose that $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 9. It follows from the definition that there is some integer m_0 for which

$$a_k + a_{k-1} + \cdots + a_1 + a_0 = 9m_0.$$

By substituting this into Equation (4.3), we obtain

$$\begin{aligned} n &= 9(a_k m_k) + 9(a_{k-1} m_{k-1}) + \cdots + 9(a_1 m_1) + 9m_0 \\ &= 9(a_k m_k + a_{k-1} m_{k-1} + \cdots + a_1 m_1 + m_0) \end{aligned}$$

As $\mathbb{Z}$ is closed under addition and multiplication, this complicated expression is just 9 times an integer, whence n must be divisible by 9.

□

Corollary 4.4.10

A number n is divisible by 3 if and only if the sum of its digits are divisible by 3.

Exercise 4.4.11

Does the same test hold for multiples of 6?

4.6 Proof By Cases

Recall that

$$\Big[(P(x) \vee Q(x)) \implies R(x)\Big]$$

is logically equivalent to

$$\Big[P(x) \implies R(x)\Big] \wedge \Big[P(x) \implies R(x)\Big].$$

Proof by Cases: $\forall x \in D, [P(x) \vee Q(x) \implies R(x)]$

1. Let c be a fixed, but arbitrary element of D.
2. Case 1:
   (a) Assume $P(c)$ is true.
   (b) Prove $R(c)$ is true.
3. Case 2:
   (a) Assume $Q(c)$ is true.
   (b) Prove $R(c)$ is true.
4. By logical equivalence, conclude $(P(c) \vee Q(c)) \implies R(c)$.
5. By universal generalization, conclude that $\forall x, (P(x) \vee Q(x)) \implies R(x)$.

Remark. $P(x)$ and $Q(x)$ do not have to be distinct/disjoint! If $P(x)$ is "x is prime" and $Q(x)$ is "x is even", then there will be overlap when $x = 2$.

Remark. You may have to come up with $P(x)$ and $Q(x)$ on your own.

Remark. You may have to come up with far more than 2 cases. Famously, Kenneth Appel and Wolfgang Haken proved the *Four Color Theorem* using more than 1500 cases. (Neil Robertson has since proven that 663 cases is sufficient.)

Exercise 4.6.1

Prove the following theorem.

Theorem. For all integers n, $n^2 - 3n$ is even.

NOTE TO INSTRUCTOR: In future iterations of these notes, turn this into an example and uncomment work.

Exercise 4.6.2

Prove the following claim.

Theorem. For every integer n, either $3|n^2$ or $3|(n^2 - 1)$.

NOTE TO INSTRUCTOR: In future iterations of these notes, turn this into an example and uncomment work.

Proof by cases and the absolute value function

Definition: absolute value

The **absolute value of a real number** x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{when } x \geq 0 \\ x & \text{when } x < 0 \end{cases}$$

Because the definition has two cases, often times proofs involving absolute values will require two (or more) cases.

Exercise 4.6.3: triangle inequality

Prove the following claim.

Theorem. For all real numbers x and y,

$$|x + y| \leq |x| + |y|.$$

NOTE TO INSTRUCTOR: In future iterations of these notes, turn this into an example and uncomment work.

4.7 Indirect Argument: Contradiction and Contraposition

4.7.1 Contradiction

Proof By Contradiction

1. Assume that the claim is false.
2. Show that this assumption leads logically to a contradiction.
3. Conclude that the claim must actually be true.

Recall that the negation of a universal conditional is logically equivalent to

$$\neg\left(\forall x, P(x) \implies Q(c)\right) \equiv \exists x, P(x) \wedge \neg Q(x).$$

Proof By Contradiction for a Universal Statement $\forall x, P(x) \Rightarrow Q(x)$

1. Assume that there exists x_0 in the domain for which $P(x_0)$ is true and $Q(x_0)$ is false.
2. Show that this assumption leads logically to a contradiction.
3. Conclude that $P(x_0) \implies Q(x_0)$ must be true.
4. Universal Generalization implies that $\forall x, P(x) \implies Q(x)$ must be true.

Remark. Althought it isn't necessary, it's often polite to clue the reader in on the fact that you're about to prove this by contradiction.

Example 4.7.1: Infinity Integers

Prove the following claim.

> **Theorem.** There is no largest integer.

Proof. Tending towards a contradiction, suppose that there is a largest integer, call it N. Choose $M = N + 1$, another integer. Then we have that $M > N$. But since N was assumed to be the largest, then we also have that $N \geq M$. Clearly N cannot be the largest and not the largest integer.

$$N \geq M > N + 1$$

Ridiculous. Contradiction.

Therefore there is no largest integer. □

Example 4.7.2

Prove the following claim.

> **Theorem.** The sum of any nonzero rational number and irrational number is irrational.

Proof. Suppose there is a rational number m, and an irrational number n for which $m + n$ is rational. Since the rationals are closed under addition and multiplication, it follows that

$(m+n)-m$ is rational. But $(m+n)-m=n$, so this contradicts our initial assumption that n was irrational.

Therefore the sum of any rational number and irrational number is irrational. □

Example 4.7.3

Prove or disprove the following claim:

Claim. $7p+21q=1$ for some integers p and q.

Disproof. The claim is false - there are no integers p, q for which $7p+21q=1$. To see this, suppose to the contrary that there are integers p, q for which this is true. Then we have that

$$1=7p+21q=7(p+3q).$$

As $p+3q$ is an integer, then 7 must divide 1. But this contradicts the previously-proven fact that all divisors of 1 must be less than (or equal to) 1. □

4.7.2 Contraposition

Proof By Contrapositive: $\forall x, P(x) \implies Q(x)$.

1. Let x_0 be a fixed, but arbitrary, element of the domain.
2. Suppose that $Q(x_0)$ is false.
3. Show that $P(x_0)$ is false by using definitions and previously established rules.
4. By contrapositive, conclude that $P(x_0) \implies Q(x_0)$.
5. By universal generalization, conclude that $\forall x \in D, P(x) \implies Q(x)$.

Remark. Althought it isn't necessary, it's polite to clue the reader in on the fact that you're about to prove this by contraposition. Maybe with a phrase like "We approach by contraposition" or "We establish the contrapositive."

Example 4.7.4

Prove the following claim.

Theorem. For all integers n, if n^2 is even, then n is even.

Notice that the contrapositive is: For all integers n, if n is odd, then n^2 is odd. That proof seems to write itself.

Proof. We approach via contraposition. Let n be an arbitrary integer and suppose that n is odd. Then there is some integer k for which $n=2k+1$. Then

$$n^2=(2k+1)^2=2(2k^2+2k)+1$$

Since $2k^2+2k$ is an integer, then n^2 is odd.

This verifies the claim. □

Example 4.7.5

Prove the following claim.

Theorem. For all integers n, if $9 \nmid n^2$, then $6 \nmid n$.

We approach with the contrapositive. Let n be an integer and suppose that $6|n$. Then there is an integer k for which $n = 6k$. Now, $n^2 = 36k^2 = 9(4k^2)$. As the integers are closed under addition, $4k^2$ is an integer, whence $9|n^2$.

Example 4.7.6

Prove the following claim.

Theorem. For all integers m, n, if $m + n$ is even, then either m and n are both even, or m and n are both odd.

Proof. We approach by contraposition. Suppose that one of m and n is even, and the other is odd. We'll prove only the case that m is even and n is odd (the opposite case is identical). Then there are integers k and ℓ for which

$$m = 2k \qquad \text{and} \qquad n = 2\ell + 1.$$

Then $m + n = 2k + 2\ell + 1 = 2(k + \ell) + 1$, and since the integers are closed under addition, $k + \ell$ is an integer, whence $m + n$ is odd. □

Contrapositive – Multiple Hypotheses

Observe that

$$\begin{aligned}
\Big[(p \wedge q) \implies r\Big] &\equiv \Big[\neg r \implies \neg(p \wedge q)\Big] && \text{(contrapositive)} \\
&\equiv \neg\neg r \vee \neg(p \wedge q) && \text{(conditional identity)} \\
&\equiv \neg\neg r \vee (\neg p \vee \neg q) && \text{(DeMorgan's Law)} \\
&\equiv (\neg\neg r \vee \neg p) \vee \neg q && \text{(associativity)} \\
&\equiv \neg(\neg r \wedge p) \vee \neg q && \text{(DeMorgan's Law)} \\
&\equiv \Big[(\neg r \wedge p) \implies \neg q\Big] && \text{(conditional identity)}
\end{aligned}$$

or equivalently

$$\equiv \Big[(\neg r \wedge q) \implies \neg p\Big]$$

Proof By Contrapositive: $\forall x, (P(x) \wedge Q(x)) \implies R(x)$.

1. Let x_0 be a fixed, but arbitrary, element of the domain.
2. Suppose that $R(x_0)$ is false and $P(x_0)$ is true.
3. Show that $Q(x_0)$ is false by using definitions and previously established rules.
4. By logical equivalence, conclude that $(P(x_0) \wedge Q(x_0)) \implies R(x_0)$.
5. By universal generalization, conclude that $\forall x \in D, (P(x) \wedge Q(x)) \implies R(x)$.

Example 4.7.7

Prove the following claim.

> **Theorem.** For all integers x, y, z, if both $x + z$ and $y + z$ are even, then $x + y$ is even.

Scratch: Let $E(a, b)$ mean "$a + b$ is even". We then have the predicates $P = E(x, z)$, $Q = E(y, z)$, $R = E(x, y)$, and thus the form of the claim above is

$$\forall x \forall y \forall z \left[(P \wedge Q) \implies R\right].$$

We'll apply the contrapositive and prove

$$\forall x \forall y \forall z \left[(\neg R \wedge Q) \implies P\right].$$

Proof. Approaching via contraposition, let x, y, z be arbitrary integers and suppose that $x + y$ is odd. We further suppose that $y + z$ is even, and intend to show that $x + z$ is odd. By definition of even and off, there are integers k, ℓ so that

$$x + y = 2k + 1 \qquad \text{and} \qquad y + z = 2\ell.$$

Now, using our basic algebra, we have that

$$\begin{aligned} x + z &= x - z + 2z \\ &= x + y - y - z + 2z \\ &= (x + y) - (y + z) + 2z \\ &= (2k + 1) - (2\ell) + 2z \\ &= 2(k - \ell + z) + 1. \end{aligned}$$

Since the integers are closed under additional mutiplication, $k - \ell + z$ is an integer, and therefore $x + z$ is odd, as desired. □

The above can also be proven directly, by noticing that

$$x + y = (x + z) - 2z + (z + y)$$

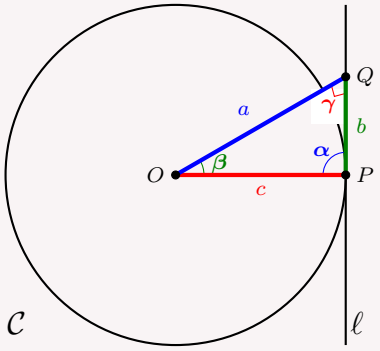
and all of these terms are even.

Exercise 4.7.8

Prove the following claim.

> **Theorem.** Let $\mathcal{C}$ be a circle with center O and let ℓ be a line tangent to the circle at a point P. Then ℓ is perpendicular to the segment $\overline{OP}$.

We begin by looking at the picture below, which will serve as the guide for the proof.



Proof. Let $\mathcal{C}$ be a circle with center O and radius c, and let ℓ be a tangent line, intersecting $\mathcal{C}$ at point P. Tending toward a contradiction, suppose the angle formed by $\overline{OP}$ and ℓ is not a right angle. The on one side of $\overline{OP}$, the angle must be less than $\frac{\pi}{2}$, so let α be this angle.

Now, there must be some other point, Q say, along ℓ where $\overline{OQ}$ meets ℓ at a right angle; let a be the length of the segment $\overline{OQ}$. Form the triangle $\triangle OPQ$ and let γ be the angle at Q.

Q must lie on the same side of c as α, since otherwise the angle sum of $\triangle OPQ$ would be at least

$$\gamma + (\pi - \alpha) = \frac{\pi}{2} + (\pi - \alpha) > \frac{\pi}{2} + \frac{\pi}{2} = \pi.$$

Since the angle sum of $\triangle OPQ$ must be π, it follows that γ is the largest angle, whence $c > a$ (this can be observed using the Law of Sines, if you wish). In turn, this ensures that Q lies somewhere in the interior of circle $\mathcal{C}$, and thus ℓ must intersect $\mathcal{C}$ in a second point, contradicting the fact that it was a tangent line.

Therefore $\overline{OP}$ and ℓ must be perpendicular. □

4.8 Indirect Argument: ~~Two~~ Three Famous Theorems

4.8.1 $\sqrt{2}$ is Irrational

To prove Theorem 4.8.2, we'll first have to prove a helper result about rational numbers.

Lemma 4.8.1: Rational Numbers – Simplified Form

For every rational number x, there exist integers a, b with $b \neq 0$ such that $x = \dfrac{a}{b}$ and the only positive integer dividing both a and b is 1.

Proof. Let x be an arbitrary rational number. We have three cases: $x = 0$, $x > 0$, and $x < 0$. Since $0 = \frac{0}{1}$, the first case is obvious. We now prove only the case that $x > 0$, noting that the proof of the negative case follows identically by replacing x with $-x$.
Suppose that x is positive. There are integers k_0, ℓ_0 with $\ell_0 \neq 0$ such that

$$x = \frac{k_0}{\ell_0}$$

We may presume that k_0, ℓ_0 are both positive. If they were both negative, we could take $x = \frac{-k_0}{-\ell_0}$ and continue with the remainder of the proof.
If there are no positive integers other than 1 dividing both k_0, ℓ_0, then choose $a = k_0$ and $b = \ell_0$. Otherwise, let $d_1 > 1$ be an integer dividing k_0, ℓ_0. Then (by definition of division) there are integers k_1, ℓ_1 such that

$$\begin{aligned} k_0 &= d_1 k_1 && \text{where } 1 \leq k_1 < k_0 \\ \ell_0 &= d_1 \ell_1 && \text{where } 1 \leq \ell_1 < \ell_0 \end{aligned}$$

and thus

$$x = \frac{k_0}{\ell_0} = \frac{d_1 k_1}{d_1 \ell_1} = \frac{k_1}{\ell_1}.$$

If there are no positive integers other than 1 dividing both k_1, ℓ_1, then choose $a = k_1$ and $b = \ell_1$. Otherwise, let $d_2 > 1$ be an integer dividing k_1, ℓ_1. Then (by definition of division) there are integers k_2, ℓ_2 such that

$$\begin{aligned} k_1 &= d_2 k_2 && \text{where } 1 \leq k_2 < k_1 < k_0 \\ \ell_1 &= d_2 \ell_2 && \text{where } 1 \leq \ell_2 < \ell_1 < \ell_0 \end{aligned}$$

and thus

$$x = \frac{k_0}{\ell_0} = \frac{k_1}{\ell_1} = \frac{d_2 k_2}{d_2 \ell_2} = \frac{k_2}{\ell_2}.$$

Continue to repeat this procedure. As there are only finitely many integers x, y satisfying $1 \leq x < k_0$ and $1 \leq y < \ell_0$, this procedure must terminate after only finitely-many steps. Suppose the n^{th} step is the terminal step. Then we take $a = k_n$ and $b = \ell_n$. □

Theorem 4.8.2: Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational.

Proof. Seeking a contradiction, suppose that $\sqrt{2}$ is rational. Then, from Lemma **??** there are integers a, b with $b \neq 0$ and a, b not both even such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of this equation yields

$$2 = \frac{a^2}{b^2}$$

and rearranging produces

$$b^2 = 2a^2 \tag{4.4}$$

whence we see that b^2 is even. By Example 4.7.4, it follows that b is an even number, and thus Lemma **??** implies that a is odd.
Since b is even, there is some integer k for which $b = 2k$. Substituting this into Equation 4.4, we get

$$\begin{aligned} (2k)^2 &= 2a^2 \\ 4k^2 &= 2a^2 \\ 2k^2 &= a^2 \end{aligned}$$

and thus a^2 is even. By Example 4.7.4, it follows that a is an even number, which contradicts the fact that a was odd.
Therefore, we conclude that $\sqrt{2}$ is, in fact, irrational. □

4.8.2 The Infinitude of Primes

Theorem 4.8.3: Infinitude of Prime Numbers

There are infinitely-many prime numbers.

Proof. Tending toward a contradiction, suppose that there are only finitely-many primes, with P the largest prime. Let N be the product of all primes, i.e.

$$N = 2 \cdot 3 \cdot 5 \cdot 11 \cdot \cdots \cdot P$$

Since P is the largest prime, then $N + 1$ must be composite, and in particular, divisible by one of the primes on the list. Let q be such a prime. Since q is a prime, it is one of the factors of N, so q divides N. By definition of division, we must have integers k and ℓ for which

$$N = qk \qquad \text{and} \qquad N + 1 = q\ell.$$

We then have that

$$1 = (N + 1) - N = q\ell - qk = q(\ell - k).$$

Because 1 and q are both positive, $\ell - k$ is also positive, and the only positive divisor of 1 is 1. It follows that

$$(\ell - k) = q = 1$$

which contradicts our assumption that q is prime. We conclude, then, that there cannot be

finitely-many primes. □

4.8.3 Area of a Circle

Archimedes famously proved that the area of a circle was equal to the familiar πr^2 using contradiction and proof by cases.
We first need to know what the Greeks knew.

Lemma 4.8.4

The circumference C of a circle of radius r is given by $C = 2\pi r$.

Lemma 4.8.5

The area A of a regular polygon with apothem h and perimeter P is given by $A = \frac{1}{2}hP$.

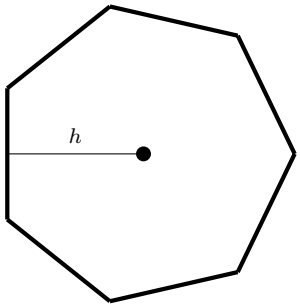


Figure 4.2: A regular polygon (all edge lengths are the same, all internal angles are the same) with *apothem*, of length h.

Lemma 4.8.6

A circle can be approximated (to any desired accuracy) by both inscribed regular polygons or circumscribed regular polygons.

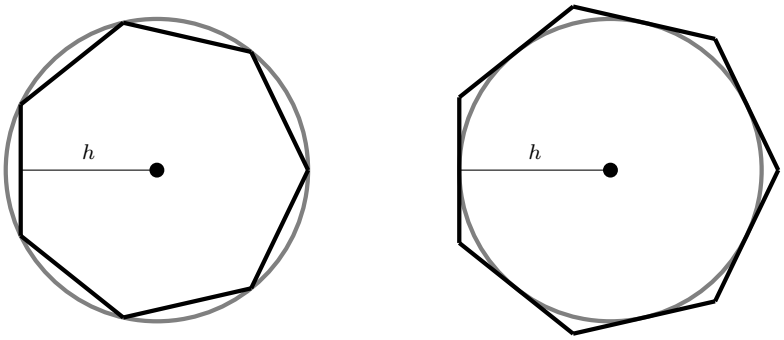


Figure 4.3: To the left, approximating a circle with an inscribed regular polygon. To the right, approximating the circle with a circumscribed regular polygon. Pay special attention to the relationship between the circle radius and the apothem.

Theorem 4.8.7: $A = \pi r^2$

The area of a circle with radius r is given by πr^2.

Proof. We first note that, by Lemma 4.8.4 above, $\pi r^2 = \frac{1}{2}rC$, where C is the circumference of the circle. Tending toward a contradiction, suppose that the area of the circle is *not* $\frac{1}{2}rC$. There are two cases: either Area(circle) $> \frac{1}{2}rC$ or Area(circle) $< \frac{1}{2}rC$.

Case 1. Suppose that Area(circle) $> \frac{1}{2}rC$. Applying Lemma 4.8.6, we find an inscribed regular polygon $\mathcal{X}$ satisfying

$$\text{Area(circle)} > \text{Area}(\mathcal{X}) > \frac{1}{2}rC$$

If $\mathcal{X}$ has apothem h and perimiter P, it's clear that $h < r$ and that $P < C$ (see Figure 4.3), hence Lemma 4.8.5 yields

$$\text{Area}(\mathcal{X}) = \frac{1}{2}hP < \frac{1}{2}rC,$$

which contradicts our assumption.

Case 2. Suppose that Area(circle) $< \frac{1}{2}rC$. Applying Lemma 4.8.6, we find a circumscribed regular polygon $\mathcal{X}$ satisfying

$$\text{Area(circle)} < \text{Area}(\mathcal{X}) < \frac{1}{2}rC$$

If $\mathcal{X}$ has apothem h and perimiter P, we observe that $h > r$ and that $P > C$ (see Figure 4.3), hence Lemma 4.8.5 yields

$$\text{Area}(\mathcal{X}) = \frac{1}{2}hP > \frac{1}{2}rC,$$

which contradicts our assumption.

Therefore, the area of the circle must be precisely $\frac{1}{2}rC = \pi r^2$. □

Remark. This proof is certainly convincing, but by modern standards the lemmas are a bit too imprecise to allow one to meet the minimum criteria for a proof.

Chapter 5

Sequences, Mathematical Induction, and Recursion

5.1 Sequences

One of the most important tasks in mathematics is to recognize and categorize regular patterns.

Definition: sequence, index

A **sequence** is a (possibly-infinite) ordered list of objects (or events):

$$\{a_1, a_2, .., a_k\}$$

Each individual element a_k is called a **(k^{th}) term**. The k in "a_k" is called the **index** and indicates its position in the sequence. Notationally, we often write $\{a_n\}_{n=1}^{k}$ or $(a_n)_{n=1}^{k}$ to denote a sequence.

Remark. Note that a sequence's index doesn't have to start at 1 (in computer science, these often start at 0). One can always perform an **index shift** to rewrite a sequence starting at $k = 1$, so there's not loss of generality in using this convention.

Definition: length of sequene

The number of ordered elements in a sequence is called its **length**. An infinite sequence has an initial term, but continues indefinitely having no final term. A finite sequence has a final term a_m, where m is some natural number.

Definition: explicit formula

An **explicit** or **general formula** for a sequence $\{a_n\}$ is a rule that shows how the value of a_k depends on k.

Example 5.1.1

Write the first four terms of the following sequences.

1. The sequence $\{a_k\}$ where $a_k = \dfrac{k}{10+k}$ for all integers $k \geq 1$.
2. The sequence $\{b_j\}$ where $b_j = \dfrac{5-j}{5+j}$ for all integers $j \geq 3$.
3. The sequence $\{c_i\}$ where $c_i = \dfrac{(-1)^i}{3^i}$ for all integers $i \geq 0$.

1. $\left\{\frac{1}{11}, \frac{2}{12}, \frac{3}{13}, \frac{4}{14}\right\}$
2. $\left\{\frac{2}{8}, \frac{1}{9}, \frac{0}{10}, \frac{-1}{11}\right\}$
3. $\left\{\frac{1}{1}, \frac{-1}{3}, \frac{1}{9}, \frac{-1}{27}\right\}$

Remark. The third sequence above is known as an **alternating sequence**.

Example 5.1.2

Given the first few terms of the sequence, find an explicit formula for it.

1. The sequence $\{a_n\}_{n=0}^{\infty}$ given by $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{64}, \ldots$
2. The sequence $\{b_j\}_{n=2}^{\infty}$ given by $1, 4, 9, 16, 25, 36, 49, 64, \ldots$

1. We have
$$\underset{a_0}{1 = \tfrac{1}{2^0}}, \quad \underset{a_1}{\tfrac{1}{2} = \tfrac{1}{2^1}}, \quad \underset{a_2}{\tfrac{1}{4} = \tfrac{1}{2^2}}, \quad \underset{a_3}{\tfrac{1}{8} = \tfrac{1}{2^3}}, \quad \underset{a_4}{\tfrac{1}{16} = \tfrac{1}{2^4}}, \quad \ldots.$$
so the explicit formula appears to be $a_n = \frac{1}{2^n}$
2. We have
$$\underset{b_2}{1 = 1^2}, \quad \underset{b_3}{4 = 2^2}, \quad \underset{b_4}{9 = 3^2}, \quad \underset{b_5}{16 = 4^2}, \quad \underset{b_6}{25 = 5^2}, \quad \ldots.$$
so the explicit formula appears to be $b_j = (j-1)^2$

Definition: sum of a sequence

If m and n are integers and $m \leq n$, the symbol $\sum_{k=m}^{n} a_k$ is the **sum** of all terms from a_m to a_n.

That is,
$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \ldots + a_{n-1} + a_n.$$

Remark. It's important to observe that one can rewrite sums by "splitting off" some number of terms.

$$\sum_{k=m}^{n} a_k \quad = \quad a_m + a_{m+1} + \cdots + a_{n-1} + a_n \quad = \quad \underbrace{a_m + \left(\sum_{k=m+1}^{n} a_k\right)}_{\text{split off first term}} \quad = \quad \underbrace{\left(\sum_{k=m}^{n-1} a_k\right) + a_n}_{\text{split off last term}}.$$

This strategy may come in handy when we get to induction.

Example 5.1.3

Calculate the following:

1. $\sum_{k=0}^{3} \frac{1}{2^k}$
2. $\sum_{j=1}^{2} \frac{(-1)^j}{j+1}$

1. $\sum_{k=0}^{3} \frac{1}{2^k} = \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} == \frac{15}{8}.$
2. $\sum_{j=1}^{2} \frac{(-1)^j}{j+1} =$

Definition: product of a sequence

If m and n are integers and $m \leq n$, the symbol $\prod_{k=m}^{n} a_k$ is the **product** of all terms from a_m to a_n. That is,

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdots a_{n-1} \cdot a_n.$$

Remark. It's important to observe that one can rewrite products by "splitting off" some number of terms.

$$\prod_{k=m}^{n} a_k \quad = \quad a_m \cdot a_{m+1} \cdots a_{n-1} \cdot a_n \quad = \quad \underbrace{a_m \cdot \left(\prod_{k=m+1}^{n} a_k \right)}_{\text{split off first term}} \quad = \quad \underbrace{\left(\prod_{k=m}^{n-1} a_k \right) \cdot a_n}_{\text{split off last term}}.$$

This strategy may come in handy when we get to induction.

Example 5.1.4

Calculate the following:

1. $\prod_{k=0}^{3} \frac{1}{2^k}$
2. $\prod_{j=1}^{3} \frac{(-1)^j}{j+1}$

1. $\prod_{k=0}^{3} \frac{1}{2^k} = \frac{1}{2^0} \cdot \frac{1}{2^1} \cdot \frac{1}{2^2} \frac{1}{2^3} = \frac{1}{2^6} = \frac{1}{64}$

2. $\displaystyle\prod_{j=1}^{3} \frac{(-1)^j}{j+1} = \frac{-1}{2} \cdot \frac{1}{3} \cdot \frac{-1}{4} = \frac{1}{24}$

Definition: factorial

For each positive integer n, the quantity n **factorial**, denoted $n!$, is defined to be the product of all integers from 1 to n:

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1,$$

where we define $0! = 1$.

Remark. It's important to observe that one can rewrite factorials by "splitting off" some number of terms.

$$n! \quad = \quad n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 \quad = \quad n \cdot \Big((n-1)! \Big).$$

This strategy may come in handy when we get to induction.

Example 5.1.5

Simplify the following expressions.

1. $\dfrac{5!}{2!3!}$
2. $\dfrac{(n+1)!}{n!}$
3. $\dfrac{n!}{(n-3)!}$
4. $n + \dfrac{(n-1)}{2!} + \dfrac{(n-2)}{3!} + \dfrac{(n-3)}{4!} + ... + \dfrac{1}{n!}$

1. $\dfrac{5!}{2!3!} = \dfrac{1 \cdot 2 \cdot 2 \cdot 3 \cdot 4 \cdot 5}{1 \cdot 2 \cdot 1 \cdot 2 \cdot 3} = \dfrac{4 \cdot 5}{1 \cdot 2} = 10$
2. $\dfrac{(n+1)!}{n!} = n$
3. $\dfrac{n!}{(n-3)!} = n(n-2)(n-1)$
4. $n + \dfrac{(n-1)}{2!} + \dfrac{(n-2)}{3!} + \dfrac{(n-3)}{4!} + ... + \dfrac{1}{n!} =$

Writing Sequences and Summations Explicitly

Example 5.1.6

Condense the following using notation from above.

1. $\left\{1, -\frac{1}{4}, \frac{1}{9}, -\frac{1}{16}, \frac{1}{25}, -\frac{1}{36}\right\}$
2. $\left(\frac{1}{n}\right)\left(\frac{2}{n+1}\right)\left(\frac{3}{n+2}\right)\cdots\left(\frac{n+1}{2n}\right)$
3. The sum of the first n odd integers
4. The sum of the first $n^2 - 1$ factorials (starting with 1!)

1. $\{a_n\}_{n=1}^{\infty}$ where $a_n = (-1)^{n+1}\frac{1}{n^2}$
2. $\displaystyle\prod_{k=0}^{n} \frac{k+1}{n+k}$
3. $\displaystyle\sum_{k=0}^{n-1} 2k+1$
4. $\displaystyle\sum_{k=1}^{n^2-1} k!$

5.2 Mathematical Induction I: Proving Formulas

Definition: Principle of Mathematical Induction

Let $P(n)$ be a predicate that is defined for integers n, and let N_0 be a fixed integer. Suppose the following two statements are true.

1. $P(N_0)$ is true.
2. For all integers $k \geq N_0$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \geq N_0$.

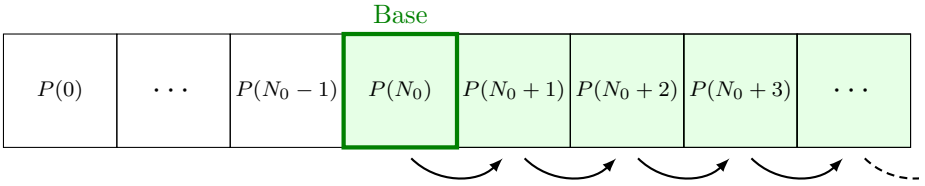


Figure 5.1: A visual interpretation of mathematical induction. Once you show that $P(k) \Rightarrow P(k+1)$, and you know that $P(N_0)$ is true, then it must be that $P(N_0+1)$ is true. From this it follows that $P(N_0+2)$ is true. From this it follows that $P(N_0+3)$ is true. And so on.

Proof By Induction

Consider a statement of the form

For every integer $n \geq N_0$, the property $P(n)$ is true.

To show this

1. [**Base Step**] Show that $P(N_0)$ is true.
2. [**Inductive Step**] Show that, for every integer $k \geq N_0$, if $P(k)$ is true, then $P(k+1)$ is true. Notice that this is a standard universal conditional. So to actually do it:
   - Let k be an arbitrary integer with $k \geq N_0$.
   - Suppose $P(k)$ is true (this is the **"induction hypothesis"**).
   - Deduce that $P(k+1)$ must be true.

Example 5.2.1: Sum of the first n integers.

Show that, for every $n \geq 1$,

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + 4 + \cdots + n = \frac{n(n+1)}{2}$$

First we identify the predicate $P(n)$ as meaning

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

. The base case will be to verify that $P(1)$ is true. When we get to the induction step, we

keep in mind that we want to see that $P(k+1)$ is true:

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

.

Proof. Let the $P(n)$ denote the equation

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

Base Step. To see that $P(1)$ is true, note that the left-hand side of the equation is 1 and the right-hand side is $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Hence $P(1)$ is true.

Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

$$\sum_{i=1}^{k} i = 1 + 2 + 3 + 4 + \cdots + k = \frac{k(k+1)}{2}.$$

Now, we have that

$$\begin{aligned}
\sum_{i=1}^{k+1} &= 1 + 2 + 3 + 4 + \cdots + k + (k+1) \\
&= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{(apply induction hypothesis)} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

hence $P(k+1)$ is true.

Therefore $P(n)$ holds for all $n \geq 1$. □

Example 5.2.2: Sum of a geometric sequence.

Let a, r be real numbers with $r \neq 1$. A **geometric sequence** is a sequence of the form

$$\{a, ar, ar^2, ar^3, ar^4, \ldots\}$$

Show that, for every $n \geq 0$,

$$\sum_{i=0}^{n} ar^i = \frac{a(1-r^{n+1})}{1-r}$$

Scratch Work.
First we identify the predicate $P(n)$ as meaning

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a(1-r^{n+1})}{1-r}$$

The base case will be to verify that $P(0)$ is true. When we get to the induction step, we keep in mind that we want to see that $P(k+1)$ is true:

$$\sum_{i=0}^{k+1} ar^i = \frac{a(1+r^{k+2})}{(1-r)}.$$

Proof. Let $P(n)$ denote the equation

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a(1-r^{n+1})}{1-r}$$

Base Step. To see that $P(0)$ is true, note that the left-hand side of the equation is a and the right-hand side is $\dfrac{a(1-r^{0+1})}{1-r} = a$.

Inductive Step. Let k be an arbitrary integer with $k \geq 0$. Suppose that $P(k)$ is true, that is

$$\sum_{i=0}^{k} ar^i = \frac{a(1-r^{k+1})}{1-r}.$$

Now, we have that

$$\begin{aligned}
\sum_{i=0}^{k+1} ar^i &= a + ar + ar^2 + ar^3 + \cdots + ar^k + ar^{k+1} \\
&= \left(\sum_{i=0}^{k} ar^i\right) + ar^{k+1} \\
&= \frac{a(1-r^{k+1})}{1-r} + ar^{k+1} && \text{(apply induction hypothesis)} \\
&= \frac{a(1-r^{k+1})}{1-r} + \frac{ar^{k+1}(1-r)}{1-r} \\
&= \frac{a(1-r^{k+1})}{1-r} + \frac{a(r^{k+1}-r^{k+2})}{1-r} \\
&= \frac{a(1-r^{k+1}+r^{k+1}-r^{k+2})}{1-r} \\
&= \frac{a(1-r^{k+2})}{1-r}
\end{aligned}$$

hence $P(k+1)$ is true.
Therefore $P(n)$ holds for all $n \geq 0$. □

Example 5.2.3: Sum of the first n odd integers

Prove that, for every $n \geq 1$,

$$\sum_{i=1}^{n}(2i-1) = 1+3+5+\cdots+(2n-1) = n^2.$$

Proof. Let $P(n)$ denote the equation

$$\sum_{i=1}^{n}(2i-1) = 1+3+5+\cdots+(2n-1) = n^2.$$

Base Step. To see that $P(1)$ is true, note that the left-hand side of this equation is $2(1)-1=1$ and the right-hand side of the equation is $(1)^2 = 1$.

Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

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

Now, we have that

$$\begin{aligned}
\sum_{i=1}^{k+1}(2i-1) &= 1+3+5+\cdots+(2k-1)+(2(k+1)-1) \\
&= \left(\sum_{i=1}^{k}(2i-1)\right)+(2(k+1)-1) \\
&= k^2+(2(k+1)-1) && \text{(apply induction hypothesis)} \\
&= k^2+2k+1 \\
&= (k+1)^2
\end{aligned}$$

hence $P(k+1)$ is true.

Therefore $P(n)$ holds for all $n \geq 1$. □

Exercise 5.2.4: Trees

A **tree**, T, is a nonempty set of vertices, V, together with a set of edges $E \subset V \times V$ with the following properties:

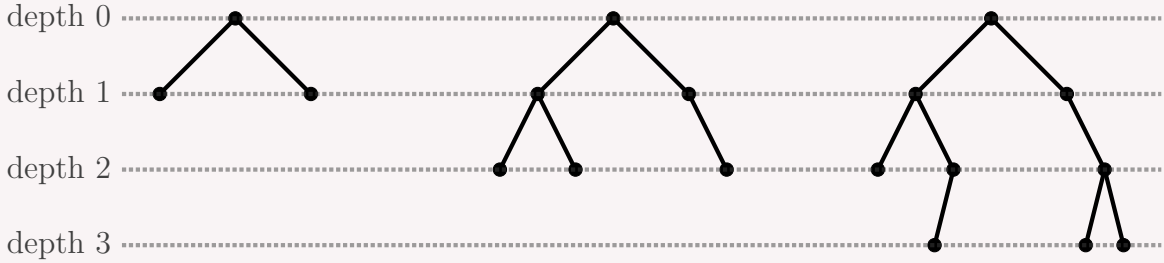
1. For all $v \in V$, the edge (v, v) *not* in E.
2. Between any two distinct vertices $u, w \in V$, there is a *unique* sequence of vertices $v_0 = u, v_1, v_2, \ldots, v_{k-1}, v_k = w$ so that the edges $(u = v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k = w)$ are all contained in E. (Call $u, v_1, \ldots, v_k, w$ a **path**.)

Prove the following claim:

If T is a tree with $|V| = p$ and $|E| = q$, then $p = q + 1$.

Exercise 5.2.5: Binary tree

A tree T is a **binary tree** if there is one vertex v_0 which is **adjancet** to precisely two vertices (that is, there are exactly two vertices v_{11} and v_{12} for which (v_0, v_{11}) and (v_0, v_{12}) are in E), and every other vertex is adjance to at most three vertices. Notably, a binary tree can always be organized into the following shape.



The **depth**, d, of a vertex v is number of edges in the path/sequence from v_0 to v. [See figure above] Prove the following claim:

If $|V| = n$, then $n \leq 2^D + 1$, where D is the maximum depth of all verices.

5.3 Mathematical Induction II: Application

Example 5.3.1: Proving Divisibility

Prove that $n^3 - n$ is divisible by 3 for all integers $n \geq 0$.

Proof. Let $P(n)$ denote the sentence

$$\text{“}n^3 - n \text{ is divisible by 3.”}$$

Base Step. We first show that $P(1)$ is true. Note that $(1)^3 - 1 = 1 - 1 = 0$ and 0 is divisible by any nonzero number.

Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, i.e. suppose that $k^3 - k$ is divisible by 3. By definition of divisiblity, this means that there exists an integer ℓ such that $k^3 - k = 3\ell$. Now, we have that

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= k^3 - k + 3k^2 + 3k \\ &= \underbrace{(k^3 - k)}_{\text{apply I.H.}} + 3k^2 + 3k \\ &= 3\ell + 3k^2 + 3k\end{aligned}$$

and so this quantity is divisible by 3. Therefore $P(k+1)$ is true.

Therefore $P(n)$ is true for all $n \geq 1$. □

Example 5.3.2: Proving Inequalities

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

Proof. Let $P(n)$ denote the inequality

$$n! > 2^n.$$

Base Step. To see that $P(4)$ is true, note that $4! = 24 > 16 = 2^4$.

Inductive Step. Let k be an arbitrary integer with $k \geq 4$. Suppose that $P(k)$ is true, that is

$$k! > 2^k.$$

We'll also remark that, since $k \geq 4$, then of course $k + 1 \geq 3 > 2$. Now we have that

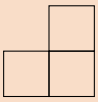
$$\begin{aligned}(k+1)! &= (k!)(k+1) \\ &> 2^k(k+1) && \text{(apply induction hypothesis)} \\ &> 2^k(2) && \text{(by our remark)} \\ &= 2^{k+1}\end{aligned}$$

hence $P(k+1)$ is true.

Therefore, $P(n)$ is true for all $n \geq 4$. □

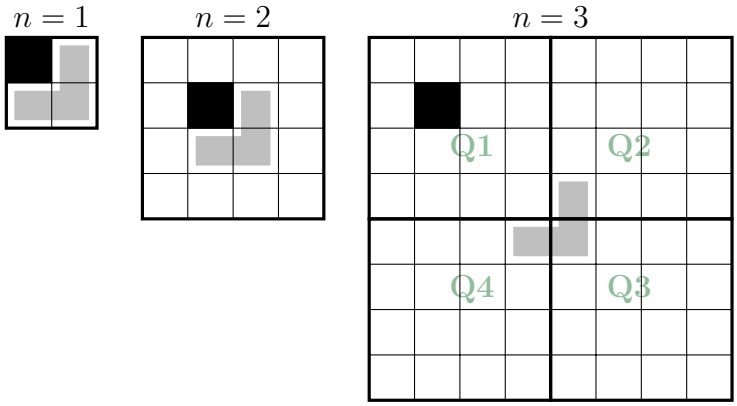
Example 5.3.3: Covering a Board with L-Shaped Trominoes

An **L-shaped tromino** is comprised of three squares arranged in an L-shape, like so:



Show that, for all integers $n \geq 1$, any $2^n \times 2^n$ checkerboard with one square removed can be covered by L-shaped trominoes.

Scratch work



Proof. Let $P(n)$ be the property

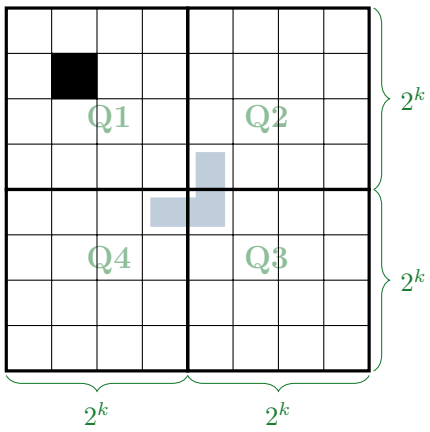
Any $2^n \times 2^n$ checkerboard with one square removed can be covered by L-shaped trominoes.

Base Step. To see that $P(1)$ is true,

Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

Any $2^k \times 2^k$ checkerboard with one square removed can be covered by L-shaped trominoes.

Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Notice that this checkerboard is comprised of four $2^k \times 2^k$ checkerboards. Let **Q1** the quadrant containing the missing square and label the other quadrants **Q2**, **Q3**, **Q4**. By the induction hypothesis, quadrant **Q1** can be covered by L-shaped trominoes. Now place an L-shaped tromino so that one square lies in each of the remaining quadrants **Q2**, **Q3**, **Q4** (see figure below).

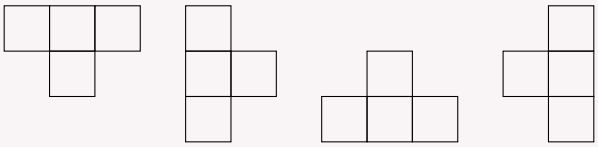


In this way, the uncovered tiles form three more $2^k \times 2^k$ checkerboards, each with a single square removed. Applying the induction hypothesis to each of these quadrants, we must have that all of **Q2**, **Q3**, **Q4** can be covered by L-shaped trominoes. That is to say, $P(k+1)$ is true.

Therefore $P(n)$ is true for every integer $n \geq 1$. □

Exercise 5.3.4: T-shaped tetrominoes

An **T-shaped tetromino** is comprised of four squares arranged in an T-shape, like so:



Prove that, for all $m \geq 1$ and for all $n \geq 1$, a $4m \times 4n$ checkerboard can be tiled by T-shaped tetrominoes.

5.4 Strong Mathematical Induction and the Well-Ordering Principle for the Integers

Motivation

Suppose you were trying to prove a statement $P(n)$ for all $n \geq N_0$, and you figured out that $P(k) \implies P(k+3)$. What base case(s) would you have to prove?

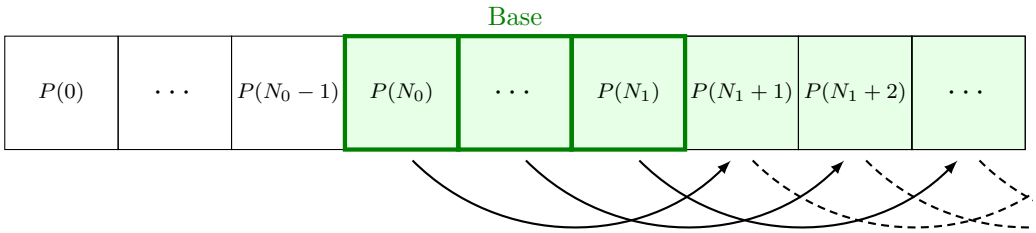


Figure 5.2: A visual interpretation of strong mathematical induction. Once you show that $P(k) \Rightarrow P(k+3)$, and you know that $P(N_0)$ is true, then it must be that $P(N_0+3)$ is true. From this it follows that $P(N_0+6)$ is true. From this it follows that $P(N_0+9)$ is true. And so on. This, however, does not prove the statement for all integers. You need to also show that $P(N_0+1)$ and $P(N_0)+2)$ are true to get that.

Suppose instead you were trying to prove a statement $P(n)$ for all $n \geq N_0$, and you figured out that $P(k) \wedge P(k+1) \wedge P(k+2) \implies P(k+3)$. What base case(s) would you have to prove?

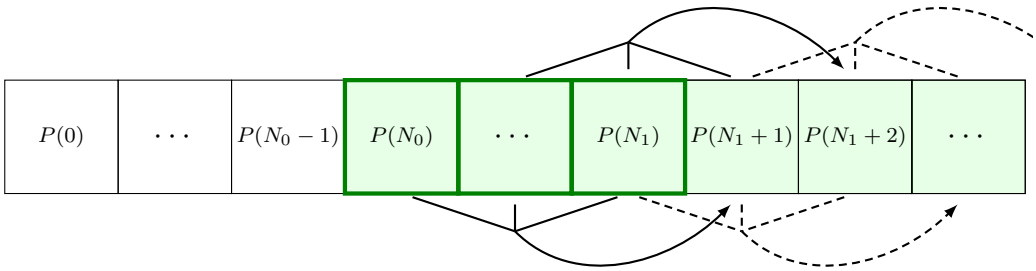


Figure 5.3: A visual interpretation of strong mathematical induction. Once you show that $P(k) \Rightarrow P(k+3)$, and you know that $P(N_0)$ is true, then it must be that $P(N_0+3)$ is true. From this it follows that $P(N_0+6)$ is true. From this it follows that $P(N_0+9)$ is true. And so on. This, however, does not prove the statement for all integers. You need to also show that $P(N_0+1)$ and $P(N_0)+2)$ are true to get that.

Definition: Principle of Strong Mathematical Induction

Let $P(n)$ be a predicate that is defined for integers n, and let N_0, N_1 be fixed integers with $N_0 \leq N_1$. Suppose the following two statements are true.

1. $P(N_0), P(N_0+1), P(N_0+2), \ldots, P(N_1)$ are true.
2. For all integers $k \geq N_1$, if $P(N_0), P(N_0+1), \ldots, P(N_1), \ldots, P(k)$ are true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \geq N_0$.

Remark. In words, the "base step" is actually a finite number of cases (not just a singular case), and the "inductive step" requires that *all* preceding cases (from the basis steps onward) are true. In practice, you may not actually need to use all preceding cases to verify the inductive step – it's overkill, sure, but you lose nothing by assuming more.

Remark. Regular ol' induction is sometimes called **weak induction**. Paradoxically, one is not actually stronger than the other (any statement provable with strong induction can be proven with weak induction).

Example 5.4.1: Recursive Sequence/Explicit Sequence

Let $\{a_n\}_{n=0}^{\infty}$ be the recursively-defined sequence

$$a_0 = 0,\ a_1 = 4,$$
$$\text{and } a_n = 6a_{n-1} - 5a_{n-2} \text{ for all } n \geq 2.$$

Show that, for all $n \geq 0$, $a_n = 5^n - 1$.

For scratch, we compute the first few terms of the sequence to confirm:

$$\begin{aligned}
a_0 &= 0 = 5^0 - 1 \\
a_1 &= 4 = 5^1 - 1 \\
a_2 &= 6a_1 - 5a_0 = 6(4) - 5(0) = 24 = 5^2 - 1 \\
a_3 &= 6a_2 - 5a_1 = 6(24) - 5(4) = 124 = 5^3 - 1 \\
a_4 &= 6a_3 - 5a_2 = 6(124) - 5(24) = 624 = 5^4 - 1
\end{aligned}$$

The claim seems reasonable. Since the recursive sequence begins with two terms, our base case should reflect this similarly: using $N_0 = 0, N_1 = 1$.

Proof. Let n be an arbitrary natural number, $\{a_n\}$ the recursive sequence defined above, and let $P(n)$ be the predicate "$a_n = 5^n - 1$."
Base steps. Take $N_0 = 0$ and $N_1 = 1$. We see that

$$a_{N_0} = a_0 = 0 = 5^0 - 1 \qquad \text{and} a_{N_1} = 4 = 5^1 - 1$$

hence $P(N_0)$ and $P(N_1)$ are true.
Inductive step. Let $k \geq 1$ and suppose that $P(0), P(1), \ldots, P(k)$ are all true, that is $a_j = 5^j - 1$ for $j = 0, 1, \ldots, k$. We then have that

$$\begin{aligned}
a_{k+1} &= 6a_k - 5a_{k-1} \\
&= 6(5^k - 1) - 5(5^{k-1} - 1) \\
&= 6(5^k) - 6 - 5^k + 5 \\
&= 5(5^k) - 1 \\
&= 5^{k+1} - 1.
\end{aligned}$$

Therefore $P(k+1)$ is true. □

Example 5.4.2: Tribonacci Sequence

Let $\{T_n\}_{n=0}^{\infty}$ be the recursively-defined sequence

$$T_0 = 0,\ T_1 = 0,\ T_2 = 1$$
$$\text{and } T_n = T_{n-1} + T_{n-2} + T_{n-3} \text{ for all } n \geq 3.$$

Show that, for all $n \geq 0$, $T_n < 2^{n-1}$.

Proof. Let n be a natural number and let $\{T_n\}$ be the recursively-defined sequence above.

Base. Take $N_0 = 0$ and $N_1 = 2$. We see that

$$T_0 = 0 < \frac{1}{2} = 2^{0-1}$$
$$T_1 = 0 < 1 = 2^{1-1}$$
$$T_2 = 1 < 2 = 2^{2-1}$$

Induction. Let $k \geq 2$ be an arbitrary natural number and suppose that, for all $m \in \mathbb{N}$ satisfying $0 \leq m \leq k$, $T_m < 2^{m-1}$. Then

$$\begin{aligned} T_{k+1} &= T_k + T_{k-1} + T_{k-2} \\ &< 2^{k-1} + 2^{k-2} + 2^{k-3} \\ &= 2^{k-3}(4 + 2 + 1) \\ &< 2^{k-3} \cdot 2^3 && \text{(since } 4 + 2 + 1 < 2^3\text{)} \\ &= 2^k = 2^{(k+1)-1}. \end{aligned}$$

Therefore, for all $k \geq 0$, we have that $T_k < 2^{k-1}$. □

Example 5.4.3: 2-adic representation

Show that every positive integer n can be uniquely written as a sum of powers of 2. Explicitly, for every n, there are natural numbers $b_0, \ldots, b_r$ with $b_0 < b_1 < \cdots < b_r$ so that

$$n = 2^{b_0} + 2^{b_1} + \cdots + 2^{b_r}.$$

Proof. **Base.** Note that $1 = 2^0$.

Induction. Let $k \geq 1$ be an arbitrary natural number and suppose that, for all $m \in \mathbb{N}$ satisfying $1 \leq m \leq k$, m has a unique representation as a sum of powers of two.

Case 1. Suppose $k + 1$ is odd. Then k is even, and by our inductive hypothesis, there are unique natural numbers $b_0, \ldots, b_r$ with $b_0 < b_1 < \ldots < b_r$ for which

$$k = 2^{b_0} + \cdots + 2^{b_r}.$$

As k is even, then $0 < b_0$, hence

$$k + 1 = 2^0 + 2^{b_0} + \cdots + 2^{b_r}.$$

Case 2. Suppose that $k+1$ is even. Writing $m = \frac{k+1}{2}$, we must have that $1 \leq m \leq k$. By our inductive hypothesis, there are then unique natural numbers $b_0, \ldots, b_r$ with $b_0 < b_1 < \ldots < b_r$ for which

$$m = 2^{b_0} + 2^{b_1} + \cdots + 2^{b_r}.$$

Then

$$k+1 = 2m = 2\left(2^{b_0} + 2^{b_1} + \cdots + 2^{b_r}\right) = 2^{b_0+1} + 2^{b_1+1} + \cdots + 2^{b_r+1}.$$

In either case above, the uniqueness of the exponents is immediate, but one could easily formalize this in Case 1 using

$$\tilde{b}_0 = 0, \text{ and } \tilde{b}_i = b_{i-1} \text{ for } i = 1, \ldots, r+1$$

or in Case 2 using

$$\tilde{b}_i = b_i + 1 \text{ for } i = 0, \ldots, r.$$

□

Remark. The above extends naturally to negative integers (just multiply everything by -1), but extending to all rational numbers requires some real thought (search term "2-adic numbers").

Theorem 5.4.4: Divisibility by Primes

Any integer greater than 1 is divisible by a prime.

The strategy is this: if a number is composite, then it is the product of two numbers that are smaller, so as long as one of those numbers is divisible by a prime, then this composite number will be as well.

Proof. Let n be an arbitrary integer and let $P(n)$ be the predicate "n is divisible by a prime."
Base step. Since $N_0 = N_1 = 2$ is prime, then N_0 is divisible by 2. Hence $P(N_0)$ is true.
Inductive step. Let $k \geq 2$ be some integer an suppose that $P(2)$, $P(3)$, …, $P(k)$ are all true. We have two cases for $k+1$:

($k+1$ is prime). If $k+1$ is prime, then $k+1$ is divisible by itself, hence $P(k+1)$ is true.

($k+1$ is composite). If $k+1$ is composite, then there are two integers, a, b for which $k = ab$ and $1 \leq a \leq k$ and $1 \leq b \leq k$. By the inductive hypothesis, a (and b) is divisible by a prime p. Since $p|a$ implies that $p|(ab)$, then $p|k+1$, hence $P(k+1)$ is true.

□

5.4.1 Well-Ordering Principle for the Integers

Well-Ordering Principle

Let N_0 be a fixed integer and let S be a nonempty set of integers, all of which are greater than N_0. Then S has a least element.

Remark. The Well-Ordering Principle is actually equivalent to the principle of mathematical induction. Since we've assumed Induction already, we could reasonably call the above a theorem and prove it. But your instructor doesn't want to, so the proof is left as an exercise to the reader.

Theorem 5.4.5: Quotient-Remainder Theorem

Let n be an integer and let d be a positive integer ($d \geq 1$). Then there are unique integers q, r with $0 \leq r < d$ satisfying

$$n = qd + r.$$

The strategy for proving this is going to be to collect all possible nonnegative remainders r, use the well-ordering principle to see that there is a smallest r, and then verify that $0 \leq r < d$. Lastly, we'll show that q and r are unique.

Proof. Let n be an arbitrary integer and let d be a positive integer.

Existence.

Let X be the set of nonnegative integers of the form $n - dq$ (so $n - dq \geq 0$, or rather $n \geq dq$), where q is some integer. We first show that X contains at least one integer.

Case 1 ($n \geq 0$). In this case, taking $q = 0$, then $n - dq = n \geq 0$, so n is contained in X.

Case 2 ($n < 0$). In this case, take $q = n$. We then have that $n - dq = n - nd = n(1 - d)$. Since $d > 0$, then $(1 - d) \leq 0$, so since both n and $(1 - d)$ are nonpositive, their product is nonnegative, hence X contains $n - nd$.

By the **??**, there must be a smallest natural number $r \geq 0$ satisfying

$$n = dq + r.$$

Now we show that $r < d$. To do this, we write $n - dq = r$. Tending toward a contradiction, suppose that $r \geq d$. We then have that

$$\begin{aligned} n - dq &\geq d \\ n - dq - d &\geq 0 \\ n - d(q + 1) &\geq 0 \end{aligned}$$

In other words, we have that $n - d(q + 1)$ is contained in X, and that $r = n - dq > n - d(q + 1)$, which contradicts that r was the least element.

Uniqueness.

At long last, we just need to show that q, r are unique. To do so, suppose that

$$n = dq_1 + r_1 = dq_2 + r_2 \tag{5.1}$$

where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1 < d$ and $0 \leq r_2 < d$. Without loss of generality, suppose that $r_2 \geq r_1$. Rearranging Equation 5.1, we have

$$(r_2 - r_1) = d(q_1 - q_2)$$

So $r_2 - r_1$ is a multiple of d. Since r_1, r_2 were assumed to be less than d, their difference also satisfies

$$0 \leq r_2 - r_1 < d.$$

The only multiple of d in this range is 0, hence $r_2 - r_1 = 0 \implies r_1 = r_2$. It follows then that

$$q_1 = \frac{n - r_1}{d} = \frac{n - r_2}{d} = q_2.$$

Therefore q and r are unique, as desired. □

Definition: quotient, remainder

The variables q and r in the Quotient-Remainder Theorem are called the **quotient** and **remainder**, respectively. One might see these written as

$$n \text{ div } d = q \qquad \text{and} \qquad n \mod d = r.$$

The proof of the quotient–remainder theorem actually suggests an algorithm to find the quotient and remainder. When n is negative, keep adding multiples of d until your number is greater than 0. When n is nonnegative, keep subtracting multiples of d until your number less than or equal to d. Explicitly

Algorithm 5.4.6: The Division Algorithm

To find the quotient $q = n \text{ div } d$ and and remainder $r = n \mod d$, break it into cases and employ the following

Case 1: $n \geq 0$	Case 2: $n < 0$
$q := 0$ $r := n$ **while** $r \geq d$ **do** $\quad q := (q + 1)$ $\quad r := (r - d)$ **end**	$q := 0$ $r := n$ **while** $r < 0$ **do** $\quad q := (q - 1)$ $\quad r := (r + d)$ **end**

Example 5.4.7

Use the division algorithm to find the quotient and remainder for...

1. ... $n = 7$, $d = 2$
2. ... $n - 8$, $d = 3$

INCOMPLETE

Exercise 5.4.8

Prove that, for all integers x, y, and for any positive integer d,

$$\Big[(x \mod \mathrm{d}) + (y \mod d)\Big] \mod d = (x + y) \mod d$$

and

$$\Big[(x \mod \mathrm{d})(y \mod d)\Big] \mod d = (x + y) \mod d.$$

5.6 Defining Sequences Recursively

Definition: recurrence relation, recursive sequence

A **recurrence relation** for a sequence $\{a_n\}$ is a formula that relates each term a_k to certain predecessorts a_{k-1}, a_{k-2}, etc. A **recursive sequence** is a sequence $\{a_n\}$ where each term satisfies a recurrence relation.

Example 5.6.1: Fibonacci Sequence

Let $\{F_n\}_{n=0}^{\infty}$ be the infinite recursive sequence defined by

$$\begin{array}{ll} F_0 = 0,\ F_1 = 1 & \text{(the initial conditions) and} \\ F_k = F_{k-1} + F_{k-2} \text{ for } k \geq 2. & \text{(the recursive formula).} \end{array}$$

Find F_2, F_3, F_4, F_5

$$\begin{aligned} F_2 &= F_1 + F_0 = 1 + 0 = 1 \\ F_3 &= F_2 + F_1 = 1 + 1 = 2 \\ F_4 &= F_3 + F_2 = 2 + 1 = 3 \\ F_5 &= F_4 + F_3 = 3 + 2 = 5 \end{aligned}$$

Example 5.6.2

Define a sequence $b_0, b_1, b_2, ..$ recursively as follows:

$$\begin{array}{ll} b_0 = 2 & \text{(the initial condition) and} \\ b_k = 1 - (b_{k-1})^k \text{ for } k \geq 1 & \text{(the recursive formula).} \end{array}$$

Find b_1, b_2, b_3.

$$\begin{aligned} b_1 &= 1 - (b_0)^1 = 1 - 2^1 = 1 - 2 = -1 \\ b_2 &= 1 - (b_1)^2 = 1 - (-1)^2 = 1 - 1 = 0 \\ b_3 &= 1 - (b_2)^3 = 1 - (0)^3 = 1 - 0 = 1 \end{aligned}$$

Chapter 6

Set Theory

6.1 Set Theory: Definitions and the Element of Proof

Definition: set,element

A **set** is an unordered list of items, called **elements**. If A is a set and a is an element of the set, we write $a \in A$. If a is not an element of the set, we write $a \notin A$.

Remark. An element of a set cannot appear twice.

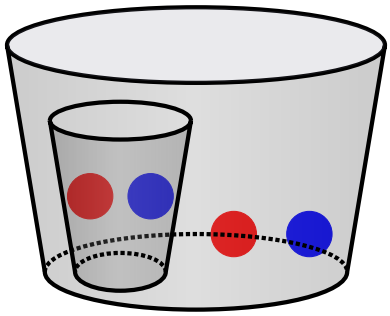
We typically write a set using curly braces and listing the elements.

Example 6.1.1

Examples of sets.

1. $S = \{1, 3, 19\}$
2. *[natural numbers]* $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$
3. ***[empty set]*** $\emptyset = \{\}$
4. $T = \{1, 2, \{1, 2\}\}$

Remark. The last example above appears to violate the remark that an element cannot appear twice, but in fact the elements of T are 1, 2, and $\{1, 2\}$. *A set can be an element of another set* (but we musn't be naïve – there famously cannot be a set containing all sets). You can make sense of this by thinking about a situation in which one is carrying a bucket of balls, and within that bucket is a smaller container which also contains a couple of balls. If you reach into the large bucket and grab an object at random, you can grab either a ball or a small container.



Sometimes sets are infinite (and writing it out explicitly is impossible) or sometimes sets are finite but we really want to communicate the pattern of the elements within the set.

Definition: set-builder notation

Let X be some set (called the **universe**) and let $P_1(x), P_2(x), \ldots$ be some properties (or predicates) with domain X. One can define a set A using **set-builder notation**

$$A = \{x \in X \ : \ P_1(x) \text{ is true}, P_2(x) \text{ is true } \ldots\}.$$

This is read

"A is the set of all elements in X such that $P_1(x), P_2(x), \ldots$ are all true"

or

"A is the set of all elements in X with properties $P_1(x), P_2(x), \ldots$"

Remark. If this feels like a truth set, it's because it is.

Remark. The universe is almost never directly stated, as it is either unimportant for the statement, or it is clear from context.

Example 6.1.2

Define $P(x) : x$ is prime, $Q(x) : x < 20$, and $R(x) : x$ is even. Determine the elements of the following sets:

1. $A = \{x \in \mathbb{Z}^+ \mid Q(x)\}$
2. $B = \{x \in \mathbb{Z}^+ \mid P(x) \wedge Q(x)\}$
3. $C = \{x \in \mathbb{Z}^+ \mid P(x) \wedge R(x)\}$

1. $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$
2. $\{2, 3, 5, 7, 11, 13, 17, 19\}$
3. $\{2\}$

Definition: subset

Let B be a set (inside of some universe X). We say that A is a **subset** of B, denoted $A \subseteq B$, if and only if

$$\forall x \in X, \text{ if } x \in A \text{ then } x \in B$$

A subset A is called a **proper subset** of B, denoted $A \subsetneq B$, if and only if

$$A \subseteq B \text{ and } \exists x \in B \text{ such that } x \notin A.$$

In other words, A is a proper subset of B if and only if (1) A is a subset of B and (2) $A \neq B$.

In either case, B is sometimes called the **superset** of A.

Remark. There are some competing notations about subsets. Some authors will prefer to make the subset notation look the same as $\leq$ and $<$ notations, using $\subseteq$ for subset and $\subset$ for a proper subset. Others will use $\subset$ for a subset and $\subsetneq$ for a proper subset. We shy away from using the $\subset$ symbol at all because is very similar to the letter C when hand-written.

Example 6.1.3

Let $A = \{1, 3, 5, 9\}, B = \{1, 2, 3, 4, 5, 7, 9\}$.

1. Is A a subset of B?
2. Is A a proper subset of B?

1. Yes. Every element of A is also contained in B.

$$\{1, 2, 3, 4, 5, 7, 9\}$$

2. Yes. There are elements of B that are not contained in A.

$$\{1, 2, 3, 4, 5, 7, 9\}$$

If we treat A and B as regions of the plane, we can think about a **Venn diagram** which relates these sets.

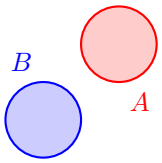


Figure 6.1: $B \not\subseteq A$ and $A \not\subseteq B$

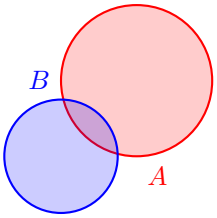


Figure 6.2: $B \not\subseteq A$ and $A \not\subseteq B$

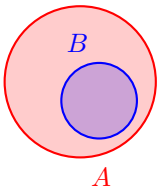


Figure 6.3: $B \subsetneq A$ and $A \not\subseteq B$

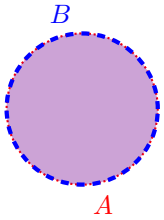


Figure 6.4: $A \subseteq B$ and $B \subseteq A$

For small sets, it is easy to just compare elements explicitly and check whether one is a subset of another. But for large sets – especially ones described in terms of set-builder notation – this can become more complicated. Look at the definition of subset more closesly

$$B \subseteq A \text{ if and only if } [\forall x \in A, x \in B \implies x \in A]$$

This yields the following technique

Element Method for Subsets

Let A, B be sets. To show that $B \subseteq A$.

1. Suppose $x \in B$, where x is arbitrary.
2. Show that $x \in A$.

Example 6.1.4

For any integer k, we define the set

$$k\mathbb{Z} := \{x \in \mathbb{Z} \ : \ x \text{ is a multiple of } k\}.$$

Show that $6\mathbb{Z} \subseteq 2\mathbb{Z}$.

In order to show that this is true, we need to show that any multiple of 6 is also a multiple of 2.

Proof. Let $x \in \mathbb{Z}$ be arbitrary and suppose that $x \in 6\mathbb{Z}$, i.e., x is a multiple of 6. Then, by

definition, there is some integer n for which $x = 6n = 2(3n)$. Since $3n$ is an integer, we see that such an x is also a multiple of 2, and therefore $x \in 2\mathbb{Z}$. □

Figure 6.4 suggests to us the following definition

Definition: set equality

set-equality Two sets A and B are said to be **equal** if and only if both are subsets of each other. Symbolically,

$$A = B \iff (A \subseteq B) \wedge (B \subseteq A).$$

Example 6.1.5

Using the notation from Example 6.1.4, let A be the set

$$A = \{x \in \mathbb{Z} \ : \ x \in 2\mathbb{Z} \wedge x \in 3\mathbb{Z}\}.$$

Show that $A = 6\mathbb{Z}$.

Showing $6\mathbb{Z} \subseteq A$. Let x be an arbitrary integer and suppose $x \in 6\mathbb{Z}$. Then by definition $x = 6k$ for some integer k. But $x = 6k = 2(3k)$ showing both that $x \in 2\mathbb{Z}$. Moreover, $x = 6k = 3(2k)$ so $x \in 3\mathbb{Z}$. Therefore $x \in A$ and thus $6\mathbb{Z} \subseteq A$.
[Showing $A \subseteq 6\mathbb{Z}$] Let x be an arbitrary integer and suppose $x \in A$. Then, by definition of A, $x \in 2\mathbb{Z}$ and $x \in 3\mathbb{Z}$. Since $x \in 3\mathbb{Z}$, there is some integer k for which $x = 3k$. Since $x \in 2\mathbb{Z}$, then x is even, and since 3 is not even, it must be that k is even, i.e., that there is an integer ℓ for which $x = 3(2\ell) = 6\ell$. Therefore $x \in 6\mathbb{Z}$ and thus $A \subseteq 6\mathbb{Z}$
Since $A \subseteq 6\mathbb{Z}$ and $6\mathbb{Z} \subseteq A$, then $A = 6\mathbb{Z}$. □

Exercise 6.1.6: Subset Transitivity

Prove the following: For all sets A, B, C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

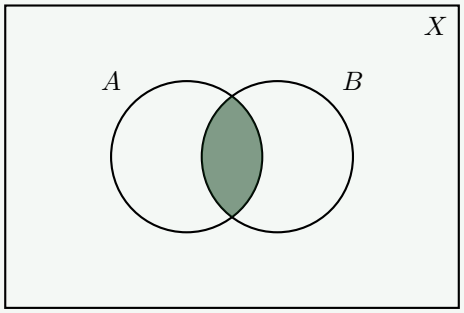
6.1.1 Set Operations

Definition

Let A and B be subsets of the same universal set X.

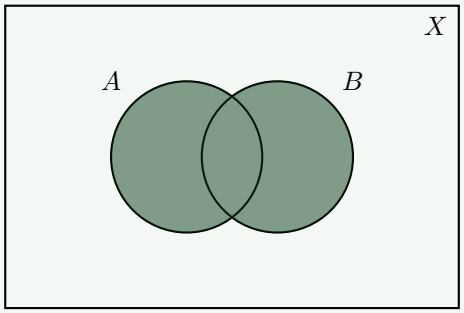
1. The **intersection of A and B**, denoted $A \cap B$, is the set of all elements common to both A and B.

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



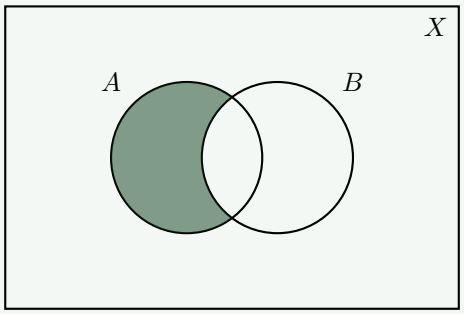
2. The **union of A and B**, denoted $A \cup B$, is the set of all elements contained in either A or B.

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



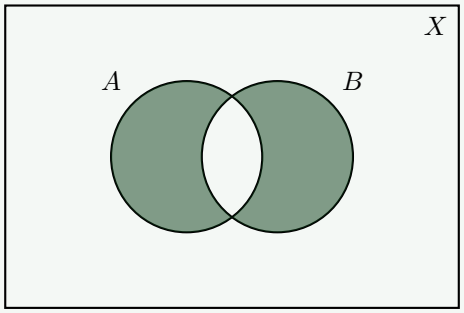
3. The **difference, A minus B** (sometimes called the **relative complement of B in A**), denoted $A - B$, is the set of all elements in A that are not contained in B.

$$A - B = \{x \in X \ : \ x \in A \text{ and } x \notin B\}$$



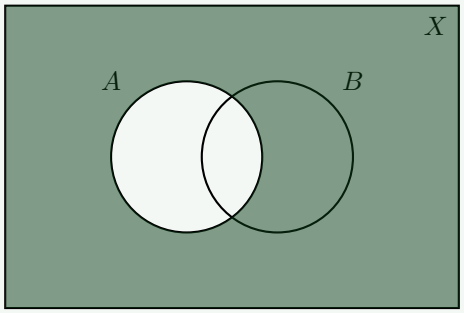
4. The **symmetric difference of A and B**, denoted $A \Delta B$, is the set of all elements in either A or B, but not in both.

$$A \Delta B = \{x \in X \ : \ (x \in A) \oplus (x \in B)\}$$



5. The **complement of A in X**, denoted A^c, is the set of all elements not in A.

$$A^c = \{x \in X \ : \ x \notin A\}$$



Example 6.1.7

Let $A = \{1, 2, 3, 4\}$, $B = \{2, 4, 6, 8\}$, $C = \{x \in \mathbb{Z} \mid x \text{ is prime}\}$, and $X = \mathbb{Z}$. Find each of the following:

1. $A \cap C$
2. $B - A$
3. A^c
4. $A^c \cap B$
5. $(A \cap C) \cup B$

1. $A \cap C = \{2, 3\}$
2. $B - A = \{6, 8\}$
3. $A^c = \{\ldots, -3, -2, -1, 0, 5, 6, 7, 8, \ldots\}$
4. $A^c \cap B = \{6, 8\}$
5. $(A \cap C) \cup B = \{2, 3\} \cup B = \{2, 3, 4, 6, 8\}$

When taking the union or intersection of a large number of sets $A_1, A_2, \ldots, A_n$, it's common to

simplify notation

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \qquad \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

To be completely clear about this notation, if $A_1, \ldots, A_n$ are sets in the same universe X, then

$$\bigcup_{i=1}^{n} A_i = \{x \in X \ : \ x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_n\},$$
$$\bigcap_{i=1}^{n} A_i = \{x \in X \ : \ x \in A_1 \wedge x \in A_2 \wedge \ldots \wedge x \in A_n\}.$$

One can extend the above to unions and intersections of a (countably) infinite number of sets $A_1, A_2, \ldots, A_n, \ldots$

$$\bigcup_{i} A_i \text{ or } \bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$$
$$\bigcap_{i} A_i \text{ or } \bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots \cap A_n \cup \cdots$$

To be completely clear about this notation, if $A_1, A_2, \ldots, A_n, \ldots$ are sets in the same universe X, then

$$\bigcup_{i=1}^{\infty} A_i = \{x \in X \ : \ \exists i \in \mathbb{N} \text{ such that } x \in A_i\},$$
$$\bigcap_{i=1}^{\infty} A_i = \{x \in X \ : \ \forall i \in \mathbb{N}, \ x \in A_i\}.$$

Remark.
1. The above really only makes sense if we know that unions and intersections are associative operations. But don't worry, we'll see this in Theorem 6.2.1.
2. If you're really feeling bold, you can even extend the definition of the above to *uncountable* sets (like $\mathbb{R}$ or $\mathbb{C}$).

Definition: disjoint sets

Two sets A and B are called **disjoint** if and only if they have no elements in common, i.e., if and only if $A \cap B = \emptyset$. A possibly-infinite collection of sets $\{A_1, A_2, \ldots\}$ is said to be **pairwise disjoint** if A_i and A_j are disjoint whenever $i \neq j$.

Definition: partition

Let A be a set and let $\{B_1, B_2, \ldots\}$ be a possibly-infinite collection of *nonempty* subsets of A. This collection is a **partition of** A if and only if
1. The B_i are pairwise disjoint, and
2. $A = \bigcup_i B_i$.

Remark. In light of the following exercise, the second item above can be replaced with

2. $A \subseteq \bigcup_i B_i$

which is faster to prove than set equality.

Exercise 6.1.8

If $A_1, \ldots, A_n, \ldots$ are (possibly an infinite number of) subsets of B, then $\bigcup_i A_i$ is also a subset of B.

Example 6.1.9

Let $A = \{2, 3, 5, 7, 11, 13\}$, $B_1 = \{2, 3, 5\}$, $B_2 = \{7, 11\}$, and $B_3 = \{13\}$. Is $\{B_1, B_2, B_3\}$ a partition of A?

Yes. By inspection, we see that B_1, B_2, B_3 are all mutually disjoint. It is equally straightforward to see that $A = B_1 \cup B_2 \cup B_3$.

Example 6.1.10

Give an example of a partition of $\mathbb{Z}$ (using *proper* subsets). Any partition at all. Have fun with it. You can give multiple examples. You can give infinitely-many examples! The possibilities are (literally) endless!

Consider the possible remainders when dividing an integer by 3. The possible options are o, 1, 2. In other words, every integer has one of the following forms:

$$3k, \qquad 3k+1, \qquad \text{or } 3k+2$$

Moreover, after dividing by 3, no integer can have two different remainders, so any integer of the form $3k$ cannot be written as an integer of the form $3k+1$, etc. With this in mind, we defined the following subsets of integers:

$$\begin{aligned} T_0 &= \{n \in \mathbb{Z} \ : n = 3k \text{ for } k \in \mathbb{Z}\} \\ T_1 &= \{n \in \mathbb{Z} \ : n = 3k+1 \text{ for } k \in \mathbb{Z}\} \\ T_2 &= \{n \in \mathbb{Z} \ : n = 3k+2 \text{ for } k \in \mathbb{Z}\} \end{aligned}$$

By our discussion above

1. $T_0 \cap T_1 = T_0 \cap T_2 = T_1 \cap T_2 = \emptyset$
2. $\mathbb{Z} = T_0 \cup T_1 \cup T_2$

and therefore $\{T_0, T_1, T_2\}$ is a partition of $\mathbb{Z}$.

Definition: power set

Given a set A, the **power set of A**, denoted, $\mathscr{P}(A)$, is the set of all subsets of A. That is, if X is the universe,

$$\mathscr{P}(A) = \{\text{sets } B \text{ in the universe } X \ : \ B \subseteq A\}$$

Example 6.1.11

Find $\mathscr{P}(A)$ given $A = \{x, y, z\}$.

The possible subsets of A are $\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}$. Thus

$$\mathscr{P}(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, A\}.$$

Example 6.1.12

Let A and B be sets. Prove that, if $A \subseteq B$, then $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

Our goal is to show that, $S \in \mathscr{P}(A) \implies S \in \mathscr{P}(B)$. Looking at the definition of the power set, this means proving that, for every subset $S \subseteq A$, we have that $S \subseteq B$.

We'll provide two proofs, depending on whether or not an exercise above has been proven in class/on homework.

Proof. Suppose $A \subseteq B$ and let $S \in \mathscr{P}(A)$ be arbitrary. By definition of the power set, we must have that $S \subseteq A$.

(Assuming we've proven Subset Transitivity...) Since $A \subseteq B$, it follows from Exercise 6.1.6 that $S \subseteq B$, and therefore $S \in \mathscr{P}(B)$.

(Assuming we've not proven Subset Transitivity...) Since $S \subseteq A$, then for every $x \in S$ we must have that $x \in A$. But since $A \subseteq B$, then we must further have that $x \in B$. Thus $S \subseteq B$, and therefore $S \in \mathscr{P}(B)$.

Therefore, $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. □

Exercise 6.1.13

Prove the converse of the previous example. That is, prove that, if $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, then $A \subseteq B$.

6.1.2 Arithmetic Operations and Set Theory - Some Interesting History

This set framework ends up being quite a bit more powerful than one might wthink. Not only does it encode logic (see the next section), but some smart folks noticed that we could come up with a correspondence between some natural numbers and sets:

$$0 \rightsquigarrow \emptyset, \qquad 1 \rightsquigarrow \{\emptyset\} \qquad 2 \rightsquigarrow \{\emptyset, \{\emptyset\}\}, \ldots$$

Using the union operation and this correspondence, we actually get a notion of addition of natural numbers:

$$\text{“}1 + 1\text{”} = \text{“}1\text{”} \cup \{\text{“}1\text{”}\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \text{“}2\text{”}$$

Russel and Whitehead, in their *Principia Mathematica* (published in 3 volumes from 1910-1913) famously spend a few hundred pages getting to this point.[1] Their work builds the rest of the natural numbers through the use of a **successor function**, S, as follows: For any natural number n

$$S(n) = n \cup \{n\}$$

[1] Yes, the proof above is the proof that $1 + 1 = 2$ that you may have heard about.

What this does is extends the correspondence between $\mathbb{N}$ and sets

$$\begin{aligned}
0 &\leftrightsquigarrow \emptyset \\
1 &\leftrightsquigarrow S(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\} \\
2 &\leftrightsquigarrow S(1) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \\
3 &\leftrightsquigarrow S(2) = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots
\end{aligned}$$

Moreover, notice the successor function allows us to define "addition" between two natural numbers in a recursive fashion:

$$\begin{aligned}
m + 0 &= m \\
m + S(n) &= S(m + n)
\end{aligned}$$

For example

$$\begin{aligned}
2 + 2 &= 2 + S(1) \\
&= S(2 + 1) \\
&= S(2 + S(0)) \\
&= S(S(2 + 0)) \\
&= S(S(2)) \\
&= S(3) \\
&= 4
\end{aligned}$$

So what this shows us is that sets with the union/intersection/complement operations are enough to encode basic logic as well as arithmetic. One of the goals of Russel and Whitehead was to completely formalize set theory and make it the logical basis for all modern mathematics. In a sense, the idea was that every true math statement could be thusly distilled down to set theory wherein it could be proven.
In 1931, work of Godel showed that this logical system actually contains true statements which are unprovable (in fact, any logical system which could encode basic arithmetic suffers from this feature). So Russel and Whitehead were sort of doomed to failure in creating a system which would be able to prove everything. However, they did lay the groundwork for a specific branch of mathematics - Type Theory (which your instructor knows absolutely nothing about, but it's definitely a thing).

6.2 Properties of Sets

The definitions of union, intersection, and complements appear to play the roles of $\vee$, $\wedge$, and $\neg$. In fact, the connection is so strong that one can essentially restate the table of logical equivalences in terms of these operations. (Note that the empty set corresponds to a contradiction, and a tautology corresponds to a tautology; which makes sense if one thinks about truth sets).

Theorem 6.2.1

Let P, Q, and R be sets in the same universe X. We then have the following table of set equalities:

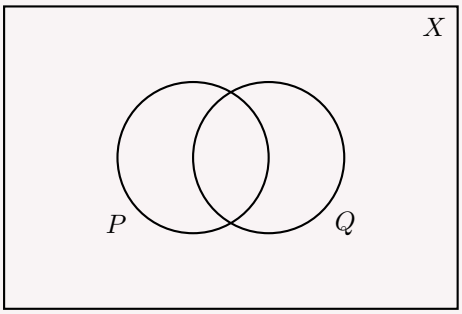
Commutative Laws	$P \cap Q = Q \cap P$	$P \cup Q = Q \cup P$
Associative Laws	$(P \cap Q) \cap R = P \cap (Q \cap R)$	$(P \cup Q) \cup R = P \cup (Q \cup R)$
Distributive Laws	$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$	$P \cup (Q \cap R) = (P \cup Q) \cap (P \cup R)$
Identity Laws	$P \cap X = P$	$P \cup \emptyset = P$
Complement Laws	$P \cup P^c = X$	$P \cap P^c = \emptyset$
Double Complement Laws	$(P^c)^c = P$	
Idempotent Laws	$P \cap P = P$	$P \cup P = P$
Universal Bound Laws	$P \cup X = X$	$P \cap \emptyset = \emptyset$
De Morgan's Laws	$(P \cap Q)^c = P^c \cup Q^c$	$(P \cup Q)^c = P^c \cap Q^c$
Absorption Laws	$P \cup (P \cap Q) = P$	$P \cap (P \cup Q) = P$
Complement of X and $\emptyset$	$X^c = \emptyset$	$\emptyset^c = X$

Now, we can – and probably *should* – prove all of these using the element method, but coloring pictures to see the intuition is more fun.

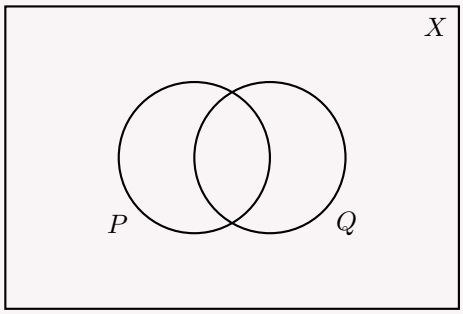
Exercise 6.2.2: Proof of Commutative Laws

Color the diagram below to show the Commutative Laws in Theorem 6.2.1.

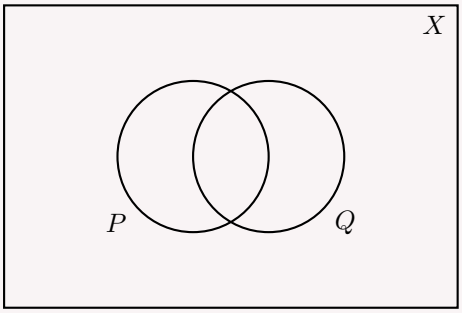
$P \cap Q$



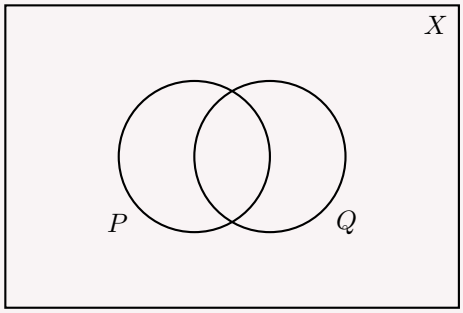
$Q \cap P$



$P \cup Q$



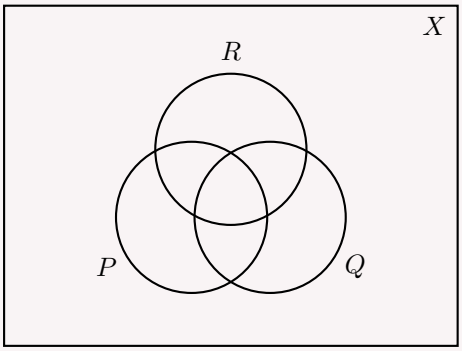
$Q \cup P$



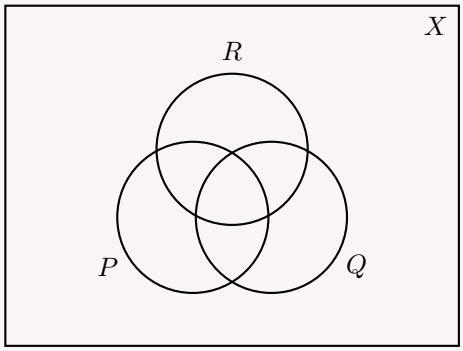
Exercise 6.2.3: Proof of Associative Laws

Color the picture below to show the Associative Laws in Theorem 6.2.1.

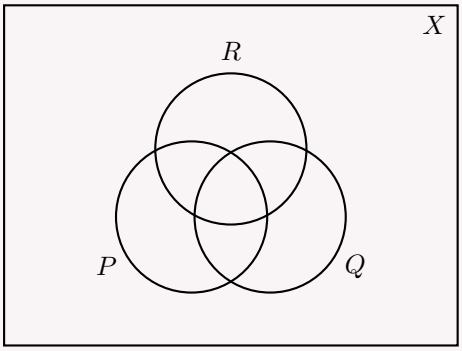
$(P \cap Q) \cap R$



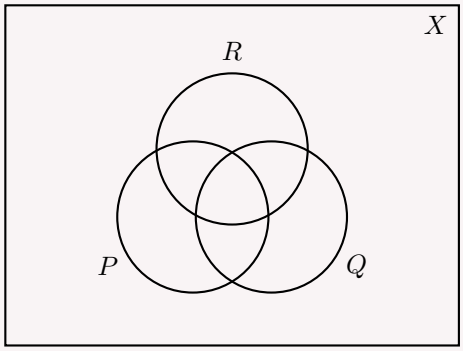
$P \cap (Q \cap R)$



$(P \cup Q) \cup R$



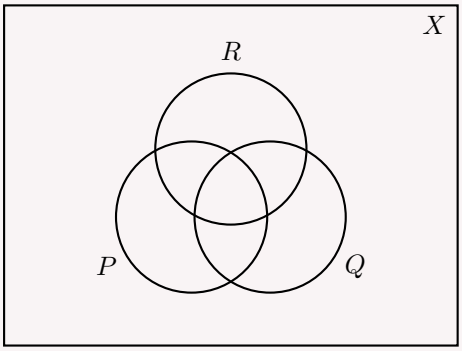
$P \cup (Q \cup R)$



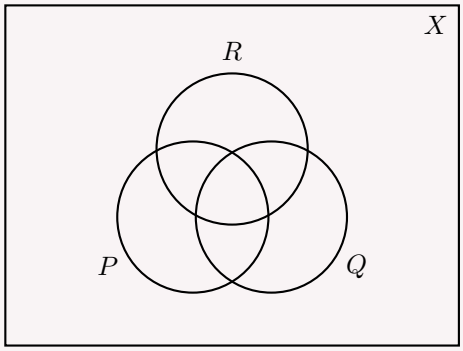
Exercise 6.2.4: Proof of Distributive Laws

Color the picture below to show the Distributive Laws in Theorem 6.2.1.

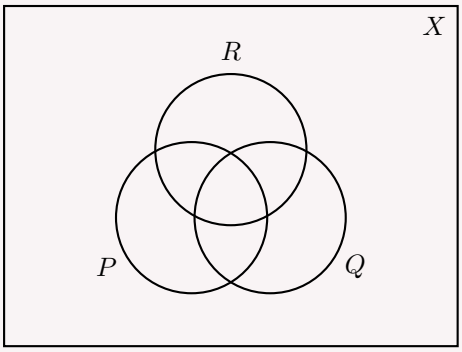
$P \cap (Q \cup R)$



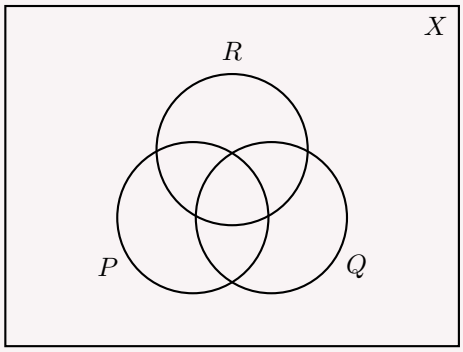
$(P \cap Q) \cap (P \cap R)$



$P \cup (Q \cap R)$



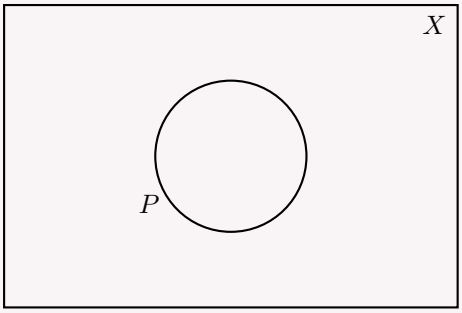
$(P \cup Q) \cap (P \cup R)$



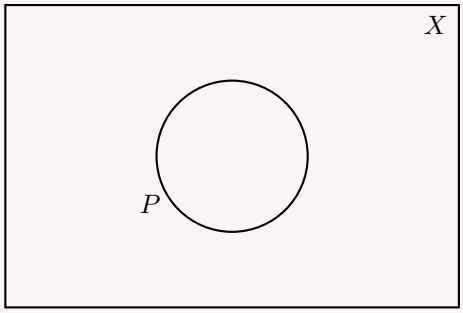
Exercise 6.2.5: Proof of Identity Laws

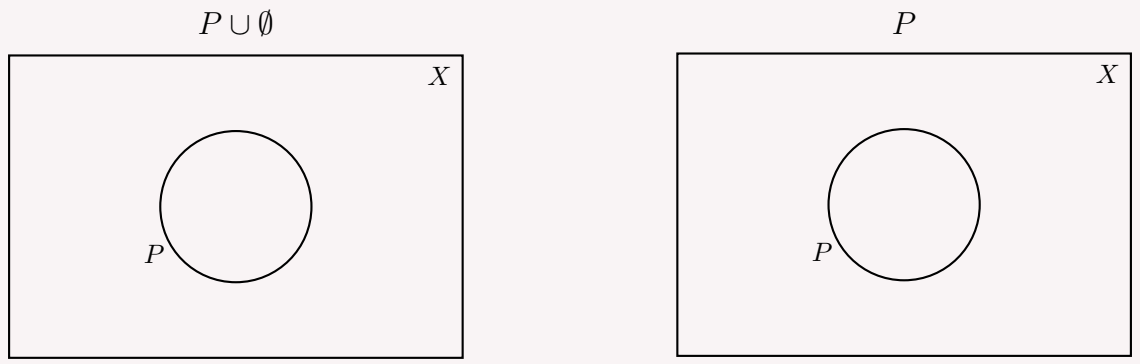
Color the picture below to show the Identity Laws in Theorem 6.2.1.

$P \cap X$



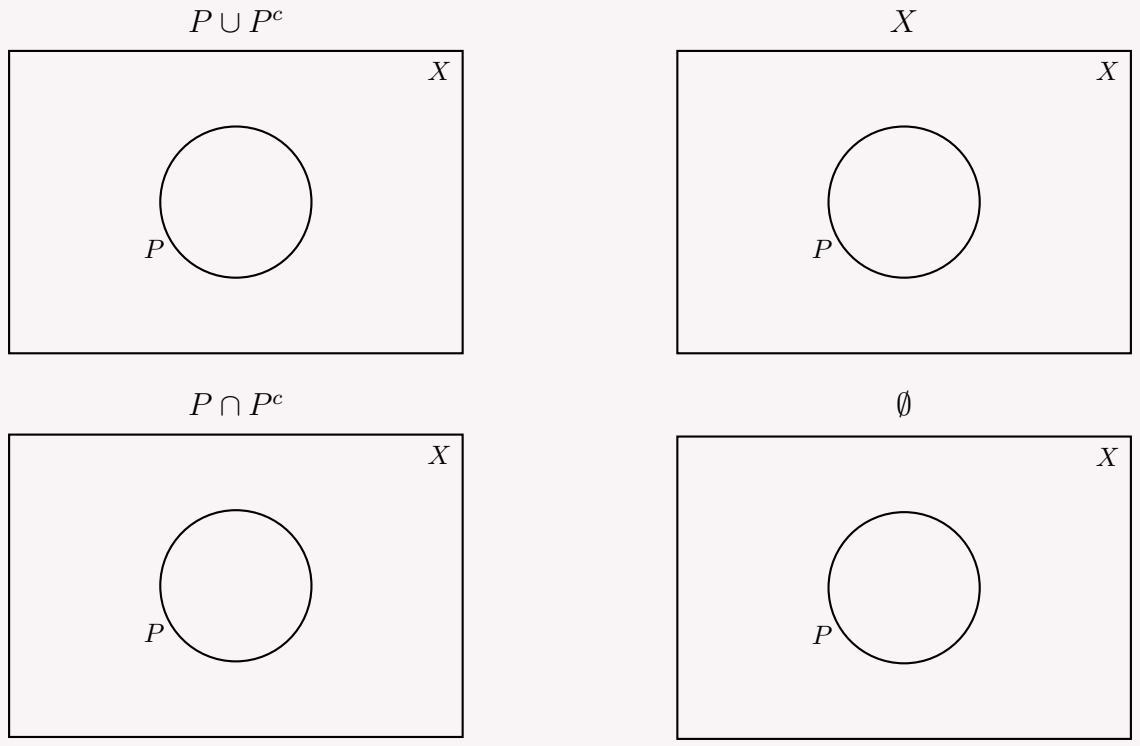
P





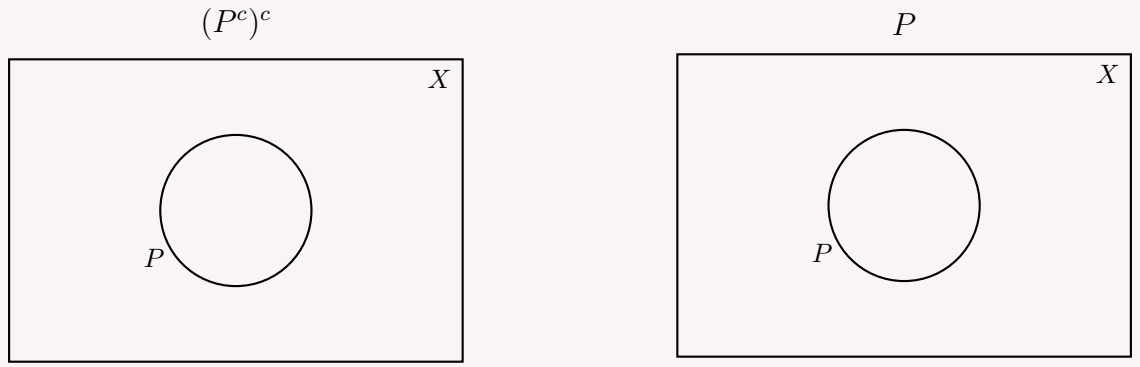
Exercise 6.2.6: Proof of Complement Laws

Color the picture below to show the Complement Laws in Theorem 6.2.1.



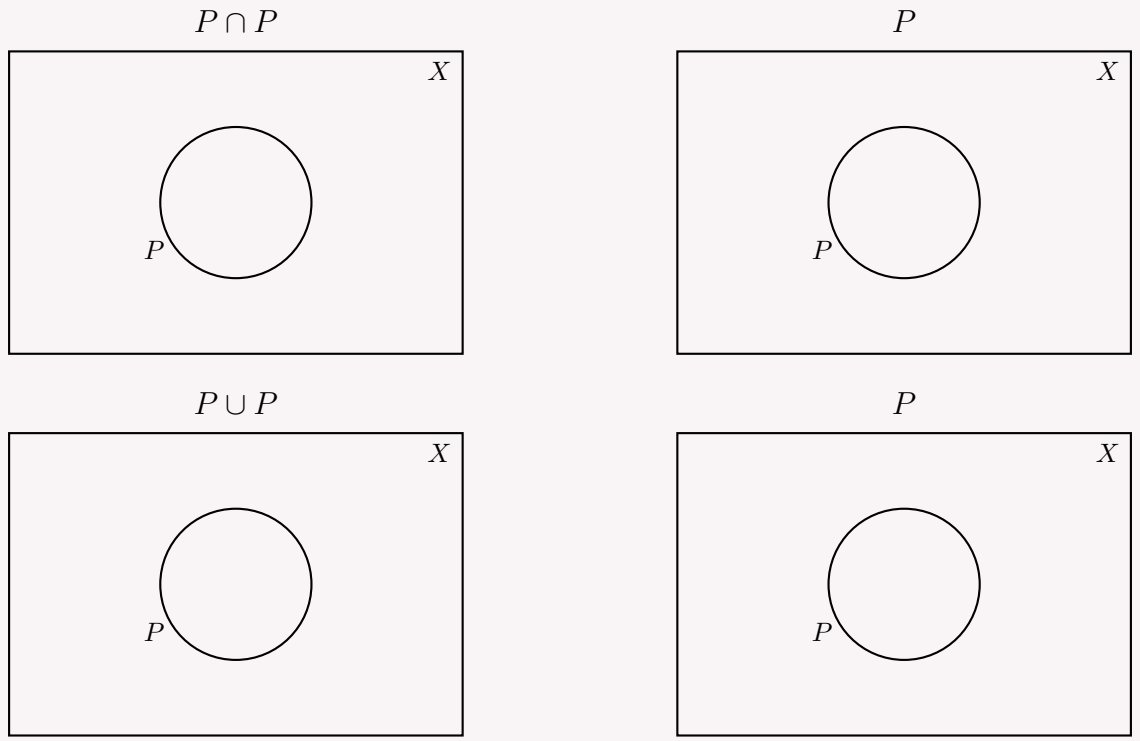
Exercise 6.2.7: Proof of Double Complement Law

Color the picture below to show the Double Complement Law in Theorem 6.2.1.



Exercise 6.2.8: Proof of Idempotent Laws

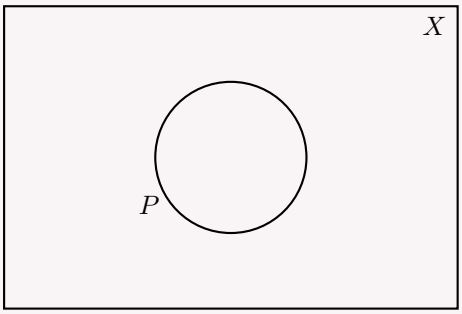
Color the picture below to show the Idempotent Laws in Theorem 6.2.1.



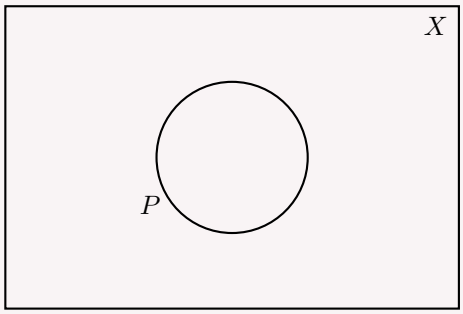
Exercise 6.2.9: Proof of Universal Bound Laws

Color the picture below to show the Universal Bound Laws in Theorem 6.2.1.

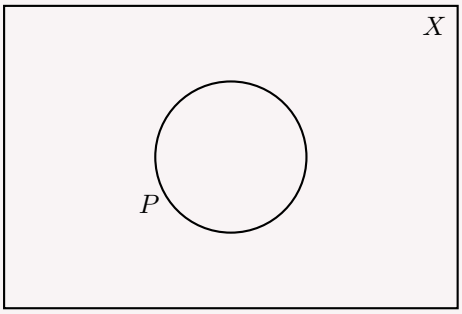
$P \cup X$



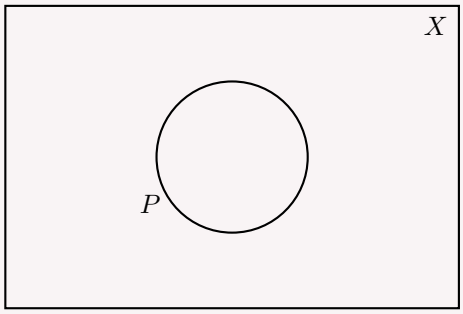
X



$P \cap \emptyset$



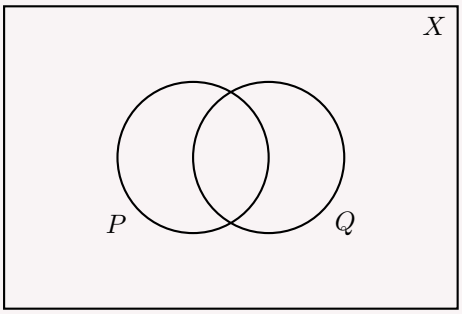
$\emptyset$



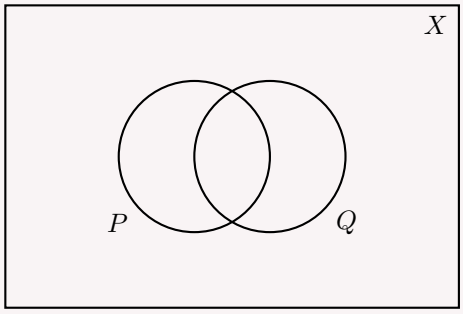
Exercise 6.2.10: Proof of DeMorgan's Laws

Color the diagram below to show DeMorgan's Laws in Theorem 6.2.1.

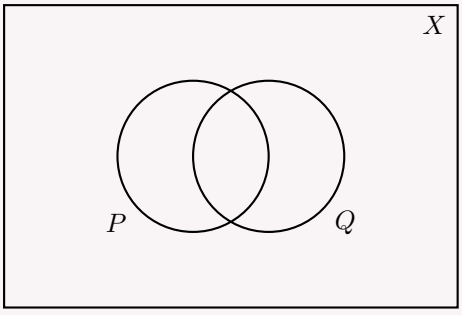
$(P \cap Q)^c$



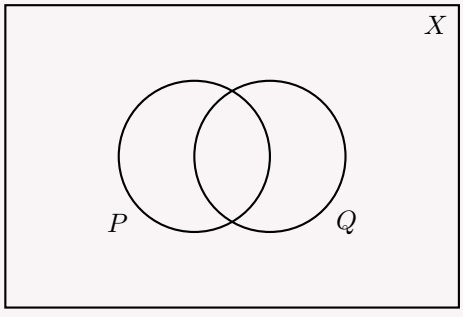
$P^c \cup Q^c$



$(P \cup Q)^c$



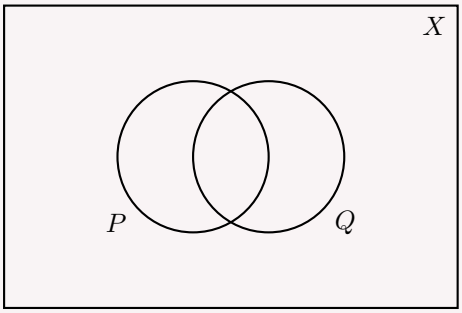
$P^c \cap Q^c$



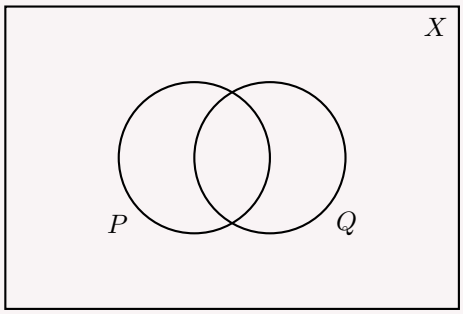
Exercise 6.2.11: Proof of Absorption Laws

Color the diagram below to show the Absorption Laws in Theorem 6.2.1.

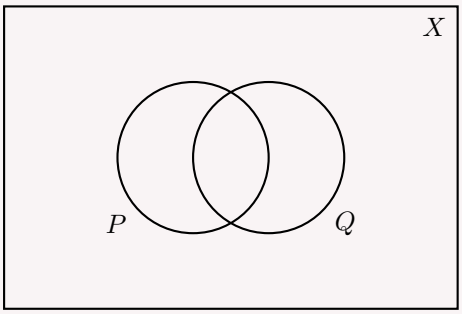
$P \cup (P \cap Q)$



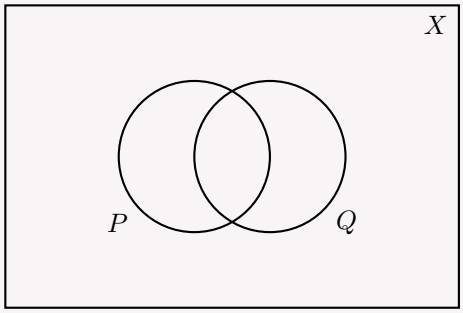
P



$P \cap (P \cup Q)$



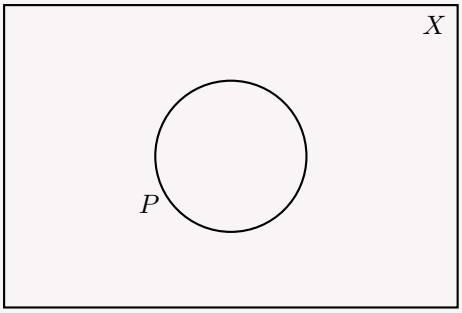
P



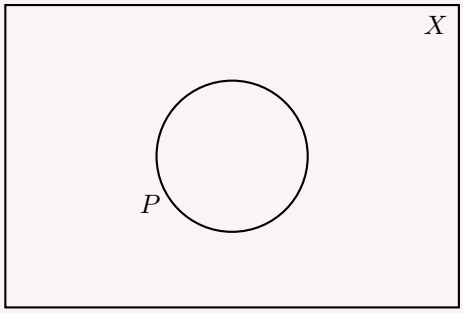
Exercise 6.2.12: Proof of Complement of X and $\emptyset$

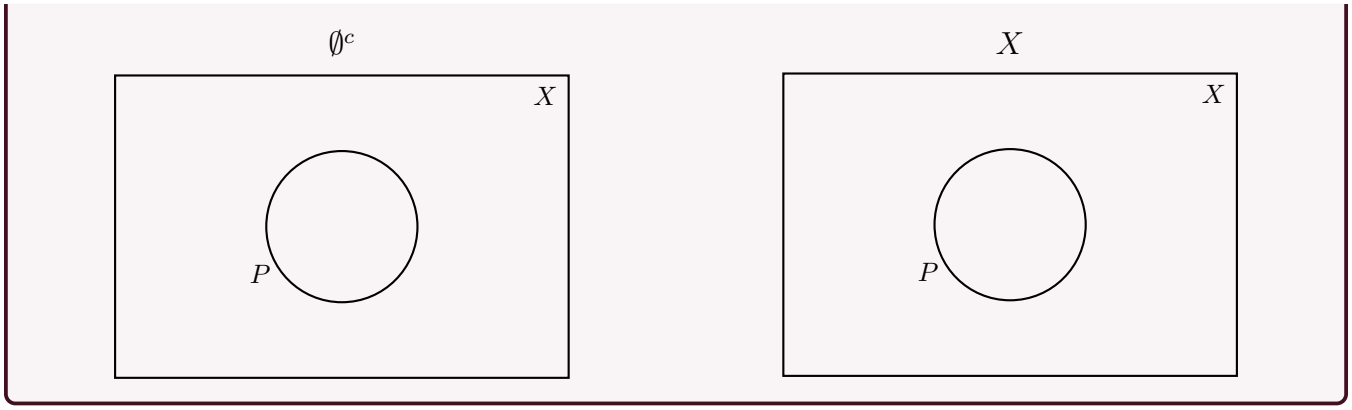
Color the picture below to show the Complement of X and $\emptyset$ Laws in Theorem 6.2.1.

X^c



$\emptyset$





6.2.1 Properties of Subsets

Because subsets are defined by an implication " $\implies$ ", there is a natural ordering to reading statements about them so that we may omit extranneous parentheses. "$A \cap B \subseteq C$" means "$(A \cap B) \subseteq C$".

Proposition 6.2.13: Some Subset Relations

Let A, B be sets (in the same universe). Then

1. $A \cap B \subseteq A$ and $A \cap B \subseteq B$
2. $A \subseteq A \cup B$ and $B \subseteq A \cup B$
3. if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$
4. [Set Difference Law] $A - B = A \cap B^c$

Proof. We use the Element Method of Proof.

1. Suppose $x \in A \cap B$. Then, $x \in A$ and $x \in B$. Therefore $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
2. Let A, B be sets. If $x \in A$, then $x \in A \vee x \in B$, hence $x \in A \cup B$. Therefore $A \subseteq A \cup B$. If $x \in B$, then $x \in A \vee x \in B$, hence $x \in A \cup B$. Therefore $B \subseteq A \cup B$.
3. Let A, B, C be sets wth $A \subseteq B$ and $B \subseteq C$. Suppose that $x \in A$. Then, since $A \subseteq B$, $x \in B$. Moreover, since $B \subseteq C$, then $x \in C$. We have shown that $x \in A \implies x \in C$ and therefore $A \subseteq C$.
4. Let A, B be sets. We have to show both that $A - B \subseteq A \cap B^c$ and that the opposite containment is true.

   [$\subseteq$] Suppose that $x \in A - B$. Then $x \in A$ and $x \notin B$, hence $x \in A$ and $x \in B^c$, and thus $x \in A \cap B^c$. Therefore $A - B \subseteq A \cap B^c$.

   [$\supseteq$] Suppose now that $x \in A \cap B^c$. Then $x \in A$ and $x \in B^c$, that is, $x \in A$ and $x \notin B$, and thus $x \in A - B$. Therefore $A \cap B^c \subseteq A - B$.

□

6.3 Disproofs and Algebraic Proofs

An "algebraic" proof is the language your author uses to indicate that the proof is handled by a string of equalities coming from Theorem 6.2.1 and Proposition 6.2.13.

Example 6.3.1

Prove the following statement using the element method, and then again with the Table of Set Equalities and Proposition 6.2.13:

For all sets A, B, C,

$$(A \cap B) - (A \cap C) = A \cap (B - C).$$

Element Method. *Proof.* Let A, B, C be arbitrary sets.

[$\subseteq$] Suppose $x \in (A \cap B) - (A \cap C)$. Then $x \in A \cap B$ and $x \notin A \cap C$. That $x \in A \cap B$ implies that $x \in A$ and $x \in B$. As well, $x \notin A \cap C$ is equivalent to the statement $\not[x \in A \cap C] \equiv \not[x \in A \wedge x \in C]$, which, by DeMorgan's Law (for logical statements), implies $x \notin A$ or $x \notin C$.

At this point we have that $x \in A$ and $x \in B$, and that $x \notin A$ or $x \notin C$. We can't have that $x \notin A$, so it can only be that $x \notin C$. Thus $x \in B - C$, and therefore $x \in A \cap (B - C)$.

[$\supseteq$] Suppose $x \in A \cap (B - C)$. Then $x \in A$ and $x \in B - C$, hence $x \in B$ and $x \notin C$. Since $x \in A$ and $x \in B$, then $x \in A \cap B$. Also, since $x \notin C$, then in particular, $x \notin (A \cap C)$. It follows that $x \in (A \cap B) - (A \cap C)$ and therefore $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$.

□

Table of Set Equalities *Proof.* Let A, B, C be sets. Then

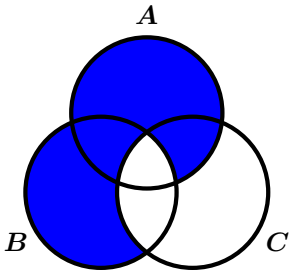
$$\begin{aligned}
(A \cap B) - (A \cap C) &= (A \cap B) \cap (A \cap C)^c && \text{(Set Difference Law)} \\
&= (A \cap B) \cap (A^c \cup C^c) && \text{(DeMorgan's)} \\
&= (A \cap B \cap A^c) \cup (A \cap B \cap C^c) && \text{(distributive)} \\
&= (A \cap A^c \cap B) \cup (A \cap B \cap C^c) && \text{(commutative)} \\
&= \emptyset \cup (A \cap B \cap C^c) && \text{(Complement law)} \\
&= A \cap B \cap C^c && \text{(identity)} \\
&= A \cap (B \cap C^c) && \text{(associative)} \\
&= A \cap (B - C) && \text{(Set Difference Law)}
\end{aligned}$$

Since $A \cap (B - C) = (A \cap B) - (A \cap C)$, then in particular $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$. □

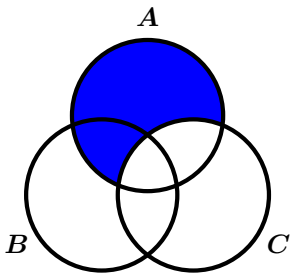
Example 6.3.2

Prove or disprove the following claim.

Claim. For all sets A, B, C, then $(A - B) \cup (B - C) = A - C$.



$(A - B) \cup (A - C)$



$A - C$

This is false. Observe that any example which contains an element of B which is not shared by A or C (or similarly, an element of $A \cap C$ which is not also in B) will be a counter-example to the claim.

Disproof. Consider

$$A = \{1, 2, 3, 4\}, \qquad B = \{2, 4, 5, 6\}, \qquad \text{and} \qquad C = \{3, 4, 6, 7\}.$$

Then

$$A - B = \{1, 3\}, \qquad B - C = \{2, 5\}, \qquad \text{and} \qquad A - C = \{1, 2\},$$

and so

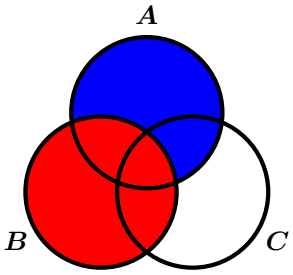
$$(A - B) \cup (B - C) = \{1, 2, 3, 5\} \neq \{1, 2\} = A - C.$$

□

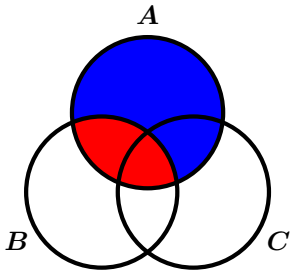
Example 6.3.3

Prove or disprove the following claim.

Claim. For all sets A, B, C, then $(A \cup B) - B = A - (A \cap B)$.



$(A \cup B) - B$



$A - (A \cap B)$

Proof. We have that

$$\begin{aligned}
(A \cup B) - B &= (A \cup B) \cap B^c && \text{(Set Difference Law)} \\
&= B^c \cap (A \cup B) && \text{(Commutative Law)} \\
&= (B^c \cap A) \cup (B^c \cap B) && \text{(Distributive Law)} \\
&= (B^c \cap A) \cup \emptyset && \text{(Complement Law)}
\end{aligned}$$

$$\begin{aligned} &= B^c \cap A && \text{(Identity Law)} \\ &= A \cap B^c && \text{(Commutative Law)} \end{aligned}$$

Also,

$$\begin{aligned} A - (A \cap B) &= A \cap (A \cap B)^c && \text{(Set Difference Law)} \\ &= A \cap (A^c \cup B^c) && \text{(DeMorgan's Law)} \\ &= (A \cap A^c) \cup (A \cap B^c) && \text{(Distributive Law)} \\ &= \emptyset \cup (A \cap B^c) && \text{(Complement Law)} \\ &= A \cap B^c && \text{(Identity Law)} \end{aligned}$$

□

Therefore

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

Power Sets

Let $A = \{1, 2, 3\}$ and $B = \{1, 2\}$. Looking at the power set of A and the power set of B, we have

$$\begin{aligned} \mathscr{P}(A) &= \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\ \} \\ \mathscr{P}(B) &= \{\ \emptyset,\ \{1\},\ \{2\},\ \{1,2\}\ \} \end{aligned}$$

We have that $\mathscr{P}(B) \subsetneq \mathscr{P}(A)$. Morover, notice that the remaining sets in $\mathscr{P}(A) - \mathscr{P}(B)$ can be cleverly written in terms of the subsets of B.

$$\begin{aligned} \{3\} &= \emptyset \cup \{3\} \\ \{1,3\} &= \{1\} \cup \{3\} \\ \{2,3\} &= \{2\} \cup \{3\} \\ \{1,2,3\} &= \{1,2\} \cup \{3\} \end{aligned}$$

This observation provides us with the inutition for the inductive step in the proof of the following.

Theorem 6.3.4

For every integer $n \geq 0$, if a set A has n elements, then $\mathscr{P}(A)$ has 2^n elements.

Proof. Let A be a set. We approach by inducting on the number of elements in A.

Base Step. Suppose A has zero elements. Then $A = \emptyset$. Moreover, $\mathscr{P}(A) = \mathscr{P}(\emptyset) = \{\emptyset\}$, which is a set with $1 = 2^0$ element (a symbol called "$\emptyset$").

Inductive Step. Suppose now $A = \{a_1, a_2, \ldots, a_k\}$ is any set with k elements and that $\mathscr{P}(A)$ has 2^k elements. Let $B = A \cup \{a_{k+1}\}$ so that B has $k+1$ elements. Notice the following:

- $\mathscr{P}(A)$ and $\mathscr{P}(B) - \mathscr{P}(A)$ are disjoint sets (on the left are subsets of A, on the right are subsets of B which are *not* subsets of A).
- $\mathscr{P}(B) = \mathscr{P}(A) \cup \big(\mathscr{P}(B) - \mathscr{P}(A)\big)$ (this is just the complement law)

so $\mathscr{P}(A)$ and $\mathscr{P}(B) - \mathscr{P}(A)$ provide a partition of $\mathscr{P}(B)$. In this way, we should be able to count both sets separately and add them up.

By the inductive hypothesis, $\mathscr{P}(A)$ has 2^k elements.

Observe that a_{k+1} is the only element of B which is not in A, hence every set in $\mathscr{P}(B) - \mathscr{P}(A)$ must be a set of the form $X \cup \{a_{k+1}\}$ where $X \in \mathscr{P}(A)$. Since $\mathscr{P}(A)$ has 2^k elements, then there must be 2^k sets of the form $X \cup \{a_{k+1}\}$, whence $\mathscr{P}(B) - \mathscr{P}(A)$ also has 2^k elements.

It follows then that $\mathscr{P}(B)$ has

$$\underbrace{2^k}_{\mathscr{P}(A)} + \underbrace{2^k}_{\mathscr{P}(B)-\mathscr{P}(A)} = 2(2^k) = 2^{k+1}$$

elements.

Therefore, for all $n \geq 0$, if A has n elements, then $\mathscr{P}(A)$ has 2^n elements.

□

Example 6.3.5

Prove or disprove the following claim.

Claim. For all sets A, B, then $\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B)$.

Proof. Let X be an arbitrary set. We have the following string of biconditionals

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

This shows that $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$ and $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$. Therefore,

$$\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B).$$

□

Example 6.3.6

Prove or disprove the following claim.

Claim. For all sets A, B, then $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

Proof. Let X be an arbitrary set. We have the following string of coniditionals

$$\begin{aligned} & X \in \mathscr{P}(A) \cup \mathscr{P}(B) \\ \iff & X \subseteq A \text{ or } X \subseteq B \\ \implies & X \subseteq A \cup B \end{aligned}$$

$$\iff X \in \mathscr{P}(A \cap B)$$

This shows that

$$\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B).$$

□

6.4 Boolean Algebras, Russell's Paradox, and the Halting Problem

We saw that set theory and logic both seemed to contain some certain structure. So since the same structure appears in multiple separate contexts, that must mean that it's important. As such, we give a name to this feature, which is named after the 19th century English mathematician George Boole.

Definition: boolean algebra

A **Boolean algebra** is a set B together with two operations, generally denoted $\oplus$ and $\otimes$, such that for all $a, b \in B$, both

$$a \oplus b \in B, \qquad a \otimes b \in B$$

and the following properties hold:

1. Commutative Laws: For all $a, b \in B$,
   (a) $a \oplus b = b \oplus a$ (b) $a \otimes b = b \otimes a$
2. Associative Laws: For all $a, b, c \in B$,
   (a) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (b) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
3. Distributive Laws: For all $a, b, c \in B$,
   (a) $a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$ (b) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
4. Identity Laws: There exist distinct elements $\mathrm{Id}_\oplus$ and $\mathrm{Id}_\otimes$ in B such that for all $b \in B$,
   (a) $b \oplus \mathrm{Id}_\oplus = b$ (b) $b \otimes \mathrm{Id}_\otimes = b$
5. Complement Laws: For each $b \in B$, there exists an element in B, denoted $\overline{b}$ and called the complement or negation of b, such that
   (a) $b \oplus \overline{b} = \mathrm{Id}_\otimes$ (b) $b \otimes \overline{b} = \mathrm{Id}_\oplus$

A Boolean algebra is sometimes shortened to the ordered triple $(B, \oplus, \otimes)$.

Remark. Many use the symbols $+, \times, 0, 1$ instead of $\oplus, \otimes, \mathrm{Id}_\oplus, \mathrm{Id}_\otimes$, respectively. While this makes a lot of sense, I'm going to continue with my chosen notation so as not to confuse symbols (since it could be that B is a set of numbers in which case distinguishing between "+" in the Boolean algebra operation vs. "+" in the usual set operation.

Example 6.4.1

$\big(\{\text{logical statements}\}, \vee, \wedge\big)$ is a Boolean algebra where the complement/negation is given by $\overline{p} = \neg p$, and the "identity elements" are $\mathrm{Id}_\vee = \mathbf{c}$ (contradiction) and $\mathrm{Id}_\wedge = \mathbf{t}$ (tautology).

It is straightforward to check the Boolean algebra properties.

- Commutative Laws:
- Associative Laws:
- Distributive Laws:
- Identity Laws:
- Complement Laws:

Example 6.4.2

$\big(\{\text{subsets of a universe } X\}, \cup, \cap\big)$ is a Boolean algebra where the complement/negation is given by $\overline{A} = A^c$, and the identity elements are $\mathrm{Id}_\cup = \emptyset$ and $\mathrm{Id}_\cap = X$.

- Commutative Laws:
- Associative Laws:
- Distributive Laws:
- Identity Laws:
- Complement Laws:

Example 6.4.3

Let $B = \{0, 1\}$ and define the following operations on B:

$$\begin{aligned} x \oplus y &= xy + x + y \pmod 2 \\ x \otimes y &= xy \pmod 2 \\ \overline{x} &= x + 1 \pmod 2 \\ \mathrm{Id}_\oplus &= 0 \pmod 2 \\ \mathrm{Id}_\otimes &= 1 \pmod 2 \end{aligned}$$

Is $(B, \oplus, \otimes)$ a Boolean algebra?

It is! We check the properties in the definition of a Boolean algebra. By commutativity and associativity of the real numbers yield commutativity of $\oplus$ and $\otimes$ almost immediately. The others can be checked with a table.

- Distributive Laws:

a	b	c	$a \oplus (b \otimes c)$	$(a \oplus b) \otimes (a \oplus c)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

a	b	c	$a \otimes (b \oplus c)$	$(a \otimes b) \oplus (a \otimes c)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

- Identity Laws:

b	$\mathrm{Id}_\oplus$	$b \oplus \mathrm{Id}_\oplus$
0	0	0
1	0	1

b	$\mathrm{Id}_\otimes$	$b \otimes \mathrm{Id}_\otimes$
0	1	0
1	1	1

- Complement Laws:

b	$\overline{b}$	$b \oplus \overline{b}$	$\mathrm{Id}_\otimes$
0	1	1	1
1	0	1	1

b	$\overline{b}$	$b \otimes \overline{b}$	$\mathrm{Id}_\oplus$
0	1	0	1
1	0	0	1

Theorem 6.4.4: Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Law*
   For all a and x in B, if $a \oplus x = \mathrm{Id}_\otimes$ and $a \otimes x = \mathrm{Id}_\oplus$, then $x = \overline{a}$.
2. *Uniqueness of* $\mathrm{Id}_\oplus$ *and* $\mathrm{Id}_\otimes$
   If there exists $x \in B$ such that $a \oplus x = a \quad \forall a \in B$, then $x = \mathrm{Id}_\oplus$.
   If there exists $y \in B$ such that $a \otimes y = a \quad \forall a \in B$, then $y = \mathrm{Id}_\otimes$.
3. *Double Complement Law*
   For all $a \in B$, $(\overline{\overline{a}}) = a$.
4. *Idempotent Law*
   For all $a \in B$,
   (a) $a \oplus a = a$ (b) $a \otimes a = a$
5. *Universal Bound Law*
   For all $a \in B$,
   (a) $a \oplus \mathrm{Id}_\otimes = \mathrm{Id}_\otimes$ (b) $a \otimes \mathrm{Id}_\oplus = \mathrm{Id}_\oplus$
6. *De Morgan's Laws*
   For all $a, b \in B$,
   (a) $\overline{a \oplus b} = \overline{a} \otimes \overline{b}$ (b) $\overline{a \otimes b} = \overline{a} \oplus \overline{b}$

7. *Absorption Laws*
   For all $a, b \in B$,

   (a) $(a \oplus b) \otimes a = a$ (b) $(a \otimes b) \oplus a = a$

8. *Complements of* $\mathrm{Id}_\oplus$ *and* $\mathrm{Id}_\otimes$

   (a) $\overline{\mathrm{Id}_\oplus} = \mathrm{Id}_\otimes$ (b) $\overline{\mathrm{Id}_\otimes} = \mathrm{Id}_\oplus$

Proof. 1.

2.

3.

4. Let $a \in B$. Then

$$\begin{aligned} a \oplus a &= (a \oplus a) \otimes \mathrm{Id}_\otimes && \text{(Identity Law)} \\ &= (a \oplus a) \otimes (a \oplus \overline{a}) && \text{(Complement Law)} \\ &= a \oplus (a \otimes \overline{a}) && \text{(Distributive Law)} \\ &= a \oplus \mathrm{Id}_\oplus && \text{(Complement Law)} \\ &= a && \text{(Identity Law)} \end{aligned}$$

   (and the proof that $a \otimes a = a$ is nearly identical with symbols swapped).

5.

□

Example 6.4.5

Let $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$ and define the following operations on B:

$$\begin{aligned} x \oplus y &= \mathrm{lcm}(x, y) \\ x \otimes y &= \gcd(x, y) \\ \overline{x} &= \frac{24}{x} \end{aligned}$$

Is $(B, \mathrm{lcm}, \gcd)$ a Boolean algebra?

This is much harder to tell by simply looking at it, and checking with tables – while not unreasonable for a computer, is not practical by hand (each distributive law will use 216 rows, for example).
The first task might be to try to better understand this collection. What are $\mathrm{Id}_\oplus$ and $\mathrm{Id}_\ominus$? This should be inferrable from the Complement Law, since $a \oplus \overline{a} = \mathrm{Id}_\otimes$. But writing out this relatively short table, we have

b	$\overline{b}$	$b \oplus \overline{b}$
1	24	24
2	12	12
3	8	24
4	6	12
6	4	12
8	3	24
12	2	12
24	1	24

But the third column is not constant, so there cannot be a unique choice of $\mathrm{Id}_{\otimes}$, which violates one of the Boolean Algebra Properties. Therefore $(B, \mathrm{lcm}, \gcd)$ is not a Boolean algebra.

Chapter 7

Properties of Functions

7.1 Functions Defined on General Sets

Definition

Let A, B be sets. The **Cartesian product of A and B** is the set

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

Example 7.1.1: Cartesian Plane

The Cartesian plane, usually denoted $\mathbb{R}^2$ or $\mathbb{R} \times \mathbb{R}$ is the collection of all ordered pairs of real numbers (x, y).

Example 7.1.2

Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. What are

1. $A \times B$
2. $(A \times A) \cap (B \times B)$

1. INCOMPLETE
2. INCOMPLETE

Exercise 7.1.3

Prove the following claim:

Claim. If $A_1 \subseteq A_2$ and $B_1 \subseteq B_2$, then $(A_1 \times B_1) \subseteq (A_2 \times B_2)$.

You've probably always thought about a function f via its graph $y = f(x)$. But what is the graph of the function other than ordered pairs of the form $(x, f(x))$ where the inputs $x \in \mathbb{R}$ and the outputs $f(x) \in \mathbb{R}$. This is the motivation to keep in mind as we work on introducing the formal definition of a limit.

Definition: function

A **function** or **map**, f, from a set A (the **domain**) to a set B (the **codomain**), denoted $f : A \to B$, is a subset of $A \times B$ with the following properties:

1. [uses the whole domain] For every $a \in A$, "$f(a)$" is defined.

$$\forall a \in A, \exists b \in B \text{ such that } (a, b) \in f$$

2. [**well-defined**] For every $a \in A$, the set "$\{f(a)\}$" contains exactly one element.

$$\forall a \in A \text{ and } \forall b_1, b_2 \in B, \text{ if } (a, b_1) \in f \text{ and } (a, b_2) \in f, \text{ then } b_1 = b_2.$$

Since the codomain element b is uniquely associated with the domain element a, one usually writes $f(a) = b$. We also sometimes say that a is "mapped" to b if $f(a) = b$.

Remark. You probably know "well-definedness" as "passing the vertical line test".

Example 7.1.4

Let $f \subseteq \{1, 2, 3, 4\} \times \{5, 6, 7, 8\}$ be given by

$$f = \{(1, 5), (2, 7), (3, 7), (4, 6)\}$$

Is f a function?

Yes. We see that $f(1), f(2), f(3), f(4)$ are all defined, and moreover, each of $1, 2, 3, 4$ are paired with exactly one element of $\{5, 6, 7, 8\}$.

Example 7.1.5

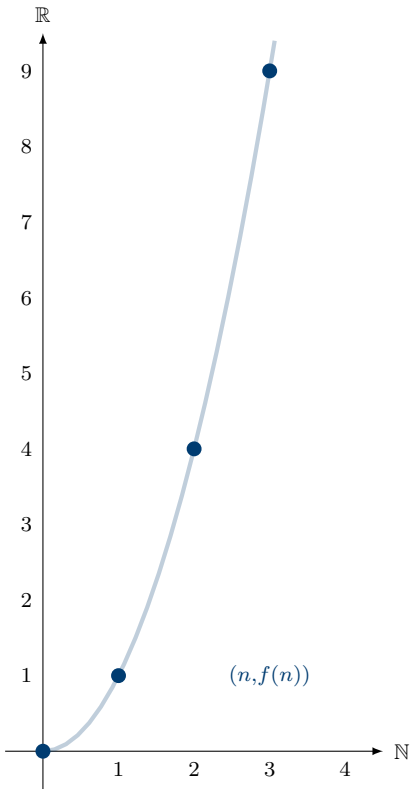
Let $f \subseteq \mathbb{N} \times \mathbb{R}$ be given by

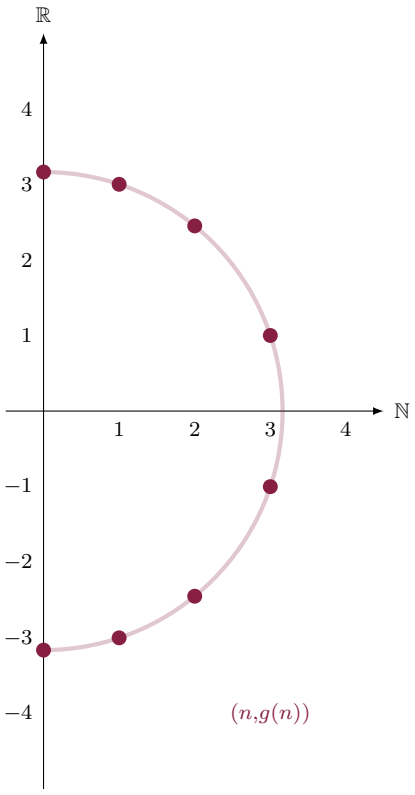
$$f = \left\{(n, y) \ : \ n^2 - y = 0\right\}$$

Let $g \subseteq \mathbb{N} \times \mathbb{R}$ be given by

$$g = \left\{(n, y) \ : \ n^2 + y^2 = 10\right\}$$

Are either of f or g functions?





***f* is a function.** Its defining equation can be rewritten as $x = n^2$, so every unique $n \in \mathbb{N}$ is mapped to only one $x \in \mathbb{R}$.

***g* is not a function.** Both $(5, \sqrt{75})$ and $(5, -\sqrt{75})$ are elements of g. Notably the defining equation can be rearranged to $x = \sqrt{100 - n^2}$ or $x = -\sqrt{100 - n^2}$, so there are two real numbers paired with n when $n \neq 0, 10$.

Example 7.1.6

Let $f : \mathbb{Q} \to \mathbb{Z}$ be given by

$$f\left(\frac{p}{q}\right) = p.$$

Is f a function?

No, f is not a function as it fails to be well-defined. Notice that $\frac{1}{3} = \frac{2}{6}$, but

$$1 = f\left(\frac{1}{3}\right) \neq f\left(\frac{2}{6}\right) = 2.$$

7.1.1 Arrow Diagram

Definition: arrow diagram

Given a function $f : A \to B$, an **arrow diagram** is formed by drawing an arrow from $a \in A$ to $b \in B$ if and only if $f(a) = b$.

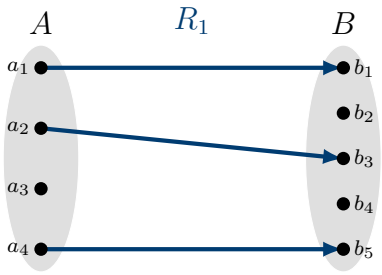
Example 7.1.7: Arrow Diagrams

Let $A = \{a_1, a_2, a_3, a_4\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$. Draw the arrow diagram for each of the following sets:

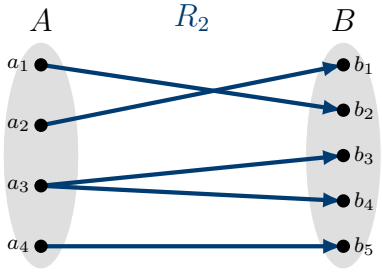
1. $R_1 = \{(a_1, b_1), (a_2, b_3), (a_4, b_5)\}$ Function
2. $R_2 = \{(a_1, b_2), (a_2, b_1), (a_3, b_3), (a_3, b_4), (a_4, b_5)\}$ Not a function
3. $R_3 = \{(a_1, b_2), (a_2, b_3), (a_3, b_1), (a_4, b_3)\}$ Function

Which of these are functions?

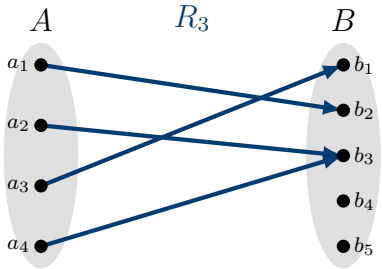
1. $R_1 = \{(a_1, b_1), (a_2, b_3), (a_4, b_5)\}$



2. $R_2 = \{(a_1, b_2), (a_2, b_1), (a_3, b_3), (a_3, b_4), (a_4, b_5)\}$



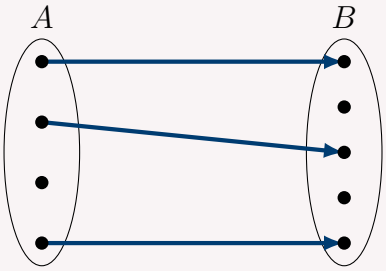
3. $R_3 = \{(a_1, b_2), (a_2, b_3), (a_3, b_1), (a_4, b_3)\}$



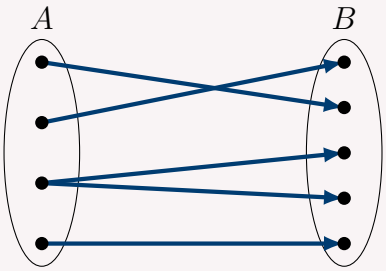
Exercise 7.1.8: Function or Not?

Determine which of the following are functions by looking at the arrow diagram.

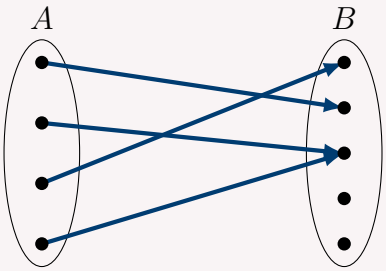
1. f



2. g



3. h



7.1.2 Range, Preimage

Definition: range, preimage

Let $f : A \to B$ be a function. The **range of** f, sometimes denoted $f(A)$, is the set

$$\text{Range}(f) = \{b \in B \ : \ b = f(a) \text{ for some } a \in A\}.$$

Given a subset $S \subseteq B$, the **preimage of** S **under** $\boldsymbol{f}$ is the set

$$\text{Preim}(S) = \{a \in A \ : \ f(a) = s \text{ for some } s \in S\}.$$

Remark. The preimage of S under f is quite commonly written as $f^{-1}(S)$, but so as to avoid confusion, we'll not utilize such notation here.

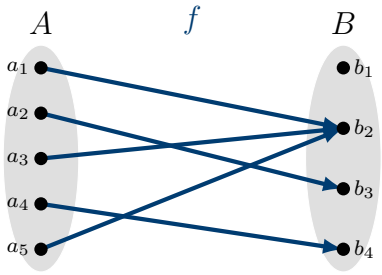
Example 7.1.9

Let $A = \{a_1, a_2, a_3, a_4, a_5\}$ and $B = \{b_1, b_2, b_3, b_4\}$ and let $f : A \to B$ be the function

$$f = \{(a_1, b_2),\ (a_2, b_3),\ (a_3, b_2),\ (a_4, b_4),\ (a_5, b_2)\}\,.$$

Find each of the following.

1. Range(f)
2. Preim($\{b_1\}$)
3. Preim($\{b_2\}$)
4. Preim($\{b_3\}$)
5. Preim($\{b_3, b_4\}$)



1. Range(f) $= \{b_2, b_3, b_4\}$
2. Preim($\{b_1\}$) $= \emptyset$
3. Preim($\{b_2\}$) $= \{a_1, a_3, a_5\}$
4. Preim($\{b_3\}$) $= \{a_2\}$
5. Preim($\{b_3, b_4\}$) $= \{a_2, a_4\}$

Definition

Two functions $f : X \to Y$ and $g : X \to Y$ are **equal** if and only if $f(x) = g(x)$ for every $x \in X$.

Remark. This is implicit in the definition, but f and g must have the same domain and codomain in order to be equal.

Remark. Note that this is equivalent to saying that the sets

$$\{(x, y) \in X \times Y \ :\ f(x) = y\} \qquad \text{and} \qquad \{(x, y) \in X \times Y \ :\ g(x) = y\}$$

are equal

Example 7.1.10

Determine which of the following pairs of functions, f and g, are equal:

1. $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(x) = \dfrac{1}{x^2 + 1}$,

$g : \mathbb{R} \to \mathbb{R}$ given by $\beta(x) = \dfrac{1}{x^2+1}$.

2. $f : \mathbb{Z} - \{1\} \to \mathbb{Z}$, $f(x) = \dfrac{x^2-1}{x-1}$,
   $g : \mathbb{Z} \to \mathbb{Z}$ given by $g(x) = x + 1$.
3. $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = \dfrac{x^3+x}{x^2+1}$,
   $g : \mathbb{Z} \to \mathbb{Z}$ given by $g(x) = x$.
4. $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x^2$,
   $g : \mathbb{Z} \to \mathbb{N}$ given by $g(x) = x^2$.

1. f and g are not equal because $f(\pi)$ is undefined, but $g(\pi)$ is defined.
2. f and g are not equal because $f(1)$ is undefined, but $g(1)$ is defined.
3. Noting that $\dfrac{x^3+x}{x^2+1} = \dfrac{x(x^2+1)}{x^2+1} = x$, we see that $f(x) = g(x)$ for all $x \in \mathbb{Z}$. Thus $f = g$.
4. Even though both sets have the same domains and seem to have the same ranges (because $x^2 \geq 0$), the codomains are different so the functions are not equal.

7.2 One-to-One, Onto, and Inverse Functions

Definition: one-to-one, onto, bijection

Let $f : A \to B$ be a function. f is said to be **one-to-one** or **injective** if and only if

$$\text{for all } a_1, a_2 \in A, \text{ if } f(a_1) = f(a_2) \text{ then } a_1 = a_2.$$

The tagline is that *"two distinct inputs cannot have the same output."*
f is said to be **onto** or **surjective** if and only if

$$\text{for all } b \in B, \text{ there is some } a \in A \text{ for which } f(a) = b.$$

The tagline is that *the range of f is all of B.*
f is called **bijective** or a **bijection** if and only if it is both one-to-one and onto.

Remark. A bijection is sometimes called a **one-to-one correspondence**. We will be avoiding this term for obvious reasons.

Remark. *One-to-one* and *onto* are universal statements and should be proven according to the usual strategies from 4.1 (note that "onto" is even a statement with nested quantifiers.)

Example 7.2.1

Use arrow diagrams to give examples of functions $f : A \to B$ that are all combinations of one-to-one (or not) and onto (or not).

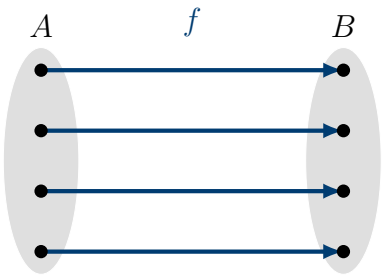


Figure 7.1: f is both one-to-one and onto.

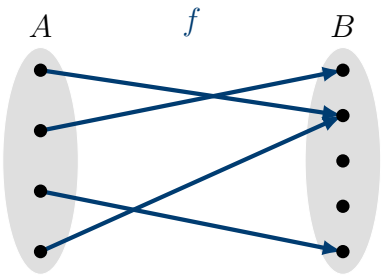


Figure 7.2: f is one-to-one, but not onto.

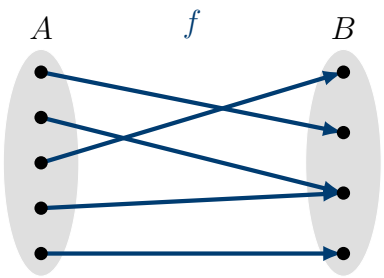


Figure 7.3: f is not one-to-one, but is onto.

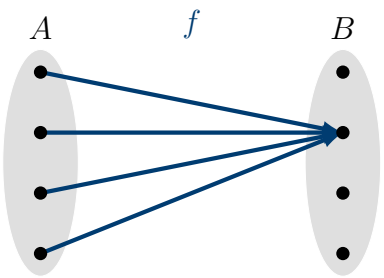


Figure 7.4: f is neither one-to-one nor onto.

Example 7.2.2

Give examples of functions $R \to \mathbb{R}$ that are all combinations of one-to-one (or not) and onto (or not).

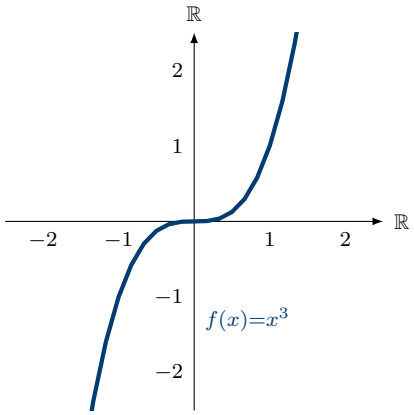


Figure 7.5: f is both one-to-one and onto.

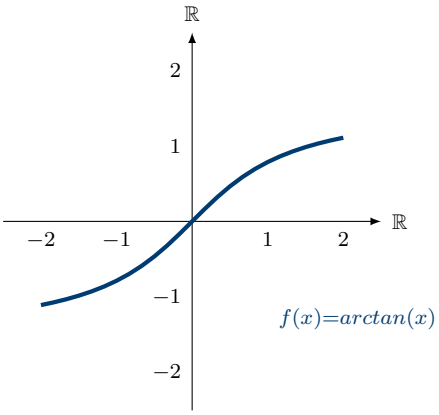


Figure 7.6: g is one-to-one, but not onto.

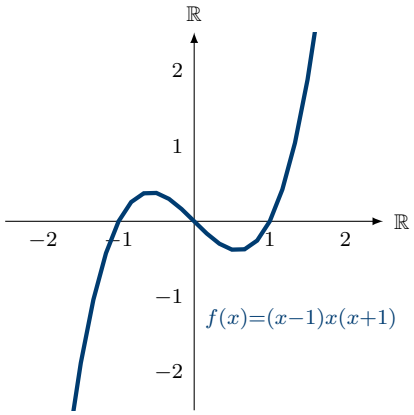


Figure 7.7: f is not one-to-one, but is onto.

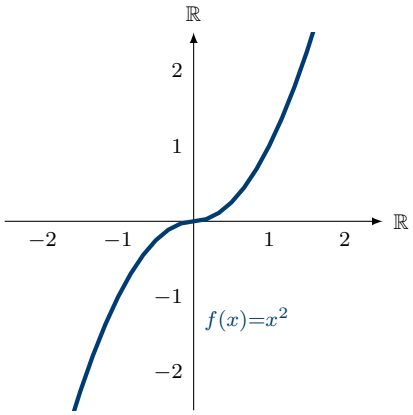


Figure 7.8: f is neither one-to-one nor onto.

Let's look at Example 7.2.2 and for every function f, draw the reverse arrows (call them g).

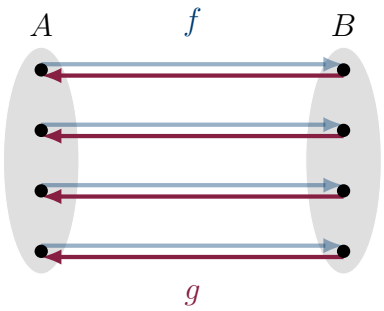


Figure 7.9: f is both one-to-one and onto.
g is both one-to-one and onto.

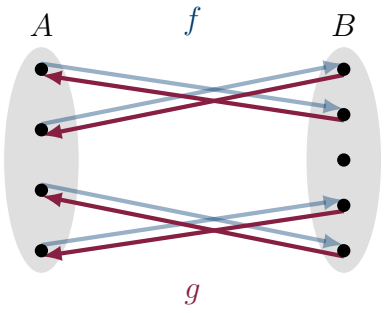


Figure 7.10: f is one-to-one, but not onto.
g is not a function because
it fails the first condition in the definition.

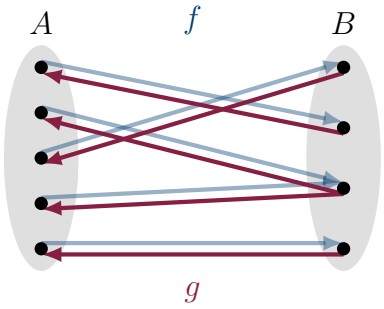


Figure 7.11: f is not one-to-one, but is onto. g is not a function.

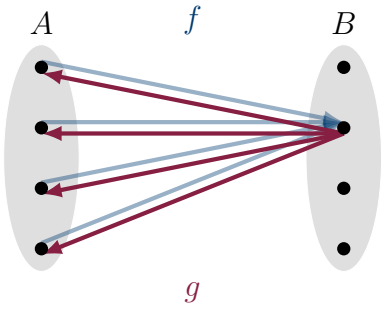


Figure 7.12: f is neither one-to-one nor onto. g is not a function.

Naïvely, we would want to define an inverse function by just reversing the arrows. What we see is that the "inverse" only exists in the case that f is one-to-one and onto. Explicitly,

Theorem 7.2.3: Existence of an inverse

Let $f : A \to B$ be a function and define the following subset of $B \times A$:

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

f^{-1} is a function if and only if f is a bijection.

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

Uses whole domain. For every $b \in B$, there exists $a \in A$ so that $f^{-1}(b) = a$ if and only if there exists $a \in A$ so that $f(a) = b$ (i.e., if and only if f is surjective).

Well-defined. For every $a_1, a_2 \in A$ and $b \in B$,

$$f^{-1}(b) = a_1 \wedge f^{-1}(b) = a_2 \implies a_1 = a_2$$

is true if and only if

$$f(a_1) = b \wedge f(a_2) = b \implies a_1 = a_2$$

(i.e., if and only if f is one-to-one).

□

Definition: inverse

Let $f : A \to B$ be a function. The function $f^{-1} : B \to A$ defined in Theorem 7.2.3 is called an **inverse of f**. If f^{-1} exists, then f is called **invertible**.

Example 7.2.4

Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = 3|x| - 5$.

1. Prove or disprove: f is one-to-one.
2. Prove or disprove: f is onto.
3. If f is both one-to-one and onto, find an inverse for f.

1. INCOMPLETE
2. INCOMPLETE

3. INCOMPLETE
4. INCOMPLETE

Example 7.2.5

Let $g : \mathbb{R} \to \mathbb{R}$ be given by $g(x) = \sqrt[3]{x^5 + 1}$.

1. Prove or disprove: g is one-to-one.
2. Prove or disprove: g is onto.
3. If g is both one-to-one and onto, find an inverse for f.

1. INCOMPLETE
2. INCOMPLETE
3. INCOMPLETE

Example 7.2.6

Let $h : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ be given by $h(x, y) = (x + y, x - y)$.

1. Prove or disprove: h is one-to-one.
2. Prove or disprove: h is onto.
3. If h is both one-to-one and onto, find its inverse.

1. h is one-to-one. To see this, suppose that there are pairs $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$ for which
$$h(x_1, y_1) = (x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2) = h(x_2, y_2).$$
Then $x_1 + y_1 = x_2 + y_2$ rearranges to $x_1 = x_2 - y_1 + y_2$, and thus
$$\begin{aligned} x_1 - y_1 = x_2 - y_2 &\implies x_2 - y_1 + y_2 - y_1 = x_2 - y_2 \\ &\implies -2y_1 = -2y_2 \\ &\implies y_1 = y_2 \end{aligned}$$
Then $y_1 = y_2$ implies that $x_1 = x_2 - y_1 + y_2 = x_2 - 0 = x_2$. So it follows that $(x_1, y_1) = (x_2, y_2)$.
2. h is onto. To see this, let $(w, z) \in \mathbb{R} \times \mathbb{R}$ be a point in the codomain. We seek a pair (x, y) so that $h(x, y) = (w, z)$. This can be achieved by solving a linear system (with standard techniques):
$$h(x, y) = (x + y, x - y) = (w, z) \implies \begin{cases} x + y = w \\ x - y = z \end{cases} \implies \begin{cases} x = \frac{w+z}{2} \\ y = \frac{w-z}{2} \end{cases}$$
Therefore, for every (w, z), we have that $h\left(\frac{w+z}{2}, \frac{w-z}{2}\right) = (w, z)$.
3. We secretly found the inverse in the previous part.
$$h(x, y) = \left(\frac{x + y}{2}, \frac{x - y}{2}\right).$$

Remark. The astute reader will realize that the last example was a linear transformation, given by multiplication by $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, and whose inverse transformation is given by multipliation by $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$

Example 7.2.7

Let $j : \mathbb{R} \to \mathbb{R}$ be given by $j(x) = e^x$.

1. Prove or disprove: j is one-to-one.
2. Prove or disprove: j is onto.
3. If j is both one-to-one and onto, find its inverse.

1. INCOMPLETE
2. INCOMPLETE
3. INCOMPLETE
4. INCOMPLETE

7.3 Composition of functions

Definition: function composition

Let $f : A \to B$ and $g : B \to C$ be functions. Define a new function $g \circ f : A \to C$ as follows:

$$(a, c) \in g \circ f \text{ iff } \exists b \in B \text{ s.t. } (a, b) \in f \text{ and } (b, c) \in g$$

The function $g \circ f$ is called the **composition of f and g** and is usually said aloud as "g of f."

In the above definition, the function definition requires that $b \in \text{range}(F)$, so we can freely use familiar notation: $(g \circ f)(a) = g(f(a))$ for all $a \in A$.

Example 7.3.1

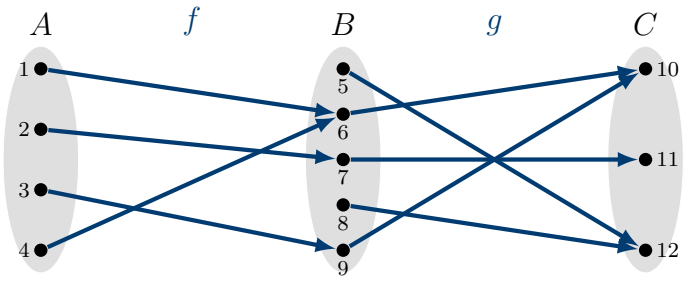
Let $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7, 8, 9\}$, and $C = \{10, 11, 12\}$. Let f and g be functions given by

- $f = \{ (1, 6), (2, 7), (3, 9), (4, 6) \}$
- $g = \{ (5, 12), (6, 10), (7, 11), (8, 12), (9, 10) \}$

Determine $g \circ f$.

$$g \circ f = \{ (1, 10), (2, 11), (3, 10), (4, 10) \}.$$

We can also draw the arrow diagram to see this – composition is just following the arrow paths from A to C.



Theorem 7.3.2: Inverses and Composition

Let $f : A \to B$ and $g : B \to A$ be two functions. Then $g = f^{-1}$ if and only if, for all $a \in A$ and forall $b \in B$,

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

That is, $g \circ f$ and $f \circ g$ are both the identity functions.

Proof. Let $f : A \to B$ and $g : B \to A$ be functions.

Case (⇒). Suppose that $g = f^{-1}$ and let $(a, b) \in f$ be arbitrary. By definition of the inverse $(b, a) \in g$, hence

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

Case ($\Leftarrow$). Suppose now that, for all $a \in A$ and forall $b \in B$, we have

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

Let $(a_0, b_0) \in f$ be arbitrary but fixed. $(g \circ f)(a_0) = a_0$ implies that there exists some $b_1 \in B$ for which $(a_0, b_1) \in f$ and $(b_1, a_0) \in g$. However, since f is well-defined, then $b_0 = b_1$, i.e, $(b_0, a_0) \in g$.

Similarly, let $(b_0, a_0) \in g$ be arbitrary but fixed. $(f \circ g)(b_0) = b_0$ implies that there exists some $a_1 \in A$ for which $(a_1, b_0) \in f$ and $(b_0, a_1) \in g$. However, since g is well-defined, then $a_1 = a_0$, i.e, $(b_0, a_0) \in g$.

We now that have $(a_0, b_0) \in f \iff (b_0, a_0) \in g$, whence $g = f^{-1}$ as desired.

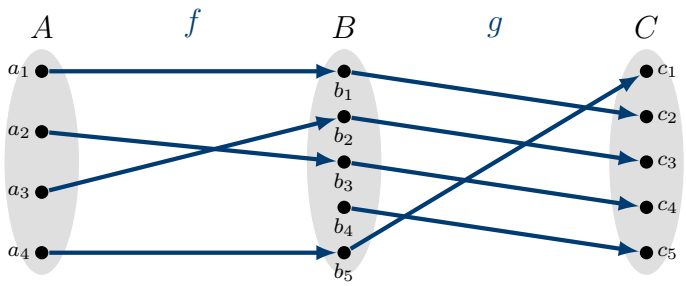
□

Example 7.3.3

Let $f : A \to B$ and $g : B \to C$ be functions.

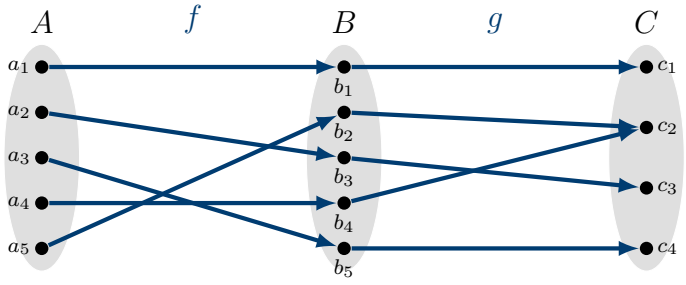
1. Draw an arrow diagram where both f and g are one-to-one. What do you observe about $g \circ f$?
2. Draw an arrow diagram where both f and g are onto. What do you observe about $g \circ f$?

1. Let f and g be the one-to-one functions shown below.



We see that $g \circ f$ is also one-to-one.

2. Let f and g be the onto functions shown below.



Theorem 7.3.4

Let $f : A \to B$ and $g : B \to C$ be functions.

1. If f, g are both one-to-one, then so is $g \circ f$.

2. If f, g are both onto, then so is $g \circ f$.

Proof. Let $f : A \to B$ and $g : B \to C$ be functions.

1. Suppose f and g are both one-to-one. Let $a_1, a_2 \in A$ and suppose that

$$g \circ f(a_1) = g(f(a_1)) = g(f(a_2)) = g \circ f(a_2).$$

   Since g is one-to-one, then it must follow that $f(a_1) = f(a_2)$, and since f is one-to-one, it follows that $a_1 = a_2$. Therefore $g \circ f$ is one-to-one.

2. Suppose f and g are both onto and let $c \in C$. Since g is onto, there must be some $b \in B$ such that $g(b) = c$. Since f is onto, there must be some $x \in A$ such that $f(x) = b$, i.e., that $g \circ f(x) = g(f(x)) = g(b) = c$. Therefore $g \circ f$ is onto.

□

Corollary 7.3.5

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

Corollary 7.3.5 is actually very useful in practice. It can be hard to construct a bijection from a set A to a set D. But it may be straightforward to construct a bijection $f : A \to B$, a bijection $g : B \to C$, and a bijection $h : C \to D$. The result then tells us that

$$h \circ g \circ f : A \to D$$

is a bijection.

7.4 Cardinality

Consider the following three situations:

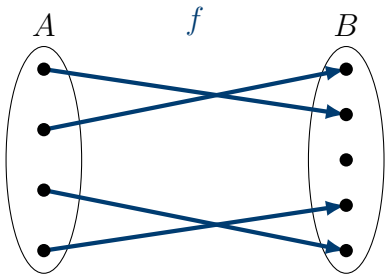


Figure 7.13: f is one-to-one, but not onto.

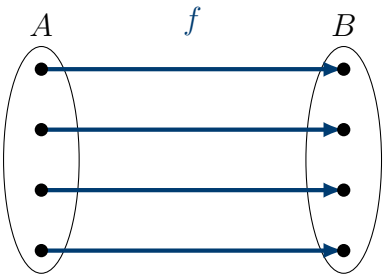


Figure 7.14: f is both one-to-one and onto.

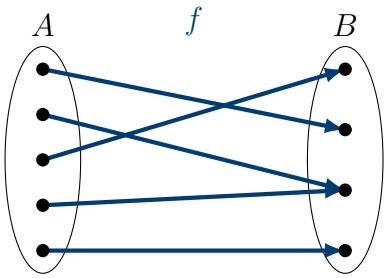


Figure 7.15: f is not one-to-one, but is onto.

When A and B have the same number of elements, f is a bijection, but when the sets have different numbers of elements, then f can only be one-to-one or onto (and not both). If we let $|A|$ and $|B|$ denote the number of elements in each of A and B, the observation can be stated as follows:

- $|A| \leq |B|$ if and only if there is a one-to-one function $f : A \to B$.
- $|A| \geq |B|$ if and only if there is an onto function $f : A \to B$.
- $|A| = |B|$ if and only if there is a bijective function $f : A \to B$.

This allows us to reframe and formalize a notion of "size" of sets via functions.

Definition: cardinality

Let A, B be sets. A and B are said to have the same **cardinality** if there is a bijection between A and B. We write "$|A|$" or "$\#A$" to denote the cardinality of A.

Example 7.4.1: Shift-by-m map

Let m and n be positive integers. Show that the sets $\{1, \ldots, n\}$ and $\{m+1, \ldots, m+n\}$ have the same cardinality by proving that the function

$$\begin{aligned} f :&\{1, \ldots, n\} \to \{m+1, \ldots, m+n\} \\ &f(x) = x + m \end{aligned}$$

is a bijection.

Lemma 7.4.2

For all finite sets A and B,

$$|A \cup B| \leq |A| + |B|.$$

The proof of Lemma 7.4.2 will be reserved for an appendix. The proof isn't hard, it's just obnoxiously tedious given how obvious the result is.

Example 7.4.3

Prove that, for all natural numbers $n \geq 2$,

$$|A_1 \cup \cdots \cup A_n| \leq |A_1| + \cdots + |A_n|.$$

We approach via induction, using Lemma 7.4.2 for the base case and, along with associativity of the union operation, using it again for the inductive step. INCOMPLETE

Definition: types of cardinality

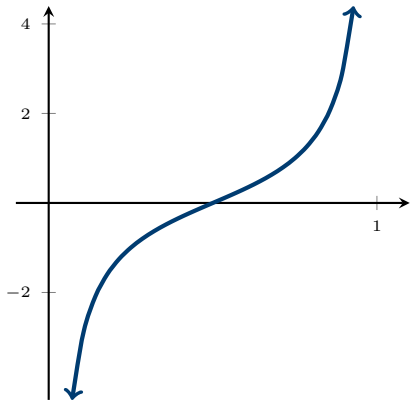
A set A is called...

- **finite** if it is either empty or is in one-to-one correspondence with the set $\{0, 1, 2, 3, \ldots, n\}$ for some $n \in \mathbb{N}$.
- **infinite** if it is not finite.
- **countable** (or **countably-infinite**) if it has the same cardinality as $\mathbb{N}$.
- **uncountable** if it is neither finite nor countable.

Remark. Some authors allow "countable" to include finite sets. In this class we'll only use the term in the case of infinite sets, so such conventional discrepancies won't matter.

Example 7.4.4

Find a bijection $f : (0, 1) \to \mathbb{R}$.



The function

$$f : (0, 1) \to \mathbb{R}$$
$$f(x) = \tan\left(\pi x - \frac{\pi}{2}\right)$$

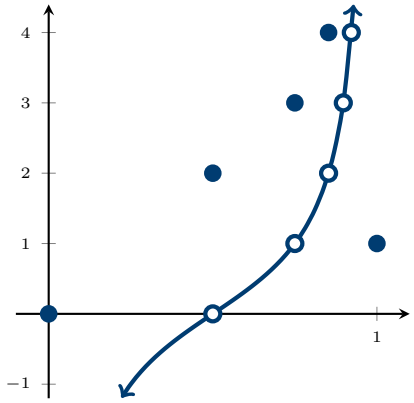
is a bijection with inverse

$$f^{-1}(x) = \frac{1}{\pi}\arctan(x) + \frac{1}{2}.$$

Example 7.4.5

Find a bijection $f : [0, 1] \to \mathbb{R}$.

The motivation for this is to take the tangent function (which can be modified simply to send $(0, 1)$ to $\mathbb{R}$) and to define it in a piecewise way so as to involve the interval endpoints $\{0, 1\}$).

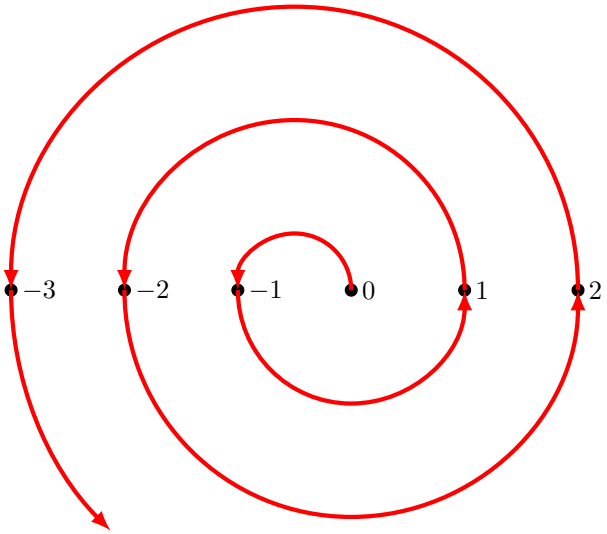


Let $g = \tan\left(\pi x - \frac{\pi}{2}\right)$. Then the bijection $f : [0, 1] \to \mathbb{R}$ is given by

$$f(x) = \begin{cases} 0 & \text{when } x = 0 \\ 1 & \text{when } x = 1 \\ g(x) & \text{when } g(x) \notin \mathbb{N} \\ 2 + g(x) & \text{otherwise.} \end{cases}$$

Example 7.4.6: $\mathbb{Z}$ is countable

Find a bijection $f : \mathbb{N} \to \mathbb{Z}$.



$$\begin{aligned} f(0) &= 0 \\ f(1) &= -1 \\ f(2) &= 1 \\ f(3) &= -2 \\ f(4) &= 2 \\ &\vdots \end{aligned}$$

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{when } n \text{ is even,} \\ -\dfrac{n+1}{2} & \text{when } n \text{ is odd.} \end{cases}$$

Proof. We now prove that f is bijective.

One-to-one. To see that f is one-to-one, we consider three separate cases. Let $x, y \in \mathbb{N}$.

- ***x* and *y* are both even.** Suppose $f(x) = f(y)$ where x and y are both even. Then
$$\frac{x}{2} = \frac{y}{2} \qquad \Longrightarrow \qquad x = y.$$
- ***x* and *y* are both odd.** Suppose $f(x) = f(y)$ where x and y are both odd. Then
$$-\frac{x+1}{2} = -\frac{y+1}{2} \qquad \Longrightarrow \qquad x = y.$$
- ***x* is even and *y* is odd.** *(We use the contrapositive of the one-to-one definition here.)* Suppose That x is even and y is odd (so in particular we are supposing $x \neq y$). Then
$$\frac{x}{2} = -\frac{y+1}{2} \qquad \Longrightarrow \qquad x = -(y+1)$$
Since $x \geq 0$ and $-(y+1) < 0$, it follows that $f(x) \neq f(y)$.

Onto. To see that f is onto, we consider two separate cases. Let $y \in \mathbb{Z}$ be arbitrary.

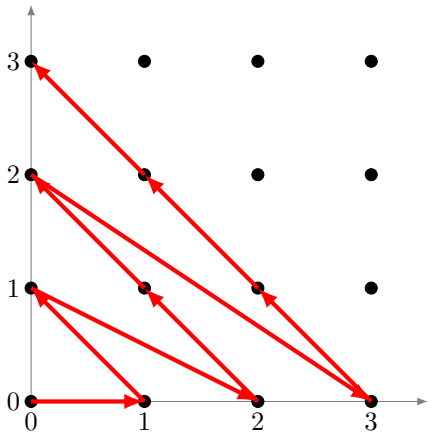
- ***y* < 0.** Suppose $y < 0$. Then we choose $x = -2y - 1$ and see that
$$f(x) = -\frac{-2y - 1 + 1}{2} = y.$$
- ***y* ≥ 0.** Suppose $y \geq 0$. Then we choose $x = 2y$ and see that
$$f(x) = \frac{2y}{2} = y.$$

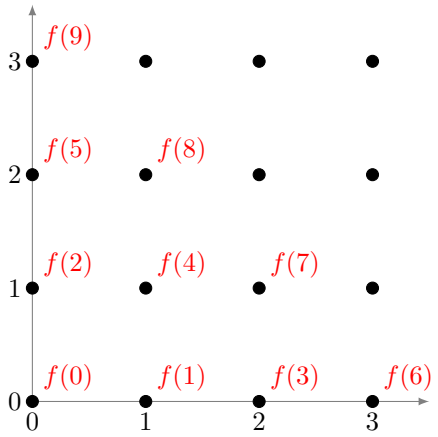
□

Example 7.4.7: $\mathbb{N} \times \mathbb{N}$ is countable.

Find a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

Visually, we'll define f to iterate through all pairs of natural numbers as shown below.





We're going to define the function

$$f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$$
$$f(x) = (x - \ell_x, \ell_x)$$

but we'll need to explain a bit about this ℓ_x.

Looking at the x-axis in the figure above, see that every point on this axis is $f\left(\frac{k(k+1)}{2}\right)$ for some $k \in \mathbb{N}$. This leads us to the first observation: for every $x \in \mathbb{N}$, there exists a unique $n \in \mathbb{N}$ such that

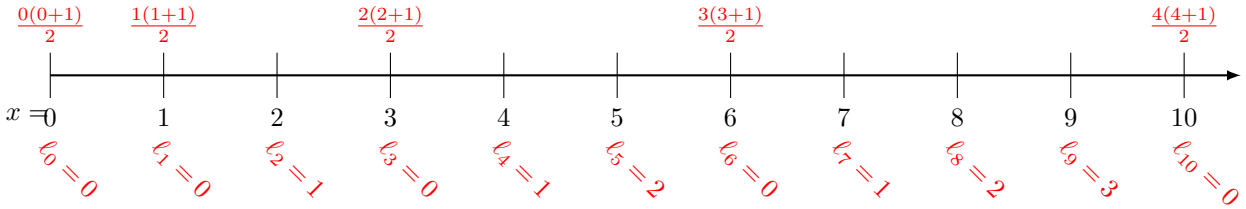
$$\frac{n(n+1)}{2} \leq x < \frac{(n+1)(n+2)}{2}.$$

As such, we x we define a number ℓ_x by

$$\ell_x = x - \frac{n(n+1)}{2}$$

where n is the particular number in the above inequality.

Notice, in particular, that $0 \leq \ell_x \leq n$ and that ℓ_x attains every value between 0 and n as x varies.



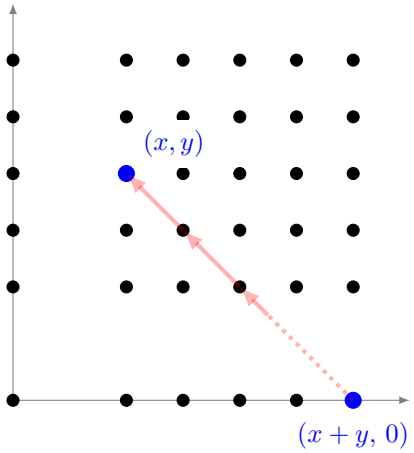
Now we prove that this function f is a bijection.

Proof. To see that f is injective, suppose that $f(x) = f(y)$ for some $x, y \in \mathbb{N}$:

$$(x - \ell_x, \ell_x) = (y - \ell_y, \ell_y).$$

Since $\ell_x = \ell_y$, then $x - \ell_x = y - \ell_y$ implies that $x = y$.

To see that f is surjective, we first make the following observation



The point $(n, 0)$ is obtained via $f\left(\frac{n(n+1)}{2}\right)$, so we must have that

$$(x+y, 0) = f\left(\frac{(x+y)(x+y+1)}{2}\right).$$

whence

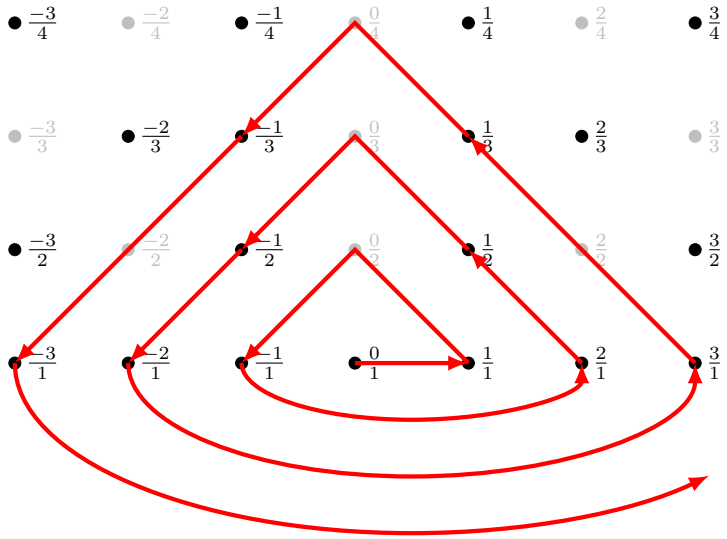
$$(x, y) = f\left(\frac{(x+y)(x+y+1)}{2} + y\right).$$

In fact, $f^{-1}(x, y) = \dfrac{(x+y)(x+y+1)}{2} + y$. □

Example 7.4.8

Show that $\mathbb{Q}$ is countable.

Note that every rational number can be written in the form $\dfrac{p}{q}$ with $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$. In this way, we draw out a grid for $\mathbb{Z} \times \mathbb{Z}^+$ and label the point (p, q) with the fraction $\frac{p}{q}$. There will be several fractions that are not written in lowest terms, so cross out each of these points. We then start counting outwards from $0 = \dfrac{0}{1}$ according to the diagram below (which mimics the strategy which shows that $\mathbb{N} \times \mathbb{N}$ is countable).



7.4.1 Infinity Infinities: "To Infinity and Beyond"

Theorem 7.4.9: Cantor, 1891

$\mathbb{R}$ is uncountable.

The proof of this theorem uses a technique which is now called a "Diagonal Argument" or "Cantor's Diagonal Argument." We note that, from Example 7.4.4, it suffices to show that $(0, 1)$ is

uncountable.

Proof. We approach by contradiction. Suppose that $(0,1)$ is countable. Then there is some way to list all real numbers $\{x_0, x_1, x_2, x_3, \ldots\}$ in $(0,1)$. Writing these down in binary, we would have a table that could look something like the one below (which was randomly generated by Mathematica):

$$\begin{array}{lllllllllll}
x_1 = 0 & . & \boxed{4} & 8 & 2 & 9 & 1 & 3 & 2 & 3 & \ldots \\
x_2 = 0 & . & 3 & \boxed{2} & 8 & 2 & 0 & 5 & 8 & 9 & \ldots \\
x_3 = 0 & . & 4 & 6 & \boxed{5} & 1 & 9 & 9 & 3 & 8 & \ldots \\
x_4 = 0 & . & 5 & 8 & 1 & \boxed{0} & 8 & 1 & 3 & 1 & \ldots \\
x_5 = 0 & . & 3 & 5 & 5 & 4 & \boxed{7} & 2 & 3 & 3 & \ldots \\
x_6 = 0 & . & 5 & 3 & 8 & 2 & 3 & \boxed{1} & 2 & 6 & \ldots \\
x_7 = 0 & . & 6 & 3 & 1 & 3 & 3 & 6 & \boxed{9} & 1 & \ldots \\
x_8 = 0 & . & 0 & 1 & 4 & 3 & 3 & 3 & 8 & \boxed{5} & \ldots \\
\vdots & & & & & & & & & & \ddots
\end{array}$$

For each natural number m in the range $0 \leq m \leq 9$, we define the "swap of m," denoted $\overset{\circ}{m}$, as $9 - m$. Now we have that $0 \leq \overset{\circ}{m} \leq 9$ and there are no numbers for which $m = \overset{\circ}{m}$.

Let d_k represent the k^{th} digit in x_k, and let $x = 0.\, \overset{\circ}{d_1}\overset{\circ}{d_2}\overset{\circ}{d_3}\overset{\circ}{d_4} \ldots$ be the decimal formed from these digits, after "swapping." With the example table above, we have that

$$x = 0.\, \overset{\circ}{4}\overset{\circ}{2}\overset{\circ}{5}\overset{\circ}{0}\overset{\circ}{7}\overset{\circ}{1}\overset{\circ}{9}\overset{\circ}{5} \ldots = 0.58492804\cdots$$

Such an x is specifically designed to disagree with x_k at the k^{th} digit, for every natural number k. We have thus constructed a real number which was not counted. (If it did appear on the table somewhere, we could write $x = x_n$ for some n, but then x and x_n would agree at their n^{th} digit). This contradicts the assumption that $(0,1)$ was countable. □

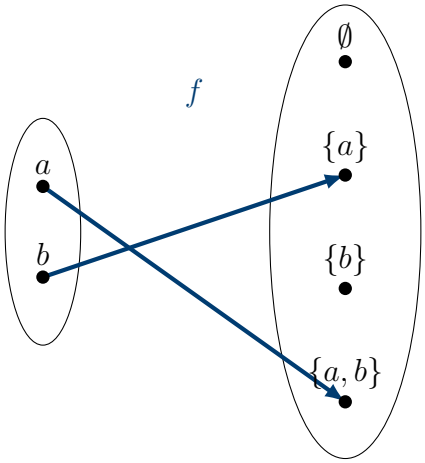
This blew the minds of many mathematicians at the time (and stirred up some controversy), because it implied that there were different sizes of infinity, and the cardinality of $\mathbb{R}$ was a "larger infinity" than the cardinality of $\mathbb{N}$.

It also leads to an interesting question: how many different infinities are there? The answer is infinitely-many (actually, uncountably-many!) This discussion is quite heavy, but there is a way to always get a "larger infinity."

Example 7.4.10

Show that there is no bijection between $\{a, b\}$ and $\mathscr{P}(\{a, b\})$ using only functions (i.e. without appealing to simply counting.)

This is pretty obvious from a counting perspective: $\{a, b\}$ has 2 elements and its power set has $2^2 = 4$ elements. Nevertheless, let's draw a random function $f : \{a, b\} \to \mathscr{P}(\{a, b\})$



Observe that

$$a \in f(a) = \{a, b\} \qquad \text{and} \qquad b \notin f(b) = \{a\}$$

Define the set

$$T = \big\{x \in \{a, b\} \ : \ x \notin f(x)\big\},$$

which in our particular case is $T = \{b\}$. By construction, T is a subset of $\{a, b\}$ and is *not* in the range of f. You can try playing around with different functions, and every time you'll find that T is not in the range of f. It's precisely this way that one proves the above theorem.

Theorem 7.4.11

For every set X, there is no bijection between X and the power set $\mathscr{P}(X)$.

Proof of Theorem 7.4.11. Let X be a set and $\mathscr{P}(X)$ its power set. Let $f : X \to \mathscr{P}(X)$ be any function, and define the (possibly empty) set:

$$T = \big\{x \in X \ : \ x \notin f(x)\big\}.$$

Tending toward a contradiction, assume that f is bijective. In particular, f is surjective, so there is some $y \in X$ for which $f(y) = T$.

- If $y \in T$, then since $f(y) = T$ it must be that $y \in f(y)$. But by definition of T, $y \notin f(y)$. Contradiction.
- If $y \notin T$, then since $f(y) = T$, it must be that $y \notin f(y)$. But by definition of T, $y \in T$. Contradiction.

Therefore f cannot be a surjective map, hence there cannot be any bijection $f : X \to \mathscr{P}(X)$. □

Since there is an obvious injection from X to $\mathscr{P}(X)$

$$f(x) = \{x\}$$

this means that the cardinality of $\mathscr{P}(X)$ must be strictly larger than the cardinality of X.

By repeatedly applying this result, one can find an infinite sequence of infinite sets with larger and larger cardinalities

$$\mathbb{N},\ \mathscr{P}(\mathbb{N}),\ \mathscr{P}(\mathscr{P}(\mathbb{N})),\ \mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{N}))),\ \ldots$$

To simplify symbols, the cardinalities of the above sets are usually defined using the symbols

$$\aleph_0,\ 2^{\aleph_0},\ 2^{2^{\aleph_0}},\ 2^{2^{2^{\aleph_0}}},\ldots$$

which matches how we think about the size of the power set in the finite case.

Corollary 7.4.12

$\mathscr{P}(\mathbb{N})$ is uncountable.

Exercise 7.4.13

Find a bijection $f : \mathbb{R} \to \mathscr{P}(\mathbb{N})$.

Exercise 7.4.14

Let X be any set and f, g both one-to-one functions for which

$$\mathbb{N} \xrightarrow{f} X \xrightarrow{g} \mathscr{P}(\mathbb{N}).$$

Show that one of f or g must be an onto function.

7.4.2 New Bijections from Old

Recall that Theorem 7.3.4 allows us to compose bijections and retain a bijection - this is extremely convenient because it allows us to come up with more "obvious" bijections and compose them.

Example 7.4.15

Let $E = \left\{e^k \ : \ k \in \mathbb{Z}\right\}$. Find a bijection $E \to \mathbb{N}$.

Let $f : \mathbb{N} \to \mathbb{Z}$ be the bijection from Example 7.4.6. We consider a composition of bijections:

$$\delta : E \xrightarrow{\ln} \mathbb{Z} \xrightarrow{f^{-1}} \mathbb{N}$$

where

$$\delta(x) = f^{-1}(\ln(x)).$$

Since f^{-1} is a bijection, we just need to prove that ln is a bijection.

Proof. **ln is one-to-one.** This fact easily follows from calculus - $ln(x)$ is strictly increasing on $(0, \infty)$. But to see it with out current methods, let that e^{k_1}, e^{k_2} be arbitrary elements of E and suppose that $\ln(e^{k_1}) = \ln(e^{k_2})$. Then $k_1 = k_2$, whence $e^{k_1} = e^{k_2}$.

ln is onto. Let $k \in \mathbb{Z}$ be arbitrary. Choosing $e^k \in E$, one see that $\ln(e^k) = k$.

□

Explicitly, the bijection δ is given by

$$\begin{aligned}\delta(x) &= f^{-1}(\ln(x)) \\ &= \begin{cases} 2\ln(x) & \text{when } \ln(x) \geq 0 \\ -2\ln(x) - 1 & \text{when } \ln(x) < 0 \end{cases} \\ &= \begin{cases} 2\ln(x) & \text{when } x \geq 1 \\ -2\ln(x) - 1 & \text{when } x < 1 \end{cases}\end{aligned}$$

Proposition 7.4.16: Cartesian product of bijections

If $f_1 : A \to B$ and $f_2 : C \to D$ are bijections, then

$$\begin{aligned}\tilde{f} :& A \times C \to B \times D \\ \tilde{f}(x, y) &= \big(f_1(x), f_2(y)\big)\end{aligned}$$

Is also a bijection.

Proof. Let A, B, C, D, f_1, f_2, and $\tilde{f}$ be as in the proposition.

One-to-one. Let $(a_1, c_1), (a_2, c_2) \in A \times C$ and suppose that $\tilde{f}(a_1, c_1) = \tilde{f}(a_2, c_2)$, i.e., suppose that

$$\big(f_1(a_1), f_2(c_1)\big) = \big(f_1(a_2), f_2(c_2)\big)$$

which, by definition of the Cartesian product, yields

$$\begin{cases} f_1(a_1) = f_1(a_2) \\ f_2(c_1) = f_2(c_2) \end{cases}$$

and since f_1 and f_2 are bijections (in particular, are one-to-one), it follows that

$$a_1 = a_2 \qquad \text{and} \qquad c_1 = c_2.$$

Therefore $(a_1, c_1) = (a_2, c_2)$.

Onto. Let $(b, d) \in B \times D$. Since f_1 and f_2 are bijections (and in particular, are onto), then there must be some $a \in A$ and $c \in C$ so that

$$f_1(a) = b \qquad \text{and} \qquad f_2(c) = d$$

and therefore, there is a pair $(a, c) \in A \times C$ for which

$$\tilde{f}(a, c) = \big(f_1(a), f_2(c)\big) = (b, d).$$

□

Example 7.4.17

Find a bijection $\mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$.

From previous examples, we know two useful bijections already:

$$\alpha : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad \beta : \mathbb{Z} \to \mathbb{N}$$

$$\alpha(x,y) = \frac{(x+y)(x+y+1)}{2} + y \qquad \beta(x) = \begin{cases} 2x & \text{when } x \geq 0, \\ -2x-1 & \text{when } x < 0 \end{cases}$$

With this in mind, we can make $\tilde{\beta}$ as in Proposition 7.4.16, and compose it with α (which will again be a bijection by Corollary 7.3.5.

$$\gamma : \mathbb{Z} \times \mathbb{Z} \xrightarrow{\tilde{\beta}} \mathbb{N} \times \mathbb{N} \xrightarrow{\alpha} \mathbb{N}$$

Explicitly, the bijection γ is given by

$$\begin{aligned} \gamma(x) &= \alpha(\tilde{\beta}(x,y)) \\ &= \alpha(\beta(x), \beta(y)) \\ &= \frac{(\beta(x)+\beta(y))(\beta(x)+\beta(y)+1)}{2} + \beta(y) \\ &= \begin{cases} \dfrac{(2x+2y)(2x+2y+1)}{2} + 2y & x \geq 0 \wedge y \geq 0 \\ \dfrac{(2x-2y-1)(2x-2y)}{2} - 2y - 1 & x \geq 0 \wedge y < 0 \\ \dfrac{(-2x-1+2y)(-2x+2y)}{2} + 2y & x < 0 \wedge y \geq 0 \\ \dfrac{(-2x-2y-2)(-2x-2y-1)}{2} - 2y - 1 & x < 0 \wedge y < 0 \end{cases} \end{aligned}$$

Example 7.4.18

Use induction to prove that, for every n, the n-fold Cartesian product of $\mathbb{N}$, i.e.

$$\prod_{j=1}^{n} \mathbb{N} = \underbrace{\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{n \text{ times}} = \{(n_1, n_2, \ldots, n_k) \ : \ \text{each } n_i \in \mathbb{N}\}$$

is countable.

Hint:

$$\underbrace{\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{k \text{ times}} = \mathbb{N} \times \left(\underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{k-1 \text{ times}} \right)$$

INCOMPLETE. Although frankly, I'm not even sure we'll actually do this in class. Maybe move it to be an "exercise" in a future semester?.

Example 7.4.19

Prove that the infinite Cartesian product of $\mathbb{N}$, i.e.

$$\prod_{j=1}^{\infty} \mathbb{N} = \mathbb{N} \times \mathbb{N} \times \mathbb{N} \cdots = \{(n_1, n_2, n_3, \ldots) \ : \ \text{each } n_i \in \mathbb{N}\}$$

is uncountable.

HINT: Consider a diagonal argument, like in the proof of Theorem 7.4.9. INCOMPLETE. Although frankly, I'm not even sure we'll actually do this in class. Maybe move it to be an "exercise" in a future semester?.

Exercise 7.4.20: "weaving" pairs of real numbers

Let x, y be real numbers in (0,1). Write out x, y in terms of their decimal digits, which we'll denote with x_i's and y_j's:

$$x = 0.x_1x_2x_3x_4x_5\ldots$$
$$y = 0.y_1y_2y_3y_4y_5\ldots$$

Show that the function

$$w : (0,1) \times (0,1) \to (0,1)$$
$$w(x,y) = 0.x_1y_1x_2y_2x_3y_3x_4y_4x_5y_5\ldots$$

is a bijection.

Example 7.4.21

Find a bijection $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

In Example 7.4.4, we constructed a function $f : (0,1) \to \mathbb{R}$, and its inverse was given by

$$f^{-1}(x) = \frac{1}{\pi}\arctan(x) + \frac{1}{2}$$

Combining this with the "weaving" bijection w from Exercise 7.4.20 and the Cartesian product bijection $\tilde{f}$ one gets from Proposition 7.4.16, the following composition is a bijection:

$$\mathbb{R} \times \mathbb{R} \xrightarrow{\tilde{f}^{-1}} (0,1) \times (0,1) \xrightarrow{w} (0,1) \xrightarrow{f} \mathbb{R}$$

Example 7.4.22

Find a bijection $\mathbb{Z} \cup E \to \mathbb{Z}$ where $E = \left\{e^k \ : \ k \in \mathbb{Z}\right\}$ as in Example 7.4.15.

We remark that $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ (where, for lack of a better notation, $-\mathbb{N}$ denotes the set of nonpositive integers $\{\ldots, -2, -1, 0\}$). We already have bijections $f^{-1} : \mathbb{Z} \to \mathbb{N}$ (from

Example 7.4.6) and $\delta : E \to \mathbb{N}$ (from Example 7.4.15), so we naively try

$$\begin{aligned} \beta :& \mathbb{Z} \cup E \to \mathbb{N} \cup (-\mathbb{N}) \\ \beta(x) =& \begin{cases} f^{-1}(x) & \text{when } x \in \mathbb{Z} \\ -\delta(x) & \text{when } x \in E \end{cases} \end{aligned}$$

We note that $E \cap \mathbb{Z} = \{1\}$ and $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$, so there should be some concern that this function is not well-defined, or isn't one-to-one. We observe the following

$$\begin{aligned} f^{-1}(\mathbb{Z}) &= \{0, 1, 2, \ldots\} & f^{-1}(1) &= 2 \\ -\delta(E) &= \{\ldots, -2, -1, 0\} & \delta(1) &= 0 \end{aligned}$$

By simply removing the intersection $\{1\}$ from both E and Z, we eliminate the overlap at 0, and we can then define $\beta(1) = 2$ to plug the hole at 2.

$$\begin{aligned} \beta :& \mathbb{Z} \cup E \to \mathbb{Z} \\ \beta(x) =& \begin{cases} f^{-1}(x) & \text{when } x \in \mathbb{Z} - E \\ -\delta(x) & \text{when } x \in E - \mathbb{Z} \\ 2 & \text{when } x \in E \cap \mathbb{Z} \end{cases} . \end{aligned}$$

Explicitly, our function is doing this:

$$\begin{aligned} \beta(\mathbb{Z} - E) &= \{0, 1, 3, 4, 5, \ldots\} \\ \beta(E - \mathbb{Z}) &= \{\ldots, -3, -2, -1\} \\ \beta(E \cap \mathbb{Z}) &= \{2\} \end{aligned}$$

Now we prove that β is a bijection.

Proof. Let β, δ, f be as described above.

β is one-to-one. Let $x_1, x_2 \in \mathbb{Z} \cup E$. We approach by cases.

- **Case 1.** [$x_1, x_2 \in \mathbb{Z} - E$] Left as an exercise.
- **Case 2.** [$x_1, x_2 \in E - \mathbb{Z}$] Left as an exercise.
- **Case 3.** [$x_1, x_2 \in \mathbb{Z} \cap E$] Left as an exercise.
- **Case 4.** [$x_1 \in \mathbb{Z} - E$ **and** $x_2 \in E - \mathbb{Z}$] Left as an exercise.
- **Case 5.** [$x_1 \in \mathbb{Z} - E$ **and** $x_2 \in \mathbb{Z} \cap E$] Left as an exercise.
- **Case 6.** [$x_1 \in E - \mathbb{Z}$ **and** $x_2 \in \mathbb{Z} \cap E$] Left as an exercise.

β is onto. Let $y \in \mathbb{Z}$ be an integer. We approach by cases.

- **Case 1.** Suppose that $y \in \{0, 1, 3, 4, 5, \ldots\}$
  - **Subcase 1.** Suppose that y is even. Left as an exercise.
  - **Subcase 2.** Suppose that y is odd. Left as an exercise.
- **Case 2.** Suppose that $y \in \{\ldots, -3, -2, -1\}$. Left as an exercise.
- **Case 3.** Suppose that $y = 2$. Left as an exercise.

Therefore, β is a bijection. □

Theorem 7.4.23

Let A, B be countable. Then $A \cup B$ is countable.

In order to prove this, we first need the following lemma.

Lemma 7.4.24

If A is countable and $B \subseteq A$, then B is either finite or countable.

Proof. If B is finite, then we're done. So, suppose B is infinite and let $f : A \to \mathbb{N}$ be a bijection (in particular an injection). Since $B \subseteq A$, there is the natural inclusion map $\iota : B \to A$ (where $\iota(b) = b$). This map is clearly injective, so the composition of functions

$$f \circ \iota : B \to \mathbb{N}$$

is also injective (by Theorem 7.3.4). Therefore

$$|B| \leq |\mathbb{N}|.$$

□

Proof of Theorem 7.4.23. Consider the sets $A - B$ and B, which are disjoint. Since B is countable, there is a bijection $\beta : B \to \mathbb{N}$. Since A is countable and $A - B$ is a subset of A, then $A - B$ is either finite or countable.

Case 1 ($A - B$ is finite). Suppose that $A - B$ is finite. Then there is a bijection $\alpha : A - B \to \{0, \ldots, n\}$ for some $n \in \mathbb{N}$. We thus define

$$\gamma : A \cup B \to \mathbb{N} \gamma(x) = \begin{cases} \alpha(x) & \text{when } x \in A - B \\ n + 1 + \beta(x) & \text{when } x \in B \end{cases}$$

Left as an exercise - prove that γ is a bijection.

Case 1 ($A - B$ is countable). Suppose that $A - B$ is countable. Then there is a bijection $\alpha : A - B \to \mathbb{N}$. So we define

$$\gamma : A \cup B \to \mathbb{Z} \gamma(x) = \begin{cases} \alpha(x) & \text{when } x \in A - B \\ -\beta(x) - 1 & \text{when } x \in B \end{cases}$$

Left as an exercise - prove that γ is a bijection.

Since both $\mathbb{N}$ and $\mathbb{Z}$ are countable, so is $A \cup B$. □

Chapter 8

Properties of Relations

8.1 Relations on Sets

Definition: binary relation

A **(binary) relation** $\mathcal{R}$ from a set A to a set B is a subset $\mathcal{R} \subseteq A \times B$. We write $a\mathcal{R}b$ if and only if $(a, b) \in \mathcal{R}$. If $\mathcal{R}$ is a relation from a set A to the same set A, we simply say that $\mathcal{R}$ is a **deffy on A**.

One can think of a relation on a set as a generalization of a function $f : A \to A$, but what we'll see is that a relation (with certain properties) more appropriately provides a way of comparing elements of a set, and gives rise to generalizations of equality and greater-than/less-than on sets.

Example 8.1.1

Let $A = \{1, 2, 3, 4\}$ and let $\mathcal{R}$ be the relation defined by

$$a\mathcal{R}b \iff a - b \text{ is even.}$$

Write down $\mathcal{R}$.

$$\mathcal{R} = \big\{(1,1),\ (1,3),\ (2,2),\ (2,4),\ (3,1),\ (3,3),\ (4,2),\ (4,4)\big\}.$$

Example 8.1.2

Let $\mathcal{R}$ be the relation defined on $\mathbb{Z}$:

$$xRy \iff x - y \text{ is even.}$$

Describe $\mathcal{R}$.

Since the difference of two even numbers is again even, and the difference of two odd numbers is even, then

$$\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \ :\ x \text{ and } y \text{ have the same parity}\}.$$

Example 8.1.3

Let $A = \{1, 2, 3, 4\}$ and let $\mathcal{R}$ be the relation defined by

$$a\mathcal{R}b \iff a|b.$$

Write down $\mathcal{R}$.

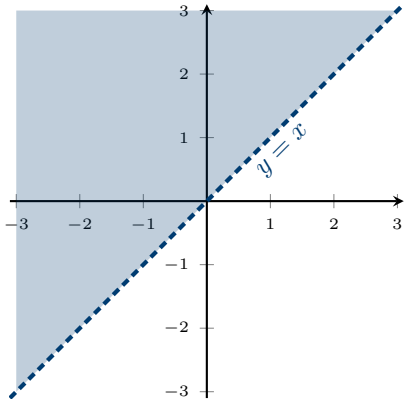
$$\mathcal{R} = \big\{(1,1),\ (1,2),\ (1,3),\ (1,4),\ (2,2),\ (2,4),\ (3,3),\ (4,4)\big\}.$$

Example 8.1.4

Let $\mathcal{R}$ be the relation defined on $\mathbb{R}$:

$$xRy \iff x < y$$

Describe $\mathcal{R}$ by plotting the pairs (x, y) in the plane.



8.1.1 Arrow Diagrams/Directed Graphs

One can visually represent relations on sets by drawing a point for every element in the set, and an arrow from a to b if and only if $a\mathcal{R}b$. This is a special type of arrow diagram that more commonly is referred to as a **directed graph** (or **digraph** for short).

Example 8.1.5

Let A and $\mathcal{R}$ be as in Example 8.1.1, that is,

$$A = \{1, 2, 3, 4\} \quad \text{and} \quad a\mathcal{R}b \iff a - b \text{ is even.}$$

Draw the arrow diagram from this relation.

2

3 1

4

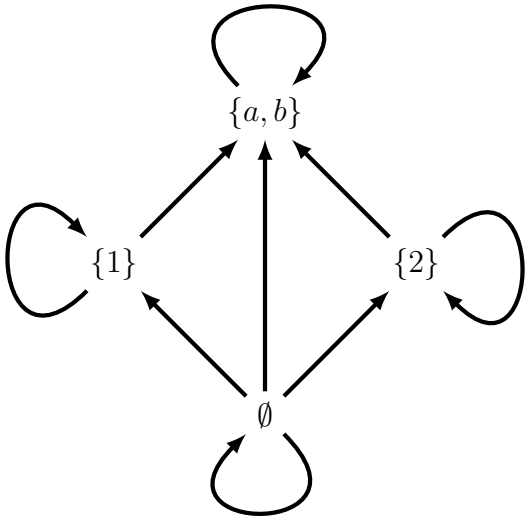
INCOMPLETE

Example 8.1.6

Let $\mathcal{R}$ be a relation on the set $\mathscr{P}(\{1,2\})$ be given by

$$X\mathcal{R}Y \iff X \subseteq Y$$

Draw the directed graph for this relation.



Instructor Note: still tidying up below.

Example 8.1.7

Let $\mathcal{R}$ be the relation defined on $\mathscr{P}(\{a,b\})$:

$$X\mathcal{R}Y \iff \#X \geq \#Y,$$

where $\#X$ represents the cardinality of X. Write down all related subsets of $\{a,b\}$.

- $\{a,b\}\mathcal{R}\emptyset$
- $\{a,b\}\mathcal{R}\{a\}$
- $\{a,b\}\mathcal{R}\{b\}$
- $\{a,b\}\mathcal{R}\{a,b\}$
- $\{a\}\mathcal{R}\emptyset$
- $\{a\}\mathcal{R}\{a\}$
- $\{a\}\mathcal{R}\{b\}$
- $\{b\}\mathcal{R}\emptyset$
- $\{b\}\mathcal{R}\{a\}$
- $\{b\}\mathcal{R}\{b\}$
- $\emptyset\mathcal{R}\emptyset$

8.1.2 Inverse Relations

Definition: inverse relation

Given a relation $\mathcal{R}$ from A to B, the **inverse relation**, denoted $\mathcal{R}^{-1}$ is a relation from B to A defined as follows:

$$b\mathcal{R}^{-1}a \iff a\mathcal{R}b.$$

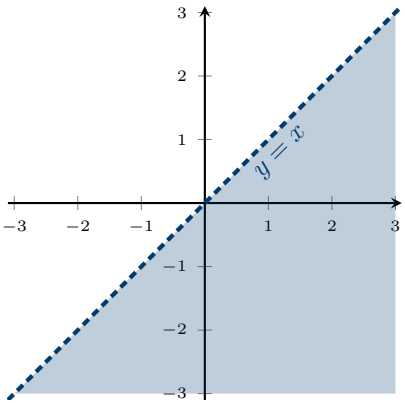
Example 8.1.8

Let $\mathcal{R}$ be the relation from Example 8.1.4:

$$xRy \iff x < y$$

Find the inverse relation $\mathcal{R}^{-1}$.

$\mathcal{R}$ consisted of all ordered pairs (a, b) where $a < b$. So $\mathcal{R}^{-1}$ consists of all ordered pairs (x, y) with $x > y$. In other words,



Example 8.1.9

Let $\mathcal{R}$ be the relation from Example 8.1.2:

$$xRy \iff x - y \text{ is even.}$$

Find the inverse relation $\mathcal{R}^{-1}$.

Notice that, for any integers x, y, $x - y$ is even if and only if $y - x$ is even. That means that, whenever $x\mathcal{R}y$, then also $y\mathcal{R}x$, hence $x\mathcal{R}^{-1}y$. It follows that $\mathcal{R} = \mathcal{R}^{-1}$.

Example 8.1.10

Let $\mathcal{R}$ be the relation from Example 8.1.7:

$$X\mathcal{R}Y \iff X \subseteq Y$$

Find the inverse relation $\mathcal{R}^{-1}$.

- $\emptyset \mathcal{R} \{a, b\}$
- $\{a\} \mathcal{R} \{a, b\}$
- $\{b\} \mathcal{R} \{a, b\}$
- $\{a, b\} \mathcal{R} \{a, b\}$
- $\emptyset \mathcal{R} \{a\}$
- $\{a\} \mathcal{R} \{a\}$
- $\emptyset \mathcal{R} \{b\}$
- $\{b\} \mathcal{R} \{b\}$
- $\emptyset \mathcal{R} \emptyset$

8.2 Reflexivity, Symmetry, and Transitivity

Definition: (anti)reflexive, (anti)symmetric, transitive

Let $\mathcal{R}$ be a relation on a set A. We say that $\mathcal{R}$ is...

- ...**reflexive** if it has the following property:

$$\text{for all } a \in A,\ a\mathcal{R}a.$$

- ...**anti-reflexive** if it has the following property:

$$\text{for all } a, b \in A, \text{ if } a\mathcal{R}b, \text{ then } a \neq b.$$

- ...**symmetric** if it has the following property:

$$\text{for all } a, b \in A, \text{ if } a\mathcal{R}b \text{ then } b\mathcal{R}a.$$

- ...**anti-symmetric** if it has the following property:

$$\text{for all } a, b \in A, \text{ if } a\mathcal{R}b \text{ and } b\mathcal{R}a, \text{ then } a = b.$$

- ... **transitive** if it has the following property:

$$\text{for all } a, b, c \in A, \text{ if } a\mathcal{R}b \text{ and } b\mathcal{R}c, \text{ then } a\mathcal{R}c.$$

Example 8.2.1

Let $\mathcal{R}$ be the relation from Example 8.1.4:

$$\text{For all } x, y \in \mathbb{R},\ xRy \iff x < y.$$

Which of the above properties does it have?

Anti-reflexive, Transitive

Example 8.2.2

Let $\mathcal{R}$ be the relation from Example 8.1.2;

$$\text{For all } x, y \in \mathbb{Z},\ xRy \iff x - y \text{ is even.}$$

Which of the above properties does it have?

Refleexive, Transitive, Symmetric

Example 8.2.3

Let $\mathcal{R}$ be the relation from Example 8.1.7:

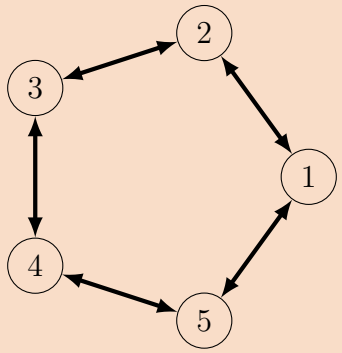
$$\text{For all } X, Y \in \mathcal{P}(\{1,2\}),\ X\mathcal{R}Y \iff X \subseteq Y.$$

Which of the above properties does it have?

Reflexive, antisymmetric, Transitive

Example 8.2.4

Let $\mathcal{R}$ be a relation on $A = \{1,2,3,4,5\}$ be given by the directed graph below.



Which of the properties does the above relation have?

Symmetric

Exercise 8.2.5

Let $A = \{1,2,3,4,5\}$. Draw directed graphs representing relations $\mathcal{R}$ on A which have the following properties:

1. $\mathcal{R}$ is not reflexive, not neither symmetric, and not transitive.
2. $\mathcal{R}$ is reflexive, but neither symmetric nor transitive.
3. $\mathcal{R}$ is transitive, but neither reflexive nor symmetric.
4. $\mathcal{R}$ is reflexive and symmetric, but not transitive.
5. $\mathcal{R}$ is reflexive and transitive, but not symmetric.
6. $\mathcal{R}$ is symmetric and transitive, but not reflexive.
7. $\mathcal{R}$ is reflexive, symmetric, and transitive.

8.2.1 Proving and disproving properties of binary relations

Example 8.2.6

Let $n > 0$ be an integer. Define a relation $\mathcal{R}$ on $\mathbb{Z}$ as follows:

$$x \mathcal{R} y \iff n|(x-y).$$

Prove that $\mathcal{R}$ is reflexive, symmetric, and transitive.

Proof. Let $n > 0$ and let $x, y, z \in \mathbb{Z}$ be arbitrary.

Reflexive. Since $x - x = 0$ and $n|0$, then $x \mathcal{R} x$ for every $x \in \mathbb{Z}$.

Symmetric. Suppose $x \mathcal{R} y$. Then $n|(x-y)$, that is, there is some $k \in \mathbb{Z}$ for which $x - y = nk$. It follows that

$$y - x = -(x-y) = -nk = n(-k)$$

and thus $n|(y-x)$ as well. Therefore $y \mathcal{R} x$.

Transitive. Suppose that $x \mathcal{R} y$ and that $z \mathcal{R} y$. Then $n|(x-y)$ and $n|(y-z)$, and thus there are integers k, ℓ for which $x - y = nk$ and $y - z = n\ell$. We then have that

$$x - z = x - y + y - z = nk + n\ell = n(k + \ell)$$

whence $n|(x-z)$.

□

Example 8.2.7

Define a relation $\mathcal{R}$ on $\mathbb{Z} \times \mathbb{Z}$ as follows:

$$(a_1, b_1) \mathcal{R} (a_2, b_2) \iff \begin{cases} a_1 < a_2, \text{or} \\ a_1 = a_2 \text{ and } b_1 \leq b_2 \end{cases}$$

Prove that $\mathcal{R}$ is reflexive, antisymmetric, and transitive.

Proof. Let (a_1, b_1), (a_2, b_2), and (a_3, b_3) be arbitrary ordered pairs in $\mathbb{Z} \times \mathbb{Z}$.

Reflexive. Observe that $a_1 = a_2$ and $b_1 \leq b_1$, hence

$$(a_1, b_1) \mathcal{R} (a_1, b_1).$$

Symmetric. Suppose $(a_1, b_1) \mathcal{R} (a_2, b_2)$ and $(a_2, b_2) \mathcal{R} (a_1, b_1)$. This implies that both $a_1 \leq a_2$ and $a_2 \leq a_2$, whence $a_1 = a_2$. Since $a_1 = a_2$, then this implies both that $b_1 \leq b_2$ and $b_2 \leq b_1$, and thus $b_1 = b_2$. Therefore $(a_1, b_1) = (a_2, b_2)$.

Transitive. Suppose $(a_1, b_1) \mathcal{R} (a_2, b_2)$ and $(a_2, b_2) \mathcal{R} (a_3, b_3)$. We examine the following cases.

- **Case 1 ($a_1 < a_2$)**
  - **Subcase 1 ($a_2 < a_3$)** Left as an exercise.

  - **Subcase 2 ($a_2 = a_3$)** Left as an exercise.
- **Case 2 ($a_1 = a_2$)**
  - **Subcase 1 ($a_2 < a_3$)** Left as an exercise.
  - **Subcase 2 ($a_2 = a_3$)** Left as an exercise.

□

8.3 Equivalence Relations

Definition: equivalence relation

A relation $\mathcal{R}$ on a set A is called an **equivalence relation** if and only if it is

- reflexive,
- symmetric, and
- transitive.

Example 8.3.1: Revisiting Example 8.2.6

The relation $\mathcal{R}$ on $\mathbb{Z}$ given in Example 8.2.6 is an equivalence relation.

For each fixed positive integer n,

$$x\mathcal{R}y \iff n|(x-y).$$

Example 8.3.2: "Mod 1" (aka, S^1)

Let $\mathcal{R}$ be the following relation on $\mathbb{R}$.

$$x\mathcal{R}y \iff \exists k \in \mathbb{Z} \text{ such that } x = y + k.$$

Show that $\mathcal{R}$ is an equivalence relation.

Proof. Let $x, y, z \in \mathbb{R}$.

Reflexive. Since $x = x + 0$, then $x\mathcal{R}x$.

Symmetric. Suppose $x\mathcal{R}y$. Then there is an integer $k \in \mathbb{Z}$ so that $x = y + k$. It follows that $y = x + (-k)$, and since $-k \in \mathbb{Z}$, then $y\mathcal{R}x$.

Transitive. Suppose $x\mathcal{R}y$ and $y\mathcal{R}z$. Then there are integers k, ℓ for which $x = y + k$ and $y = z + \ell$. Hence

$$x = y + k = (z + \ell) + k = z + (\ell + k)$$

and since $\ell + k$ is an integer, $x\mathcal{R}z$, as desired.

Therefore $\mathcal{R}$ is an equivalence relation. □

Exercise 8.3.3

Let $\mathcal{R}$ be the relation on $\mathbb{R} \times \mathbb{R}$ given by

$$(x_1, y_1)\mathcal{R}(x_2, y_2) \iff (x_1, y_1) = (x_2 + k, y_2 + \ell) \text{ for some } k, \ell \in \mathbb{Z}.$$

Prove that $\mathcal{R}$ is an equivalence relation.

Example 8.3.4

Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and let $\mathscr{A} = \{A_1, A_2, A_3\}$ be the following partition of A:

$$A_1 = \{1, 3, 5, 7, 9\}$$
$$A_2 = \{2, 4, 6\}$$
$$A_3 = \{8, 10\}$$

Let $\mathcal{R}$ be the relation on A given by

$$x\mathcal{R}y \iff \exists i \text{ such that } x, y \in A_i.$$

Prove that $\mathcal{R}$ is an equivalence relation.

Theorem 8.3.5: Equivalence relation induced by a partition.

Let A be some set and let $\mathscr{A} = \{A_1, A_2, \ldots, A_n, \ldots\}$ be a (possibly-infinite) partition of A. Define a relation $\mathcal{R}$ on A by

$$x\mathcal{R}y \iff \exists i \text{ s.t. } x \in A_i \text{ and } y \in A_i.$$

Then $\mathcal{R}$ is an equivalence relation.

Proof. Let $x, y, z \in A$ be arbitrary and suppose $\mathcal{R}$ is the relation described above.

Reflexive. Let $A_i \in \mathscr{A}$ be the set containing x. Then $x \in A_i$ as well, so $x\mathcal{R}x$.

Symmetric. Suppose $x\mathcal{R}y$. Then there is some set A_i in the partition for which $x \in A_i$ and $y \in A_i$. Since logical conjunction is commutative, this implies $y \in A_i$ and $x \in A_i$. Thus $y\mathcal{R}x$.

Transitivity. Suppose $x\mathcal{R}y$ and $y\mathcal{R}z$. Then there is some set A_i in the partition for which $x, y \in A_i$, and some set A_j in the partition for which $y, z \in A_j$. Since sets in a partition are pairwise disjoint, then $y \in A_i \cap A_j \implies A_i = A_j \implies i = j$. Thus we have that $x, z \in A_i$ and so $x\mathcal{R}y$.

Therefore $\mathcal{R}$ is an equivalence relation. □

Definition

Given a set A and a partition $\{A_1, \ldots, A_n, \ldots\}$, the relation $\mathcal{R}$ on A given by

$$x\mathcal{R}y \iff x, y \in A_i$$

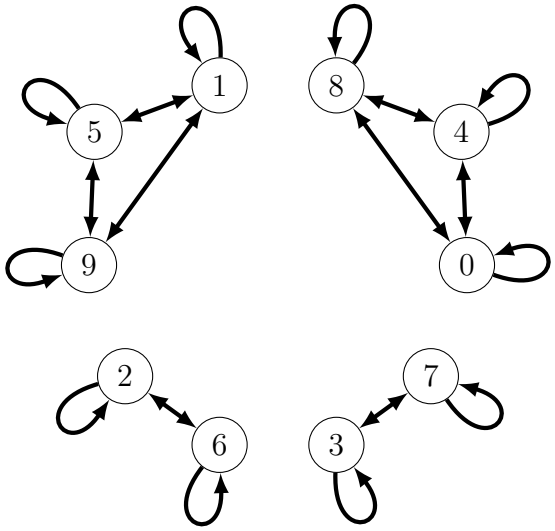
is called the **equivalence relation on A induced by a partition**.

Example 8.3.6

Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and let $\mathcal{R}$ be the equivalence relation on A given by

$$x\mathcal{R}y \iff 4|(x - y)$$

Draw the directed graph representing for this relation.



Notice that this graph is naturally clustered into four connected components. Each of these components are related by the fact that they have the same remainder after dividing by 4. This is true more generally with the relation from Example 8.2.6. In general, we can expect n different clusters

$$\begin{aligned} &x = nk \quad \text{and} && y = n\ell \\ &x = nk+1 \quad \text{and} && y = n\ell + 1 \\ &x = nk+2 \quad \text{and} && y = n\ell + 2 \\ &\vdots && \vdots \\ &x = nk+(n-1) \quad \text{and} && y = n\ell + (n-1) \end{aligned}$$

By collecting integers with the same remainder (after dividing by n), we form a partition of $\mathbb{Z}$. Letting A_j be the set

$$A_j = \{z \in \mathbb{Z} \ : \ z = nk + j \text{ for some } k \in \mathbb{Z}\},$$

we have

$$\mathbb{Z} = \bigcup_{j=0}^{n-1} A_j.$$

Clearly these sets must be pairwise disjoint (because numbers cannot have two different remainders), so $x\mathcal{R}y$ precisely when x, y are in the same set of this partition.
We know that partitions induce equivalence relations, but it also seems that the converse is true. On our way to showing this, we introduce the following term:

Definition: equivalence class

Let A be a set and $\mathcal{R}$ an equivalence relation on A. For each $a \in A$, the **(equivalence) class of a**, denoted $[a]_{\mathcal{R}}$ (or just $[a]$ when the relation is clear), is the set

$$[a]_{\mathcal{R}} = \{x \in A \ : \ x\mathcal{R}a\}.$$

The set of all distinct equivalence classes is denoted $A/\mathcal{R}$.

Remark. In the case of integers "mod n," these may also be called "congruence classes" since two numbers are said to be "congruent modulo n."

Example 8.3.7: Revisiting Example 8.3.6

Let $\mathcal{R}$ be the equivalence relation on $\mathbb{Z}$ given by

$$x\mathcal{R}y \iff 4|(x-y)$$

Find all equivalence classes, $\mathbb{Z}/\mathcal{R}$.

Looking at the diagram in Example 8.3.6, we see that equivalence classes are determined by the remainder after dividing by 4. So

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \ : \ x = 4k+0 \text{ for some } k \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
[1] &= \{x \in \mathbb{Z} \ : \ x = 4k+1 \text{ for some } k \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
[2] &= \{x \in \mathbb{Z} \ : \ x = 4k+2 \text{ for some } k \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
[3] &= \{x \in \mathbb{Z} \ : \ x = 4k+3 \text{ for some } k \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}
\end{aligned}$$

Example 8.3.8: Revisiting Example 8.3.2

Let $\mathcal{R}$ be the equivalence relation on $\mathbb{R}$ given by

$$x\mathcal{R}y \iff \exists k \in \mathbb{Z} \text{ such that } y = x + k.$$

Describe all equivalence classes.

INCOMPLETE

Exercise 8.3.9

Let $\mathcal{R}$ be the equivalence relation on $\mathbb{R} \times \mathbb{R}$ given by

$$(x_1, y_1)\mathcal{R}(x_2, y_2) \iff (x_1, y_1) = (x_2 + k, y_2 + \ell) \text{ for some } k, \ell \in \mathbb{Z}.$$

Describe all equivalence classes.

Lemma 8.3.10

Let $\mathcal{R}$ be an equivalence relation on A and let $[x], [y]$ be two equivalence classes. Then either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Proof. Let $[x], [y]$ be arbitrary equivalence classes. If $[x] \cap [y] = \emptyset$, then we're done, so suppose that $z \in [x] \cap [y]$. Then we have that $x\mathcal{R}z$ and $z\mathcal{R}y$, and thus, by transitivity, $x\mathcal{R}y$. In turn, this implies that every element of $[y]$ is related to every element of $[x]$, and vice versa. Therefore $[x] = [y]$. □

Theorem 8.3.11

Let A be some set and let $\mathcal{R}$ be an equivalence relation on A. The equivalence classes $A/\mathcal{R}$ form a partition of A.

Proof. Lemma 8.3.10 shows that the equivalence classes are disjoint, so all that's left to prove is that their union is equal to A. Since the equivalence classes are subsets of A, so is their union, so in fact we just need to show that $A \subseteq \bigcup_{[x] \in A/\mathcal{R}} [x]$. To see this, let $a \in A$. By the reflexive property of an equivalence relation, $a \mathcal{R} a$, which means that $a \in [a] \in A/\mathcal{R}$. □

.1 Proofs Skipped In Class

Definition: disjoint union

Let A_1, A_2 be sets. The **disjoint union** of A_1 and A_2 is the set

$$A_1 \sqcup A_2 := \{(a, i) \in (A_1 \cup A_2) \times \mathbb{N} \ : \ a \in A_i\}.$$

Lemma: Lemma 7.4.2

Prove that, for all finite sets A_1 and A_2,

$$|A_1 \cup A_2| \leq |A_1| + |A_2|.$$

Proof. The function

$$\begin{aligned} \varphi : A_1 \sqcup A_2 &\to A_1 \cup A_2 \\ \varphi(x, i) &= x \end{aligned}$$

is a surjection, so we get that $|A_1 \cup A_2| \leq |A_1 \sqcup A_2|$. As such, we only need to prove that

$$|A_1 \sqcup A_2| = |A_1| + |A_2|.$$

By definition of finiteness, there are natural numbers m and n and bijections α, β for which

$$\alpha : A_1 \to \{1, \ldots, m\} \qquad \text{and} \qquad \beta : A_2 \to \{1, \ldots, n\}$$

Let s_m be the "shift-by-m" bijection from **??**. It follows that

$$\begin{aligned} \gamma : &A_1 \sqcup A_2 \to \{1, \ldots, m+n\} \\ \gamma(x, i) &= \begin{cases} \alpha(x) & \text{if } i = 1 \\ s_m(\beta(x)) & \text{if } i = 2 \end{cases} \end{aligned}$$

INCOMPLETE □

Index