1 Propositional Logic

1.1 Propositions

Definition 1.1. A proposition is a declarative sentence that is either true or false, but not both. Another way to say this is that it has a truth value (T or F). A proposition must be a statement (not a question) with both a subject and verb.

Example 1.2. The following are all examples of propositions:
New Britain is a city in Connecticut.
$5 \times 3 = 15$.
$5 \times 3 < 12$.

Exercise 1.3. Find the subject and verb (could be one or multiple words) of each of the above propositions. Then determine their truth value.

Exercise 1.4. Why is “$5 \times 3$” not a proposition?

We use letters, such as $p$ and $q$, to denote propositions. These letters are called propositional variables.

Example 1.5. Let $p$ be the proposition “January 25 is a Tuesday” or “$x > 0$”. Notice that in this case, we don’t know if $p$ is true or false, but it is still a proposition since it is a statement with a subject and verb that could be true or false.

Definition 1.6. Let $p$ be a proposition. The negation of $p$, denoted by $\neg p$, is the statement “It is not the case that $p$”. The proposition $\neg p$ is read “not $p$”, and the truth value of $\neg p$ is the opposite of the truth value of $p$.

Problem 1.7. Negate the following propositions into a fluid English sentence (hint: it helps to start by placing “It is not the case that” at the beginning of each proposition):

1. “Tigers are cats”.
2. “Exactly half of the students in this 218 course are under 21.”
3. “At least half of the students in this 218 course are under 21.”
4. “There are fewer than 10 students in this 218 course who are under 21.”

Definition 1.8. Let $p$ and $q$ be propositions. The conjunction of $p$ and $q$, denoted by $p \land q$, is the proposition “$p$ and $q$”. The conjunction $p \land q$ is true only when $p$ and $q$ are BOTH true.

Definition 1.9. Let $p$ and $q$ be propositions. The disjunction of $p$ and $q$, denoted by $p \lor q$, is the proposition “$p$ or $q$”. The disjunction $p \lor q$ is true when either $p$ or $q$ is true (false only when both $p$ and $q$ are false).
Note: The disjunction “or” refers to the inclusive or, as opposed to the exclusive or. The inclusive or includes the possibility that both options may hold, as in “Cream or sugar?” The exclusive or does not include the possibility of both, as in “Fries or baked potato?”

Order of Operations

So far we have learned three symbolic logical operators: ¬, ∧, and ∨. They take precedence in this order:

1. ¬
2. ∧
3. ∨

For example, ¬p ∧ q is not equivalent to ¬(p ∧ q). The former is equivalent to (¬p) ∧ q.

Truth Tables

We use what are called truth tables to display all the possible truth values for a given proposition or propositions. Probably the most basic is that of the negation:

<table>
<thead>
<tr>
<th>p</th>
<th>¬p</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Each proposition involved in the final statement to be examined (in this case, ¬p) is given a column, and each possible combination of truth values of these propositions is given a row. In the cases of p ∧ q and p ∨ q, the truth table would begin as follows:

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>p ∧ q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Exercise 1.10. Use the table started above to create truth tables for conjunction and disjunction.

Exercise 1.11. Use your truth tables from above to determine the truth value of the following statements:

1. The sky is red or Hartford is the capital of Connecticut.
2. The sky is blue or Hartford is the capital of Connecticut.
3. President Obama is 10 feet tall and 1 + 1 = 7.
4. The sky is blue and Hartford is the capital of Connecticut.
5. Hartford is the capital of Connecticut and President Obama is 10 feet tall.
1.2 Conditional and Biconditional Statements

**Definition 1.12.** Let $p$ and $q$ be propositions. The conditional statement $p \rightarrow q$ is the proposition “if $p$, then $q$”. (The “then” is often left off.) $p$ is called the hypothesis and $q$ is called the conclusion. A conditional statement is also called an implication.

**Example 1.13.** If my alarm goes off, then I will wake up.

$p$: My alarm goes off.

$q$: I will wake up.

**Example 1.14.** If $0 < x < 1$, then $x^2 < x$.

$p$: $0 < x < 1$.

$q$: $x^2 < x$.

**Example 1.15.** I’ll be successful if I graduate.

$p$: I graduate.

$q$: I am successful.

What is the truth value of a conditional statement? We explore this in the following problem.

**Problem 1.16.** Your Uncle Ted says that he will buy you a new car if you get all A’s this semester. In which case(s) is Ted a liar?

To answer this, first deconstruct the conditional statement “He will buy you a new car if you get all A’s this semester”.

$p$: 

$q$: 

Now consider the possible truth values of each component $p$ and $q$ separately in a truth table.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \rightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

For each possible pairing of truth values from the table above, write a conjunction in words using your $p$ and $q$. Then decide which one(s), if any, represent cases where you would call Uncle Ted a liar. Lastly, use this to fill in the third column of the truth table with “T” or “F”.

**Problem 1.17.** Now use the truth table from the previous exercise to decide the truth value of the following statements:

1. If there are 365 days in the year 2011, then CCSU is in New Britain.

2. If there are 400 days in the year 2011, then a liger is a real animal.
3. For all \( x \), if \( x \) is an integer, then \( x^3 > 0 \).

4. If Homer Simpson is the President of the United States, then \( 3 = 5 \).

5. If Earth is the center of our galaxy, then \( 3^2 = 9 \).

We add the symbol \( \rightarrow \) to our order-of-operations list. Our order of precedence is now:

1. \( \neg \)
2. \( \land \)
3. \( \lor \)
4. \( \rightarrow \)

There are different ways to express conditional statements. For example, the following are ways in which the logical statement \( p \rightarrow q \) can be read:

- \( q \) if \( p \)
- \( p \) implies \( q \)
- \( p \) only if \( q \)
- \( p \) is sufficient for \( q \)
- \( q \) when \( p \)
- \( q \) whenever \( p \)
- \( q \) is necessary for \( p \)
- \( q \) follows from \( p \)
- \( q \) unless \( \neg p \)

**Problem 1.18.** Rewrite the following statements in the form “If..., then....”.

1. It’s raining whenever I carry an umbrella.
2. It is necessary for you to get a C- in MATH 218 to graduate.
3. We never have class on Friday.
4. To get a promotion, you must wash the boss’s car.
5. You can access the website only if you pay a subscription fee.

**Problem 1.19.** Let \( p, q, \) and \( r \) be the propositions:

- \( p \): You get an A on the final exam.
- \( q \): You do every problem assigned.
- \( r \): You get an A in this class.

Write the following propositions using \( p, q \) and \( r \) and logical connectives (i.e., in symbols).

1. You get an A in this class, but you do not do every problem assigned.
2. You get an A on the final, you do every problem assigned, and you get an A in this class.
3. To get an A in this class, it is necessary for you to get an A on the final.
4. You get an A on the final, but you don’t do every problem assigned; nevertheless, you get an A in this class.

5. Getting an A on the final and doing every problem assigned is sufficient for getting an A in this class.

6. You must do every problem assigned or get an A on the final to get an A in the class.

Biconditionals

**Definition 1.20.** Let \( p \) and \( q \) be propositions. The biconditional statement \( p \leftrightarrow q \) is the proposition “\( p \) if and only if \( q \)”, which is often abbreviated “\( p \) iff \( q \)”. 

\[ p \leftrightarrow q \] is equivalent to \( (p \rightarrow q) \land (q \rightarrow p) \). Notice that \( p \leftrightarrow q \) is equivalent to \( q \leftrightarrow p \).

**Problem 1.21.** Construct a truth table for the expression \( (p \rightarrow q) \land (q \rightarrow p) \) to determine the truth values of the biconditional statement \( p \leftrightarrow q \).

**Example 1.22.** You get paid if and only if you have a job.

\( p \): You get paid.
\( q \): You have a job.
\( p \rightarrow q \): If you get paid, you have a job.
\( q \rightarrow p \): If you have a job, you get paid.

**Exercise 1.23.** In the above example, what is the conclusion if you don’t get paid? What is the conclusion if you don’t have a job?

Another way to say \( p \leftrightarrow q \) is “\( p \) is necessary and sufficient for \( q \)”. We deconstruct the statement as follows:

\( p \rightarrow q \): \( p \) is sufficient for \( q \)
\( q \rightarrow p \): \( p \) is necessary for \( q \)

Note how these relate to the alternative ways to read \( p \rightarrow q \).

We now add \( \leftrightarrow \) to our order of precedence:

1. \( \neg \)
2. \( \land \)
3. \( \lor \)
4. \( \rightarrow, \leftrightarrow \)

**Problem 1.24.** Construct a truth table for the statement \( p \rightarrow q \land \neg p \leftrightarrow q \).
**Converse, Contrapositive, and Inverse**

**Definition 1.25.** Let \( s \) be the conditional statement \( p \rightarrow q \). The **converse** of \( s \) is the statement \( q \rightarrow p \), the **contrapositive** of \( s \) is the statement \( \neg q \rightarrow \neg p \), and the **inverse** of \( s \) is the statement \( \neg p \rightarrow \neg q \).

**Example 1.26.** Let \( s \) be the statement “If Roger drinks coffee, Roger will be alert.”

We see that \( p \) is the statement “Roger drinks coffee” and \( q \) is the statement “Roger will be alert” (or “Roger is alert”).

**Problem 1.27.**

1. Write the converse, contrapositive, and inverse of the statement in Example 1.26, first in symbols and then in words. You may change the tenses of the statement to make it make sense.

2. Decide from your statements in question (1) which, if any of the converse, contrapositive, and inverse follow from the original. In other words, if the original statement is true, are any of the others also necessarily true and if so, which one(s)?

3. Corroborate your answer from (2) with a truth table.

**Problem 1.28.** Consider the following statement: “Another debt-ceiling debate in 2012 will spell the loss of the next presidential election for the Republicans.”

Suppose your friend has made this statement while in a political debate with you. Which of the following statements (if any) represent conclusions that can also be drawn from your friend’s statement? Be sure to explain your reasoning for each one, using the terminology from Definition 1.25. (Hint: write the above statement as a conditional statement, denoting \( p \) and \( q \).)

1. “The next presidential election will go to the Republicans if Boehner puts the kaibosh on a second debt-ceiling debate.”

2. “There will surely have been another debt-ceiling debate if Obama wins the next election.”

3. “If Obama loses the next election then the government will not have debated raising the debt ceiling again.”

4. Having no more debt-ceiling debates is necessary for the Republicans to win the next presidential election.

**Definition 1.29.** A **compound proposition** is one that is formed from propositional variables and logical operators (e.g. \( p \land q, p \lor q \), etc.).

**Definition 1.30.** Two compound propositions are **logically equivalent** if they have all the same truth values for corresponding sets of truth values of the propositions that occur in them. The notation \( p \equiv q \) denotes that \( p \) and \( q \) are logically equivalent.

**Example 1.31.** We see by the fifth and seventh columns of the following truth table that the statements \((p \land q) \rightarrow r\) and \(p \land (q \rightarrow r)\) are NOT logically equivalent (i.e. the order of parentheses matters) and write \((p \land q) \rightarrow r \neq p \land (q \rightarrow r)\):
<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$p \land q$</th>
<th>$(p \land q) \rightarrow r$</th>
<th>$q \rightarrow r$</th>
<th>$p \land (q \rightarrow r)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
</tbody>
</table>

**Definition 1.32.** A compound proposition that is always true, no matter what the truth values of the propositions that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. A compound proposition that is neither a tautology nor a contradiction is called a contingency.

**Exercise 1.33.** Two compound propositions $p$ and $q$ are also defined to be logically equivalent if the statement $p \leftrightarrow q$ is a tautology. Why does this match the definition given above for “logically equivalent”?

**Exercise 1.34.** Consider the conditional statement $p \rightarrow q$. Of the four statements: $p \rightarrow q$, its converse, its contrapositive, and its inverse, which are logically equivalent?

**Exercise 1.35.** How does a biconditional statement relate to this discussion?

**Problem 1.36.** Using at least two propositional variables for each one, find examples of a tautology and a contradiction, and verify with truth tables for each one.

### 1.3 Propositional Equivalences

The following are some established logical equivalences, where “$T$” represents a statement that is true and “$F$” represents a statement that is false:

#### Identity Laws
$p \land T \equiv p$
$p \lor F \equiv p$

#### Domination laws
$p \lor T \equiv T$
$p \land F \equiv F$

#### Idempotent Laws
$p \lor p \equiv p$
$p \land p \equiv p$

#### Double Negation Law
$\neg(\neg p) \equiv p$

#### Commutative Laws
$p \lor q \equiv q \lor p$
$p \land q \equiv q \land p$

#### Associative Laws
$(p \lor q) \lor r \equiv p \lor (q \lor r)$
$(p \land q) \land r \equiv p \land (q \land r)$

#### Distributive Laws
$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$
$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$

#### De Morgan’s Laws
$\neg(p \land q) \equiv \neg p \lor \neg q$
$\neg(p \lor q) \equiv \neg p \land \neg q$

#### Absorption Laws
$p \lor (p \land q) \equiv p$
$p \land (p \lor q) \equiv p$

#### Negation Laws
$p \lor \neg p \equiv T$
$p \land \neg p \equiv F$
All of the above can be proved using truth tables, i.e. where it is shown that each side of an equivalence has the same truth values for corresponding truth values of \( p \) and \( q \).

**Problem 1.37.** Use the distributive and commutative laws from above (NOT a truth table) to prove the following “alternate” versions of the distributive laws:
\[
(q \land r) \lor p \equiv (q \lor p) \land (r \lor p) \\
(q \lor r) \land p \equiv (q \land p) \lor (r \land p)
\]

**Example 1.38.** Let \( p \) and \( q \) be the following propositions:
\[p: \text{I get a sandwich.}\]
\[q: \text{I get soup.}\]
\[r: \text{I get dessert.}\]

We demonstrate some of the above laws using these propositions.

Absorption law 1: I get a sandwich or I get both a sandwich and soup \( \equiv \) I get a sandwich.
Observe that if I get a sandwich, both sides are true and if I don’t get a sandwich, both sides are false (so whether or not I get soup does not affect the equivalence here).

Distributive law 1: I get a sandwich or I get both soup and dessert \( \equiv \) I get a sandwich or soup and I get a sandwich or dessert.
Observations: I get a sandwich makes both sides true. I get both soup and dessert also makes both sides true. Otherwise (i.e. for all other combinations of truth values), both sides are false.

**Exercise 1.39.** Translate DeMorgan’s laws into sentences using \( p \) and \( q \) from Example 1.38.

**Exercise 1.40.** Show using a truth table that absorption law 2 holds.

**Exercise 1.41.** Show using a truth table that De Morgan’s law 2 holds.

**Exercise 1.42.** Show using a truth table that \( p \rightarrow q \equiv \neg p \lor q \).

**Problem 1.43.** Show using a truth table that \( (p \rightarrow r) \land (q \rightarrow r) \equiv p \lor q \rightarrow r \).
Example 1.44. Show using a chain of equivalences that \((p \rightarrow r) \land (q \rightarrow r) \equiv p \lor q \rightarrow r\).

We start by picking one side and making it look like the other through a series of equivalences. Note that we are using the result of Exercise (1.43), which we are calling \((\ast)\).

\[ p \lor q \rightarrow r \equiv \neg (p \lor q) \lor r \text{ by } (\ast) \]
\[ \equiv (\neg p \land \neg q) \lor r \text{ by DeMorgan’s law 2} \]
\[ \equiv (\neg p \lor r) \land (\neg q \lor r) \text{ by distributive law 1} \]
\[ \equiv (p \rightarrow r) \land (q \rightarrow r) \text{ by } (\ast) \]

OR

\[ (p \rightarrow r) \land (q \rightarrow r) \equiv (\neg p \lor r) \land (\neg q \lor r) \text{ by } (\ast) \]
\[ \equiv (\neg p \land \neg q) \lor r \text{ by dist. law 1} \]
\[ \equiv \neg (p \lor q) \lor r \text{ by DeMorgan’s law 2} \]
\[ \equiv p \lor q \rightarrow r \text{ by } (\ast) \]

Problem 1.45. Show using a chain of logical equivalences that \(p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)\). Be sure to justify each step using one of the established laws or \((\ast)\). (Hint: remind yourself what \(p \leftrightarrow q\) is equivalent to from when it was defined.)

Problem 1.46. Show using a chain of logical equivalences that \(\neg p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \lor r)\). Be sure to justify each step using one of the established laws or \((\ast)\).

1.4 Predicates and Quantifiers

Definition 1.47. A propositional function \(P(x)\) is a statement that is a proposition when a value is assigned to the variable \(x\). A propositional function consists of a subject \(x\) and a predicate, which describes a property relating to \(x\).

Example 1.48. Let \(P(x)\) be the statement “\(x < 2\)”. \(P\) has no truth value until an \(x\) is chosen. The predicate is “is greater than 2”. \(P(1)\) has truth value True whereas \(P(2)\) has truth value False.

A propositional function may contain more than one variable.

Example 1.49. Let \(P(x, y)\) be the statement “\(x\) is taller than \(y\)”. \(P(\text{Dr. Schwell, Dr. Schwell’s mom})\) has truth value True whereas \(P(\text{Dr. Schwell, Michael Jordan})\) has truth value False.

Exercise 1.50. Write your own statement \(P(x, y)\) and define domains for your variables. Make sure it is a statement that has at least one set of values \(x, y\) that make it true and at least one set that makes it false.

Observe: a propositional function may even have more than two variables, and could be of the form \(P(x_1, x_2, \ldots, x_n)\).
Quantifiers

**Definition 1.51.** The domain of discourse or just the domain of a propositional function is the set of values which are possible values for \( x \). A multi-valued propositional function (e.g. \( P(x, y) \)) may have different domains for each variable.

**Example 1.52.** Let \( P(x, y) \) be the statement “\( x \) has completed at least \( y \) credits at CCSU”.

We choose domains for the two variables:
Domain for \( x \): \{Students enrolled at CCSU\}
Domain for \( y \): \( \mathbb{N} \) (the natural numbers \{0, 1, 2, \ldots \})

Note we could have chosen differently, for example the domain for \( x \) could simply be \{people\} and the domain for \( y \) could be \( \mathbb{R} \).

**Definition 1.53.** The universal quantification of a propositional function \( P(x) \) is “\( P(x) \) for all values of \( x \) in the domain.”
Notation: \( \forall x P(x) \), where \( \forall \) is called the universal quantifier. Read as “for all \( x \) \( P(x) \)” or “for every \( x \) \( P(x) \)”. An element \( x \) for which \( P(x) \) is false is called a counterexample of \( \forall x P(x) \).

Other ways to say \( \forall \):
All of...
For each....
Given any.....
For any....
For arbitrary....

IMPORTANT: The universal quantification depends on the domain!!

**Example 1.54.** Let \( P(x) \) be the statement \( x \geq 0 \). If the domain is \( \mathbb{N} \), \( \forall x P(x) \) is true; if the domain is \( \mathbb{R} \) or \( \mathbb{Z} \) (the integers), \( \forall x P(x) \) is false.

**Example 1.55.** Let \( P(x) \) be the statement “\( x \) attends CCSU”. If the domain of \( x \) is \{students in this class\}, the statement \( \forall x P(x) \) is true. However, if the domain is \{New Britain residents\}, the statement \( \forall x P(x) \) is false (because a counterexample exists).

**Problem 1.56.** Let \( P(x) \) be the statement “If \( x > 0 \) then \( x^2 \geq 1 \)”.

1. What is the truth value of the statement \( \forall x P(x) \), where the domain for \( x \) is \( \mathbb{R} \)? If your answer is “True”, explain why. If your answer is “False”, provide a counterexample.

2. What is the truth value of the statement \( \forall x P(x) \), where the domain for \( x \) is \( \mathbb{Z} \)? If your answer is “True”, explain why. If your answer is “False”, provide a counterexample.

3. Find another domain of \( x \) that makes the statement \( \forall x P(x) \) true.
Definition 1.57. The existential quantification of a propositional function \( P(x) \) is the proposition “There exists an element \( x \) in the domain such that \( P(x) \).”

Notation: \( \exists x P(x) \), where \( \exists \) is called the existential quantifier.

Once again, the domain must be specified.

Other ways to read \( \exists \):

“There is an \( x \) such that \( P(x) \).”
“There is at least one \( x \) such that \( P(x) \).”
“For some \( x \), \( P(x) \).”

Example 1.58. Let \( P(x) \) be the statement “\( x^2 < x \)”. If the domain is \( \mathbb{N} \), then what is the truth value of \( \exists x P(x) \)?

FALSE, because there is no \( x \) in the natural numbers that is less than its square. 0 and 1 are equal to their squares, and if \( x > 1 \) then its square is larger. These are the only options in \( \mathbb{N} \).

Exercise 1.59. In the above example, what is the truth value of the statement \( \exists x P(x) \) if the domain is \( \mathbb{R} \)?

Negation of Quantifiers

As with negation in general, we read the statement \( \neg \forall x P(x) \) as “It is not the case that for all \( x \), \( P(x) \)” and the statement \( \neg \exists x P(x) \) as “It is not the case that there exists an \( x \) such that \( P(x) \)”.

However, we can take these negations “inside” the quantifier and come up with some general rules for doing so, which we explore in the problem below.

Problem 1.60. Form the negation of each statement below, bringing each negation inside the quantifier (i.e. not simply replacing “all” with “not all” and “there exists” with “there does not exist”).

1. All mammals have hair.
2. All rational numbers are natural numbers.
3. There exists a MATH 218 student who has tried out for American Idol.
4. There exists a real number whose square is not positive.
5. Every person in New Britain, CT has seen a movie starring William Shatner.

Now use what you have done above to complete the following, which are called DeMorgan’s Laws for Quantifiers (i.e. find another symbolic expression that does not have a \( \neg \) in front that is equivalent to the given one):

\[
\neg \exists x P(x) \equiv \quad \\
\neg \forall x P(x) \equiv \quad \\
\]
Logical Expressions Involving Quantifiers

Note on precedence of quantifiers (order of operations): ∀ and ∃ have precedence over all other logical operators except ¬. For example, ∀xP(x) ∧ Q(x) means (∀xP(x)) ∧ Q(x), not ∀x(P(x) ∧ Q(x)), but ∀x¬P(x) means ∀x(¬P(x)).

Exercise 1.61. Use the statement P(x) given by “x likes reggae” to explain the difference between ∀x¬P(x) and ¬∀xP(x), and between ¬∃xP(x) and ∃x¬P(x).

Problem 1.62. Let P(x) be the statement “x grows tomatoes” and Q(x) be the statement “x grows cucumbers”. Explain the difference between the two sentences “Everyone grows tomatoes and cucumbers” and “Everyone who grows tomatoes grows cucumbers”, and write each one symbolically using the universal quantifier ∀. (Hint: use → for one of them.)

Problem 1.63. Let P(x), Q(x), and R(x) be the following propositional functions, all with domain {students in this 218 class}.

P(x): x was born in the United States.
Q(x): x speaks more than one language.
R(x): x has a passport.

Translate the following into fluid English sentences that demonstrate understanding:

1. ∀x[Q(x) ∨ ¬R(x)]
2. ∃x[¬P(x) ∧ (Q(x) ∨ R(x))]
3. ∀x(R(x) → (P(x) ∧ Q(x))). (Hint: consider Problem 1.62)

Now translate the following statements into quantifier form:

1. “There is a student in this 218 class who wasn’t born in the U.S. and speaks more than one language, but doesn’t have a passport.”
2. “No one in this 218 class was both born abroad and speaks more than one language.”
3. “No one in this 218 class who was born abroad speaks more than one language.”

Nested Quantifiers

Definition 1.64. Two quantifiers are nested if one is in the scope of the other (i.e. one is affected by the other).

Example 1.65. Let P(x, y) be the statement “x has eaten y”, where the domain for x is {people} and the domain for y is {the desserts at The Cheesecake Factory}. Then the statement ∀x∃yP(x, y) is the statement “For each person, there exists a dessert at The Cheesecake Factory that that person has eaten”, or, more fluidly, “Everyone has eaten a dessert at The Cheesecake Factory.” We know in this case that x is a person and y is a dessert by their placement in the proposition P.
Problem 1.66. Using $P(x, y)$ from the above example, answer the following questions:

1. Explain the difference in meaning between $\forall x \exists y P(x, y)$ and $\forall y \exists x P(x, y)$.

2. Explain the difference in meaning between $\forall x \exists y P(x, y)$ and $\exists y \forall x P(x, y)$.

A note on counterexamples: recall that a counterexample is an example that satisfies the hypothesis of a conditional statement but not the conclusion (thus rendering the conditional statement false). Another interpretation of “counterexample” is an example that disproves a $\forall$ statement. We use this notion of counterexample in the following problems.

Problem 1.67. Determine the truth value of the following statements, where the domain for all variables is $\mathbb{R}$. If you believe the statement is false, find a counterexample.

1. $\forall x \forall y (2x - y = 6)$.
2. $\forall x \exists y (2x - y = 6)$.
3. $\exists x \forall y (2x - y = 6)$.
4. $\exists x \exists y (2x - y = 6)$.
5. $\exists x \exists y (2x - y = 6 \land y = x + 1)$.

Problem 1.68. Determine the truth value of the following statements, where the domain for all variables is set $\{-3, -2, -1, 0, 1, 2, 3, 4, 5\}$. If you believe the statement is false, find a counterexample.

1. $\forall x \forall y (2x - y = 6)$.
2. $\forall x \exists y (2x - y = 6)$.
3. $\exists x \forall y (2x - y = 6)$.
4. $\exists x \exists y (2x - y = 6)$.
5. $\exists x \exists y (2x - y = 6 \land y = x + 1)$.

Note: To negate nested quantifiers, just use DeMorgan’s Laws to continue moving the negation inside the expression.

More Translations

Example 1.69. Let $P(x, y)$ be the statement “$x$ has been exposed to $y$”, where the domain of $x$ is \{students in this class\} and the domain of $y$ is \{contagious diseases\}.

IMPORTANT: Note that it is not the NAMES of the variables but the POSITION that determines their meaning. I.e., $P(y, x)$ means $y$ is the person and $x$ is the disease. So in the above and in multi-variable propositions in general, the domains refer to the positions, not the names of the variables.
Translate the following sentences:
\( \exists x \forall y \forall z (P(x, y) \rightarrow P(x, z)) \).
Translation: There is a student \( x \) in this class such that if \( x \) has been exposed to any contagious disease then \( x \) has been exposed to all others.

\( \exists x \forall y \exists z (P(x, y) \rightarrow P(x, z) \land y \neq z) \).
Translation: There is a student \( x \) in this class such that if \( x \) has been exposed to any contagious disease then \( x \) has been exposed to at least one other.

(Question: why do we need the \( y \neq z \)?)

“Every student in this class has been exposed to chicken pox and at least one other contagious disease.”
Translation: \( \forall x \exists y (P(x, \text{chicken pox}) \land P(x, y) \land y \neq \text{chicken pox}) \).

“Every student in this class who has been exposed to chicken pox has been exposed to at least one other contagious disease.”
Translation: \( \forall x \exists y ([P(x, \text{chicken pox}) \rightarrow P(x, y)] \land y \neq \text{chicken pox}] \).

“Bob has been exposed to exactly two contagious diseases.”
Translation: This is a tricky one. We have a special technique for translating statements with exact quantities, which is to first state there are at least two (or the number in question) and then state that there are at most two. The “at least two” part is easy, because we can simply use the existential quantifier twice. So, we first start by “naming” those two diseases with variables, say \( x \) and \( y \), which gives us the following statement:
\( \exists x \exists y (P(\text{Bob}, x) \land P(\text{Bob}, y) \land x \neq y) \).

This says that Bob has been exposed to at least two (different) contagious diseases \( x \) and \( y \), but of course this is not the same as “exactly two”. We now combine another universal quantifier and a conditional statement to get the “at most two” part by saying that for every other contagious disease, if Bob has been exposed to it, then it must be one of the two that we already named.
\( \exists x \exists y [P(\text{Bob}, x) \land P(\text{Bob}, y) \land x \neq y \land \forall z (P(\text{Bob}, z) \rightarrow (z = x \lor z = y])] \).

**Problem 1.70.** Consider the following proposition:
\( F(x, y) \): \( x \) has bought \( y \) flowers, where the domain for both variables is \{people\}.

Translate the following:

1. Someone has bought Greg flowers.
2. Nancy has bought at least three people flowers.
3. No one has bought Jessica flowers.
4. Everyone has bought someone flowers.
5. There is exactly one person for whom everyone has bought flowers.
6. There are exactly two people who have never had flowers bought for them.
Problem 1.71. Using the same proposition as in the previous problem, translate the following into fluid English sentences that demonstrate understanding of their meaning:

1. \( \forall x \exists y (F(x, y) \land F(x, \text{Peter}) \land x \neq \text{Peter}) \).
2. \( \forall x \exists y (F(x, y) \land \forall z (F(x, z) \rightarrow z = y)) \).
3. \( \exists y \forall x (F(x, y) \land \forall z (\forall x F(x, z) \rightarrow z = y)) \).

1.5 Introduction to Proofs

Definition 1.72. A theorem is a statement that can be shown to be true (i.e., a fact or result). A proposition is a smaller/less important theorem. An axiom or a postulate is a statement we assume to be true. A lemma is a less important theorem used in the proof of another theorem. A corollary is a less important theorem that follows from another larger theorem. A conjecture is a statement that is being proposed as a true statement, but is not yet proven.

Definition 1.73. A proof is a valid argument that establishes the truth of a theorem (or anything that can be true or false). Note that axioms and postulates do not need to be proved (think of them as the most basic words in the dictionary that are the building blocks for other definitions).

In general, the kind of statements that we prove are conditional statements \((p \rightarrow q)\). This means that we are trying to show that this conditional statement can never take the truth value “False”. If the hypothesis \(p\) is false, the conditional statement is automatically true, and in that case we say that the entire statement is vacuously true and there is no work to be done. Thus, we only really consider the case where \(p\) is true, and we prove the entire conditional statement by showing that \(q\) MUST then also be true. There are several main methods for accomplishing this, which we discuss in the remainder of this section. We start off with the most straightforward of the techniques.

Direct Proofs

1. State/assume that \(p\) is true (or simply “assume \(p\)”). \(p\) may consist of multiple propositions.
2. Make any immediate conclusions regarding the truth of \(p\).
3. Use the conclusions from (2) to show that \(q\) is also true. (This step is usually the longest/hardest part.)

Definition 1.74. If we know (or are assuming) the statement \(\forall x P(x)\) is true for a given domain of \(x\), if we have any element \(c\) of the domain we can make the conclusion “\(P(c)\)”. This is called universal instantiation. If we know (or are assuming) \(P(c)\) for an arbitrary \(c\) in a given domain, we can make the conclusion “\(\forall x P(x)\)”’. This is called universal generalization.

Example 1.75. Suppose that \(P(x)\) is the statement “\(x\) watches Desperate Housewives”, the domain for \(x\) is \{CCSU students\}, and we assume that \(\forall x P(x)\) is true, i.e. every CCSU student watches Desperate Housewives. Then if John is a CCSU student, we know that John watches Desperate Housewives by universal instantiation. If, on the other hand, we can show that an arbitrary CCSU student (i.e. any student randomly chosen) watches Desperate Housewives, we can conclude that all CCSU students watch
Desperate Housewives, or $\forall x P(x)$ is true by universal generalization. **Moral:** to show a statement is true for all values, pick an arbitrary $x$ and prove the statement for that one. More on this later.

**Definition 1.76.** If we know (or are assuming) the statement $\exists x P(x)$ is true, we can conclude that the statement $P(c)$ is true for some element $c$ in the domain. This is called **existential instantiation.** If we know (or are assuming) the statement “$P(c)$ for some element $c$”, we can conclude that $\exists x P(x)$. This is called **existential generalization.**

**Example 1.77.** We once again use the statement $P(x)$: “$x$ watches Desperate Housewives” with domain {CCSU students}. If we know that $\exists x P(x)$ is true, i.e. there is a CCSU student who watches Desperate Housewives, then we can call that student “$c$” and say “Let $c$ be that student” by existential instantiation. Note however, that $\exists x P(x)$ only guarantees the existence of one. There may be others, but only one is guaranteed. On the other hand, if we have found even one CCSU student $c$ that watches Desperate Housewives, we can now assert the truth of the statement $\exists x P(x)$ by existential generalization.

A few more notes:

1. In any proof, we must always start by naming the players. I.e., if we are talking about two arbitrary real numbers $r$ and $s$ in the proof, we must start with the statement “Let $r$ and $s$ be real numbers.”

2. We use “we” as opposed to “I” or “you”.

3. We start each proof with **Proof**: and end each proof with either QED (quod erat demonstrandum, Latin for “which was to be demonstrated”) or $\blacksquare$.

**Example 1.78.** This is an example of a direct proof that uses universal generalization and existential generalization.

Statement to be proved: Every real number has an additive inverse.

Though this statement is not written as a conditional, we will write it as such using universal generalization. Because we would like to show the statement is true for every real number, we pick an arbitrary real number and call it, say, $x$ (universal generalization will extend our result for $x$ to all real numbers). Using this arbitrary real number, we can rephrase the original statement as a conditional: “If $x$ is a real number, then $x$ has an additive inverse.” We now move to the steps of the direct proof.

1. Assume $p$ and name the player: Let $x$ be a real number.

2. Make any immediate conclusions to be drawn - in this case there are none.

3. Attempt to show that $q$ is true, which requires showing that $x$ has an additive inverse: We see that $-x$ is the additive inverse of $x$ because $x + (-x) = -x + x = 0$. Because we have shown that there is one additive inverse for $x$, $-x$, we have shown that $x$ has at least one by existential generalization. Also, because this $x$ has an additive inverse and $x$ was an arbitrary real number, every real number $x$ has an additive inverse by universal generalization.

This is not how we write up the final answer, though. The final answer should be written in fluid paragraph form with complete sentences, as follows:
Proof: Let \( x \) be a real number. Then \(-x\) is its additive inverse because \( x + (-x) = -x + x = 0 \). Thus, every real number has an additive inverse.

We now introduce two more definitions that we will use to practice proofs.

**Definition 1.79.** The integer \( n \) is **even** if there exists an integer \( k \) such that \( n = 2k \).

**Definition 1.80.** The integer \( n \) is **odd** if there exists an integer \( k \) such that \( n = 2k + 1 \).

**Example 1.81.** We see that 24 is even because it can be written as \( 2(12) \), and 12 is also an integer (i.e. \( k = 12 \)). Similarly, 23 is odd because it can be written as \( 2(11) + 1 \), and 11 is also an integer (i.e. \( k = 11 \)).

The above definitions are the only information we assume regarding even and odd. Every other result about even and odd numbers we will prove.

**Axiom 1:** An integer is either even or odd (but not both or neither).

**Axiom 2:** Adding, subtracting, multiplying, and raising integers to a power yields another integer. For example, if \( k \) is an integer, \( 5k^2 - 3k + 1 \) is also an integer.

**Example 1.82.** Give a direct proof that the square of an odd number is odd.

First translate the statement into a conditional using universal generalization. Since we want to prove this is true for any odd number, we pick an arbitrary odd number and call it, say, \( n \). Using this, we rephrase the original statement to “If \( n \) is an odd number, then \( n^2 \) is odd.” We now move on to the steps of a direct proof.

1. Assume \( p \) and name our player(s): Let \( n \) be an odd number.

2. Draw any immediate conclusions from \( p \): Since \( n \) is odd, \( n = 2k + 1 \) for some integer \( k \).

3. Show \( q \) is true too: this is the “meat” of the proof, and the part that requires the most thought. We do not have one cookie cutter method of going from \( p \) to \( q \). However, it is always good to be constantly reminding yourself of what you **want to show** (WTS), which is in this case that \( n^2 \) is odd. We thus take a look at \( n^2 \) using the conclusion drawn in (2):

\[
\begin{align*}
  n^2 &= (2k + 1)^2 \\
  &= 4k^2 + 4k + 1
\end{align*}
\]

Now where do we go from here? Remind ourselves again what we WTS, which is that \( n^2 \) is odd. What do we mean by that? According to the definition of odd, we mean that \( n^2 \) can be written as \( 2(\text{integer}) + 1 \), so let’s see if we can do that from the above calculation. We want to be left with a +1 at the end, which we have, and we want to pull a 2 out of the rest, which it seems we can do. So we now have
\[ n^2 = (2k + 1)^2 \\
= 4k^2 + 4k + 1 \\
= 2(2k^2 + 2k) + 1 \]

We did it! The one last thing we need to cover is to make sure that we have written \( n^2 \) in the form \( 2(\text{INTEGER}) + 1 \) (right now we have it written as \( 2(\text{number}) + 1 \)). So why is \( 2k^2 + 2k \) an integer? Thanks to Axiom 2, since \( k \) itself was assumed to be an integer.

Once again, this is not how we write up our final answer; this is just the process we undergo to get there. We write our solution in fluid paragraph form with complete sentences as follows:

**Proof:** Let \( n \) be an odd integer. Then \( n = 2k + 1 \) for some integer \( k \). We have

\[ n^2 = (2k + 1)^2 \\
= 4k^2 + 4k + 1 \\
= 2(2k^2 + 2k) + 1 \]

Since \( k \) is an integer, so is \( 2k^2 + 2k \) by Axiom 2. Thus, \( n^2 \) is odd.

\[ \blacksquare \]

A couple of notes:

1. Sometimes, you will be asked to prove or disprove a statement. **You should always try to decide if you think it’s true or false first, before you start trying to prove it.** If you believe the statement is true you must prove it. If you believe the statement is false, you should disprove it by finding a counterexample. Recall that there is only one way in which a conditional statement can be false (what is it?), and your counterexample must satisfy those conditions.

2. To prove a biconditional \((p \rightarrow q)\), you must break the statement up into the two conditionals \((p \rightarrow q)\ and \( q \rightarrow p \) and prove both separately. In other words, it will be two proofs in one. To disprove a biconditional, all you have to do is disprove one of the conditionals (which can - and should - be done with a counterexample as stated in (1)).

3. Regarding vocabulary, you can (and should) use your own words to write your proofs; they do not have to look like carbon copies of mine. However, there are a few words of which you must be mindful. I call them “assumption words” and “conclusion words”. Assumption words are words such as “let”, “suppose”, and “assume”, which all imply that you are **making an assumption**, i.e. you are choosing to say that a statement is true. Conclusion words are words such as “thus”, “therefore”, “then”, and “so”, which all imply that you are **drawing a conclusion** based on previous statements. If you misuse these words you are misstating the reasoning. For example, I may start a proof with “Let \( n \) be even”, because that is an assumption I am choosing to make. However, from there, I should NOT say “Let \( n = 2k \) for some integer \( k \)” because this follows from the previous statement, i.e. it is a conclusion I am drawing. I should instead say, “Then \( n = 2k \) for some integer \( k \),” or use another conclusion word.

**Problem 1.83.** 1. Prove or disprove: The sum of two even numbers is even.
2. Prove or disprove: The sum of two numbers is even if and only if the two numbers are themselves even.

**Problem 1.84.** Prove or disprove: If \( n \) is even then \((n + 3)^2\) is odd.

**Problem 1.85.** Prove that if \( n + 2 \) is odd, then so is \( n^3 \).

**Problem 1.86.** Prove or disprove: \( 2n + 4 \) is even if and only if \( n \) is even.

**Common Mistakes in Proofs**

The most common mistake in proving the statement \( p \rightarrow q \) is assuming \( q \). This mistake is called affirming the conclusion. Another common mistake is to assume \( \neg p \), and this mistake is called denying the hypothesis. These are to be avoided at all costs!

**Example 1.87.** Prove that \( n \) is even if \( 7n - 2 \) is even.

**Proof:** Let \( n \) be even. Then \( n = 2k \) for some integer \( k \).......NOPE! We have just affirmed the conclusion.

**Indirect Proofs**

In general, we try the following techniques after attempting a direct proof. There are two types of indirect proofs, proof by contraposition and proof by contradiction. Proof by contraposition is simply a direct proof of the contrapositive of the statement (so we are relying heavily on the fact that the contrapositive is logically equivalent to the original here).

**Example 1.88.** Let \( n \) be a perfect square. Show that if \( n \) is odd, then \( \sqrt{n} \) is also odd.

We will first try a direct proof.

1. Assume \( p \): Let \( n \) be an odd perfect square.
2. Draw any immediate conclusions: Since \( n \) is odd, \( n = 2k + 1 \) for some integer \( k \). Since \( n \) is a perfect square, \( n = m^2 \) for some integer \( m \) (why can’t we use \( k \) again?).
3. Attempt to show \( q \): We have that
   \[ \sqrt{n} = \sqrt{m^2} = m \text{ and} \]
   \[ \sqrt{n} = \sqrt{2k + 1} \text{ so} \]
   \[ \sqrt{2k + 1} = m. \]

We remind ourselves what we WTS here....that \( \sqrt{n} = m \) is odd. To do this, we need \( m = 2(\text{integer}) + 1 \), but we don’t have that (we have an extra \( \sqrt{\cdot} \) which is NOT part of the definition of odd), and there’s no obvious next step to get that. Thus, now is a good time to consider an indirect proof.

Take Two: try proving the contrapositive of the statement, which is “If \( \sqrt{n} \) is not odd, then \( n \) is not odd,” or “If \( \sqrt{n} \) is even, then \( n \) is even.” (We have used Axiom 1 here, which states that an integer is even or odd, i.e. if it’s not one it’s the other.)

1. Assume \( \neg q \): Let \( \sqrt{n} \) be even.
2. Draw any immediate conclusions: Since $\sqrt{n}$ is even, $\sqrt{n} = 2k$ for some integer $k$.

3. Attempt to show $\neg p$: We have that

\[
\begin{align*}
\sqrt{n} &= 2k \\
n &= 4k^2
\end{align*}
\]

We once again remind ourselves what we WTS, which is that $n$ is even. Recalling the definition of even, this means we need to write $n$ in the form $2$\,(integer), which we almost have. We factor out a $2$ to get

\[n = 2(2k^2)\]

Lastly, we verify that $2k^2$ is an integer since $k$ is by Axiom 1.

Of course, this is not our final proof. We write the solution below in fluid paragraph form, with complete sentences.

**Proof:** Suppose that $\sqrt{n}$ is not odd, i.e. $\sqrt{n}$ is even. Then $\sqrt{n} = 2k$ for some integer $k$. Then $n = (\sqrt{n})^2 = (2k)^2 = 4k^2 = 2(2k^2)$. $2k^2$ is an integer because $k$ is, by Axiom 2. Thus, $n$ is even since it is two times an integer. Therefore, the original statement must hold, i.e. if $n$ is odd and $n$ is a perfect square, then $\sqrt{n}$ is also odd.

\[\blacksquare\]

Why did the contrapositive work better in this case? Because we had a “next step” when squaring something but not a “next step” when taking the square root.

**Problem 1.89.** Prove that if $n^2$ is even, $n$ is even.

**Problem 1.90.** Prove that $3n + 4$ is even if and only if $n$ is even.

**Definition 1.91.** A real number $r$ is **rational** if there exist integers $p$ and $q$ with $q \neq 0$ such that $r = \frac{p}{q}$. A number that is not rational is **irrational**.

**Notes:**

1. We sometimes assume the fraction $\frac{p}{q}$ is in **lowest terms**, i.e. $p$ and $q$ have no common factors (other than 1). (Why can we assume this?)

2. To show that a number is rational, you must get it in the form $\frac{\text{integer}}{\text{integer}}$ and make it clear why you know both the numerator and denominator are indeed integers, as well as why you know the denominator is not equal to 0.

3. Since the definition of “irrational” is just “not rational”, there are really no immediate conclusions to be drawn if you assume that a number is irrational (i.e. step (2) of a direct proof). Thus, when you are asked to show that a number is irrational you will almost always want to use an indirect proof so that you can start off by assuming that the number is not irrational, i.e. rational.

**Problem 1.92.**

1. Prove that if $x$ is rational, then $3x$ is rational.
2. Prove that if \( x \) and \( y \) are rational numbers, then \( x + y \) is also rational.

**Problem 1.93.** Prove that a nonzero real number \( x \) is rational if and only if \( \frac{1}{x} \) is rational.

**Problem 1.94.** Prove that the number \( x \) is rational if and only if \( 2x + 3 \) is rational.
A proof by contradiction is a little more interesting than a proof by contraposition, and we break it down into the following steps:

1. Assume $q$ is not true but $p$ is true.
2. Move forward in direct proof fashion until you reach a contradiction of some kind, either mathematical or contradicting a conclusion already drawn based on the first assumption.

We often indicate that we have found a contradiction by the symbol $\rightarrow\leftarrow$. The following example is one of the most classic and well-known proofs by contradiction in mathematics.

**Example 1.95.** Prove that $\sqrt{2}$ is irrational.

**Proof:** Suppose not, i.e. assume that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{p}{q}$ for some integers $p$ and $q$ with $q \neq 0$. We may assume that the fraction $\frac{p}{q}$ is in lowest terms.

Then $2 = \frac{p^2}{q^2}$ and so $p^2 = 2q^2$. Thus, $p^2$ is even since $q^2$ is an integer, because $q$ is. By problem 1.88, $p$ is even since $p^2$ is even. Then $p = 2s$ for some integer $s$, so $(2s)^2 = 2q^2$.

Then we have $4s^2 = 2q^2$ or $2s^2 = q^2$. Thus, $q^2$ is even since $s^2$ is an integer, because $s$ is. We see then that $q$ is also an integer by problem 1.88. Then $q = 2r$ for some integer $r$. Then we have that $\sqrt{2} = \frac{p}{q} = \frac{2s}{2r}$ which is not in lowest terms, which is a contradiction! $\rightarrow\leftarrow$

Thus, $\sqrt{2}$ must be irrational. ■

**Problem 1.96.** Prove that $\sqrt[3]{2}$ is irrational. You may have to prove a lemma along the way.

**Problem 1.97.** Prove that there is no greatest odd integer.

**Problem 1.98.** Use a proof by contradiction to prove that there is no pair of positive integers $(x, y)$ that satisfy the equation $x^2 - y^2 = 1$. (Hint: factor the left side and draw conclusions about what the values of those factors must be.)

**Problem 1.99.** Find the mistake in the following “proof”:

Suppose that $a$ and $b$ are two real numbers, with $a = b$. Then

1. $a = b$
2. $a^2 = ab$ multiply both sides by $a$
3. $a^2 - b^2 = ab - b^2$ subtract $b^2$ from both sides
4. $(a - b)(a + b) = b(a - b)$ factor
5. $a + b = b$ cancel $(a - b)$
6. $2b = b$ substitute $a$ in for $b$ since they are equal by assumption
7. $2 = 1$ divide by $b$
Equivalence Proofs and Proofs by Cases

Often, we state theorems of the form “The following are equivalent:” and then list several statements.

1. $p$
2. $q$
3. $r$

This statement should be interpreted as $p \iff q \iff r$; i.e., if one is true they’re all true, and if one is false they’re all false. If we proved all the directions in the above double biconditional, we would have a LOT of statements to prove (how many?). But luckily, we do not need to. We only need to prove as few as are necessary to yield all dependencies. The usual way to do so is to show $p \rightarrow q$, $q \rightarrow r$, and $r \rightarrow p$. We can use what is known as transitivity of $\rightarrow$ to show the rest; for example, using just $p \rightarrow q$, $q \rightarrow r$, and $r \rightarrow p$ we can get $p \rightarrow r$ because $p \rightarrow q$ and $q \rightarrow r$ imply $p \rightarrow r$. In general, you need as many proofs as there are original statements to cover all the possible conditional statements.

A proof by cases is a proof in which we divide the hypothesis up into two or more cases. For example, if we would like to prove something is true for all real numbers, we might have reason to consider positives, negatives, and 0 all separately. This is just an example of a set of possible cases; what the cases are and how many there are of them depends on the statement to be proved.

Problem 1.100. Prove that if $n$ is an integer, then $n^2 + 5n + 7$ is odd.
2 Set Theory

2.1 Introduction to Sets

Definition 2.1. A set is an unordered collection of “objects”. The objects in a set are called the elements or members of the set. A set contains its elements. A set is usually denoted by a capital letter, say $A$, and an element is usually denoted by a lowercase letter, say $a$ or $b$. We write $a \in A$ to mean “$a$ is an element of $A$”. $a \notin A$ means the statement $\neg(a \in A)$, or “$a$ is not an element of $A$”.

Definition 2.2. The set $A$ is a subset of the set $B$ if and only if every element of $A$ is also an element of $B$, and denote this as $A \subseteq B$. Note that $A \subseteq B$ if and only if $\forall x(x \in A \rightarrow x \in B)$.

Definition 2.3. Two sets $A$ and $B$ are equal if and only if $\forall x(x \in A \leftrightarrow x \in B)$. Note that this can be interpreted as $A = B$ if and only if $\forall x(x \in A \rightarrow x \in B) \land (x \in B \rightarrow x \in A)$. I.e., $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. We often use this notion to prove that two sets are equal.

Definition 2.4. We can write sets in roster notation, which is simply a list of the elements, or in set-builder notation, which describes a defining characteristic common to all the elements of the set. In either case, we encase the list or description in curly brackets $. . .$. Set-builder notation is set up as follows:

$\{\text{kind or name of object} : \text{specific description}\}$ or $\{\text{kind or name of object} | \text{specific description}\}$. We read the $:$ or $|$ as “such that”.

Example 2.5. $A = \{\text{red, yellow, blue}\}$ is a set in roster notation, and $A = \{x \text{ is a color} | x \text{ is primary}\}$. We read the second one as, “$x$ is a color such that $x$ is primary.”

Example 2.6. $\{a, \text{dog, math, } -2\}$ is a set which is equal to $\{-\frac{4}{3}, \text{dog, a, math}\}$ and $\{a, \text{dog, a, } -\frac{4}{3}, \text{math, } -2\}$ but not $\{a, \text{dog, math, } -1\}$. In other words, order does not matter nor does number of appearances of an element, nor the manner in which it is expressed (as long as it is indeed the same element). Note that in this case, we would probably not attempt to use set-builder notation since it would be difficult to find a defining property common to all of these elements.

More examples: (note that none of these symbols take curly brackets)

- $\mathbb{R}$: the real numbers
- $\mathbb{Z}$: the integers
- $\mathbb{Z}^+$: the positive integers
- $\mathbb{Q}$: the rational numbers
- $\mathbb{C}$: the complex numbers

Using this notation, we can now say “$x$ is an integer”, for example, by simply writing $x \in \mathbb{Z}$. With this in mind, note that $\mathbb{Q}$ can also be described in set-builder notation as $\{x \in \mathbb{R} : x = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0\}$ or simply $\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ and $\mathbb{C}$ can be described in set-builder notation as $\{a + bi : a, b \in \mathbb{R}, i = \sqrt{-1}\}$.

Problem 2.7. Write the following sets in roster notation.

1. $\{x \in \mathbb{N} : x = 2s \text{ for some } s \in \mathbb{Z}, 3 \leq x < 10\}$
2. $\{2s - 1 : s \in \mathbb{Z}, 3 \leq s < 10\}$
3. \( \{ x \in \mathbb{Z}^+ : x \text{ is prime and } x \leq 30 \} \)
4. \( \{ x \in \mathbb{R} : x^3 + 4x = 0 \} \)
5. \( \{ z \in \mathbb{C} : z^3 + 4z = 0 \} \)

**Problem 2.8.** Write the following sets in set-builder notation.

1. \( \{ 2, 4, 6 \} \)
2. \( \{ 0, 3, 6, 9 \} \)
3. \( \{ 0, 1, 16, 81, 625, 1296, \ldots \} \)
4. \( \{ \ldots, 100000, 10000, 1000, 100, 1, .01, .001, .0001, \ldots \} \)
5. \( \{ \ldots, -8, -2, 4, 10, 16, \ldots \} \)

**Definition 2.9.** A set containing exactly one element is called a singleton set.

**Definition 2.10.** The set with no elements is called the empty set, denoted \( \emptyset \) or \{ \} but not \{\emptyset\}, because the last one means the set that contains the empty set.

**Problem 2.11.** For every set \( S \), prove that

1. \( \emptyset \subseteq S \)
2. \( S \subseteq S \)

Hint: recall that to prove that \( A \subseteq B \), you need to prove the truth of the statement \( \forall x (x \in A \rightarrow x \in B) \).

**Definition 2.12.** A set \( A \) is a proper subset of a set \( B \) if \( \forall x (x \in A \rightarrow x \in B) \land \exists x (x \in B \land x \notin A) \). In other words, it is not possible that \( A = B \) (whereas the symbol “ \( \subseteq \) ” DOES allow for that possibility). We denote this \( A \subset B \). The proper subset notation should never be used unless you are sure that equality is not possible (as with “ \( < \) ” - one should never write \( x < y \) unless it is certain that \( x \neq y \)).

**Definition 2.13.** Given a set \( S \), the power set of \( S \) is the set of all subsets of the set \( S \). We denote this \( P(S) \).

**Example 2.14.** Let \( S = \{ \pi, 3, 0 \} \). Then \( P(S) = \{ \emptyset, \{ \pi \}, \{ 3 \}, \{ 0 \}, \{ \pi, 3 \}, \{ \pi, 0 \}, \{ 0, 3 \}, \{ \pi, 3, 0 \} \} \). Now let \( S = \{ \pi, 3, 0 \} \). Then \( P(S) = \{ \emptyset, \{ \pi \}, \{ 3 \}, \{ \pi, 3 \}, \{ \pi, 0 \}, \{ 0, 3 \}, \{ \pi, 3, 0 \} \} \). While it may seem confusing to see a set within a set within a set, just think of each set as a bag. So the power set is a larger bag than the original set, and it contains bags of all possible combinations from the original bag. Similarly, the set \( \{ \{ 0 \} \} \) can be thought of as the bag containing the bag containing 0.

Observe: we can recover \( S \) from \( P(S) \) by looking at the singleton sets. For example, the set \( \{\{a\}, \{b\}, \{a, b\}, \{a, c\}, \{b, c\} \} \) couldn’t be the power set of any set \( S \), first of all because it doesn’t contain \( \emptyset \) but also because it doesn’t contain the singleton set \( \{c\} \), which it would have to because \( c \) is contained within other sets.
Exercise 2.15. If $S \neq \emptyset$, what is the fewest number of elements $P(S)$ could have?

Exercise 2.16. Find $P(\emptyset)$.

Problem 2.17. Find the power sets of the following sets.

1. $\{a, \text{bagel}, \$\}$
2. $\{a, \emptyset\}$
3. $\{a, \{a\}\}$
4. $\{a, \{a, \emptyset\}\}$

Problem 2.18. Prove or disprove: If $P(A) = P(B)$, then $A = B$. (Hint: recall the definition of set equality - there are two statement to be proved.)

Definition 2.19. The ordered $n$-tuple $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has $a_1$ as its first element, $a_2$ as its second element, ..., and $a_n$ as its $n$th element. Two $n$-tuples $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are equal if and only if $a_i = b_i$ for all $i = 1, 2, \ldots, n$.

Definition 2.20. 2-tuples are called ordered pairs. For example, in the Cartesian plane: $(x, y) \neq (y, x)$ unless $x = y$.

Definition 2.21. Let $A$ and $B$ be sets. The Cartesian product of $A$ and $B$, denoted by $A \times B$, is the set of all ordered pairs $(a, b)$ where $a \in A$ and $b \in B$. That is,

$$A \times B = \{(a, b) : a \in A \land b \in B\}$$

Exercise 2.22. Let $A = \{0, 1\}$ and $B = \{\text{dog, cat, mouse}\}$. Compute the set $A \times B$. Do you think this is the same as $B \times A$?

Exercise 2.23. Let $A = \{0, 1\}$ and $B = \emptyset$. Compute the set $A \times B$. Do you think this is the same as $B \times A$?

Definition 2.24. The Cartesian product of the sets $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered $n$-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in A_i$. That is,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i, i = 1, 2, \ldots, n\}$$

2.2 Set Operations

Definition 2.25. Let $A$ and $B$ be sets. The union of the sets $A$ and $B$, denoted by $A \cup B$, is the set that contains those elements that are either in $A$ or $B$ or both. That is,

$$A \cup B = \{x : x \in A \lor x \in B\}$$
Definition 2.26. Let $A$ and $B$ be sets. The intersection of the sets $A$ and $B$, denoted by $A \cap B$, is the set containing those elements in both $A$ and $B$. That is,$$
abla = \{ x : x \in A \land x \in B \}$$

Definition 2.27. Let $A$ and $B$ be sets. The difference of $A$ and $B$, denoted by $A - B$, is the set containing those elements that are in $A$ but not in $B$. That is,$$A - B = \{ x : x \in A \land x \notin B \}$$

$A - B$ is also called the complement of $A$ in $B$ or the complement of $A$ with respect to $B$.

Exercise 2.28. Suppose that for sets $A$ and $B$, $A \cup B = \{0, 1, 2, 3, 4, 5, 8, 9\}$, $A - B = \{1, 4, 8\}$, and $B - A = \{0, 2, 5\}$. Find $A \cap B$.

Definition 2.29. Let $S$ be a set. If there are exactly $n$ distinct elements in $S$ where $n$ is a nonnegative integer, we say that $S$ is a finite set and that $n$ is the cardinality of $S$. The cardinality of $S$ is denoted by $|S|$.

Definition 2.30. A set is said to be infinite if it is not finite.

Exercise 2.31. If $A$ and $B$ are two finite sets, find a formula for $|A \cup B|$. (Careful: remember that $A$ and $B$ may have some elements in common.)

Note: $|A| - |B|$ means subtraction of natural numbers. $A - B$ is a set.

Definition 2.32. Let $U$ be the universal set. Then the complement of the set $A$, denoted $\sim A$, is the set $U - A$. That is, $\sim A = \{ x : x \notin A \}$. Another way to say this is that $\forall x(x \in \sim A \leftrightarrow x \notin A)$.

Note that you must know what the universe $U$ is for $\sim A$ to be defined.

Exercise 2.33. Let $U = \{0, 1, 2, \ldots, 10, 11\}$ (universe), $A = \{0, 3, 7\}$ and $B = \{x \in U : x = 5k \text{ for some } k \in \mathbb{Z}\}$. Find $A \cup B$, $A \cap B$, $A - B$, and $B - A$. Then find the complements of $A, B, A \cup B, A \cap B, A - B,$ and $B - A$.

Problem 2.34. Consider the following sets, assuming that the universe of discourse $U = \{\text{U.S. residents who are capable of speaking a language}\}$:

$A = \{x \in U : x \text{ speaks English}\}$
$B = \{x \in U : x \text{ speaks English and Spanish}\}$
$C = \{x \in U : x \text{ speaks Spanish}\}$
$D = \{x \in U : x \text{ speaks only Spanish}\}$

Determine if the statements below are true or false (and explain). (Hint: keep in mind the definition of $A \subseteq B$.)

1. $A \subseteq B$
2. \( B \subseteq A \)
3. \( B \subset A \)
4. \( A \cup C = B \)
5. \( A \cap D = \emptyset \)
6. \( A \subseteq \overline{D} \)
7. \( B - A = C \)

Example 2.35. Show that if \( A \subseteq B \), then \( \overline{B} \subseteq \overline{A} \).

We will prove this statement using a method called “element-chasing”. In general, to show \( R \subseteq S \) we pick an arbitrary element, say \( x \) in \( R \) and show that that arbitrary element must be in \( S \).

Proof: Let \( x \in \overline{B} \). Then \( x \notin B \) by definition of \( \overline{B} \). \( A \subseteq B \) is the statement \( \forall x (x \in A \rightarrow x \in B) \), which is equivalent by contrapositivity to \( \forall x (x \notin B \rightarrow x \notin A) \). Since \( x \notin B \), \( x \notin A \), and so \( x \in \overline{A} \) by definition of \( \overline{A} \). We have thus shown that if \( x \in \overline{B} \) then \( x \in \overline{A} \), so \( \overline{B} \subseteq \overline{A} \).

\[ \blacksquare \]

Set Identities

<table>
<thead>
<tr>
<th>Identity Laws</th>
<th>Commutative Laws</th>
<th>DeMorgan’s Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A \cup \emptyset = A )</td>
<td>( A \cup B = B \cup A )</td>
<td>( A \cup \overline{B} = A \cap \overline{B} )</td>
</tr>
<tr>
<td>( A \cap U = A )</td>
<td>( A \cap B = B \cap A )</td>
<td>( A \cap \overline{B} = A \cup \overline{B} )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domination Laws</th>
<th>Associative Laws</th>
<th>Absorption Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A \cup U = U )</td>
<td>( A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C )</td>
<td>( A \cup (A \cap B) = A )</td>
</tr>
<tr>
<td>( A \cap \emptyset = \emptyset )</td>
<td>( A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C )</td>
<td>( A \cap (A \cup B) = A )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Idempotent Laws</th>
<th>Distributive Laws</th>
<th>Complement Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A \cup A = A )</td>
<td>( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) )</td>
<td>( A \cup A = U )</td>
</tr>
<tr>
<td>( A \cap A = A )</td>
<td>( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) )</td>
<td>( A \cap \overline{A} = \emptyset )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complementation Law</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( (\overline{A}) = A )</td>
<td></td>
</tr>
</tbody>
</table>

Exercise 2.36. Use the laws above to prove the following “alternate” distributive laws:

\[
(B \cup C) \cap A = (B \cap A) \cup (C \cap A) \\
(B \cap C) \cup A = (B \cup A) \cap (C \cup A)
\]

Problem 2.37. Use the laws above to prove that \( A \cap B \cap C = \overline{A} \cup B \cup C \).
We can prove all of the laws in the table above independently from each other via element-chasing, i.e. using only definitions of set operations and not needing any of the other laws.

**Example 2.38.** Prove the second distributive law, \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \).

We show that \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \) by showing that \( A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \) and \( (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C) \).

**Proof:**

\[
A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C):
\]

Let \( x \in A \cup (B \cap C) \). Then \( x \in A \) or \( x \in B \cap C \) by definition of \( \cup \). Suppose that \( x \in A \). Then \( x \in A \cup B \) and \( x \in (A \cup C) \) by definition of \( \cup \). Thus, \( x \in (A \cup B) \cap (A \cup C) \) by definition of \( \cap \). Now suppose that \( x \not\in A \). Then \( x \in B \cap C \). Thus \( x \in B \) and \( x \in C \) by definition of \( \cap \). Then \( x \in A \cup B \) since \( x \in B \) by definition of \( \cup \) and \( x \in A \cup C \) since \( x \in C \) by definition of \( \cup \). Thus, \( x \in (A \cup B) \cap (A \cup C) \) by definition of \( \cap \).

The other direction is left for the following problem.

**Problem 2.39.** Show the other set containment from the previous example to prove the set equality \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \).

**Problem 2.40.** Show that if \( A \) and \( B \) are sets, then \( A - B = A \cap \overline{B} \).

**Problem 2.41.** Show that \( (B - A) \cup (C - A) = (B \cup C) - A \).

**Definition 2.42.** Two sets are called disjoint if their intersection is the empty set. That is, \( A \) and \( B \) are disjoint if \( A \cap B = \emptyset \).

**Exercise 2.43.** Let \( A = \{2k : k \in \mathbb{Z}, 0 \leq k < 10\} \) and \( B = \{x \in \mathbb{Z}^+ : x \leq 7\} \). Are \( A \) and \( B \) disjoint? Are \( A - B \) and \( B - A \) disjoint?

**Problem 2.44.** Prove or disprove: For any two sets \( A \) and \( B \), \( A - B \) and \( B - A \) are disjoint.

**Problem 2.45.** Prove that if \( A \subseteq (B \cap C) \), then \( A \) and \( B \cup C \) are disjoint.

### 2.3 Functions

**Definition 2.46.** Let \( A \) and \( B \) be nonempty sets. A function \( f \) from \( A \) to \( B \) is an assignment of exactly one element of \( B \) to each element of \( A \). We write \( f(a) = b \) if \( b \) is the unique element of \( B \) assigned by the function \( f \) to the element \( a \) of \( A \). If \( f \) is a function from \( A \) to \( B \), we write \( f : A \rightarrow B \). Functions are also often called mappings or transformations.

Another way to define a function is as a subset of the Cartesian product \( A \times B \) such that there is a unique ordered pair corresponding to each \( a \in A \). In this representation of a function, the first element of the ordered pair can be considered the input element and the second element of the ordered pair can be considered the output element. See the following example.

**Example 2.47.** Let \( A = \{a, b, c\} \) and \( B = \{1, 2, 3, 4\} \). Then \( A \times B = \{(a, 1), (a, 2), (a, 3), (a, 4), (b, 1), (b, 2), (b, 3), (b, 4), (c, 1), (c, 2), (c, 3), (c, 4)\} \). We consider \( f \) as a subset of \( A \times B \), say, \( f = \{(a, 3), (b, 2), (b, 4), (c, 2)\} \). But, this does not represent a function because \( f(b) = 2 \) and \( f(b) = 4 \) and according to the definition of function, **exactly one** element of \( B \) must be assigned to each element of \( A \). However, the subset \( f = \{(a, 3), (b, 2), (c, 2)\} \) IS a function from \( A \) to \( B \) because each element of \( A \) is assigned exactly one element of \( B \).
Definition 2.48. If \( f \) is a function from \( A \) to \( B \), we say that \( A \) is the **domain** of \( f \) and \( B \) is the **codomain** of \( f \). If \( f(a) = b \) we say that \( b \) is the **image** of \( b \) and \( a \) is a **pre-image** of \( b \). The **range** of \( f \) is the set of all images of elements of \( A \), i.e. the set \( \{b \in B : b = f(a) \text{ for some } a \in A\} \). Note that in a function, each element of the domain must have exactly one image, but an element of the codomain may have 0, 1, 2, \ldots \ pre-images. An element \( y \) of the codomain will be in the range of \( f \) if and only if it has at least one pre-image. Lastly, we say that \( f \) maps \( A \) to \( B \).

Example 2.49. We revisit the function in the previous example, where \( A = \{a, b, c\} \) and \( B = \{1, 2, 3, 4\} \), and \( f = \{(a, 3), (b, 2), (c, 2)\} \). \( A \) is the domain, \( B \) is the codomain, and \( \{2, 3\} \) is the range. 3 is the image of \( a \), and 2 is the image of \( b \) and \( c \). 3 has one pre-image, \( a \), and 2 has two pre-images, \( b \) and \( c \).

Example 2.50. Let \( f \) be the function that inputs a student in this class and outputs his/her age in years. (Why is this a function?)

**Domain:** \{students in this class\}

**Codomain:** \( \mathbb{R} \) or \( \mathbb{N} \) or \( Z^+ \) etc.

**Range?** The only way to find this is to determine the age of all the students in the class and see which ages are covered. One guess might be \{19, 20, 21, 22, 23, 24\}.

Exercise 2.51. Find the images of your group members in the above example.

Definition 2.52. Let \( f \) be a function from the set \( A \) to the set \( B \) and let \( S \) be a subset of \( A \). The image of \( S \) under the function \( f \) is the subset of \( B \) that consists of the images of the elements of \( S \). We denote the image of \( S \) by \( f(S) \), so \( f(S) = \{t \in B : \exists s \in S \text{ such that } t = f(s)\} \)

Exercise 2.53. Let \( S \) be the set consisting of your group members. Find \( f(S) \), where \( f \) is defined as in the previous example.

Example 2.54. Suppose that \( f : A \rightarrow B \) is a function, with \( S \subseteq T \subseteq A \). Show that \( f(S) \subseteq f(T) \).

We prove the statement “If \( y \in f(S) \), then \( y \in f(T) \).” (I chose “\( y \)” because it is an element of \( B \) and can be thought of as an output element as opposed to an input.)

**Proof:** Let \( y \in f(S) \). Then by definition of \( f(S) \), there exists \( x \in S \) such that \( y = f(x) \). Since \( x \in S \) and \( S \subseteq T \), by definition of \( \subseteq \), \( x \in T \). Then \( f(x) \in f(T) \) by definition of \( f(T) \). But \( y = f(x) \), so \( y \in f(T) \), which proves the statement \( f(S) \subseteq f(T) \).

Problem 2.55. Let \( f : A \rightarrow B \) be a function, with \( S, T \subseteq A \). Show that \( f(S \cup T) = f(S) \cup f(T) \). (Note that this is a statement claiming equality of sets, so you must prove both set containments.)

Problem 2.56. Let \( f : A \rightarrow B \) be a function, with \( S, T \subseteq A \). Show that \( f(S \cap T) \subseteq f(S) \cap f(T) \). Give an example where equality fails.

Problem 2.57. Let \( f : A \rightarrow B \) be a function, with \( S, T \subseteq A \). Show that \( f(S) - f(T) \subseteq f(S - T) \). Give an example where equality fails.

Definition 2.58. Let \( f : A \rightarrow B \) be a function, and let \( U \subseteq B \). Then \( f^{-1}(U) \) is defined to be the set of pre-images of elements of the set \( U \), i.e. \( f^{-1}(U) = \{x \in A : f(x) = y \text{ for some } y \in U\} \). Be careful: \( f^{-1}(U) \) is a **set**.

Exercise 2.59. Let \( A = \{a, b, c, d\}, B = \{1, 2, 3, 4\} \), and let \( f : A \rightarrow B \) be defined by \{\((a, 3), (b, 1), (c, 3), (d, 2)\}\). Find \( f^{-1}(\{2\}) \), \( f^{-1}(\{3\}) \) and \( f^{-1}(\{2, 3\}) \).
Problem 2.60. Suppose that \( f : A \to B \) is a function, with \( U \subseteq V \subseteq B \). Show that \( f^{-1}(U) \subseteq f^{-1}(V) \).

Problem 2.61. Let \( f : A \to B \) be a function, with \( U, V \subseteq B \). Show that \( f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V) \).

Problem 2.62. Let \( f : A \to B \) be a function, with \( U, V \subseteq B \). Show that \( f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V) \).

Problem 2.63. Let \( f : A \to B \) be a function, with \( U, V \subseteq B \). Show that \( f^{-1}(U - V) = f^{-1}(U) - f^{-1}(V) \).

One-to-one and Onto Functions

We first begin with a discussion of Existence and Uniqueness Proofs.

Definition 2.64. An existence proof is a proof of a proposition of the form \( \exists x P(x) \).

There are two main kinds of existence proofs: constructive and non-constructive. A constructive proof uses existential generalization: \( P(c) \), therefore \( \exists x P(x) \). In other words, we prove that the object exists by producing it and then proving that it has the desired property. A non-constructive proof is one in which we prove it using full-proof circumstantial evidence.

Example 2.65. Consider the statement “There is a CCSU student who passed Discrete Math”. To prove this statement constructively, you would first produce the student, and then offer proof that that student has indeed passed Discrete Math (transcripts, etc.) One important thing to note: in a constructive existence proof, you do not need to (and therefore should not) explain how you found that student to prove that it’s true. In other words, explaining that you went to the computer lab, shouted, “Who here took Discrete Math?!”, and took the first student that responded, is all superfluous and thus does not belong in the proof. All you have to do is produce the student along with proof that (s)he passed Discrete Math.

A non-constructive proof of this statement might consist of the following steps: Count the number of students in say, Linear Algebra, which has Discrete Math as a prerequisite. Count the number of exceptions/pre-req overrides that were made. Assuming that there are more students in the class than pre-req overrides that were made, you can then conclude that there must have been at least one student that passed Discrete Math.

Example 2.66. Show that there exist real numbers \( x \) and \( y \) such that \( x^2 - y^2 = 5 \).

Proof: Let \( x = 3 \) and \( y = 2 \). We have that \( 3^2 - 2^2 = 9 - 4 = 5 \).

This is again a constructive proof, because we simply produced the objects with the desired property and then showed that they had the desired property. Note again that we do not need to show how we found those values of \( x \) and \( y \).

Example 2.67. Show that the function \( f(x) = x^3 - 5x^2 + 3x + 1 \) has a real zero.

A constructive proof:

Proof: Let \( x = 1 \). Observe that \( f(1) = 1^3 - 5(1^2) + 3(1) + 1 = 1 - 5 + 3 + 1 = 0 \).
A non-constructive proof:

**Proof:** Observe that $f(0) = 1$ (positive) and $f(2) = 8 - 20 + 6 + 1 = -5$ (negative), and $f$ is continuous since it is a polynomial. Thus, by the Intermediate Value Theorem $f$ must have a zero between $x = 0$ and $x = 2$.

Exercise 2.68. Describe constructive and non-constructive proofs for the statement “There exists a man who has been to the moon.”

Uniqueness

A uniqueness proof is a proof of a statement of the form “There is exactly one $x$ such that $P(x)$”. Recall from the section on nested quantifiers how we translate such a statement. We first start by stating that there is at least one $x$ such that $P(x)$: $\exists x P(x)$. But that is not enough, because “at least one” does not mean “exactly one”. Thus, we then state that if there are any other, say, $y$’s such that $P(y)$, then $y = x$: $\exists x [P(x) \land \forall y (P(y) \rightarrow y = x)]$. Uniqueness proofs usually follow existence proofs, and we use an idea similar to the one we just described: we suppose that there exists, say $y$, such that $P(y)$, and then show that we must have $x = y$.

Example 2.69. Show that there exists a unique $x$ such that $3x^3 - 2 = 5$.

**Proof:**

Existence

Observe that $x = \sqrt[3]{\frac{7}{3}}$ yields $3 \left( \sqrt[3]{\frac{7}{3}} \right)^3 - 2 = 3(\frac{7}{3}) - 2 = 7 - 2 = 5$.

Uniqueness

Suppose that there exists $y$ such that $3y^3 - 2 = 5$. Then

1. $3x^3 - 2 = 3y^3 - 2$ add 2 to both sides
2. $3x^3 = 3y^3$ divide both sides by 3
3. $x^3 = y^3$ take cube root of both sides
4. $x = y$.

Thus, there exists a unique $x$ such that $3x^3 - 2 = 5$.

Exercise 2.70. Where does the above proof of uniqueness fall apart for the equation $3x^2 - 2 = 5$?

Example 2.71. Suppose that $a$ and $b$ are odd integers with $a \neq b$. Show that there is a unique integer $c$ such that $|a - c| = |b - c|$.

Recall that $|x - y|$ is the distance between $x$ and $y$. (So, what we want to show here is that there is a unique integer that is equidistant to the two integers - this should give you a hint as to how I came up with the $c$ that follows.)
Proof:

Existence
Let \( c = \frac{a+b}{2} \). Then \(|a-c| = |a-\frac{a+b}{2}| = |\frac{a-b}{2}|\) and \(|b-c| = |b-\frac{a+b}{2}| = |\frac{b-a}{2}|\). Thus, \(|a-c| = |b-c|\).

We must also show that \( c \) is an integer. Since \( a, b \) are odd, we have \( a = 2k+1 \) and \( b = 2l+1 \) for integers \( k \) and \( l \). Then \( c = \frac{2k+1+2l+1}{2} = \frac{2k+2l+2}{2} = \frac{2(k+l+1)}{2} = k+l+1 \). Since \( k, l \) are integers, so is \( k+l+1 \) by Axiom 2.

Uniqueness

Suppose there exists \( d \) such that \(|a-d| = |b-d|\). Then \( a - d = \pm(b-d) \), i.e. \( a - d = b - d \) or \( a - d = -(b-d) = d - b \). But \( a - d = b - d \) implies \( a = b \) which contradicts our assumption, so it must be that \( a - d = d - b \). Similarly, i.e. by the same reasoning, \( a - c = c - b \).

Manipulating the two equations yields \( a + b = 2d \) and \( a + b = 2c \). Thus, \( 2d = 2c \) and \( d = c \).

\[ \square \]

**Problem 2.72.** Prove that there exists a continuous function \( f(x) \) such that \( f'(x) = 3x^4 - 10x^2 + 2x + 1 \) and such that \( f(2) = 5 \).

**Problem 2.73.** Prove that for every real number \( x \), if \( x \neq 0 \) and \( x \neq 1 \) then there is a unique real number \( y \) such that \( \frac{y}{x} = y - x \). (Hint: you are not finding \( x \) - you are finding \( y \) in terms of \( x \).)

**Problem 2.74.** Prove that there is exactly one additive identity for the real numbers. (Recall that an additive identity is a number \( h \) such that \( h + a = a + h = a \) for every real number \( a \).

**Definition 2.75.** A function \( f \) is **one-to-one** (1-1), or injective, if and only if \( f(a) = f(b) \) implies that \( a = b \) for all \( a \) and \( b \) in the domain of \( f \). A function is said to be an **injection** if it is one-to-one.

Another way to say this is \( f \) is one-to-one if and only if \( \forall a \forall b[f(a) = f(b) \rightarrow a = b] \) where \( a \) and \( b \) are elements of the domain of \( f \).

**Exercise 2.76.** Let \( A = \{1, 2, 3\} \) and \( B = \{a, b, c, d\} \). Find both a one-to-one function and a non one-to-one function using this domain and codomain (use ordered pair notation).

**Exercise 2.77.** Let \( A = \{a, b, c, d\} \) and \( B = \{1, 2, 3\} \). Is it possible to have a one-to-one function with this domain and codomain? Explain.

**Definition 2.78.** A function \( f : A \rightarrow B \) is called **onto** or surjective if and only if for every element \( b \in B \) there is an element \( a \in A \) such that \( f(a) = b \). A function \( f \) is called a **surjection** if it is onto.

**Exercise 2.79.** Let \( A = \{1, 2, 3\} \) and \( B = \{a, b, c, d\} \). Is it possible to have an onto function with this domain and codomain? Explain.

Observe: A function is ALWAYS onto its range by definition.

How do one-to-one and onto relate to existence and uniqueness proofs? Recall the definition of onto: if \( f : A \rightarrow B \), we must show that for an arbitrary element \( y \) of \( B \), there exists an element \( x \) of \( A \) such that \( f(x) = y \). So this is an existence proof! Similarly, to show that \( f \) is one-to-one, we must show that if \( f(x_1) = f(x_2) \) for elements \( x_1, x_2 \) of \( A \), then \( x_1 = x_2 \); i.e., we are showing that assuming there exists \( x_1 \) in \( A \) such that \( f(x_1) = y \), this is the **only** \( x_1 \) that satisfies this. In other words, we are showing that \( x_1 \) is unique. We keep this in mind in the following examples.
Example 2.80. Determine if the function \( f(x) = |x + 1| \) is one-to-one and/or onto, if \( f : \mathbb{Z} \rightarrow \mathbb{R} \).

Solution: We claim that \( f \) is neither one-to-one nor onto. To disprove that \( f \) is onto, we disprove the statement \( \forall y (y \in \mathbb{R} \rightarrow \exists x [x \in \mathbb{Z} \land f(x) = y]) \) by finding a counterexample. In other words, we find \( y \in \mathbb{R} \) such that there does not exist \( x \in \mathbb{Z} \) with \( f(x) = y \) (this makes the hypothesis true and the conclusion false). Note that we only need one such \( y \in \mathbb{R} \) to prove the claim. Let \( y = \frac{1}{2} \). Then we would need \( \frac{1}{2} = |x + 1| \), or \( x + 1 = \pm \frac{1}{2} \), which tells us we must have \( x = -\frac{3}{2} \) or \( x = -\frac{1}{2} \). Neither of these is an integer, so there does not exist \( x \) in the domain such that \( f(x) = \frac{1}{2} \) and so \( f \) is not onto. To disprove that \( f \) is one-to-one, we disprove the statement \( \forall x \forall y ([x \in \mathbb{Z} \land y \in \mathbb{Z} \land f(x) = f(y) \rightarrow x = y]) \) by again finding a counterexample. In other words, we find \( x, y \in \mathbb{Z} \) such that \( f(x) = f(y) \) but \( x \neq y \). Let \( x = 1 \), \( y = -3 \). Then \( |1 + 1| = 2 = |−3 + 1| \) but \( 1 \neq -3 \). Thus, \( f \) is not one-to-one.

Example 2.81. Determine if the function \( f(x) = |x + 1| \) is one-to-one and/or onto, if \( f : \mathbb{N} \rightarrow \mathbb{Z}^+ \).

We claim that \( f \) is both one-to-one and onto, which we prove below.

Proof:

**Onto**

Let \( y \in \mathbb{Z}^+ \), and let \( x = y − 1 \). Then \( f(y − 1) = |y − 1 + 1| = |y| = y \) since \( y \in \mathbb{Z}^+ \) so \( y > 0 \). Also, since \( y \geq 1 \), \( x = y − 1 \geq 0 \) so \( x \in \mathbb{N} \) Thus, \( f \) is onto.

(Note that we had to find \( x \), show that it satisfied \( f(x) = y \), and show that \( x \) was indeed an element of the domain, which was \( \mathbb{Z}^+ \).

**One-to-one**

Let \( x, y \in \mathbb{N} \) and suppose that \( f(x) = f(y) \). Then \( |x + 1| = |y + 1| \), so \( x + 1 = \pm (y + 1) \). If \( x + 1 = y + 1 \) then \( x = y \) and we are done. If \( x + 1 = −(y + 1) = −y − 1 \) then \( x + y = −2 \). But \( x, y \in \mathbb{N} \) so \( x, y \geq 0 \), so they could not have a negative sum. Thus, \( x = y \) and \( f \) is one-to-one. ■

Problem 2.82. Find a domain and codomain for the above function \( f(x) = |x + 1| \) such that the result is onto but not one-to-one, and prove your claim.

Problem 2.83. Find a domain and codomain for the above function \( f(x) = |x + 1| \) such that the result is one-to-one but not onto, and prove your claim.

Definition 2.84. The function \( f \) is a **bijection** if it is both one-to-one and onto (both an injection and a surjection).

Problem 2.85. Show that every linear function is a bijection from \( \mathbb{R} \rightarrow \mathbb{R} \).

Problem 2.86. Consider the function \( f(x) = e^x \). Find a domain and codomain such that \( f \) is a bijection, and prove your claim.

Inverse Functions and Compositions of Functions

Definition 2.87. Let \( f \) be a bijection from the set \( A \) to the set \( B \). The **inverse function** of \( f \) is the function that assigns to an element \( b \in B \) the unique element \( a \in A \) such that \( f(a) = b \). The inverse function of \( f \) is denoted \( f^{-1} \), and we thus write

\[
 f^{-1}(b) = a \iff f(a) = b.
\]
How is this different from the previous definition of inverse? Note that in the previous definition, \( f^{-1} \) is defined on a set, and outputs a set (which may be the empty set, a singleton set, or neither). Also in the previous definition, \( f \) is not necessarily a bijection and so is not necessarily one-to-one (or onto). This means that \( f^{-1} \) is not necessarily a function because \( |f^{-1}(\{y\})| \geq 2 \). In this new definition, we know \( f^{-1} \) is indeed a function, so we may call it the inverse function.

**Problem 2.88.** Prove that if \( f \) is a bijection, \( f^{-1} \) is a bijection.

**Definition 2.89.** Let \( g : A \rightarrow B \) be a function and let \( f : B \rightarrow C \) be a function. The composition of the functions \( f \) and \( g \), \( f \circ g : A \rightarrow C \), is defined by \((f \circ g)(a) = f(g(a))\) for every \( a \in A \).

**Exercise 2.90.** Is \( \circ \) a commutative operation on functions?

**Problem 2.91.** Let \( f : B \rightarrow C \) and \( g : A \rightarrow B \) be functions. Show that if \( f \) and \( g \) are one-to-one then \( f \circ g \) is one-to-one.

**Problem 2.92.** Let \( f : B \rightarrow C \) and \( g : A \rightarrow B \) be functions. Show that if \( f \) and \( g \) are onto then \( f \circ g \) is onto.

**Problem 2.93.** Let \( f : B \rightarrow C \) and \( g : A \rightarrow B \) be functions. Show that if \( f \circ g \) is one-to-one, then \( g \) is one-to-one.

**Problem 2.94.** Let \( f : B \rightarrow C \) and \( g : A \rightarrow B \) be functions. Show that if \( f \circ g \) is onto, then \( f \) is onto.

### 2.4 Cardinality - Different-Sized Infinites

We start by recalling our prior definition of cardinality, given in Definition 2.29: Let \( S \) be a set. If there are exactly \( n \) distinct elements in \( S \) where \( n \) is a nonnegative integer, we say that \( S \) is a finite set and that \( n \) is the cardinality of \( S \). The cardinality of \( S \) is denoted by \( |S| \).

We now give a more general definition of cardinality that will yield the same definition as above if the two sets \( A \) and \( B \) are finite.

**Definition 2.95.** The sets \( A \) and \( B \) have the same cardinality if and only if there exists a bijection from \( A \) to \( B \).

**Definition 2.96.** A set that is either finite or has the same cardinality as \( \mathbb{Z}^+ \) is called countable. A set that is not countable is called uncountable. When an infinite set \( S \) is countable, we denote its cardinality by \( \aleph_0 \) and write \( |S| = \aleph_0 \) (read as aleph nought or aleph null - aleph is the first letter of the Hebrew alphabet; note its similarity to the Greek letter “alpha”). Also, we often call a countable, infinite set countably infinite to distinguish it from finite and countable.

**Example 2.97.** \(|\{x \in \mathbb{Z} : x = 2k \text{ for some integer } k, -5 \leq x \leq 5\}| = 5\). Since the set is finite, it is countable.
The fundamental difference between countable and uncountable can be encapsulated in the question, "Can you list them?" i.e., is there a way to pick a “first” element and then know what the “next” element is following a clear pattern that will guarantee you hit them all? If our set is $\mathbb{Z}^+$ or $\mathbb{N}$, this is obvious because there is a clear “first” element and a clear way to get from one element to the next until you’ve hit them all (start with 0 or 1 and count up). Using this intuitive understanding of countable, it should seem obvious that the set of even positive integers is countable as well since we can start counting at 2 and count up by twos: $2, 4, 6, \ldots$. But, let’s think about what else this is saying, according to the definition of “countable”: that $\mathbb{Z}^+$ is the same cardinality as the set $S$ of even positive numbers, or there are as many even positive integers as there are positive integers. This should seem counterintuitive since $S \subset \mathbb{Z}^+$. This is the nature of sets of infinite size, and we illustrate this with the following metaphor, known as Hilbert’s Hotel Infinity.

The following excerpt is taken from Wikipedia:

“Consider a hypothetical hotel with countably infinitely many rooms, all of which are occupied - that is to say every room contains a guest. One might be tempted to think that the hotel would not be able to accommodate any newly arriving guests, as would be the case with a finite number of rooms.

Suppose a new guest arrives and wishes to be accommodated in the hotel. Because the hotel has infinitely many rooms, we can move the guest occupying room 1 to room 2, the guest occupying room 2 to room 3 and so on, and fit the newcomer into room 1. By repeating this procedure, it is possible to make room for any finite number of new guests.

It is also possible to accommodate a countably infinite number of new guests: just move the person occupying room 1 to room 2, the guest occupying room 2 to room 4, and in general room $n$ to room $2n$, and all the odd-numbered rooms will be free for the new guests.”

Example 2.98. We now prove that the set of even positive integers is indeed countable. There are several steps to a proof of this kind. First, we must note that it is an existence proof because we are asked to show that there exists a bijection between $\mathbb{Z}^+$ and the set of even positive integers. So, we will use a constructive proof and produce the function, and prove it is a bijection. Note that the bijection can go in either direction, but once you have a bijection $f$ in one direction you will automatically have a bijection in the other direction by taking the inverse of $f$.

Finding the function is often the hardest part. To begin with, we will express the set in question using set-builder notation: $S = \{2k : k \in \mathbb{Z}^+\}$. This actually gives us a hint as to how we will define our function. We need to pair all the elements of $S$ with all the elements of $\mathbb{Z}^+$ in a one-to-one way. The diagram below represents the pairings we will make. We use this diagram to find a formula for the function we will use.

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & \ldots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
2 & 4 & 6 & 8 & 10 & \ldots 
\end{array}
\]

Proof: Let $f : \mathbb{Z}^+ \rightarrow S$ be defined by $f(k) = 2k$. We now need to show two things:
1. \( f \) does indeed have codomain \( S \) as we claim. In other words, we must prove that when applying \( f \) to elements of the set \( S \), the outputs can only be even positive integers since those are the only elements of \( S \).

2. \( f \) is a bijection.

We start with (1). We need to show that the output of our function \( f \) will always be in set \( S \), i.e. it will always be an integer, will always be even, and will always be positive (and since it must be even, this will mean \( \geq 2 \)). Since \( k \in \mathbb{Z}^+ \), it is an integer so \( 2k \) is also an integer by axiom 2. Also, \( 2k \) is even by definition of even. Lastly, since \( k \geq 1 \), \( 2k \geq 2 \).

We now show that \( f \) is a bijection. We start with one-to-one:

Suppose that \( f(x) = f(y) \). Then \( 2x = 2y \) so \( x = y \) and so \( f \) is one-to-one.

We now show \( f \) is onto:

Let \( y \in S \), and let \( x = \frac{y}{2} \). Then \( f(x) = f(\frac{y}{2}) = 2(\frac{y}{2}) = y \). Also, since \( y \in S \), \( y = 2k \) for some \( k \in \mathbb{Z}^+ \). Thus \( x = \frac{y}{2} = \frac{2k}{2} = k \in \mathbb{Z}^+ \), i.e. \( x \in \mathbb{Z}^+ \) (which is one of the properties that \( x \) must have).

Thus, \( f \) is a bijection from \( \mathbb{Z}^+ \) to \( S \), the set of even positive integers, and so \( |\mathbb{Z}^+| = |S| \) and \( S \) is countable.

**Problem 2.99.** Prove that the set of negative odd integers is countable.

**Problem 2.100.** Prove that the set of nonnegative (includes 0) even integers is countable.

**Problem 2.101.** Let \( S = \{ x \in \mathbb{N} : x = 3k \text{ for some } k \in \mathbb{Z}, x \geq 6 \} \). Prove that \( |S| = \aleph_0 \).

For some sets, it is not so obvious that there is a way to list them such that there is a “first” element and then a clear way to get the “next” element, for example, \( \mathbb{Z} \). What would be our “first” element? Can we conclude that this set is not countable because it is not obvious how to start? Hopefully you said, “No!” So, to prove that \( \mathbb{Z} \) is indeed countable, we go to the definition of countable and find a bijection from \( \mathbb{Z}^+ \to \mathbb{Z} \) or from \( \mathbb{Z} \to \mathbb{Z}^+ \).

**Example 2.102.** Prove that \( \mathbb{Z} \) is countable.

We need to pair all the elements of \( \mathbb{Z} \) with all the elements of \( \mathbb{Z}^+ \) in a one-to-one way. It is not at all obvious how to pick the “first” element, i.e. the image of 1 under the bijection \( f \) we will produce. The technique we use in the following is standard. We pick 0 as the “starting point”, then go up to 1, back to -1, up to 2, back to -2, up to 3, etc., or in other words, we list the elements of \( \mathbb{Z} \) as \{0, 1, -1, 2, -2, 3, -3, \ldots \}. We represent this in the diagram below.

```
1  2  3  4  5  . . .
. . . -2 -1  0  1  2 . . .
```
To prove that this works, we of course must find a bijection \( f : \mathbb{Z}^+ \to \mathbb{Z} \) (or \( \mathbb{Z} \to \mathbb{Z}^+ \)) and prove it is such, but as we have just demonstrated a way to list the elements of \( \mathbb{Z} \), this should be easy. We want the first element to be 0, so \( f(1) = 0 \), the second element to be 1, so \( f(2) = 1 \), the third element to be \(-1\), so \( f(3) = -1 \), etc. Now how do we express this as a formula? We note that odd numbers get sent to nonpositive numbers, and even numbers get sent to positive numbers; thus, there are two different formulas at play. In other words, \( f \) must be a piecewise-defined function.

\[
f(x) = \begin{cases} 
0 & \text{if } x \text{ is even} \\
1 & \text{if } x \text{ is odd}
\end{cases}
\]

**Problem 2.103.** Find the formula for the even inputs in the piecewise function defined above, and prove that it is a bijection between the set of even positive integers and the positive integers.

**Problem 2.104.** Find the formula for the odd inputs in the piecewise function defined above, and prove that it is a bijection between the set of odd positive integers and the nonpositive integers.

**Problem 2.105.** Let \( S = \{2k + 1 : k \in \mathbb{Z}\} \). Find a bijection between \( \mathbb{Z}^+ \) and \( S \) (you do not have to prove that it is a bijection, just find the function).

There is one more important set that is countable, which is the set of rational numbers \( \mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}\} \). We address this in the next example.

**Example 2.106.** It may seem counterintuitive that the rationals are a countable set, but to prove this we simply need to come up with a way to “list” the rational numbers. Recall that this means we must pick a “first” element and then demonstrate a way to get to the next one. We first start by considering only the positive rational numbers, which we show in the diagram below. Note that each row represents a fixed denominator and each column represents a fixed numerator.

We start at the upper left-hand corner, which is \( \frac{1}{1} \), and follow the direction of the arrows. This tells us what the first element is (\( \frac{1}{1} \)), and the arrows tell us how to get to the next element. There is one small flaw in this argument, which is that this function as it currently is would not be one-to-one and therefore not a bijection, because note that the image of 1 is \( \frac{1}{1} \), which is also the image of 5 (the fifth number on the list) since \( \frac{2}{2} = 1 \), for example (can you find other repeats?). But, we can avoid this issue by simply skipping a number if it represents one that has already been counted. Thus, the list would start as follows: \( \{1, \frac{1}{2}, 2, 3, \frac{1}{3}, 1, \frac{2}{3}, \frac{3}{2}, 4, \ldots\} \). To write a formula down expressing this function, and then to prove that it is indeed a bijection, is more involved than we care to get here. But, it is probably not too difficult to
convince yourself that every positive rational number will be hit in this list. Of course, we are not done, because we must list the negative rational numbers and 0, but we can simply use the technique of the previous example (when we found a bijection between \( \mathbb{Z} \) and \( \mathbb{Z}^+ \)) to acquire these missing values.

**Exercise 2.107.** Use the idea from the above example to describe a way of listing the set of ordered pairs with integer entries; that is, the set \( S = \{(a, b) : a, b \in \mathbb{Z}\} \).

**Example 2.108.** The last set we discuss in this section is \( \mathbb{R} \), the real numbers. If it seems that this set must be uncountable, you are correct. We prove this now using what is known as the Cantor diagonalization argument. We will actually show that just the interval \((0, 1)\) is uncountable, which is an even stronger statement, and the argument below can be extended to the entire set of real numbers.

**Proof:** By contradiction: suppose that the interval \((0, 1)\) is a countable set. Then we can list all the elements of this interval, which we do below. We describe them in terms of their decimal expansions.

\[
\begin{align*}
n_1 & : 0.d_{11}d_{12}d_{13}d_{14} \ldots d_{1k} \ldots \\
n_2 & : 0.d_{21}d_{22}d_{23}d_{24} \ldots d_{2k} \ldots \\
n_3 & : 0.d_{31}d_{32}d_{33}d_{34} \ldots d_{3k} \ldots \\
n_4 & : 0.d_{41}d_{42}d_{43}d_{44} \ldots d_{4k} \ldots \\
\end{align*}
\]

etc.

where each \( d_{ij} \) is a decimal digit between 0 and 9. (Note that if the number has a finite decimal expansion, all the \( d_{ij} \) after the end of its expansion will just be 0, e.g. \( 0.5 = 0.500000 \ldots \))

We now build a number \( n \) as follows:

1. Take the “diagonal” element of each \( n_i \), i.e. \( d_{11}, d_{22}, \ldots, d_{kk}, \ldots \), and put them together as \( 0.d_{11}d_{22}d_{33} \ldots d_{kk} \ldots \)

2. Now for each \( d_{ii} \), if it isn’t already a 5, change it to a 5, and if it is already a 5, change it to a 6.

We see that this new number \( n \) cannot be equal to any of the ones on the list, because it differs from \( n_k \) in the \( k \)th spot (since we originally took the \( k \)th spot’s digit from \( n_k \) but then changed it). We have thus created another real number that is not on the list, which is a contradiction since we said this was a list of all the real numbers in the interval \((0, 1)\), which we must have if \((0, 1)\) is countable. Thus, the interval \((0, 1)\) is not countable (which in turns makes the entire set of real numbers uncountable).

A natural question one might think of, is “countable” the smallest-sized infinity, and is there any size between countable and uncountable? It is fairly straightforward to show that \( \aleph_0 \) is indeed the smallest infinity that is possible. However, the second question, which can be rephrased as, \( |\mathbb{R}| = \aleph_1 \) (i.e is the cardinality of the real numbers the next largest cardinality after the cardinality of the positive integers), is not as simple to answer. It can be shown that it is impossible to prove that this statement is true and impossible to prove it is false! The statement \( |\mathbb{R}| = \aleph_1 \) is called the continuum hypothesis (CH), and is one of math’s greatest intrigues. In 1940, it was proved that the CH cannot be disproved, and in 1963, it was proved that the CH cannot be proved. So what to do? Most modern mathematics today assumes the continuum hypothesis as an axiom, but there is a branch of mathematics that explores the possibilities if this is not assumed to be true.
3 Induction

3.1 Sequences and Summations

Definition 3.1. A sequence is a function from a subset of the set of integers (usually either the set \{0, 1, 2, 3, \ldots\} or \{1, 2, 3, 4, \ldots\}) to a set \(S\). We use the notation \(a_n\) to denote the image of the integer \(n\). We call \(a_n\) a term of the sequence, and we denote the sequence \((a_n)\). It is usually assumed to start at \(n = 1\) unless otherwise noted.

Example 3.2. The sequence \((a_n)\) given by \(a_n = \frac{1}{n^2}\) is the sequence \(a_1, a_2, a_3, a_4, \ldots\) or \(\frac{1}{1}, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \ldots\).

Definition 3.3. A geometric progression or geometric sequence is a sequence of the form \((ar^k) = a, ar, ar^2, ar^3, \ldots\) where \(a, r\) are real numbers, \(a\) is the initial term, and \(r\) is the common ratio. Observe that \(a = ar^0\), so \(a_0 = a, a_1 = ar, a_2 = ar^2, \) etc. Geometric sequences are usually assumed to start at 0.

Example 3.4. Consider \((a_n) = (\frac{1}{2}(3^n)), (b_n) = (3(-2)^n),\) and \((c_n) = (3(\frac{1}{2})^n)\).

\[(a_n) = \frac{1}{2}, \frac{3}{2}, \frac{9}{2}, \frac{27}{2}, \frac{81}{2}, \ldots\]
\[(b_n) = 3, -6, 12, -24, 48, -96, \ldots\]
\[(c_n) = 3, -\frac{3}{2}, -\frac{3}{4}, \frac{3}{8}, \frac{3}{16}, \ldots\]

Observe: \(\frac{a_{n+1}}{a_n} = \frac{ar^{n+1}}{ar^n} = \frac{r^{n+1}}{r^n} = r\), i.e. dividing any term by the previous one should yield the common ratio \(r\).

Example 3.5. Find a formula for the sequence given by \(-4, 20, -100, 500, -2500, \ldots\).

Observe that \(\frac{a_{n+1}}{a_n} = -5\) for any \(a_n, a_{n+1}\) you pick and the first term is \(-4 = -4(5^0)\), so \(a_n = -4(-5)^n\).

How about \(\frac{4}{5}, -4, 20, -100, 500, \ldots\) Notice we still have that \(\frac{a_{n+1}}{a_n} = -5\), but this sequence starts one term “earlier” than the other. We can thus express this as \(b_n = -4(-5)^{n-1}\), or \(b_n = \frac{4}{5}(-5)^n\).

Summations

Definition 3.6. Summation- or \(\Sigma\)-notation tells us to add the terms. \(\Sigma\) is the Greek letter sigma (capital) and so \(\Sigma\)-notation is also read “sigma notation”. We write

\[\sum_{i=m}^{n} a_i = a_m + a_{m+1} + a_{m+2} + \cdots + a_n,\] where \(i\) is the index.

We can think of the index “\(i\)” as the “counter”, and we can of course use any letter we would like for the index. \(i, j,\) and \(k\) are all common choices.
Example 3.7. Consider the following sums:

\[
\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n
\]
\[
\sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \cdots + n^2
\]
\[
\sum_{i=1}^{6} i^2 = 1 + 4 + 9 + 16 + 25 + 36 = 91
\]
\[
\sum_{i=2}^{6} i^2 = 4 + 9 + 16 + 25 + 36 = 90 = \sum_{i=1}^{5} (j+1)^2 \quad \text{(change of index, } j = i - 1)\]
\[
\sum_{i=1}^{6} 4 = 4 + 4 + 4 + 4 + 4 + 4 = 6(4) = 24
\]

Exercise 3.8. Compute the following sums:
\[
\sum_{i=1}^{10} i, \sum_{i=1}^{10} i^2, \sum_{i=1}^{5} 2i^3, \sum_{i=4}^{10} \frac{1}{i}
\]

Exercise 3.9. Explain the difference, if you believe there is any, between \(\sum_{i=1}^{n} a_i + k\) and \(\sum_{i=1}^{n} (a_i + k)\).

Exercise 3.10. Come up with a formula for the sum \(\sum_{i=1}^{n} k\), where \(k\) is a constant.

What if we want to compute \(\sum_{i=1}^{100} i\)? This is much more computation than we care to do! So instead, we are lucky enough to have the following formulas:

Theorem 3.11. \(\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}\)
\(\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}\)
\(\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}\)

We will prove these later using the proof technique of induction, which follows the discussion of sums.

Example 3.12. Consider the following sums:
\[
\sum_{i=1}^{100} i = \frac{(100)(101)}{2} = (50)(101) = 5050
\]
\[
\sum_{i=1}^{100} i^2 = \frac{(100)(101)(201)}{6} = (50)(101)(67) = 338,350
\]
\[
\sum_{i=1}^{100} i^3 = \frac{(10000)(101)^2}{4} = (2500)(101)^2 = 25,502,500
\]

**Theorem 3.13.** \(\sum_{i=m}^{n} (a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=m}^{n} b_i.\)

**Proof:** We see that
\[
\sum_{i=m}^{n} (a_i + b_i) = (a_m + b_m) + (a_{m+1} + b_{m+1}) + \cdots + (a_n + b_n)
\]
by definition of \(\Sigma\)
\[
= a_m + b_m + a_{m+1} + b_{m+1} + \cdots + a_n + b_n
\]
by the associative property of addition
\[
= a_m + a_{m+1} + \cdots a_n + b_m + b_{m+1} + \cdots + b_n
\]
by the commutative property of addition
\[
= (a_m + a_{m+1} + \cdots a_n) + (b_m + b_{m+1} + \cdots + b_n)
\]
by the associative property of addition
\[
= \sum_{i=m}^{n} a_i + \sum_{i=m}^{n} b_i
\]
by definition of \(\Sigma\)

\(\blacksquare\)

**Problem 3.14.** Prove that \(\sum_{i=m}^{n} c(a_i) = c \sum_{i=m}^{n} a_i.\)

**Problem 3.15.** Use the results (not the technique) of Theorem 3.13 and Problem 3.14 to prove that
\[
\sum_{i=m}^{n} (a_i - b_i) = \sum_{i=m}^{n} a_i - \sum_{i=m}^{n} b_i.
\]

**Problem 3.16.** 1. Use sum formulas from Theorem 3.11 along with the results of Theorem 3.13, Exercise 3.10 and Problems 3.14 and 3.15 to evaluate \(\sum_{k=1}^{20} (3k^2 - 2k + 4).\)

2. Now find \(\sum_{k=5}^{20} (3k^2 - 2k + 4)\) using your result from (1).

**Problem 3.17.** Prove or disprove the following:

1. \(\sum_{i=m}^{n} a_i b_i = \sum_{i=m}^{n} a_i \sum_{i=m}^{n} b_i\)

2. \(\sum_{i=m}^{n} \frac{a_i}{b_i} = \frac{\sum_{i=m}^{n} a_i}{\sum_{i=m}^{n} b_i}\)

**Definition 3.18.** A geometric series is one of the form \(\sum_{k=0}^{n} a(r^k) = a + ar + ar^2 + \cdots + ar^n.\)

Note that the terms being added are those of the geometric sequence.
**Theorem 3.19.** If \(a\) and \(r\) are real numbers and \(r \neq 0\), then
\[
\sum_{k=0}^{n} ar^k = \begin{cases} 
  a \left( \frac{r^{n+1} - 1}{r - 1} \right) & \text{if } r \neq 1 \\
  a(n + 1) & \text{if } r = 1
\end{cases}
\]

Proof: We first consider the case where \(r = 1\). Then \(ar^k = a\) for all values of \(k\), so the summation
\[
\sum_{k=0}^{n} a(r^k) = \sum_{k=0}^{n} a = a + a + a + \cdots + a
\]
which is the sum of \(n + 1\) copies of \(a\), or \(a(n + 1)\).

We now consider the case where \(r \neq 1\).

Let \(S = \sum_{j=0}^{n} ar^j\). We perform the following algebraic operations:
\[
rS = r \sum_{j=0}^{n} ar^j \\
= \sum_{j=0}^{n} rar^j \text{ by Problem 3.14} \\
= \sum_{j=0}^{n} ar^{j+1} \text{ commutative law for multiplication, exponent rule} \\
= \sum_{k=1}^{n+1} ar^k \text{ (change of index, } k = j + 1) \\
= \sum_{k=0}^{n} ar^k + ar^{n+1} - a \text{ (removing } k = n + 1 \text{ term from the summation and adding } k = 0 \text{ term to it)} \\
= S + a(r^{n+1} - 1) \text{ since } S = \sum_{j=0}^{n} ar^j = \sum_{k=0}^{n} ar^k \text{ (name of index doesn’t matter)}
\]
This yields \(rS = S + a(r^{n+1} - 1)\). We then solve for \(S\) in this equation to obtain
\[
S = a \left( \frac{r^{n+1} - 1}{r - 1} \right) \text{ (observe that since } r \neq 1 \text{ we are allowed to divide by } r - 1). \]
\[
\]
We will prove this theorem another way when we learn induction.

**Example 3.20.** Compute \(\sum_{i=2}^{20} 5(-2)^i\).
\[
\sum_{i=2}^{20} 5(-2)^i = \sum_{i=0}^{20} 5(-2)^i - 5 - (-10) \text{ (rewrite starting at 0 so formula will apply)} \\
= 2 \left( \frac{(-2)^{21} - 1}{-2 - 1} \right) - 5 + 10 \\
= 2(699051) + 5
\]

43
Exercise 3.21. Compute $\sum_{i=5}^{45} 3 \left( -\frac{1}{2} \right)^i$.

Double Sums

Definition 3.22. A double sum is a sum of the form $\sum_{i=n_0}^{n} \sum_{j=m_0}^{m} a_{ij}$, where $a_{ij}$ is a term in terms of $i$ and $j$, $n_0, m_0, n, m \in \mathbb{N}$, and $n_0 \leq n, m_0 \leq m$. Usually, $m_0$ and $m_0$ are 1 or 0, but they don’t have to be. We can interpret this sum in two ways (considering $n_0$ and $m_0$ to be 1 here for simplicity’s sake):

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{i=1}^{n} (a_{i_1} + a_{i_2} + \cdots + a_{im}) \quad \text{or} \quad \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m} a_{1j} + \sum_{j=1}^{m} a_{2j} + \cdots + \sum_{j=1}^{m} a_{nj}.$$

Problem 3.23. Show that the two representations of $\sum_{i=n_0}^{n} \sum_{j=m_0}^{m} a_{ij}$ in the above definition are the same.

Problem 3.24. Compute the following double sums:

1. $\sum_{i=1}^{5} \sum_{j=2}^{4} \frac{i}{j}$

2. $\sum_{i=1}^{100} \sum_{j=1}^{25} ij$ (Hint: use a formula.)

3.2 Induction

Mathematical induction is a technique of proof that we use when we want to prove a statement holds for every positive integer or every member of a countable set in general. We often think of this as a generalization of showing we can knock down a stack of dominoes no matter how long the stack is. We do this using the following procedure:

(1) Show that you can knock down the first domino.

(2) Show that if you assume you can knock down the $k$th domino for $k \geq 1$ you can knock down the next one, which is the $(k+1)$st domino.

Notice that since I can knock down the first one, (2) tells me that I can knock down the second one. Now that I know I can knock down the second one, (2) tells me I can knock down the third one, and so on. Now, how do we say this mathematically?
Definition 3.25. **Induction**

Suppose we have a mathematical statement \( P(n) \) that we would like to show is true for every positive integer \( n \). We perform the following steps:

1. Show \( P(1) \) is true (Base case or Basis step).
2. Show that \( P(k) \rightarrow P(k+1) \) for all \( k \geq 1 \) (Inductive Step. \( P(k) \) is called the induction hypothesis).

**Example 3.26.** Show that for all \( n \geq 1 \), \( \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \).

**Proof:**

**Base Case:** \( P(1) \)

\[ 1 = \frac{1 \cdot 2}{2} \checkmark \]

**Inductive Step:** Suppose that \( P(k) \) is true for \( k \geq 1 \), i.e. \( 1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2} \) (induction hypothesis), and show \( 1 + 2 + 3 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2} \) (the original statement for \( n = k+1 \)).

We start on the left side and show that we get the right:

\[
1 + 2 + 3 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) \text{ by induction hypothesis (i.e. we replaced the first } k\text{ terms)}
\]

\[
= \frac{k(k+1) + 2(k+1)}{2}
\]

\[
= \frac{k^2 + 3k + 2}{2}
\]

\[
= \frac{(k+1)(k+2)}{2}
\]

Thus, we have shown by induction that for all \( n \geq 1 \), \( \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \).

\[ \blacksquare \]

**Problem 3.27.** Show that \( \sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \) for all \( n \in \mathbb{Z}^+ \).

**Problem 3.28.** Show that \( \sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4} \) for all \( n \in \mathbb{Z}^+ \).

**Problem 3.29.** Use induction to show that if \( a \) and \( r \) are real numbers and \( r \neq 0 \), then

\[
\sum_{i=0}^{n} ar^i = a \left( \frac{r^{n+1} - 1}{r - 1} \right) \text{ if } r \neq 1. \text{ (Careful: note that your base case here must be } n = 0, \text{ not } 1. \)
**Problem 3.30.** If $n$ is a natural number, then \( 2 \cdot 6 \cdot 10 \cdot 14 \cdot \cdots \cdot (4n - 2) = \frac{(2n)!}{n!} \).

**Problem 3.31.** Suppose $x$ is a real number greater than $-1$. Use induction to show that if $n$ is a natural number, then \( (1 + x)^n \geq 1 + nx \).

**Notation:** When we would like to take a union or an intersection of more than two sets (say, $n$) we use a shorthand notation similar to that of $\Sigma$-notation. Consider the following expressions:

\[
A_1 \cup A_2 \cup \cdots \cup A_n \\
A_1 \cap A_2 \cap \cdots \cap A_n
\]

Note that this expression makes sense even without parentheses because of the associative law. We now combine these into one symbol as follows:

\[
\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \\
\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n
\]

Of course, the index does not have to be “$i$”; it can be anything.

**Example 3.32.** Prove the following generalization of DeMorgan’s Law:

\[
\bigcup_{j=1}^{n} A_j = \bigcap_{j=1}^{n} \overline{A_j}
\]

where $A_1, A_2, \ldots, A_n$ are subsets of a universal set $U$ and $n \in \mathbb{Z}^+$. 

**Proof:** Base case:

\[
\bigcup_{j=1}^{1} A_j = (\overline{A_1}) = \overline{A_1} = \bigcap_{j=1}^{1} \overline{A_j}
\]

**Inductive Step**

Suppose that \( \bigcup_{j=1}^{k} A_j = \bigcap_{j=1}^{k} \overline{A_j} \) for $k \geq 1$. Then

\[
\bigcup_{j=1}^{k+1} A_j = \bigcup_{j=1}^{k} A_j \cup A_{k+1} \quad \text{(split off the last set $A_{k+1}$)}
\]

\[
= \bigcup_{j=1}^{k} A_j \cap \overline{A_{k+1}} \quad \text{by DeMorgan’s Law}
\]

46
\[ \bigcap_{j=1}^{k} A_j \cap A_{k+1} \] by the induction hypothesis

\[ = \bigcap_{j=1}^{k+1} A_j \] (recombine into one big intersection)

Exercise 3.33. Prove the following “other” generalization of DeMorgan’s Law:

\[ \bigcap_{j=1}^{n} A_j = \bigcup_{j=1}^{n} \overline{A_j} \]

where \( A_1, A_2, \ldots, A_n \) are subsets of a universal set \( U \) and \( n \in \mathbb{Z}^+ \).

Problem 3.34. Prove the following generalization of (one of) the distributive law(s) for sets:

\[ \bigcup_{j=1}^{n} A_j \cap B = \bigcup_{j=1}^{n} (A_j \cap B) \], where \( A_1, A_2, \ldots, A_n, B \) are sets and \( n \in \mathbb{Z}^+ \).

Problem 3.35. Prove the following generalization of the other distributive law for sets:

\[ \bigcap_{j=1}^{n} A_j \cup B = \bigcap_{j=1}^{n} (A_j \cup B) \], where \( A_1, A_2, \ldots, A_n, B \) are sets and \( n \in \mathbb{Z}^+ \).

Definition 3.36. Strong Induction This is a technique of induction very similar to standard induction, but it is stronger, and we only call on it when needed. Suppose we have a mathematical statement \( P(n) \) that we would like to show is true for every positive integer \( n \). We perform the following steps:

1. Show \( P(1) \) is true (Base case or Basis step)
2. Show that \( \forall j(j \leq k \land P(j)) \rightarrow P(k+1) \) for all \( k > 1 \) (i.e. assume \( P \) holds for ALL positive integers less \( j \) with \( 1 \leq j \leq k \)).

We will revisit this in the next section.
4 The Integers and Division

4.1 The Division Algorithm

Definition 4.1. If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ divides $b$ if there is an integer $c$ such that $b = ac$. When $a$ divides $b$ we say that $a$ is a factor of $b$ and that $b$ is a multiple of $a$. The notation $a|b$ denotes that $a$ divides $b$ and we write $a \not| b$ when $a$ does not divide $b$.

Example 4.2. 5|−1? No, there is no integer $c$ such that $−1 = 5c$.
5|−10? Yes, $−10 = (5)(−2)$ ($c = −2$).
5|0? Yes, $0 = (5)(0)$ ($c = 0$).

CAREFUL: $a|b$ is a proposition; $\frac{a}{b}$ is a noun (a number). $a|b$ has a truth value, $\frac{a}{b}$ does not.

Theorem 4.3. Let $a$, $b$, and $c$ be integers. If $a|b$ then $a|bc$ for any integer $c$.

Proof: Let $a$, $b$ be integers such that $a|b$. Then there exists an integer $s$ such that $b = as$. Let $c$ be any integer. Multiplying both sides by $c$ yields $bc = asc = a(sc)$. Since $s, c$ are integers, $sc$ is an integer by Axiom 2 so $a|bc$ by definition of “divides”.

Problem 4.4. Prove that for integers $a, b$, and $c$, if $a|b$ and $a|c$ then $a|(b + c)$.

Problem 4.5. Prove that for integers $a, b$, and $c$, if $a|b$ and $b|c$ then $a|c$.

Problem 4.6. Use the results from above to prove that if $a, b, c$ are integers such that $a|b$ and $a|c$, then $a|(mb + nc)$ for any integers $m$ and $n$.

Problem 4.7. Prove that if $a, b, c, d$ are integers such that $a|c$ and $b|d$, then $ab|cd$.

Problem 4.8. Use induction to prove that $3|(n^2 + 2n)$ for all $n \in \mathbb{Z}^+$.

Problem 4.9. Use induction to prove that $57|(7^{n+2} + 8^{2n+1})$ for all $n \in \mathbb{N}$.

Theorem 4.10. The Division Algorithm

Let $a$ be an integer and $d$ be a positive integer. Then there are unique integers $q$ and $r$ with $0 \leq r < d$ such that $a = dq + r$.

We will not prove this here.

Definition 4.11. In the division algorithm equation, $d$ is the divisor, $a$ is the dividend, $q$ is the quotient, and $r$ is the remainder. We write $r = a \text{ mod } d$.

Example 4.12. 38 = (5)(7) + 3 so $r = 3 = 38 \text{ mod } 5$

$20 = (5)(4) + 0$ so $20 \text{ mod } 4 = 0$ and $20 \text{ mod } 5 = 0$

$−24 = (5)(−5) + 1$ so $−24 \text{ mod } 5 = 1$ (note must have $r \geq 0$)

$5 = (38)(0) + 5$ so $5 \text{ mod } 38 = 5$ (note must have $r < 38$)
**Exercise 4.13.** Find the the following:

1. $13 \mod 10$
2. $10 \mod 13$
3. $-13 \mod 10$

**Theorem 4.14.** $d|a$ if and only if $r = 0$ when $a$ is divided by $d$ according to the division algorithm (i.e. $a \mod d = 0$).

**Proof:**

$\Rightarrow$ Show that if $d|a$, then $r = 0$ when $a$ is divided by $d$ according to the division algorithm.

Let $a, d$ be integers with $d > 0$. Suppose $d|a$. Then $a = dq$ for some integer $q$, so $a = dq + 0$ and since this is in the form of the division algorithm ($0 \leq r < d$) and this form is unique, $r = 0$.

$\Leftarrow$ Show that if $r = 0$ when $a$ is divided by $d$ according to the division algorithm, then $d|a$.

Suppose that $a, d$ are integers with $d > 0$ and $a = dq + 0$ for some integer $q$ according to the division algorithm. Then $a = dq$ for an integer $q$ so $d|a$.

---

**Modular Arithmetic**

**Definition 4.15.** If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $m$ if $m$ divides $a − b$. We use the notation $a \equiv b \pmod{m}$ and usually say “$a$ is congruent to $b$ modulo $m$”. If $a$ and $b$ are not congruent modulo (mod) $m$, we write $a \not\equiv b \pmod{m}$.

**Exercise 4.16.** Show that for all $n \in \mathbb{Z}$ with $n \neq 0$, $n|0$.

**Theorem 4.17.** Let $m \in \mathbb{Z}^+$ and $d \in \mathbb{Z}$. If $-m < d < m$ and $m|d$, then $d = 0$.

**Proof:** By contradiction. Suppose that $d \neq 0$. Since $m|d$, $d = km$ for some $k \in \mathbb{Z}$ and $k \neq 0$ since $d \neq 0$.

Then because $k \in \mathbb{Z}$, $|k| \geq 1$ so $|d| = |km| \geq m$. But this contradicts that $-m < d < m$, thus $d = 0$.

**Theorem 4.18.** Let $a$ and $b$ be integers and let $m$ be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

**Proof:** ($\Leftarrow$) If $a \mod m = b \mod m$, then $a \equiv b \pmod{m}$.

Let $a, b, m$ be integers with $m > 0$, and suppose that $a \mod m = b \mod m$. Then by definition of $a \mod m$, $a = mq + r$ and $b = mp + r$ with $p, s, r$ integers and $0 \leq r < m$ (same $r$ for both by supposition). Then $a − mq = r = b − mp$. Rearranging gives $a − b = m(q − p)$. Since $q$ and $p$ are integers, $q − p$ is an integer by Axiom 2, so $m|a − b$. Thus $a \equiv b \pmod{m}$ by definition of congruence mod $m$.

($\Rightarrow$) If $a \equiv b \pmod{m}$, then $a \mod m = b \mod m$.

Let $a, b, m$ be integers with $m > 0$, and suppose that $a \equiv b \pmod{m}$. Then $m|a − b$ by definition of congruence mod $m$. We can divide $a$ and $b$ by $m$ according to the division algorithm to obtain $a = qm + r$ where $q, r \in \mathbb{Z}, 0 \leq r < m$ and $b = pm + s$ where $p, s \in \mathbb{Z}$, $0 \leq s < m$. Our goal is to show $r = s$.

Subtracting the two equations yields $a − b = qm + r − (pm + s)$, or $a − b = (q − p)m + r − s$. We can
Suppose $r = s$ or vice versa, making $|r - s| < m$, or $-m < r - s < m$. But $m|(r - s)$, so by Theorem 4.17, $r - s = 0$. Thus $r = s$, and since $r = a \mod m$ and $s = b \mod m$, $a \mod m = b \mod m$. 

**Example 4.19.** $29 \equiv 7 \pmod{3}$: $29 = 3(9) + 2$ and $7 = 3(2) + 1$, so no, since $2$ is even. 

**Exercise 4.20.** Use Theorem 4.18 to determine if the following hold:

1. $51 \equiv 8 \pmod{11}$
2. $51 \equiv -8 \pmod{11}$
3. $151 \equiv 19 \pmod{11}$
4. $1005 \equiv 361 \pmod{14}$

Verify your answers using the definition of congruence mod $m$.

**Example 4.21.** Show that if $n$ is an odd integer, then $n^2 \equiv 1 \pmod{8}$.

**Proof:** Let $n$ be an odd positive integer. Then $n = 2k + 1$ for some integer $k$ and so $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$.

**Case 1:** Suppose $k$ is even. Then $k = 2l$ for some integer $l$ so $n^2 = 4(2l)(2l + 1) + 1 = 8(2l^2 + 2l + 1)$. $2l^2 + 2l + 1$ is an integer by Axiom 2 since it is an integer, and so $n^2 \equiv 1 \pmod{8}$ according to the division algorithm.

**Case 2:** Suppose $k$ is not even. Then $k$ is odd by Axiom 1, meaning $k = 2l + 1$ for some integer $l$. We see that $n^2 = 4(2l + 1)(2l + 2) + 1 = 8(2l + 1)(l + 1) + 1$. $(2l + 1)(l + 1)$ is an integer by Axiom 2 since it is an integer, so $n^2 \equiv 1 \pmod{8}$ according to the division algorithm.

**Example 4.22.** Observe that $25 = 3(8) + 1$, $121 = 15(8) + 1$, i.e. both 25 and 121 (both perfect squares) are equivalent to 1 mod 8.

**Exercise 4.23.** Show that $n^2 = 100$ doesn’t work in Example 4.21. Why does this not contradict the result?

**Problem 4.24.** Use the result of Example 4.21 to show that 523,763 is not a perfect square.

**Theorem 4.25.** Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ for $a, b, c, d \in \mathbb{Z}$, then $a + c \equiv b + d \pmod{m}$.

**Proof:** Let $a, b, c, d, m$ be integers with $m > 0$, and suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then (1) $a - b = km$ and (2) $c - d = lm$ for integers $k$ and $l$ by definition of congruence mod $m$. We want to show that there exists an integer $s$ such that $(a + c) - (b + d) = sm$ because this is the definition of congruence mod $m$ applied to $a + c \equiv b + d \pmod{m}$. Adding equations (1) and (2) yields that $a - b + c - d = km + lm$, or $(a + c) - (b + d) = (k + l)m$. Since $k$ and $l$ are integers, $k + l$ is an integer by Axiom 2, so $a + c \equiv b + d \pmod{m}$ by definition of congruence mod $m$. 

50
Problem 4.26. Let \( m \) be a positive integer. Prove that if \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \) for \( a, b, c, d \in \mathbb{Z} \), then \( a - c \equiv b - d \pmod{m} \).

Problem 4.27. Let \( m \) be a positive integer and let \( a, b, c, d \in \mathbb{Z} \). Prove or disprove the following:

1. If \( a \equiv b \pmod{m} \) then \( an \equiv bn \pmod{m} \).
2. If \( an \equiv bn \pmod{m} \) then \( a \equiv b \pmod{m} \).

Problem 4.28. Let \( m \) be a positive integer. Prove that if \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \) for \( a, b, c, d \in \mathbb{Z} \), then \( ac \equiv bd \pmod{m} \).

Problem 4.29. Show that if \( n \mid m \), where \( n, m \) are positive integers greater than 1, and if \( a \equiv b \pmod{m} \), where \( a, b \in \mathbb{Z} \), then \( a \equiv b \pmod{n} \).

4.2 Prime Numbers

Definition 4.30. A positive integer \( p \) greater than 1 is called \underline{prime} if the only positive factors of \( p \) are 1 and \( p \). A positive integer that is greater than 1 and is not prime is called \underline{composite}.

Note: to show that a positive integer \( n \) is composite you must show there exists a positive integer \( a \) such that \( a \mid n \) and \( a \neq 1, n \).

Problem 4.31. Show that if \( n \in \mathbb{Z}^+ \), then all positive (holds trivially for negative) factors of \( n \) are less than or equal to \( n \). (Hint: use a proof by contradiction.)

Theorem 4.32. The Fundamental Theorem of Arithmetic Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

We will prove the existence part of this proof now, and the uniqueness later (we will need another tool).

Proof: Existence

Proof by strong induction (see Definition ??).

Let \( P(n) \) be the statement “\( n \) can be written as a prime or a product of two or more primes.” We can save the “order of nondecreasing size” until the end because that is just a matter of rearrangement.

Base case: \( 2=2 \) is a product of the prime number 2. (Why is our base case 2 here?)

Inductive step: Suppose \( P(j) \) is true for all \( 2 \leq j \leq k \), i.e. \( j \) can be written as a prime or a product of two or more primes. Consider the number \( k + 1 \). Suppose \( k + 1 \) is prime. Then we are done since \( k + 1 \) is written as a prime. Suppose \( k + 1 \) is not prime, i.e. \( k + 1 \) is composite. Then there exists an integer \( a \) such that \( 1 < a < k + 1 \) and \( a \mid (k + 1) \). Then \( k + 1 = ab \) for some integer \( b \), and since \( k + 1 \) and \( a \) are positive, \( b \) is positive, and \( b \neq 1, k + 1 \) since \( a \neq 1, k + 1 \) (if \( b = 1, a \) would have to be \( k + 1 \) to make the statement \( k + 1 = ab \) true and vice versa). Thus \( 1 < b < k + 1 \). Then by the inductive hypothesis, \( a \) and \( b \) can be written as a prime or a product of two or more primes so \( k + 1 = (p_1p_2 \ldots p_s)(q_1q_2 \ldots q_t) \) where \( p_i \) and \( q_t \) are primes, \( s, t \geq 1 \). Thus \( k + 1 \) can be written as a product of two or more primes. To put the primes in nondecreasing order we simply need to rearrange them if they are not already so.

Example 4.33. \( 132 = 2 \cdot 2 \cdot 3 \cdot 11 = 2^2 \cdot 3 \cdot 11 \).
Theorem 4.34. If \( n \) is a composite integer, then \( n \) has a prime divisor less than or equal to \( \sqrt{n} \).

Proof: Suppose that \( n \) is a composite integer. Then \( n \) has a factor \( a \) with \( 1 < a < n \) by Problem 4.31. Then \( n = ak \) for some integer \( k \). Since \( n, a > 0, k > 0 \), and \( k \neq 1 \) since \( n \neq a \). Thus, \( k > 1 \). Claim: either \( a \leq \sqrt{n} \) or \( k \leq \sqrt{n} \).

If not, i.e. \( a > \sqrt{n} \) and \( k > \sqrt{n} \). Then \( n = ak > \sqrt{n}\sqrt{n} = n \), a contradiction. Thus, either \( a \) or \( k \) is less than or equal to \( \sqrt{n} \). Without loss of generality, assume \( a \leq \sqrt{n} \).

If \( a \) is prime, we are done. If not, then \( a \) has a prime factor, which is less than itself by Problem 4.31 and we are done.

Example 4.35. Show that 1117 is prime.

Proof: We see that \( \sqrt{1117} = 33.42 \ldots \), so if 1117 is composite, it must have a prime factor less than or equal to 33. The only primes less than or equal to 33 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, and 31. We see that

- \( \frac{1117}{2} \notin \mathbb{Z} \)
- \( \frac{1117}{3} \notin \mathbb{Z} \)
- \( \frac{1117}{5} \notin \mathbb{Z} \)
- \( \frac{1117}{7} \notin \mathbb{Z} \)
- \( \frac{1117}{11} \notin \mathbb{Z} \)
- \( \frac{1117}{13} \notin \mathbb{Z} \)
- \( \frac{1117}{17} \notin \mathbb{Z} \)
- \( \frac{1117}{19} \notin \mathbb{Z} \)
- \( \frac{1117}{23} \notin \mathbb{Z} \)
- \( \frac{1117}{29} \notin \mathbb{Z} \)
- \( \frac{1117}{31} \notin \mathbb{Z} \)

So 1117 cannot have a factor other than itself or 1 because if it did, it would have a prime factor less than or equal to 33.

Theorem 4.36. There are infinitely many primes.

Proof: By contradiction. Suppose there are only finitely many primes, \( p_1, p_2, \ldots, p_n \). Let \( Q = p_1p_2\ldots p_n + 1 \). By the fundamental theorem of arithmetic, \( Q \) is prime or it can be written as the product of two or more primes. \( Q \) cannot be prime because it is larger than any \( p_j \) so it is not equal to any \( p_j \), and we assumed we had counted all the primes. So \( Q \) must be composite, and thus \( Q \) is a multiple of at least one prime, say \( p_j \), i.e. \( p_j | Q \). Since \( Q = p_1p_2\ldots p_n + 1 \), we have that \( Q - p_1p_2\ldots p_n = 1 \). We know that \( p_j \) divides \( Q \) and by Theorem 4.3 \( p_j \) divides \( p_1p_2\ldots p_n \), so \( p_j \) divides \( Q - p_1p_2\ldots p_n \) by Theorem 4.6. Thus \( p_j | 1 \) which is not possible. \( \rightarrow \leftarrow \)

Theorem 4.37. If \( p \) is a prime and \( a | bp \) for \( a, b \in \mathbb{Z} \) with \( a \neq p \), then \( a | b \).

Proof: not now.

Theorem 4.38. If \( p \) is a prime and \( p | ab \) for \( a, b \in \mathbb{Z} \), then \( p | a \) or \( p | b \).

Proof: not now.

Problem 4.39. Let \( a, b, p, m \in \mathbb{Z} \) with \( m, p > 0 \) and \( m \neq p \). Prove that if \( p \) is prime and \( ap \equiv bp \) (mod \( m \)), then \( a \equiv b \) (mod \( m \)).

Problem 4.40. Let \( a, b, p, m \in \mathbb{Z} \) with \( m, p > 0 \) and \( p \nmid m \). Prove that if \( p \) is prime and \( am \equiv bm \) (mod \( p \)), then \( a \equiv b \) (mod \( p \)).
5  Combinatorics and Counting

5.1  The Basics of Counting

We begin this section with a few exercises and problems to get us warmed up.

Exercise 5.1.  1. Suppose a store sells five different kinds of bagels and four different kinds of cream cheese. How many different combinations are possible?

2. Suppose you are applying to 10 different colleges and can choose from 45 different majors. How many different choices of school with major are there?

Exercise 5.2. Now suppose there are two people who are each going to pick a bagel from a set of five different ones, and there is only one of each kind available. How many ways can the two people pick?

Problem 5.3.  1. How many five-letter palindromes are there if letters can be repeated?

2. How many five-letter palindromes are there if the first three letters cannot be repeated?

3. How many five-letter palindromes are there if the first three letters must be consonant-vowel-consonant and the two consonants cannot be the same? (Assume y is a consonant.)

Exercise 5.4.  1. Students who need to take both Pre-Calculus and Trigonometry at Central can take either MATH 119 or MATH 115 and MATH 116. If there are 5 sections of MATH 119 and four sections each of MATH 115 and MATH 116, how many ways can they accomplish these two courses (assuming no time overlap b/w 115 and 116)?

2. What if there are only three sections of MATH 115 (though still four of MATH 116)?

Problem 5.5.  1. How many strings of three decimal digits (the digits 0-9) contain exactly two odd digits if digits can be repeated?

2. How many strings of three decimal digits (the digits 0-9) contain exactly two odd digits if digits cannot be repeated?

Problem 5.6. A bit string is a string of 0’s and 1’s. How many bit strings of length six are there if every 0 has a 1 immediately to its left?

5.2  Permutations and Combinations

Definition 5.7. A permutation of a set of distinct objects is an ordered arrangement of these objects. An ordered arrangement of \( n \) elements is an \( n \)-permutation.

Example 5.8. Suppose there are five competitors in an event. In how many orders can they finish?
Solution: We consider each spot at a time. There are five different people that can fill the first spot, i.e. five different ways for someone to win. Once one of those competitors has been chosen, that leaves four competitors left for the second spot, i.e. for each possible winner there are four different second-place possibilities. We continue this reasoning to see that there are \( 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 \) possible finishing orders.

Exercise 5.9. Write a formula for the number of ways to order \( n \) distinct elements.
Problem 5.10. 1. How many ways are there to order five theorems A,B,C,D,E?

2. How many ways are there to order five theorems A,B,C,D,E if theorem C must immediately follow theorem B?

3. How many ways are there to order five theorems A,B,C,D,E if theorem C must come sometime after theorem B?

Exercise 5.11. Suppose there are five competitors at an event but only three medals. How many different combinations of medalists are there? Use the technique of Example 5.8.

Exercise 5.12. If you have \( m \) tops and \( n \) pairs of pants, how many ways can you put together an outfit of one top and one pair of pants?

Exercise 5.13. 1. If there are \( m \) different bagels available (one of each kind), how many different ways can they be distributed to \( m \) people?

2. If there are \( m \) different bagels available (one of each kind), how many different ways can they be distributed to \( n \) people, where \( n < m \)?

Definition 5.14. The number of ways to order \( r \) distinct elements from a set of \( n \) distinct elements is the number of \( r \)-permutations on a set of \( n \) (distinct) elements and is denoted \( P(n, r) \).

Note: In Exercise 5.11, we found \( P(5, 3) \). If we are simply counting the number of permutations on a set of \( n \) elements, we are finding \( P(n, n) \). \( P(n, 0) \) counts just the ordered list of no elements, or the empty list, so \( P(n, 0) = 1 \) because there is one empty list (as there is one empty set).

Exercise 5.15. If \( n, r \in \mathbb{Z}^+ \) with \( r \leq n \), find a formula for \( P(n, r) \) in terms of factorials. (Note that \( 0! \) is defined to be 1.)

Problem 5.16. 1. How many functions are there from a set of \( m \) elements to a set of \( n \) elements?

2. How many one-to-one functions are there from a set of \( m \) elements to a set of \( n \) elements? (Hint: start off with a condition on \( n, m \) that must be met.)

3. How many one-to-one and onto functions are there from a set of \( m \) elements to a set of \( n \) elements? (Hint: start off with a condition on \( n, m \) that must be met.)

Problem 5.17. How many onto functions are there from a set of \( m \) elements to a set of \( n \) elements? (Hint: start off with a condition on \( n, m \) that must be met.)

5.3 Combinations

We begin with an example.

Example 5.18. How many ways are there to pick three classes from a list of 7?

In this small case, we can answer just by counting (each class is represented by a digit 1-7):

\[
\begin{align*}
123,124,125,126,127,134,135,136,137,145,146,147,156,157,167 & \quad (15) \\
234,235,236,237,245,246,247,256,257,267 & \quad (10) \\
345,346,347,356,357,367 & \quad (6) \\
456,457,467 & \quad (3) \\
567 & \quad (1) \\
\text{Total: } 35
\end{align*}
\]
But, we would like to be able to answer this question more efficiently so that we can easily extend it to higher values. To do so, we explore how performing the above task relates to $P(7, 3)$. Recall that $P(7, 3)$ reports the number of ways to order $r$ elements chosen from 7. In particular, note that in using $P(7, 3)$, 123 would be different from 132, but in the above example, we would want these to be the same and not to be counted twice since we do not care about the order of the classes, just which ones we’ve chosen. Thus, we can see that $P(7, 3)$ is too high, because it counts different orders separately (and when we compute $P(7, 3)$ we get $7 \cdot 6 \cdot 5 \cdot 4 = 210$, which is far more than 35). So to find the number of ways to simply choose elements and not order them, we want to somehow eliminate the ordering in our counting. More generally, recall the number of ways to order $r$ elements chosen from $n$, or $P(n, r)$, is the following:

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}.$$ 

This involves first choosing $r$ elements from the set of $n$, and then ordering those $r$ elements (the number of ways to do which is $P(r, r)$). Thus, if we denote the number of ways to just choose $r$ elements from $n$ (and not order them) as $C(n, r)$, we can rewrite $P(n, r)$ as below:

$$P(n, r) = C(n, r)P(r, r) = \frac{n!}{(n-r)!} = C(n, r)r!$$ 

We want a formula for $C(n, r)$, so we divide by $r!$:

$$C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n!}{r!(n-r)!}$$

This should make sense intuitively since we want to start with the number of ways to order $r$ elements chosen from $n$, but divide away the different orders that we don’t want to count more than once, leaving only the number of ways to just choose the elements. We observe that this applies to our previous example because:

$$C(7, 3) = \frac{7!}{3!4!} = \frac{P(7, 3)}{3!} = \frac{210}{6} = 35,$$

which is what we first got.

**Example 5.19.** How many bit strings of length 7 are there that contain more 1s than 0s?

Answer: We consider each spot in the string as one “element”, and we are choosing spots for say, the 1s. We must consider the ways to choose 7 spots for the 1s, 6 spots for the 1s, 5 spots for the 1s, and 4 spots for the 1s. Anything under this will not result in more 1s than 0s. Adding these gives

$$C(7, 7) + C(7, 6) + C(7, 5) + C(7, 4) = 64.$$

**Exercise 5.20.** Show that in the above example, we could have also gotten the same answer by counting the number of ways to pick the spots for the 0s (keeping in mind that there must be fewer 0s than 1s).

**Exercise 5.21.** Show that $C(n, r) = C(n, n - r)$ and then explain in words why it makes sense that these are the same.

**Problem 5.22.** Prove the identity $C(n, r)C(r, k) = C(n, k)C(n - k, r - k)$, where $n, r, k$ are nonnegative integers with $k \leq r \leq n$.  

55
Problem 5.23. How many bit strings of length 12 contain

1. exactly three 1s?
2. at most three 1s?
3. at least three 1s?
4. an equal number of 0s and 1s?

Problem 5.24. Suppose a department has 20 faculty members, 12 men and 8 women.

1. Suppose that a committee must be chosen of five members total, with at least one women. How many ways is it possible to do this?
2. Now suppose that the committee must have more women than men. How many ways are there to do this?

Generalized Permutations and Combinations

Example 5.25. How many decimal strings are there of length 13?
Answer: each of the 13 spots has 10 choices, so we get $10 \cdot 10 \cdot 10 \cdots 10 = (13 \text{ copies of 10 multiplied}) = 10^{13}$.

Theorem 5.26. The number of $r$-permutations on a set of $n$ objects with repetition allowed is $n^r$.

Notice that there definitely will be repetition. How is this different from $P(n, r)$? Repetition is not allowed in $P(n, r)$, so once an element is already chosen it’s removed from the pool. That is not the case here, as is seen in the above example where we are allowed to repeat digits so there are always 10 choices for each spot.

Example 5.27. How many ways are there to distribute donuts to three dozen people if there are 25 kinds available?
Answer: $r = 36$, $n = 25$, so $n^r = 25^{36}$. (Each of the 36 people has 25 choices, so we get 25 multiplied by itself 36 times.)

Now let’s consider the following example.

Example 5.28. In how many ways can I order 3 bagels from a shop that has 5 different kinds (assuming there are unlimited of each kind)?

Note that this is different from both the above example and from $P(n, r)$. It is different from the above example because there will be repetition of elements that we don’t want to recount (for example, an order of two sesames and one plain should count only once, not three times for the different orders SSP, SPS, PSS, which would be different ways if we were distributing them to three different people). It is different from $P(n, r)$ because here we are allowed repetition. So, the way we will answer this question is to picture this problem as a box with five slots for each of the five kinds, which we will fill with an “x” for each bagel of that kind. We will then count the number of ways to fill the slots. We represent this pictorially by x’s and vertical bars; the vertical bars create the slots for the bagels, and the x’s represent the bagels chosen. For example, the following configuration represents 1 of type 1, 2 of type 3, and 0 of the other types:

\[
| x | x | x |
\]

or just $x || x ||$
This is because the slot to the left of the first bar is filled with one x, the slot between the first two bars is empty, the slot between the second and third bars has two x’s, and there are no x’s in the slot between the third and fourth bars or to the right of the fourth bar.

If we count the number of bars and x’s total we get 7 (4 bars, 3 x’s), so 7 total spots in which we can insert bars and x’s. We thus describe the number of ways to insert 3 x’s into 7 spots, or the number of ways to choose 3 spots from 7, or $C(7, 3) = \frac{7!}{3!4!} = 35$.

Note that we got 7 from (5-1)+3, or the number of types $-1, +$ the number of bagels to be chosen.

We generalize this technique into the following theorem:

**Theorem 5.29.** The number of $r$-combinations from a set with $n$ elements when repetition of elements is allowed is $C(n + r - 1, r) = \frac{(n+r-1)!}{r!(n-1)!} = C(n + r - 1, n - 1)$.

**Proof:** Using the technique from above, we see that the number of ways to order $r$ elements chosen from $n$, when repetition is allowed, is equivalent to the number of ways to insert $r$ x’s into $n$ boxes, and the $n$ boxes can be represented by $n - 1$ vertical bars. There are thus $n + r - 1$ total spots and we count the number of ways to choose $r$ of those to get $C(n + r - 1, r)$.

Consider the question, “Find the number of ways to choose 10 items from 3 kinds.” As we know from the above theorem, this is $C(10 + 3 - 1, 10) = C(12, 10) = \frac{12!}{10!2!} = 66$. Another way to see this problem is to note that answering this question is equivalent to finding all possible positive integer solutions to the equation

$$x_1 + x_2 + x_3 = 10$$

where $x_i$ represents the number chosen of type $i$. In other words, if we needed 10 bagels from 3 kinds this would be saying that we have $x_1$ of type 1, $x_2$ of type 2, and $x_3$ of type 3, which of course must add up to 10. So we can interpret these types of questions as the sum of $n$ variables, which equals $r$. This helps us generalize the question easily, as we see in the following examples.

**Example 5.30.** What if $x_2$ must be at least 2, i.e. we must have at least two of type 2? Then there are only 8 free choices left out of the original 10, so we find the number of integer solutions to

$$x_1 + y_2 + x_3 = 8$$

which is $C(3 + 8 - 1, 1, 8) = C(10, 8) = \frac{10!}{8!2!} = 45$.

**Problem 5.31.** A croissant shop has plain croissants, cherry croissants, chocolate croissants, almond croissants, apple croissants, and broccoli croissants. How many ways are there to choose

1. a dozen croissants?
2. two dozen croissants with at least two of each kind?
3. two dozen croissants with no more than two broccoli croissants?
4. two dozen croissants with at least five chocolate croissants and at least three almond croissants?
**Problem 5.32.** How many positive integers less than 1,000,000 have exactly one digit equal to 9 and have a sum of digits equal to 13?

In the following example we explore what happens when we only have a limited number of each kind of object we are choosing.

**Example 5.33.** How many ways can the set \{sesame, sesame, plain, plain, plain, everything, blueberry, onion\} be handed out to seven people?

First we observe that the answer to this question is not simply the number of permutations of eight elements, 8!, because several of the elements are repeated, i.e. SSPPPEBO would be (incorrectly) counted six times because we would be counting the two orderings of the sesames and the three orderings of the plains as different arrangements.

To do this we will use the following technique. Consider, say, just the plains. These can be placed among the eight people in $\binom{8}{3} = 56$ ways, leaving 5 spots, because we count the number of ways to distribute the 3 plains which is equivalent to choosing a set of 3 people from among the 7. Below are a few examples of how this would be done.

\[
\begin{align*}
\text{PPPxxxx} & \quad \text{PPxPxxx} & \quad \text{xPPPxxxx} \\
\text{PxPPxxx} & \quad \text{PPxxPxxx} & \quad \text{xxPxPPxx}
\end{align*}
\]

For each of these, we have five spots left to place, say, the sesames. So for each one of these, we have $\binom{5}{2} = 10$ to place the sesames. We look at just the first one from the above list and demonstrate the ways to do this:

\[
\begin{align*}
\text{PPSSxxx} & \quad \text{PPPxSSxx} & \quad \text{PPPxSxSx} \\
\text{PPPSxSxx} & \quad \text{PPPxxSSx} & \quad \text{PPPxxSxS} \\
\text{PPPSxxSx} & \quad \text{PPPxxxSS} & \quad \text{PPPxxSSS} \\
\text{PPPSxxxS} & & \\
\end{align*}
\]

Now for each of these, we have three spots left to place the one everything bagel, which gives $\binom{3}{1} = 3$ ways. We look at just the first one from the above list:

\[
\begin{align*}
\text{PPPSSExx} & \\
\text{PPPSSxEx} & \\
\text{PPPSSxxE}
\end{align*}
\]

Now for each one of these, we have two spots left to place the blueberry, which gives $\binom{2}{1} = 2$ ways. We look at just the first one:

\[
\begin{align*}
\text{PPPSSEBx} & \\
\text{PPPSSExB}
\end{align*}
\]

And lastly, for each of these, we have just one spot left for the onion.

58
So how many is that total? \( C(8, 3)C(5, 2)C(3, 1)C(2, 1)C(1, 1) = \frac{8!}{3!5!} \cdot \frac{5!}{2!3!} \cdot \frac{3!}{1!2!} \cdot \frac{2!}{1!1!} \cdot \frac{1!}{1!1!1!} = \frac{8!}{3!2!1!1!} \)

Notice that the numerator is the number of spots and the terms in the denominator are the number of kinds.

**Theorem 5.34.** The number of different permutation of \( n \) objects, where there are \( n_1 \) indistinguishable objects of type 1, \( n_2 \) indistinguishable objects of type 2,...., and \( n_k \) indistinguishable objects of type \( k \), is

\[
\frac{n!}{n_1!n_2! \cdots n_k!}
\]

**Proof:** Note there are \( C(n, n_1) = \frac{n!}{n_1!(n-n_1)!} \) ways to place the objects of type 1, \( C(n-n_1, n_2) = \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \) ways to place the objects of type 2,.....,\( C(n-n_1-n_2-\cdots-n_{k-1}, n_k) = \frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!(n-n_1-n_2-\cdots-n_{k-1}-n_k)!} \) ways to place the objects of type \( k \). Multiplying these together yields

\[
\frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdots \frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!(n-n_1-n_2-\cdots-n_{k-1}-n_k)!}
= \frac{n!}{n_1!n_2! \cdots n_k!}
\]

**Problem 5.35.**

1. How many different strings can be made from the letters in MISSISSIPPI, using all the letters?
2. Using only 10 letters?
3. Using 6 or more letters?

**Problem 5.36.**

1. How many ways can 10 students sign up for advising slots if there are 3 on Monday, 2 on Wednesday, 4 on Thursday, and 1 on Friday (not distinguishing spots on the same day from each other)?
2. Now suppose there are 3 on Monday, 2 on Wednesday, and 4 on Thursday but none on Friday, i.e. one student will not get a spot. How many ways are there now for the students to sign up?
3. Lastly, suppose there are 4 spots on Monday, i.e. 11 total spots but still only 10 students. Find the number of ways the students can sign up.