Math 2000 Notes

Kyle Beserra

April 14, 2021

Contents

Throughout this text we will denote:

- $\mathbb{N}$ as the set of natural numbers, these are the non-negative whole numbers. Note, 0 is a natural number.
- $\mathbb{Z}$ as the set of integers.
- $\mathbb{Q}$ as the set of rational numbers.
- $\mathbb{R}$ as the set of real numbers.
- $\mathbb{C}$ as the set of complex numbers.

By $\mathbb{Z}^+$ and $\mathbb{Z}^-$, we mean the set of all positive and negative integers respectively. By $\mathbb{Z}^{\geq 0}$ and $\mathbb{Z}^{\leq 0}$, we mean the set of all non-negative and non-positive integers respectively. Similarly, we may replace the set of integers, $\mathbb{Z}$ in the previous with $\mathbb{Q}$ or $\mathbb{R}$ for the same meaning. Note that as positive and negative are not defined on the complex plane, we cannot do the same for $\mathbb{C}$.

1 Logical Forms And Equivalence

Definition 1.1. A *statement* (or *proposition*) is a sentence that is either true or false, but not both.

Definition 1.2. A *statement form* (or *proposition form*) is an expression made up of statement variables and logical connections (such as $\neg$, $\vee$, or $\wedge$) which when substituting statements for statement variables becomes a statement.

Note, statement forms are acting as *Platonic forms* of statements.

Definition 1.3. The *truth value* of a given statement is true if that sentence is itself true otherwise, the truth value of that statement is false.

Definition 1.4. Let p be a statement form. The *negation* of p, written $\neg p$, is the statement form with the opposite truth value of p.

Note, the symbol $\neg$ is not the only symbol used to denote negation. For instance, it is not uncommon to see the symbol $\sim$ used in other logic texts. Further, many c-like programming-languages will use the symbol ! for the same meaning. The Python programming-language deserves a special call-out on this note, it allows for the use of the symbol 'not' for its not symbol (which fits nicely with its use of 'and' and 'or' for its and and or logical connectives).

Definition 1.5. Let p and q be statements forms. The *disjunction* of p and q, written $p \vee q$, is the statement form that is true when either p or q is true and false precisely when p and q are both false.

Definition 1.6. Let p and q be statements forms The *conjunction* of p and q, written $p \wedge q$, is the statement form that is true precisely when both p and q are true and is otherwise false.

Just as in arithmetic, when more than one logical connective is used, we

- perform the operations from left to right,
- evaluate parenthetical terms first,
- treat $\neg$ similar to a minus sign.

Definition 1.7. A *truth table* for a statement form displays the truth values corresponding to every possible combination of truth values for its component statement variables.

Example 1.1. Write the truth tables for logical connectives: $\neg$ (not), $\vee$ (or), and $\wedge$ (and) :

p	$\neg p$
T	F
F	T

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

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

Example 1.2. Truth table for the statement form $(p \vee q) \wedge \neg(p \wedge q)$:
Note, in this example we also include the truth table for the sub-statements forming the larger statement. This is not necessary, though this does reduce the risk for error at the cost of space and ink.

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

Example 1.3. Write the truth table for the statement form $(p \wedge q) \vee \neg r$:
Note, in this example, we also include the truth table for the sub-statements forming the larger statement. This is not necessary, though this does reduce the risk for error at the cost of space and ink.

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

Definition 1.8. Two statement forms are said to be *logically equivalent* if, and only if, they have identical truth values for each possible truth value assignment for their statement variables. Let P and Q be statement forms, we write $P \equiv Q$ to mean that P is logically equivalent to Q.

Definition 1.9. Two statements are said to be *logically equivalent* if, and only if, they have logically equivalent forms after replacing identical component statements with statement variables.

Proposition 1.1. (Double negation): *The statement form p is logically equivalent to $\neg\neg p$, i.e. $p \equiv \neg\neg p$.*

Proof. In the truth table below, we will write $\neg\neg p$ and $\neg(\neg p)$. This is to highlight that we are negating the statement form $\neg p$.

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

We note that the column for p is identical to the column for $\neg\neg p$. Thus, we can conclude that after substituting a statement for the statement variable p in the statement forms p and $\neg\neg p$ the statement forms will have identical truth values. Whence, the statement forms are identical. □

The conclusion of the previous definition is certainly a mouthful, but worth repeating. Similar to the way statement forms provide a layer of abstraction to statements, examining the truth tables of two statement forms to determine equivalence abstracts away substituting actual statements for statement variables.

Example 1.4. The statement form $\neg(p \wedge q)$ is not equivalent to the statement form $\neg p \wedge \neg q$ ($\neg(p \wedge q) \not\equiv \neg p \wedge \neg q$).

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

Note the middle two rows of the $\neg(p \wedge q)$ and the $\neg p \wedge \neg q$ do not have the same values. These rows are counterexamples to the two statement forms being logically equivalent.

Proposition 1.2. (DeMorgan's Law):

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

and

$$\neg(p \vee q) \equiv \neg p \wedge \neg q\,.$$

Proof. We'll show this by examining the truth tables for each statement form and noting that the relevant columns are identical.

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

□

Exercise 1.1. Use DeMorgan's, Proposition 1.2, to write the negation of the following statements:

1. John is 6 feet tall or he weighs less than 200 pounds.

2. The bus was late or Tom's watch was slow.

3. $-1 \leq x \leq 4$.

Definition 1.10. A *tautology* is a statement form that is true independent of the truth value assignments of its truth value assignments. A statement whose statement form is a tautology is a *tautological statement.*

Definition 1.11. A *contradiction* is a statement form that is false independent of the truth value assignments of its truth value assignments. A statement whose statement form is a contradiction is a *contradictory statement.*

Theorem 1.3. *Let p, q, and r be statement variables, τ a tautology, and c a contradiction. Then the following hold:*

1. *Commutativity: $p \wedge q \equiv q \wedge p$ and $p \vee q \equiv q \vee p$.*

2. *Associativity: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ and $(p \vee q) \vee r \equiv p \vee (q \vee r)$.*

3. *Distribution:* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ *and* $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.

4. *Identity:* $p \wedge \tau \equiv p$ *and* $p \vee c \equiv p$.

5. *Negation:* $p \wedge \neg p \equiv c$ *and* $p \vee \neg p \equiv \tau$.

6. *Double negation:* $\neg\neg p \equiv p$.

7. *Idempotent:* $p \wedge p \equiv p$ *and* $p \vee p \equiv p$.

8. *Universal bound:* $p \vee \tau \equiv \tau$ *and* $p \wedge c \equiv c$.

9. *DeMorgan's Law:* $\neg(p \wedge q) \equiv \neg p \vee \neg q$ *and* $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

10. *Absorption:* $p \vee (p \wedge q) \equiv p$ *and* $p \wedge (p \vee q) \equiv q$.

11. *Negation of* τ *and* c*:* $\neg\tau \equiv c$ *and* $\neg c \equiv \tau$.

Proof. Claims (6) and (9) have been proved in Proposition 1.1 and Proposition 1.2 respectively. The remaining claims are left as an exercise to the reader. □

Exercise 1.2. Use truth tables to show that claims of Theorem 1.3.

2 Conditional Statements

Definition 2.1. Let p and q be statements forms. The *conditional statement* "p implies q", written $p \to q$, is the statement form that is false precisely when p is true and q is false (that is, when the statement "If p, then q" is violated).

In the conditional $p \to q$, p is refered to as the *hypothesis* and q is called the *conclusion.*

Conditional statements, $p \to q$ can be expressed, in English, in many ways. For instance, the conditional may be presented as "If p, then q" or "q by p".

A conditional statement is said to be vacuously true when the hypothesis is false.

In expressions with other logical connectives, → is performed last.

Example 2.1. The following is the truth table for the conditional statement $p \to q$.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 2.2. Construct the truth table for the statement form $(p \vee \neg q) \to \neg p$.

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

Proposition 2.1. $p \to q \equiv \neg p \vee q$

Proof. Left as an exercise to the reader. □

Exercise 2.1. Show, using a truth table, Proposition 2.1.

Example 2.3. Rewrite the following as an if-then statement (in English):

“Either you get your work in on time or you’re fired.”.

Let $\neg p$ be the statement “you get your work in on time”. This means that p is equivalent to the statement “ you do not get your work in on time” Let q the statement “you are fired”. Then the original statement can be written as $\neg p \vee q$. Using Proposition 2.1, we have that $\neg p \vee q \equiv p \rightarrow q$. Rewriting this in English we get:

“If you do not get your work in on time, then you are fired.”.

Example 2.4. From Proposition 2.1, we have that $p \rightarrow q \equiv \neg p \vee q$. Applying DeMorgan’s Law, Proposition 1.2, and using double negation, Proposition 1.1, we have that

$$\begin{aligned} \neg(p \rightarrow q) &\equiv \neg(\neg p \vee q) \\ &\equiv \neg\neg p \wedge \neg q \\ &\equiv p \wedge \neg q\,. \end{aligned}$$

Whence, $\neg(p \rightarrow q) \equiv p \wedge \neg q$.

Example 2.5. Write the negation of:

“If Sara lives in Athens, then Sara lives in Greece.”.

Let p be the statement “Sara lives in Athens” and q the statement “Sata lives in Greece”. Then the given statement can be written as $p \rightarrow q$. As we saw in Example 2.4, $\neg(p \rightarrow q)$ is equivalent to $p \wedge \neg q$. Thus, the negation of the original statement is:

“Sara lives in Athens and Sara does not live in Greece.”.

Definition 2.2. The *contrapositive* of a conditional statement form $p \rightarrow q$ is the statement form $\neg q \rightarrow \neg p$.

Proposition 2.2. $p \rightarrow q \equiv \neg q \rightarrow \neg q$

Proof. Left as an exercise to the reader. □

Exercise 2.2. Show, using a truth table, Proposition 2.2

Example 2.6. Write the contrapositive of:

“If today is Martin Luther King Jr. Day, then tomorrow is Tuesday.”.

Similar to as in Exercise 2.3, let p be the statement "today is Martin Luther King Jr. Day" and q the statement "tomorrow is Tuesday". So, $\neg p$ is equivalent to the statement "today is not Martin Luther King Jr. Day" and $\neg q$ is the statement "tomorrow is not Tuesday".

Using Proposition 2.2, we have that $p \to q \equiv \neg q \to \neg p$. Rewriting this in English we get:

"If tomorrow is not Tuesday, then today is not Martin Luther King Jr. Day.".

Definition 2.3. The *converse* of a conditional statement form $p \to q$ is the statement form $q \to p$.

Definition 2.4. The *inverse* of a conditional statement form $p \to q$ is the statement form $\neg p \to \neg q$.

Example 2.7. Write (in English) the converse and inverse of:

"If today is Martin Luther King Jr. Day, then tomorrow is Tuesday.".

Just as in Example 2.6, let p be the statement "today is Martin Luther King Jr. Day" and q the statement "tomorrow is Tuesday". So, $\neg p$ is equivalent to the statement "today is not Martin Luther King Jr. Day" and $\neg q$ is the statement "tomorrow is not Tuesday"

Finally, the from Definition 2.3, the converse of the original statement is $q \to p$ or in English:

"If tomorrow is Tuesday, then today is Martin Luther King Jr. Day.".

And, using Definition 2.4 the inverse of the original statement is $\neg p \to \neg q$ or in English:

"If today is not Martin Luther King Jr. Day, then tomorrow is not Tuesday.".

Exercise 2.3. Show that the converse and inverse of a conditional statement $p \to q$ are equivalent.

Definition 2.5. Let p and q be statements forms. The *biconditional statement* "p if, and only if q", written $p \leftrightarrow q$, is the statement form that is true precisely when p and q have the same truth value.

We ofter abbreviate “if, and only if” by iff.

Example 2.8. The following is the truth table for the conditional statement $p \leftrightarrow q$.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Exercise 2.4. Show, using a truth table, that $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

Definition 2.6. Let p and q be statements. We say that p is a *sufficient* condition for q to mean that $p \to q$. We say that p is a *necessary* condition for q to mean that $\neg p \to \neg q$.

3 Predicates and Quantifiers

Note the sentence

“They are a college student.”

is not a statement as it may be true or false depending on the value of “They”. In this sentence “They” is a free variable. Similarly, “$x + y > 0$” is not a statement, it has more familiar variables x and y.

The predicate refers to the part of the sentence with some or all of its nouns removed. That is, in the sentence

“James is a student at the University of North Texas.”,

“James” is the subject and

“is a student at the University of North Texas.”

is the predicate.

In logic, predicates are formed in much the same way.

Definition 3.1. A *predicate* is a sentence which contains a finite number of variables which becomes a statement when a value is assigned to each of its variables. The *domain* of a predicate variable is the set of possible values which that variable may take.

Example 3.1. Let $P(x)$ denote

“x is a student at the University of North Texas.”

and $Q(x, y)$ denote

“x is a student at y.”.

x is the predicate variable for $P(x)$ while both x and y are predicate variables for $Q(x, y)$.

Note that when values are substituted for x and y in $P(x)$ and $Q(x, y)$, these sentences become statements. For instance if we substitute x for “Taylor” and y for“Boise State University”, $P(x)$ and $Q(x, y)$ become the statements

“Taylor is a student at the University of North Texas.”

and

“Taylor is a student at Boise State University.”

respectively. Whence, $P(x)$ and $Q(x, y)$ are predicates

In Example 3.1, we referred to the example’s predicates with their full names, $P(x)$ and $Q(x, y)$. When there is no room for confusion and the variables or other ornaments are of little importance to the statement being made, we may drop those decorations from the symbol. That is, the concluding sentence of Example 3.1 could be written “Whence, P and Q are predicates.”.

Example 3.2. Let $P(x)$ denote “$x^2 > x$” with $\mathbb{R}$, the set of real numbers, as the domain of x.

$P(2)$ and $P(-\frac{1}{2})$ are true. This is because $P(2)$ and $P(-\frac{1}{2})$ denote the statement “$4 > 2$” and “$\frac{1}{4} > -\frac{1}{2}$” respectively. On the other hand, $P(\frac{1}{2})$, which is the statement “$\frac{1}{4} > \frac{1}{2}$” is false.

Definition 3.2. Let $P(x)$ be a predicate with variable x with domain D. The *truth set* of $P(x)$ is the set of elements in D so that $P(x)$ is true after substituting that element for x. That is, it is the set $\{\, x \in D \mid P(x) \,\}$.

Example 3.3. Let $P(x)$ be as in Example 3.2. It is not difficult to see that for any real number x with $x < 0$, that $x^2 > 0 > x$. So, for any real number x with $x < 0$ $P(x)$ holds.

Now, if x is a real number with $0 \leq x \leq 1$, then we can see that $0 \leq x^2 \leq x \leq 1$. So, if x is a real number with $0 \leq x \leq 1$, then $P(x)$ is false.

Finally, if x is a real number with $1 < x$, then we have that $x < x^2$. Thus, if x is a real number with $1 < x$, then $P(x)$ is true.

Puting this together, we have that the truth set of $P(x)$ are the real numbers x such that $(x < 0) \vee (1 < x)$.

Example 3.4. Let $Q(n)$ be “n is a factor of 8. Find the truth set of $Q(n)$ where:

1. the domain of n is the set of positive integers, $\mathbb{Z}^+$

$$\left\{\, n \in \mathbb{Z}^+ \mid Q(n) \,\right\} = \{\, 1, 2, 4, 8 \,\} \;.$$

2. the domain of n is the set of integers, $\mathbb{Z}$.

$$\{\, n \in \mathbb{Z} \mid Q(n) \,\} = \{\, -8, -4, -2, -1, 1, 2, 4, 8 \,\} \;.$$

Definition 3.3. An *universal statement* is a statement asserting that that $P(x)$ holds for every x in D, written $\forall x \in D(P(x))$, where $P(x)$ is a predicate and D is the domain of x in $P(x)$. $\forall x \in D(P(x))$ is true if, and only if, $P(x)$ is true for every x in D.

Example 3.5. Let $D = \{\,1, 2, 3, 4, 5\,\}$. Show that $\forall x \in D(x \leq x^2)$ is true.

As D is a finite set, and a small one at that, we can check this by brutal force. That is, check that $P(x)$ holds for each element in D:

- $x = 1$, So, $x = 1 \leq 1 = x^2$.
- $x = 2$, So, $x = 2 \leq 4 = x^2$.
- $x = 3$, So, $x = 3 \leq 9 = x^2$.
- $x = 4$, So, $x = 4 \leq 16 = x^2$.
- $x = 5$, So, $x = 5 \leq 25 = x^2$.

As we have, exhaustively, shown that $x \geq x^2$ holds for each $x \in D$. Thus, $\forall x \in D(x \geq x^2)$ is true.

Note that the technique of checking each element of the domain of an universal statement, as in the example above, is not the way to go. This method is called the *method of exhaustion*, and is aptly named.

Example 3.6. Show that $\forall x \in \mathbb{R}(x \leq x^2)$ is false.

To do this, we need to recall that $\forall x \in \mathbb{R}(x \leq x^2)$ is true, by Definition 3.3, precisely when $x \leq x^2$ for all $x \in \mathbb{R}$. So, to show it is false we need only show that $x \leq x^2$ is false for some $x \in \mathbb{R}$. That is, we need to provide a counter example to the claim.

For a counter example, consider $x = \frac{1}{2}$ and note that

$$x = \frac{1}{4} \not\leq \frac{1}{16} = \left(\frac{1}{4}\right)^2 .$$

The technique of producing a counter example is the standard way to show that an universal statement is false.

Definition 3.4. An *extistential statement* is a statement asserting that that $P(x)$ holds for any one x in D, written $\exists x \in D(P(x))$, where $P(x)$ is a predicate and D is the domain of x in $P(x)$. $\exists x \in D(P(x))$ is true if, and only if, there exists an x in D such that is true.

Example 3.7. Let $D = \{ 1, 2, 3, 4, 5 \}$. Show that $\exists x \in D(\frac{1}{x} < \frac{1}{x^2})$ is false.

As D is a finite set, and a small one at that, we can check this exhaustively. That is, check that $P(x)$ is false for each element in D:

- $x = 1$, So, $\frac{1}{x} = 1 \geq 1 = x^2$.
- $x = 2$, So, $\frac{1}{x} = \frac{1}{2} \geq \frac{1}{4} = x^2$.
- $x = 3$, So, $\frac{1}{x} = \frac{1}{3} \geq \frac{1}{9} = x^2$.
- $x = 4$, So, $\frac{1}{x} = \frac{1}{4} \geq \frac{1}{16} = x^2$..
- $x = 5$, So, $\frac{1}{x} = \frac{1}{5} \geq \frac{1}{25} = x^2$..

As we have, exhaustively, shown that $x \not< x^2$ holds for each $x \in D$. That is, that $\frac{1}{x} < \frac{1}{x^2}$ is false for each $x \in D$. Thus, $\exists x \in D(\frac{1}{x} < \frac{1}{x^2})$ is false.

Example 3.8. Show that $\exists x \in \mathbb{R}(x = x^2)$ is true.

To do this, we need to recall that $\exists x \in \mathbb{R}(x = x^2)$ is true, by Definition 3.4, precisely when $x = x^2$ for some $x \in \mathbb{R}$. So, we must find a *witness* which sees that $x = x^2$ is true.

For such a witness, consider $x = 1$ and note that$x = 1 = 1 = x^2$.

Example 3.9. Translate the following statement to a formal statement

"2 times any integer is even."

$$\forall n \in \mathbb{Z}(2n \text{ is even})$$

Definition 3.5. An *universal conditional statement* is a statement asserting that that for any $x \in D$ such that $P(x)$, $Q(x)$ holds as well. Written $\forall x \in D(P(x) \to Q(x))$, where $P(x)$ and $Q(x)$ are predicates and D is the domain of x in $P(x)$ and $Q(x)$. $\forall x \in D(P(x) \to Q(x))$ is true if, and only if, $P(x) \to Q(x)$ is true for every x in D.

Example 3.10. Rewrite the following informally

$$\forall x \in \mathbb{R}(x > 2 \to x^2 > 4)\,.$$

"If x is a real number greater than 2, then the square of x is greater than 4."

Note that the statements

"For all real numbers x if x is an integer, then x is a rational."

and

"For all integers x, x is a rational."

are equivalent.

In fact,

$$\forall x \in D(P(x) \to Q(x)) \equiv \forall x \in \{\, y \in D \mid P(x) \,\}\, (Q(x))$$

Let $P(x)$ and $Q(x)$ be predicates with D the common domain of x. We write $P(x) \implies Q(x)$ to mean $\forall x \in D(P(x) \to Q(x))$ when there is no risk for confusion of the domain D. Similarly, we write $P(x) \iff Q(x)$ to mean $\forall x \in D(P(x) \leftrightarrow Q(x))$

Theorem 3.1. *Let $P(x)$ be a predicate with D as the domain of x in P. Then the statement $\neg\,(\forall x \in D(P(x)))$ is logically equivalent to $\exists x \in D(\neg P(x))$.*

Proof. Recall, from Definition 3.3, $\forall x \in D(P(x))$ is true if, and only if, $P(x)$ is true for every x in D. Thus, $\neg\,(\forall x \in D(P(x)))$ is true if, and only if, there is some x in D such that $P(x)$ is not true. Though, that is true if, and only if, for some x in D $\neg P(x)$ is true. Thus, $\neg\,(\forall x \in D(P(x)))$ holds if, and only if, $\exists x \in D(\neg P(x))$. □

Corollary 3.2. *A statement of the form $\neg\,(\exists x \in D(P(x)))$ is logically equivalent to $\forall x \in D(\neg P(x))$.*

Proof. Left and as an exercise to the reader. □

Exercise 3.1. Prove Corollary 3.1

Example 3.11. Write the negation of the statements:

- Every prime is odd.
  The negation of the above statement is: "There exists an even prime".
- There is a triangle whose angles sum to 200°.
  The negation of the above statement is: "The sum of angles of any triangle is not 200°".

Proposition 3.3. *Let $P(x)$ and $Q(x)$ be predicate statements with D the common domain of x in P and Q. Then $\neg\,(\forall x \in D(P(x) \to Q(x)))$ is logically equivalent to $\exists x \in D(P(x) \wedge \neg Q(x))$.*

Proof. Left as an exercise to the reader. □

Exercise 3.2. Prove Proposition 3.3

Example 3.12. Write the negation of the statements:

- If any bird sings, then it is a robin.
  The negation of the above statement is: "There is a bird that sings and is not a robin".

- For any integer x, if x is not 0 or 1, then $x^2 \neq x$.
  The negation of the above statement is: "There is an integer x such that $x \neq 0, 1$ and $x^2 = x$".

Recall that we say that a conditional statement, $p \to q$ is vacuously true provided p is false. In the same way, we say that a statement of the form $\forall x \in D(P(x) \to Q(x))$ is vacuously true if $\forall x \in D \; P(x)$ is true. Further, we define the converse, inverse, and contrapositive fir quantified conditional statements similar to how we defined them for conditional statements $p \to q$. That is, for a statement of the form $P(x) \implies Q(x)$:

- its converse is $Q(x) \implies P(x)$,

- its inverse is $\neg P(x) \implies \neg Q(x)$, and

- its contrapositive is $\neg Q(x) \implies \neg P(x)$.

Exercise 3.3. Show that $P(x) \implies Q(x)$ is logically equivalent to $\neg Q(x) \implies \neg P(x)$.

Exercise 3.4. Show that $P(x) \implies Q(x)$ is not logically equivalent to $Q(x) \implies P(x)$ and $\neg P(x) \implies \neg Q(x)$.

Similar to Definition 2.6

- "For all x, $R(x)$ is a sufficient condition for $S(x)$" means $R(x) \implies S(x)$.

- "For all x, $R(x)$ is a necessary condition for $S(x)$" means $\neg R(x) \implies \neg Q(x)$.

- "For all x, $R(x)$ only if $S(x)$" means $\neg S(x) \implies \neg R(x)$.

Example 3.13. The *reciprocal* of a real number, a, is a real number, b, such that $ab = 1$.

Write the following formally using quantifiers and variables:

- Every non-zero real number has a reciprocal.

$$\forall a \in \mathbb{R}(a \neq 0 \rightarrow \exists b \in \mathbb{R}(ab = 1))\,.$$

- There is a real number with no reciprocal:

$$\exists a \in \mathbb{R} \forall b \in \mathbb{R}(ab \neq 1)\,.$$

Example 3.14. Write the following formally using quantifiers and variables:

- There is a smallest positive integer.

$$\exists a \in \mathbb{Z}(a > 0 \wedge \forall b \in \mathbb{Z}(b > 0 \rightarrow a \leq b))\,.$$

- There does not exist a smallest positive real number.

$$\forall a \in \mathbb{R}(a > 0 \rightarrow \exists b(b > 0 \wedge b < a))\,.$$

Example 3.15. The definition of a limit, from calculus, uses both $\forall$ and $\exists$ as well as an if-then statement. We say the limit of a sequence a_n as $n \rightarrow \infty$ is L, written $\lim_{n\rightarrow} a_n = L$, if, and only if, for any fixed tolerance there exists a point in the sequence where the values a_n are within that tolerance to L. That is, $\lim_{n\rightarrow\infty} a_n = L$ if, and only if,

$$\forall \epsilon \in \mathbb{R}(\epsilon > 0 \rightarrow \exists N \in \mathbb{N} \forall n \in \mathbb{N}(N < n \rightarrow |a_n - L| < \epsilon))\,.$$

Exercise 3.5. Write the following statements so that the negation is not applied directly to a quantifier.

(a) $\neg \forall x \in D \forall y \in E\, P(x, y)$

(b) $\neg \forall x \in D \exists y \in E\, P(x, y)$

(c) $\neg \exists x \in D \forall y \in E\, P(x, y)$

(d) $\neg \exists x \in D \exists y \in E\, P(x, y)$

4 Direct Proofs

Definition 4.1. An integer n is said to be *even* if there exists an integer k such that

$$n = 2k\,.$$

Definition 4.2. An integer n is said to be *odd* if there exists an integer k such that

$$n = 2k + 1\,.$$

The following exercise is incomplete, it requires the fact that $\mathbb{Z}$ is closed under $+$ and $*$. Currently, that fact is asserted without proof.

Example 4.1. Use the definitions for even and odd, Definitions 4.1 and 4.2, to justify that:

1. 0 is even.
   Note that $0 \in \mathbb{Z}$ and $0 = 2(0)$, thus by Definition 4.1 0 is even.

2. -301 is odd.
   Note that $-151 \in \mathbb{Z}$ and $-301 = 2(-151) + 1$, thus by Definition 4.2 -301 is odd.

3. if $a, b \in \mathbb{Z}$, then $6a^2b$ is even.
   Fix $a, b \in \mathbb{Z}$. Note that as $\mathbb{Z}$ is closed under $*$ and $3 \in \mathbb{Z}$, $3 * a^2b = 3aab \in \mathbb{Z}$. Similarly, as $6 \in \mathbb{Z}$ $6a^2b \in \mathbb{Z}$ Thus, by Definition 4.1 $6a^2b = 2(3a^2b)$ is even.

Definition 4.3. An integer $1 < p$ is said to be *prime* provided for all positive integers a and b if $ab = p$, then $a = p$ or $b = p$.

Definition 4.4. An integer $1 < c$ is said to be *composite* if c there exists integers a and b such that $c = ab$ and $1 < a, b < c$

This example is incomplete. It requires proof that $\forall a, b \in \mathbb{Z}^+ \; a, b \leq ab$. That is, multiplication on $\mathbb{Z}^+$ is not decreasing.

Example 4.2. 1. Show that 1 is not prime.
Note, Definition 4.3 of prime requires that a prime integer be greater than 1. $1 \not< 1$, so 1 is not prime.

2. Show that 6 is composite.
   Note that $2 * 3 = 6$ and $2, 3 \neq 1$ and $2, 3 \neq 6$. So 6 is not prime.

3. Write the first 2 primes and justify their primeness.
   Note that any prime must be larger than 1. So, we begin our search at the first integer after 1, 2.

   Note that as multiplication on $\mathbb{Z}^+$ is not decreasing, the only possible factors of 2 are in the set $\{1, 2\}$. As $1 * 1 \neq 2$ and $2 * 2 \neq 2$ but $1 * 2 = 2 * 1 = 2$, we have that 2 is prime.

   The only positive integer less than 3 but not 1 or 3 is 2. Though, we note that none of $1*2$, $2*2$, and $2*3$ are not 3. Thus, the only integers whose product is 3 are 1 and 3.

The following proof uses that $\forall a, b, c \in \mathbb{Z}(a(b + c) = ab + ac)$ without proof.

The following are some examples utilizing a style of proof called a *constructive proof*. This style of proof is used to show existential statements, that is to show the existence of some object. constructive proofs are those proofs which explicitly produce a desired object.

Example 4.3. 1. Show that there exists an even integer which can be written two ways as the sum of two positive integers.

   Proof. Note that $n = 10 = 2 * 5$ is even and

$$n = 5 * 5 = 7 + 3\,.$$

□

2. Let $r, s \in \mathbb{Z}$, show that $22r + 18s$ is even.

   Proof. Fix $r, s \in \mathbb{Z}$. To show that $22r + 18s$ is even, we must show that there exists (or construct) $k \in \mathbb{Z}$ such that

$$22r + 18s = 2k\,.$$

Let $k = 11r + 9s$. Note that

$$\begin{aligned} 2k &= 2(11r + 9s) \\ &= 2 * 11r + 2 * 9s \\ &= 22r + 18s \end{aligned}$$

as desired. □

3. Show that $\forall a, b \in \mathbb{Z}(a^2 = b^2 \to a = b)$ is not true.

   Proof. To show that $\forall a, b \in \mathbb{Z}(a^2 = b^2 \to a = b)$ is not true, it sufficese to show that there exists $a, b \in \mathbb{R}$ distinct such that $a^2 = b^2$. Consider $a = 1$ and $b = -1$. Note that $a = 1 \neq -1 = b$ but $1^2 = 1 = (-1)^2$. □

Proposition 4.1. *The sum of two even integers is even.*

Proof. Let a and b be arbitrary even integers. As a and b are even there exists $k, l \in \mathbb{Z}$ such that $a = 2k$ and $b = 2l$. Then, we note that

$$\begin{aligned} a + b &= 2k + 2l \\ &= 2(k + l)\,. \end{aligned}$$

Though, as $k, l \in \mathbb{Z}$, $k + l \in \mathbb{Z}$, set $m = k + l$. Then we note that $m \in \mathbb{Z}$ and $a + b = 2m$, and whence $a + b$ is even. □

Proposition 4.2. *The sum of two odd integers is even.*

Proof. Left as an exercise to the reader. □

Exercise 4.1. Prove Proposition 4.2.

Proposition 4.3. *The sum of an even integer and an odd integer is odd.*

Proof. Left as an exercise to the reader. □

Exercise 4.2. Prove Proposition 4.3.

Proposition 4.4. *The product of two odd integers is odd.*

Proof. Left as an exercise to the reader. □

Exercise 4.3. Prove Proposition 4.4.

Proposition 4.5. *The product of an even integer and an odd integer is even.*

Proof. Left as an exercise to the reader. □

Exercise 4.4. Prove Proposition 4.5.

Exercise 4.5. Use Propositions 4.1. 4.2, 4.3, 4.4, and 4.5 to show that if $a \in \mathbb{Z}$ is even and $b \in \mathbb{Z}$ is odd, then

$$\frac{a^2 + b^2 + 1}{2}$$

is an integer.

Definition 4.5. A real number r is said to be *rational* if, and only if, $\exists a, b \in \mathbb{Z}$ with $b \neq 0$ and $rb = a$.

We denote the set of rational numbers $\mathbb{Q}$.

Example 4.4.

1. Show $\frac{10}{3}$, $-\frac{5}{34}$, 0.28, are rational.

2. is 0 rational?

3. is $0.\overline{21}$ rational?

4. if m, n are rational, show $\frac{m+n}{nm}$ is rational.

Proposition 4.6. $\forall n \in \mathbb{Z}(n \in \mathbb{Q})$.

Proof. Fix $n \in \mathbb{Z}$ arbitrary. To show n is rational, i.e. $n \in \mathbb{Q}$, it suffices to show that there exists $a, b \in \mathbb{Z}$ such that $nb = a$. Note $n, 1 \in \mathbb{Z}$, $1 \neq 0$, and $1n = n$. Thus by Definition 4.5, n is rational. □

Proposition 4.7. *If r and s are rational, then $r + s$ is rational.*

Proof. Fix r and s rational. This means, by Definition 4.5, there exists $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$ such that $sb = a$ and $rd = c$. Note that as $a, b, c, d \in \mathbb{Z}$, $ad + bc, bd \in \mathbb{Z}$ and as $b, d \neq 0$ $bd \neq 0$. Finally, we see that

$$\begin{aligned} bd(s + r) &= bds + bdr \\ &= da + bc\,. \end{aligned}$$

Thus, by Definition 4.5, $s + r$ is rational. □

Proposition 4.8. *The double of a rational is rational.*

Proof. Fix $r \in \mathbb{Q}$. As $r \in \mathbb{Q}$ we have by Proposition 4.7, the double of r, $2r = r + r$ is rational. □

Proposition 4.9. *If r and s are rational, then rs is rational.*

Proof. Fix r and s rational. This means, by Definition 4.5, there exists $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$ such that $sb = a$ and $rd = c$. Note that as $a, b, c, d \in \mathbb{Z}$, $ac, bd \in \mathbb{Z}$ and as $b, d \neq 0$ $bd \neq 0$. Finally, we see that

$$\begin{aligned} bd(sr) &= bdsr \\ &= bsdr \\ &= ac\,. \end{aligned}$$

Thus by Definition 4.5, sr is rational. □

Definition 4.6. An integer $d \neq 0$ is said to *divide* an integer n provided, written $d|n$, provided there exists an integer k such that $n = dk$. We will write $a \nmid b$ to mean $\neg(a|b)$.

Example 4.5. If $n \in \mathbb{Z}$, then does n divide 0?
Yes, as for any integer n, $0 \in \mathbb{Z}$ and $0 = 0k$. Whence, $n|0$.

5 Proofs Which May Branch

Proposition 5.1. *For any integers a and b if a and b are positive and $a|b$, then $a \leq b$.*

Proof. Fix $a, b \in \mathbb{Z}$ such that a and b are positive and $a|b$. As $a|b$ there exists $k \in \mathbb{Z}$ such that $b = ak$. As $a, b > 0$, $\frac{b}{a} > 0$, thus

$$0 < \frac{b}{a} = k\,.$$

Whence, $k > 0$. As $k \in \mathbb{Z}$ and $k > 0$, $k \geq 1$. Finally, we have

$$a \leq ka = b$$

. □

Proposition 5.2. *The divisors of* 1 *are* 1 *and* -1.

Proof. Note that $1 = 1 \cdot 1 = -1 \cdot -1$. So, $-1, 1|1$.

Now, it suffices to show that $\forall m \in \mathbb{Z}(m|1 \to m = 1, -1)$. Suppose $m \in \mathbb{Z}$ and $m|1$. As $m|1$ there exists $n \in \mathbb{Z}$ such that $mn = 1$ We note that either m and n are both positive, or both negative.

Case 1. m and n are both positive. Then Proposition 5.1, $m \leq 1$. But, m is positive, so $0 < m \leq 1$. Finally, as $m \in \mathbb{Z}$ and $0 < m \leq 1$, $m = 1$.

Case 2. m and n are both negative. Then $(-m)(-n) = mn = 1$. So, $-m$ and $-n$ are positive. Thus, the previous case gives that $-m = 1$. Whence, $m = -1$. □

Proposition 5.3. *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.*

Proof. Fix $a, b, c \in \mathbb{Z}$ such that $a|b$ and $b|c$. As $a|b$ and $b|c$ there exists $r, s \in \mathbb{Z}$ such that

$$b = ra \text{ and } c = sb\,.$$

So,

$$\begin{aligned} c &= sb \\ &= s(ra) \\ &= (sr)a\,. \end{aligned}$$

And as $s, r \in \mathbb{Z}$ $sr \in \mathbb{Z}$. Therefore, $a|c$. □

Lemma 5.4. *For every integer $n > 1$, n is prime if, and only if, n is not composite.*

Proof. Fix any integer $n > 1$. Suppose n is prime. By the definition of n prime, the only factors of n are 1 and n. Thus, $\nexists r, s \in \mathbb{Z}(n = rs \wedge 1 < r, s < n)$. Showing that n is not composite.

Suppose that n is not prime. As n is not prime, there exists $r, s \in \mathbb{Z}$ such that $n = rs$ and neither r nor s are 1 or n. Note, as n is positive, r and s share the same sign. With out loss of generality, we may assume r and s are positive as otherwise we may replace them with $-r$ and $-s$. Finally, as $rs = n$ and multiplication of positive integers is non-decreasing, $r, s \leq n$. As neither r nor s is 1 and r, s is positive we have that $1 < r, s$ and $r, s \leq n$. Thus, by Definition 4.4, n is composite. □

Proposition 5.5. *For any integer n if $n > 1$, then n is divisible by a prime.*

Proof. Fix $n \in \mathbb{Z}$ such that $n > 1$. If n is prime, then there is nothing to show. So, suppose that n is not prime.

As n is not prime, it is composite, and there exists integers r_0, s_0 such that $n = r_0 s_0$ and $1 < r_0, s_0 < n$. As $n = r_0 s_0$, $r_0 | n$.

If r_0 is prime, we are dode. Otherwise, there exists $r_1, s_1 \in \mathbb{Z}$ such that $1 < r_1, s_1 < r_0$ and $r_0 = r_1 s_1$. As $r_0 = r_1 s_1$, we have that $r_1 | r_0$. Though, as $r_1 | r_0$ and $r_0 | n$, by Proposition 5.3, $r_1 | n$.

If r_1 is prime, we are done. Otherwise, we continue in this fashion producing ever smaller integers which divide n. This process must terminate, as each successive factor is greater than 1 but less than n, and there are only finitely many integers between 1 and n. □

The proof of this next lemma requires a technique which we have not covered, yet. This techniques is called strong induction. Strong induction is a strengthening of regular induction. Regular induction is a proof technique to show a claim holds over a well-ordered sets (which do not contain a limit – this is outside the scope of this class). You show that a claim holds at a base cases. After the base case you show the successor case; that if the claim holds at a specific place, then it necessarily holds at the next place. After you show these two things, Strong induction differs from regular, weak, induction in the successor case. In strong induction, we suppose that the claim holds everywhere at and bellow a point and then show that it holds at the next point.

The above exposition is not necessary. Though, as induction is one of the more valuable skills learned in this course, I want to get a little jump start the the subject.

Lemma 5.6. *Every integer $n > 1$ is either prime or a product of primes.*

Proof. We show this via strong induction on n. For the base case, where $n = 2$, we note that 2 is prime. Thus, the claim holds at $n = 2$.

Now, suppose that $n > 1$ and every integer $m > n$ is either prime or a product of primes. If n is prime, there is nothing to show. Otherwise n is not prime, so by Lemma 5.4 n is composite. Thus, there exists $r, s \in \mathbb{Z}$ such that $1 < r, s < n$. Though, as $1 < r, s < n$ our inductive hypothesis applies to r and s, so r and s are a product of primes. Whence, $n = rs$ is a product of primes. □

The proof of the next theorem requires the use of the fact that $\mathbb{N}$ is well-ordered by $<$. This means two things. First, $\mathbb{N}$ is totally ordered by $<$, that is $\forall a, b \in \mathbb{N}\ a < b \vee a = b \vee b < a$. Second, every nonempty subset of $\mathbb{N}$ has a $<$ least element.

Theorem 5.7. ***(Fundamental Theorem Of Arithmetic)*** *Given any integer $n > 1$, there exists a positive integer k, distinct primes $p_1, p_2, \ldots, p_k$ and positive integers $a_1, a_2, \ldots, a_k$ such that*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

and any other expression is identical up to order.

Proof. First, we will show existence of such a factorization. Let $n > 1$ be an arbitrary integer. If n is prime, we are done. Otherwise, by Lemma 5.6, n is a product of primes. Say $n = q_1 q_2 \cdots q_{k'}$ for some $k' \in \mathbb{N}$. Certainly, it need not be the case that the k_is are unique. Let $k \leq k'$ be the number of unique primes within $q_1, q_2, \ldots q_{k'}$. Enumerate the unique primes within $q_1, q_2, \ldots q_{k'}$ as $p_1, p_2, \ldots, p_k$. Finally, for each i let a_i be the number of times p_i occurs within $q_1, q_2, \ldots q_{k'}$. Then,

$$\begin{aligned} n &= q_1 q_2 \cdots q_{k'} \\ &= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \end{aligned}$$

as desired. Though, as $1 < n \in \mathbb{Z}$ was arbitrary, such a factorization exists for all integers larger than 1.

Now, we show uniqueness. Suppose, towards a contradiction that there exists an integer which can be factored as above in two distinct ways. As there exists such an integer, as $\mathbb{N}$ is well-ordered by $<$ we may let n be the least $n > 1$ with two distinct prime factorizations as above. Note, this implies n is not prime. Say

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l} .$$

Note, as n is not prime $k, l \geq 2$. As $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, p_1 divides n. So, n divides $q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$, and so there exists some $i < l$ so that $p_1 | q_i$. Without loss of generalit, we may reorder the q_is so that $p_1 | q_1$. As q_1 is prime and $p_1 | q_1$, $p_1 = q_1$. Thus

$$p_1^{a_1 - 1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1 - 1} q_2^{b_2} \cdots q_l^{b_l}$$

are distinct prime factorizations for an integer below n. contradicting the minimality of n. Thus, no such n may exist. □

Theorem 5.8. ***(Quotient-Remainder Theorem)*** *Given an integer n and positive integer d, there exists unique integers q and r such that $0 \leq r < d$ and $n = qd + r$.*

Proof. Fix $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.

First, we will show existence. Consider the set of non-negative integers of the form $n - dq$. This set is clearly non-empty. Thus, as $\mathbb{N}$ is well-ordered, this set contains a least element, say $r = n - dq$. Certianly, $r \geq 0$. Now, $r < d$ as as otherwise $n - d(q + 1)$ contradicts the minimality of r.

Now to show uniqueness. Suppose that there exists $q_0, q_1, r_0, r_1 \in \mathbb{Z}$ with $0 \leq r_0, r_1 < d$ and

$$n = dq_0 + r_0 = dq_1 + r_1 .$$

Note, as $dq_0 + r_0 = dq_1 + r_1$, it suffices to show $r_0 = r_1$. Rewriting $dq_0 + r_0 = dq_1 + r_1$, we see that $r_0 - r_1 = d(q_1 - q_0)$ showing that $d | (r_0 - r_1)$. Further, as $0 \leq r_1 < d$, $-d < r_1 \leq 0$. So, $-d < r_0 - r_1 < d$. Though, as $d | (r_0 - r_1)$ and $-d < r_0 - r_1 < d$, $r_0 - r_1 = 0$. □

Exercise 5.1. Show that any integer can be written in the form $4q + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < 4$.

Proposition 5.9. *Every integer is either even or odd, but not both.*

Proof. Fix $n \in \mathbb{Z}$ arbitrary. As $2 \in \mathbb{Z}$ is positive and $n \in \mathbb{Z}$, the Quotient Remainder Theorem, Theorem 5.8, applies, and there exist $q, r \in \mathbb{Z}$ such that $0 \leq r < 2$ and $n = 2q + r$. Though, as $r \in \mathbb{Z}$ and $0 \leq r < 2$, $r = 0, 1$. Therefore, $n = 2q$ or $n = 2q + 1$. Thus, n is either even or odd. Moreover, as the Quotient Remainder Theorem give that q and r are unique, n cannot be even and odd. □

Definition 5.1. Let n be an integer. The *parity* of n refers to n being even or odd. We say that n has even parity if n is even and odd parity to say n is odd. We say two integers have opposite parity to mean one is even and the other odd.

Proposition 5.10. *Any pair of consecutive integers have opposite parity.*

Proof. Fix $n \in \mathbb{Z}$ arbitrary. Using Proposition 5.9, m is either even or odd.

Case 1: m is even. As m is even $m = 2k$ for some k. So, $m + 1 = 2k + 1$, so $m + 1$ is odd. Thus, m and $m + 1$ have opposite parity.

Case 2: m is odd. As m is even $m = 2k+1$ for some k. So, $m+1 = 2(k+1)$, so $m + 1$ is even. Thus, m and $m + 1$ have opposite parity. □

Proposition 5.11. *The square of an odd integer has the form $8m + 1$ for some $m \in \mathbb{Z}$.*

Proof. Fix $n \in \mathbb{Z}$ odd. Using the Quotient Remainder Theorem, we hav have that n has the form $4q + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < 4$. As $n = 4q + r$ is odd, $r \neq 0, 2$. So, $r = 1$ or $r = 3$.

In the case that $r = 1$, then $n = 4q + 1$. So,

$$\begin{aligned} n^2 &= (4q + 1)^2 \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1\,. \end{aligned}$$

Note that as $q \in \mathbb{Z}$ $2q^2 + q \in \mathbb{Z}$. Thus, n^2 has the desired form.

In the case that $r = 1$, then $n = 4q + 3$ we have that

$$\begin{aligned} n^2 &= (4q + 3)^2 \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + 8 + 1 \\ &= 8(2q^2 + 3q + 1) + 1\,. \end{aligned}$$

Note that as $q \in \mathbb{Z}$ $2q^2 + 3q + 1 \in \mathbb{Z}$. Thus, n^2 has the desired form. □

Definition 5.2. Let n be an integer and d a positive integer. Then the Quotient Remainder Theorem, Theorem 5.8, applies, and there exists unique integers q and r such that $0 \leq r < d$ and $n = qd + r$. We define

$$n \bmod d = r \quad \textit{and} \quad n \operatorname{div} d = q$$

to denote the integer quotient and remainder after division by d respectively.

Example 5.1. Suppose $m \in \mathbb{Z}$ and $m \bmod 11 = 6$. Compute $4m \bmod 11$.

$m \bmod 11 = 6$ means there exists $q \in \mathbb{Z}$ such that $m = 11q + 6$. Whence,

$$\begin{aligned} 4m &= 4(11q + 6) \\ &= 11 \cdot 4q + 24 \\ &= 11 \cdot 4q + 11 \cdot 2 + 2 \\ &= 11(4q + 2) + 2\,. \end{aligned}$$

Thus, $4m \bmod 11 = 2$.

Definition 5.3. Let x be a real number, then the *absolute value* of x, $|x|$ is defined as

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

Lemma 5.12. $\forall r \in \mathbb{R}(-|r| \leq r \leq |r|)$.

Proof. Fix $r \in \mathbb{R}$. Either $r \geq 0$ or $r < 0$.

In the case that $r \geq 0$, then by Definition 5.3, $r = |r|$. As $r = |r|$, $r \leq |r|$. As $r \geq 0$, $-r \leq 0$ So, $-r = -|r| \leq 0 \leq r \leq |r|$.

In the case that $r <$, then by Definition 5.3, $|r| = -r$. So, $-|r| = r$, and hence $-|r| \leq r$. Further, as $r < 0$, $-r = |r| > 0$. Thus, $-|r| \leq r \leq |r|$. □

Lemma 5.13. $\forall r \in \mathbb{R}(|r| =\leq |-r|)$.

Proof. Certanily, from Definition 5.3, for any $x \in \mathbb{R}$

$$\begin{aligned} |x| &= \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} \\ &= \begin{cases} x & x > 0 \\ 0 & x = 0 \\ -x & x < 0 \end{cases} \end{aligned}$$

Now, fix $r \in \mathbb{R}$. Using the observation above, we have

$$\begin{aligned} |-r| &= \begin{cases} -r & -r > 0 \\ 0 & -r = 0 \\ r & -r < 0 \end{cases} \\ &= \begin{cases} r & r < 0 \\ 0 & r = 0 \\ r & r > 0 \end{cases} \\ &= |r| \end{aligned}$$

□

Lemma 5.14. $\forall x, y \in \mathbb{R}(|x + y| \leq |x| + |y|)$.

Proof. Fix $x, y \in \mathbb{R}$. Either $x + y \geq 0$ or $x + y < 0$.

In the case that $x + y \geq 0$, then by Definition 5.3, $|x + y| = x + y$. Applying Lemma 5.12, $x \leq |x|$ and $y \leq |y|$. So, $|x + y| = x + y \leq |x| + |y|$.

In the case that $x + y <$, then by Definition 5.3,

$$\begin{aligned} |x + y| &= -(x + y) \\ &= -x - y \end{aligned}$$

Applying Lemma 5.12, $-x \leq |-x|$ and $-y \leq |-y|$. Applying Lemma 5.13, $|-x| = |x|$ and $|-y| = |y|$. So, $-x \leq |x|$ and $-y \leq |y|$ Finally, we have that

$$\begin{aligned} |x + y| &= -(x + y) \\ &= -x - y \\ &= -x + (-y) \\ &\leq |x| + |y| . \end{aligned}$$

□

6 Suppose Otherwise

The central idea of proving a statement by contradiction is that mathematics must be non-contradictory. That is, for any statement ϕ either ϕ is true or ϕ is false but not both! More formally, the statement form $\neg(p \wedge \neg p)$ is a tautology.

It should be noted that proofs by contrition, while valid, are often undesirable. This is because proofs by contradiction often do not reveal the same insight offered by constructive or direct proofs. Further, proofs by contradiction can often, if done without care, feel inelegant, much like a sledgehammer.

Suppose we are attempting to prove a statement ϕ via contradiction. The common structure of a proof by contradiction is as follows.

Proof. Suppose, towards a contradiction, $\neg\phi$.
Unpack what $\neg\phi$ means.
Perform some work and obtain a formula $\neg\psi$ where we know ψ to be true before we supposed $\neg\phi$.
This gives ψ and $\neg\psi$, a contradiction.
Whence, ϕ. □

Now, the above is a simple sketch of a near ideal argument. In practice, this argument can take many forms. In this section, we will show some examples of this technique to help the reader become more familiar with the process.

Proposition 6.1. *There is no greatest integer.*

Proof. Suppose, towards a contradiction, that there is a greatest integer. That is, there exists some $n \in \mathbb{Z}$ such that $\forall m \in \mathbb{Z}\ m \leq n$. Consider $n+1$. As $\mathbb{Z}$ is closed under successors, the operation $\cdot \mapsto \cdot + 1$, $n+1 \in \mathbb{Z}$. Though, $n \lneq n+1$ contradicting our assumption of n. Thus, there is not greatest integer. □

Proposition 6.2. *No integer is both even and odd.*

Proof. Suppose, towards a contradiction, that there is an integer which is both even and odd. Let $n \in \mathbb{Z}$ be such an integer. As n is both even and odd, there exists $a, b \in \mathbb{Z}$ such that

$$2a = n = 2b + 1\,.$$

Though,

$$\begin{aligned} && n &= n \\ \implies && 2a &= 2b + 1 \\ \implies && 2a - 2b &= 1 \\ \implies && a - b &= \frac{1}{2} \\ && &\notin \mathbb{Z} \end{aligned}$$

Though, as $a, b \in \mathbb{Z}$ $a - b \in \mathbb{Z}$, a contradiction. Whence, there is no integer which is both even and odd. □

Definition 6.1. A real number r is said to be *irrational* if, and only if, r is not rational

Proposition 6.3. *The sum of a rational number and an irrational number is irrational.*

Proof. Suppose towards a contradiction that this is false. Thus, there exists a rational r and an irrational s so that $r + s$ is rational. Though, as r is rational by Proposition 4.9, $-r$ is rational. Further, as $r+s$ and $-r$ are ration applying Proposition 4.7, $r + s + (-r) = s$ is rational, a contradiction. □

Proof by contrapositive.
Suppose we are tasked with proving a statement of the form $\forall x(P(x) \to Q(x))$. Suppose further that the predicate $P(x)$ gives little in the way of describing $Q(x)$ (that is, showing $\forall x(P(x) \to Q(x))$ is hard). Then, maybe before we attempt a proof via contradiction, we can attack the problem directly from a different direction. That is, recall that $\forall x(P(x) \to Q(x))$ is logically equivalent to its contrapositive $\forall x(\neg Q(x) \to \neg P(x))$. So, a proof of $\forall x(P(x) \to Q(x))$ by contradiction is a direct proof of $\forall x(\neg Q(x) \to \neg P(x))$. The following lemma is an example of this technique.

Lemma 6.4. *For every integer n if n^2 is even, then n is even.*

Proof. Fix $n \in \mathbb{Z}$ and suppose that n is not even. As n is not even, we have by Proposition 5.9 that n is odd. As n is odd, there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. So,

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1\,, \end{aligned}$$

showing n^2 is odd. Again, by Proposition 5.9, as n^2 is odd n^2 is not even. $\square$

7 Some Proofs Worth Knowing

The following section contains some classic Theorems the proofs of which every young mathematician is expected to be familiar with.

Theorem 7.1. $\sqrt{2}$ *is irrational.*

Proof. Suppose otherwise. That is, $\sqrt{2}$ is rational.

As $\sqrt{2}$ is rational, there exists $a, b \in \mathbb{Z}$ such that $\sqrt{2}b = a$ and $b \neq 0$. Write $\sqrt{2} = \frac{a}{b}$.

Suppose further that a and b share no common factors. That is, $\forall k \in \mathbb{Z}(k \nmid a \vee k \nmid b)$. (We can do this by using the Fundamental Theorem of Arithmetic, writing out the finite prime factorizations of a and b and 'cancelling' like primes.)

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

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

Thus,

$$a^2 = 2b^2\,,$$

showing that a^2 is even. So, using Proposition 6.4, we have that a is even. As a is even, there exists $k \in \mathbb{Z}$ such that $a = 2k$. Substituting $a = 2k$ in $2 = \frac{a^2}{b^2}$, we have

$$2 = \frac{4k^2}{b^2}\,,$$

thus

$$b^2 = 2k^2\,.$$

So, b^2 is even. Using Proposition 6.4 yet again shows that b is even. So, b can be written as $2l$ for some $l \in \mathbb{Z}$.

Though, this shows that a and b are divisible by 2, contradicting that a and b share no common factors. Thus, $\sqrt{2}$ is irrational. □

Legend holds that the previous Theorem cost the life of a mathematician thousands of years ago. The legend, as I was taught, is as follows:

The Pythagoreans, those that follow the philosophy Pythagoras, believed that the universe was built of whole numbers. What we call integer. Further, they believed that the universe, and every measurement within it, is rational.

Now, the name Pythagoras aught to be familiar, as that is the name which we attribute the following well know geometric theorem:

Theorem 7.2. ***(Pythagorean Theorem)*** *Let a and b the length of the legs of a right triangle and c the length of its hypotenuse c, then $a^2 + b^2 = c^2$.*

Proof. Proof to come. □

The Pythagorean Theorem, Theorem 7.2, can be proved using a straightedge and compass. Further, the object which the Pythagorean Theorem applies can be construct, in a real way. Thus, the measurement given by the Pythagorean Theorem truly exist. So, if one draws a unit square, whatever that unit may be, then the diagonal of that square must necessarily square to be 2 units. That is, the square root necessarily exists within our world.

The consequences of Theorem 7.1, when presented to them, were catastrophic to the world view of the Pythagoreans. Necessarily, their world view was, provably, incorrect. So, when Hippasus of Metapontum presented this theorem to his fellow Pythagoreans, his fellow Pythagoreans drowned him.

Proposition 7.3. *For any integer a and prime p if $p|a$, then $p \nmid (a+1)$.*

Proof. Suppose otherwise. That is, there exists some $a \in \mathbb{Z}$ and p prime such that $p|a$ and $p|(a+1)$. As $p|a$ and $p|(a+1)$, there exists $r, s \in \mathbb{Z}$ such that

$$rp = a \quad \text{and} \quad sp = a + 1\,.$$

Then,

$$\begin{aligned} 1 &= a + 1 - a \\ &= rp - sp \\ &= (r - s)p\,. \end{aligned}$$

So, as $(r - s) \in \mathbb{Z}$, $p|1$. So, by Proposition 5.2, $p = \pm 1$. But p is prime, so $p > 1$, a contradiction. □

Theorem 7.4. *There are infinitely many primes.*

Proof. Suppose otherwise. That is, there exists finitely many primes. As there are finitely many primes, we may enumerate them as

$$p_1, p_2, \ldots, p_n$$

for some $n \in \mathbb{N}$. Set,

$$P := p_1 p_2 \cdots p_n\,.$$

Let i any integer with $1 \leq i \leq n$. As $P = p_1 p_2 \cdots p_n$, $p_i | P$. Thus, by Proposition 7.3, $p \nmid (P+1)$. Thus, $P+1$ is not divisible by any prime p_i. Though, the p_i enumerate all of the primes, so $P+1$ is not divisible by a prime.

As $P+1$ is not divisible by any prime, the Fundamental Theorem Of Arithmetic provides, the prime factorization of $P+1$ is itself. Whence, $P+1$ itself is prime. Though, there does not exist an i with $1 \leq i \leq n$ such that $p_i = P+1$, as shown earlier. Thus the prime $P+1$ is not on our list of all primes, contradicting that we listed all of the primes. Thus, there are infinitely many primes. □

8 Sequences

Definition 8.1. A *sequence* is a function whose domain is some subset of $\mathbb{N}$. For a sequence s, we typically write s_i in place of $s(i)$. We refer to an individual value, s_i, as a *term* in the sequence and i as the *index* of that term

For a sequence s, an *explicit formula* of s is a rule or formula which depends on the index of the sequence.

Example 8.1. Compute the first four terms of the sequences:

1. $a_k = \frac{k}{k+1}$ where $k \geq 1$.

$$a_1 = \frac{1}{2} \quad a_2 = \frac{2}{3} \quad a_3 = \frac{3}{4} \quad a_4 = \frac{4}{5}$$

2. $b_i = \frac{i-1}{i}$ where $i \geq 2$.

$$b_2 = \frac{1}{2} \quad b_3 = \frac{2}{3} \quad b_4 = \frac{3}{4} \quad b_5 = \frac{4}{5}$$

3. $c_j = (-1)^j$ where $j \in \mathbb{N}$.

$$c_0 = 1 \quad c_1 = -1 \quad c_2 = 1 \quad c_3 = -1$$

Example 8.2. Write an explicit formula for the sequence:

$$1, -\frac{1}{4}, \frac{1}{9}, -\frac{1}{16}, \frac{1}{25}, -\frac{1}{36}\,.$$

$s_k = (-1)^k \frac{1}{(k+1)^2}$ where $k \in \mathbb{N}$.

Definition 8.2. Let $n, m \in \mathbb{N}$ with $n < m$, and s be a sequence of reals such that $\{\, i \in \mathbb{N} \mid m \leq i \leq n \,\} \subseteq \operatorname{dom}(s)$. We write the *sum* of s_i form n to m as

$$\sum_{i=n}^{m} s_i := s_n + s_{n+1} + s_{n+2} + \cdots + s_{m-1} + s_m\,.$$

Example 8.3.

$$\begin{aligned}\sum_{k=1}^{5} k^2 &= 1^2 + 2^2 + 3^2 + 4^2 + 5^2 \\ &= 1 + 4 + 9 + 16 + 25 \\ &= 55\,.\end{aligned}$$

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k(k+1)} &= \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{(n-1)\cdot n} + \frac{1}{n\cdot(n+1)} \\ &= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= 1 - \frac{1}{n+1}\end{aligned}$$

Definition 8.3. Let $n, m \in \mathbb{N}$ with $n < m$, and s be a sequence of reals such that $\{\, i \in \mathbb{N} \mid m \leq i \leq n \,\} \subseteq \mathrm{dom}(s)$. We write the *product* of s_i form n to m as

$$\Pi_{i=n}^{m} s_i := s_n s_{n+1} s_{n+2} \cdots s_{m-1} s_m\,.$$

Definition 8.4. For $n \in \mathbb{N}$, n *factorial*, $n!$, is defined, recursively, by $0! := 1$ and $n! := n(n-1)!$.

Example 8.4. Compute $n!$ for $n = 0, 1, 2, \ldots, 10$.

1. $0! = 1$, by definiton.

2. $1! = 1 \cdot 0!$ by definition, thus $1! = 1 \cdot 1 = 1$.

3. $2! = 2 \cdot 1! = 2$

4. $3! = 3 \cdot 2! = 3 \cdot 2 = 6$.

5. $4! = 24$

6. $5! = 120$

7. $6! = 720$

8. $7! = 5040$

9. $8! = 40320$

10. $9! = 362880$

11. $10! = 3628800$

Example 8.5. Simplify the following:

1. $\frac{8!}{7!}$

$$\begin{aligned}\frac{8!}{7!} &= \frac{8 \cdot 7!}{7!}\\ &= \frac{8}{1}\\ &= 1\end{aligned}$$

2. $\frac{5!}{2!3!}$

$$\begin{aligned}\frac{5!}{2!3!} &= \frac{5 \cdot 4 \cdot 3!}{2!3!}\\ &= \frac{5 \cdot 4}{2!}\\ &= \frac{5 \cdot 4}{2}\\ &= 5 \cdot 2\\ &= 10\end{aligned}$$

3. $\frac{(n+1)!}{n!}$

$$\begin{aligned}\frac{(n+1)!}{n!} &= \frac{(n+1)n!}{n!}\\ &= \frac{n+1}{1}\\ &= n+1\end{aligned}$$

4. $\frac{n!}{(n-3)!}$

$$\begin{aligned}\frac{n!}{(n-3)!} &= \frac{n(n-1)!}{(n-2)!} \\ &= \frac{n(n-1)(n-2)!}{(n-2)!} \\ &= \frac{n(n-1)}{1} \\ &= n-1\end{aligned}$$

Definition 8.5. Let $n, k \in \mathbb{N}$ with $0 \leq k \leq n$. $\binom{n}{k}$ is read n *choose* k and is defined as

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}\,.$$

Example 8.6. Compute:

1. $\binom{8}{5}$

$$\begin{aligned}\binom{8}{5} &= \frac{8!}{5!(8-5)!} \\ &= \frac{8!}{5!3!} \\ &= \frac{8 \cdot 7 \cdot 6 \cdot 5!}{5!3!} \\ &= \frac{8 \cdot 7 \cdot 6}{3!} \\ &= \frac{8 \cdot 7 \cdot 6}{6} \\ &= 8 \cdot 7 \\ &= 56\end{aligned}$$

2. $\binom{4}{0}$

$$\begin{aligned}\binom{4}{0} &= \frac{4!}{0!(4-0)!}\\ &= \frac{4!}{0!4!}\\ &= \frac{1}{1}\\ &= 1\end{aligned}$$

3. $\binom{n+1}{n}$

$$\begin{aligned}\binom{n+1}{n} &= \frac{(n+1)!}{n!(n+1-n)!}\\ &= \frac{(n+1)n!}{n!(1)!}\\ &= \frac{(n+1)}{1}\\ &= n+1\end{aligned}$$

9 Induction

The principle of mathematical induction is: Let $P(n)$ some predicate where the domain of n is the integers, or some subset of the integers. Let $a \in \mathbb{Z}$ be some fixed value, and suppose that for all $c \geq a$, c is in the domain of n in $P(n)$. Then, if

1. $P(a)$ is true and
2. $\forall k \geq a$ if $P(k)$ is true, then $P(k+1)$ is true,

then $\forall k \geq a(P(k))$ is true. This is known as *weak induction.* Proofs by induction generally follow a common pattern. First, the proof shows (1) holds, this is known as the *base step.* Second, the proof shows (2), which is called the *inductive step.* During the inductive step, the assumption that $P(k)$ holds for some fixed $k \geq a$ is called the *inductive hypothesis.*

Put simply, if $P(n)$ is some predicate with the variable n an integer, then if we can show that $P(a)$ holds for some starting value and that P holding at some value implies that P holds at the next value, then P holds at every value greater that or equal to the base value.

You can think of this as a line of dominos standing upright so that if you knock down one domino, then that domino knocks down its neighbor. Mathematical induction is saying that, in this scenario, if you knock down the first domino, then all of the dominos will be knocked down!

We will see many examples of induction in the future.

Proposition 9.1. *For all integers $n \geq 8$, n¢ can be made with only 3¢ and 5¢ coins.*

Proof. We'll prove this by induction on integers $n \geq 8$.

Base step. 8¢ can be formed using a single 3¢ coin and a single 5¢ coin. Thus, 8¢ can be formed using only 3¢ and 5¢ coins.

Inductive step. Suppose $n \geq 8$ and n¢ can be formed using only 3¢ and 5¢ coins. Let t be the number of 3¢ coins used to form n¢. Similarly, let f be the number of 5¢ coins used to form n¢. Then, out inductive hypothesis gives that $n¢ = t \cdot 3¢ + f \cdot 5¢$. We'll break into cases depending on the value of f. Either $f > 0$ or $f = 0$.

In the case that $f > 0$, then $f - 1 \geq 0$ and

$$\begin{aligned}(n+1)¢ &= n¢ + 1¢ \\ &= (t \cdot 3 + f \cdot 5 + 1)¢ \\ &= (t \cdot 3 + f \cdot 5 + 2 \cdot 3 - 5)¢ \\ &= (t+2)3¢ + (f-1)5¢\,.\end{aligned}$$

Thus, we can form $(n+1)¢$ using just 3¢ and 5¢ coins.

in the case that $f = 0$, we have that $n¢ = t \cdot 3¢$. As $n \geq 8$, we have that $t \geq 3$. So, $t - 3 \geq 0$. Now, similar to before, we have

$$\begin{aligned}(n+1)¢ &= n¢ + 1¢ \\ &= (t \cdot 3 + 1)¢ \\ &= (t \cdot 3 + 2 \cdot 5 - 3 \cdot 3)¢ \\ &= (t-3)3¢ + 2 \cdot 5¢\,.\end{aligned}$$

Thus, we can form $(n+1)¢$ using just 3¢ and 5¢ coins.

So, in either case we can form $(n+1)¢$ using only 3¢ and 5¢ coins. □

Proposition 9.2.

$$\forall n \in \mathbb{N} \quad \sum_{i=0}^{n} i = \frac{n(n+1)}{2}\,.$$

Proof. We'll prove this by induction on integers $n \in \mathbb{N}$.

Base step. By Definition 8.2 and some simple arithmatic, we have that

$$\begin{aligned}\sum_{i=0}^{0} i &= 0 \\ &= \frac{0(0+1)}{2}\,,\end{aligned}$$

and so the claim holds at $n = 0$.

Inductive step. Let $n \in \mathbb{N}$ and suppose that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. Then, by Definition 8.2,

$$\sum_{i=0}^{n+1} i = \left(\sum_{i=0}^{n} i\right) + (n+1)\,.$$

Now, using our inductive hypothesis we have

$$\begin{aligned}
\sum_{i=0}^{n+1} i &= \left(\sum_{i=0}^{n} i\right) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}\,.
\end{aligned}$$

□

Proposition 9.3.

$$\forall n \in \mathbb{N} \quad \sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}\,.$$

Proof. Left as an exercise to the reader. □

Exercise 9.1. Prove Proposition 9.3.

Proposition 9.4. *For all $r \in \mathbb{R}$ with $r \neq 1$ and for all $n \in \mathbb{N}$*

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}\,.$$

Proof. Left as an exercise to the reader. □

Exercise 9.2. Prove Proposition 9.4.

Proposition 9.5. *For all $n \in \mathbb{N}$ $2^{2n} - 1$ is divisible by 3.*

Proof. We prove this by induction on $n \in \mathbb{N}$.

If $n = 0$, then

$$\begin{aligned}
2^{2n} - 1 &= 2^{2\cdot 0} - 1 \\
&= 1 - 1 & &= 0\,.
\end{aligned}$$

Though, as $0 = 3 \cdot 0$, we have that $2^{2\cdot 0} - 1$ is divisible by 3.

Now, suppose that $n \in \mathbb{N}$ is such that $2^{2n} - 1$ is divisible by 3. As $2^{2n} - 1$ is divisible by 3, there exists some $a \in \mathbb{Z}$ so that $3a = 2^{2n} - 1$. Now,

$$\begin{aligned} 2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\ &= 2^{2n}4 - 1 \\ &= 2^{2n}(3+1) - 1 \\ &= 3 \cdot 2^{2n} + 2^{2n} - 1 \\ &= 3 \cdot 2^{2n} + 3a \\ &= 3(2^{2n} + a)\,. \end{aligned}$$

So, as $2^{2n} + a \in \mathbb{Z}$ $3|2^{2(n+1)} - 1$. □

Proposition 9.6. *For all $n \in \mathbb{N}$ if $n \geq 2$, then $2n + 1 < 2^n$.*

Proof. We prove this by induction on $n \in \mathbb{N}$ with $n > 2$.

If $n = 3$, then

$$\begin{aligned} 2n + 1 &= 2 \cdot 3 + 1 \\ &= 7 \\ &< 8 \\ &= 2^3 \\ &= 2^n \end{aligned}$$

Now, suppose that $n \in \mathbb{N}$ with $n > 3$ is such that $2n + 1 < 2^n$. Then,

$$\begin{aligned} 2(n+1) + 1 &= 2n + 3 \\ &= 2n + 1 + 2 \\ &< 2^n + 2 \\ &< 2^n + 2^n \\ &= 2^{n+1}\,. \end{aligned}$$

□

Example 9.1. Define the sequence a by $a_0 = 2$ and $a_{k+1} = 5a_k$.

1. Write the first four terms of the sequence a.

$$a_0 = 2,\ a_1 = 10,\ a_2 = 50,\ a_3 = 250\,.$$

2. Use induction to show that $a_k = 2 \cdot 5^k$ for $k \in \mathbb{N}$.
We first note, that when $k = 0$, we have that

$$\begin{aligned} 2 \cdot 5^0 &= 2 \cdot 1 \\ &= 2 \\ &= a_0 \,. \end{aligned}$$

Now, suppose $k \in \mathbb{N}$ and $a_k = 2 \cdot 5^k$. Then, by definition we have,

$$\begin{aligned} a_{k+1} &= 5a_k \\ &= 5 \cdot 2 \cdot 5^k \\ &= 2 \cdot 5^{k+1} \,. \end{aligned}$$

Thus, by induction, we have that $\forall k \in \mathbb{N}\, a_k = 2 \cdot 5^k$.

10 Strong Induction

The principle of strong induction is: Let $P(n)$ some predicate where the domain of n is the integers, or some subset of the integers. Let $a, b \in \mathbb{Z}$ be some fixed values with $a < b$, and suppose that for all $c \geq a$, c is in the domain of n in $P(n)$. Then, if

1. $P(a), P(a+1), \ldots, P(b)$ are true and
2. $\forall k \geq b$ if $\forall i \in \mathbb{Z}$ with $a \leq i \leq k$ $P(i)$ holds, then $P(k+1)$ is true,

then $\forall k \geq a(P(k))$ is true. This is known as *strong induction.* You'll notice that both the base and inductive steps of strong induction differ slightly from weak induction covered in Section 9.

Strong induction allows for proving statements which require checking some finite number of values in the base step. One case where you may want this power is when proving that some recurrence relation which is defined using more than one previous value. Further, and more importantly, strong induction differs from its weaker counterpart in that the inductive step makes the assumption that the desired claim holds for all values up to and included some value before moving to the next value.

Example 10.1. Define the sequence s as

$$s_0 = 0,\ s_1 = 4, s_k = 6s_{k-1} - 5s_{k-2}\,.$$

We want to show that $\forall n \in \mathbb{N}$ $s_n = 5^n - 1$.

We do so by strong induction on $n \in \mathbb{N}$.

Base step, we check that the claim holds for $n = 0$ and $n = 1$. Here, we note that $s_0 = 0 = 5^0 - 1$ and $s_1 = 4 = 5^1 - 1$. So, the claim holds at the first two values for n.

Now, we check the inductive step. Let $n \in \mathbb{N}$ and suppose that for all $k \in \mathbb{N}$ with $k \leq n$ $s_k = 5^k - 1$. Now, by definition $s_{n+1} = 6s_n - 5s_{n-1}$. Though, out inductive hypothesis provides that $s_n = 5^n - 1$ and $s_{n-1} = 5^{n-1} - 1$. Thus,

$$\begin{aligned}
s_{n+1} &= 6s_n - 5s_{n-1} \\
&= 6(5^n - 1) - 5(5^{n-1} - 1) \\
&= 6 \cdot 5^n - 6 - 5^n - 5 \\
&= 5 \cdot 5^n - 1 \\
&= 5^{n+1} - 1\,.
\end{aligned}$$

showing that the claim holds at $n+1$.

Thus, by induction, we have that $\forall n \in \mathbb{N}\ s_n = 5^n - 1$.

Proposition 10.1. *Each integers larger than* 1 *is divisible by a prime.*

Proof. We prove this by strong induction on $n \in \mathbb{N}$ with $n > 1$.

Consider the case where $n = 2$. Then n is prime and divides itself. Thus, the claim holds.

Now, suppose that $n \in \mathbb{N}$ with $n > 1$ is such that every k with $1 < k \leq n$, k is divide by a prime. Certainly, $n+1$ is either prime or is not prime.

If $n+1$ is prime, then as before, as $n+1$ divides itself the claim holds.

Otherwise, by Lemma 5.4 $n+1$ is composite. As $n+1$ is composite, there exists a, b so that $1 < a, b < n+1$ and $ab = n+1$. Though, as $1 < a < n+1$ $1 < a \leq n$, and our inductive hypothesis provides that a is divisible by a prime. Though, as a divides $n+1$ and a is divisible by a prime, proposition 5.3, $n+1$ is divisible by a prime. □

11 Naive Set Theory

Definition 11.1. A *set* is a collection of things. The symbol $\in$ is used denote the *membership* relation on sets. For S a set and x arbitrary, we say $x \in S$ precisely when x is a member (or element) of S.

In this section, and in those that follow, everything is a set.

Definition 11.2.

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

If A and B have the same elements, then $A = B$.

Example 11.1. Let $A = \{ 1 \}$, $B = \{ 1, 2 \}$, and $C = \{ 1, 1 \}$.

As $2 \in B$ but $2 \notin A$, $A \neq B$.

Clearly, as every element of A is an element of C. The reverse is also true; that is, every element of C is an element of B. Thus, $A = C$.

Definition 11.3. The *subset* relation, $\subseteq$, is defined as

$$x \subseteq y \iff \forall z (z \in x \rightarrow z \in y) \,.$$

We use $x \subset y$, or $x \subsetneq y$, to abbreviate $x \subseteq y \land x \neq y$. If $x \subsetneq y$, we say that x is a *proper subset* of y. We use $A \supseteq B$ to mean $B \subseteq A$, and is read A is a super set of B. The $\supset$ and $\supsetneq$ variations are similar to the subset variations.

Example 11.2. Set

$$A := \{ n \in \mathbb{Z} \mid \exists r \in \mathbb{Z}(n = 6r) \}$$

and

$$B := \{ n \in \mathbb{Z} \mid \exists s \in \mathbb{Z}(n = 3s) \} \,.$$

Note

$$A = \{ \dots, -18, -12, -6, 0, 6, 12, 18, \dots \}$$

and

$$B = \{ \dots, -9, -6, -3, 0, 3, 6, 9, \dots \} \,.$$

First, let us show that $A \subseteq B$. That is, $\forall x(x \in A \to x \in B)$. Let x be arbitrary, and suppose that $x \in A$. From the definition of A, $x \in A$ means that $\exists r \in \mathbb{Z}(x = 6r)$. Let $r \in \mathbb{Z}$ be such that $x = 6r$. Set $s = 2r$, and observe that

$$\begin{aligned} x &= 6r \\ &= 3 \cdot 2r \\ &= 3s\,. \end{aligned}$$

So, $x = 3s$ for some s, showing that $x \in B$. Finally, as x was arbitrary in A, we have that $A \subseteq B$.

Now, the reverse is not true. That is, $B \nsubseteq A$. This is becuase there is some element of B which is not an element of A. One such element is 3. Note, as $3 = 3 \cdot 1$, $3 \in B$. Though, as there does not exist a $r \in \mathbb{Z}$ such that $3 = 6r$, $3 \notin A$. So, $B \nsubseteq A$.

Thus, A is a proper subset of B.

Definition 11.4. The set which contains nothing is called the *emptyset*. We use $\emptyset$ to denote the emptyset.

Proposition 11.1. *For any A, $\emptyset \subseteq A$.*

Proof. This holds trivially. □

Note, to show that two sets A and B are equal, it suffices to show that $A \subseteq B$ and $B \subseteq A$.

Example 11.3. Let

$$A := \{\, 2a \mid a \in \mathbb{Z} \,\}$$

and

$$B := \{\, 2b - 2 \mid b \in \mathbb{Z} \,\}\ .$$

Fix $x \in A$. As $x \in A$, $x = 2a$ for some $a \in \mathbb{Z}$. As $a \in \mathbb{Z}$, $a + 1 \in \mathbb{Z}$. Set $b = a + 1$, and observe that

$$\begin{aligned} x &= 2a \\ &= 2a + 2 - 2 \\ &= 2(a + 1) - 2 \\ &= 2b - 2\,, \end{aligned}$$

showing that that $x \in B$. So, as x was arbitrary, $A \subseteq B$.

Now, fix $x \in B$. As $x \in B$, $x = 2b - 2$ for some $b \in \mathbb{Z}$. Set $a = b - 1$, and as $b \in \mathbb{Z}$ $a \in \mathbb{Z}$ as well. Finally,

$$\begin{aligned} x &= 2b - 2 \\ &= 2b - 2 + 2 - 2 \\ &= 2(b-1) \\ &= 2a\,, \end{aligned}$$

showing that $x \in A$. So, as x was arbitrary, $B \subseteq A$.

Thus, as $A \subseteq B$ and $B \subseteq A$, $A = B$.

Proposition 11.2. *For any A, B, and C. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof. Fix A, B, and C such that $A \subseteq B$ and $B \subseteq C$. Fix $a \in A$. As $A \subseteq B$, $a \in B$. As $B \subseteq C$, $a \in C$. But, $a \in A$ was arbitrary, so $A \subseteq C$. □

Definition 11.5. Let A and B sets. The *union* of A and B, $A \cup B$ is the set which contains everything which is in A or in B.

$$A \cup B := \{\, x \mid x \in A \vee x \in B \,\} \,.$$

Let A_i be a set for each $i \in I$, then

$$\bigcup_{i \in I} A_i := \{\, x \mid \exists i \in I (x \in A_i) \,\} \,.$$

In the case that $i = \{\, i \in \mathbb{Z} \mid n \le i \le m \,\}$ for some $n, m \in \mathbb{Z} \cup \{\, \infty, -\infty \,\}$, then we may write

$$\bigcup_{i=n}^{m} A_i := \bigcup_{i \in I} A_i \,.$$

Definition 11.6. Let A and B sets. The *intersection* of A and B, $A \cap B$ is the set which contains everything which is in A and in B.

$$A \cap B := \{\, x \mid x \in A \wedge x \in B \,\} \,.$$

Let A_i be a set for each $i \in I$, then

$$\bigcap_{i \in I} A_i := \{\, x \mid \forall i \in I (x \in A_i) \,\} \,.$$

In the case that $i = \{ i \in \mathbb{Z} \mid n \leq i \leq m \}$ for some $n, m \in \mathbb{Z} \cup \{ \infty, -\infty \}$, then we may write

$$\bigcap_{i=n}^{m} A_i := \bigcap_{i \in I} A_i \, .$$

Definition 11.7. Let A and B sets. The *difference* of A and B, $A \setminus B$ is the set which contains everything which is in A and not in B.

$$A \setminus B := \{ x \in A \mid x \notin B \} \, .$$

Example 11.4. Let $A = \{ a, c, e, g \}$ and $B = \{ d, e, f, g \}$.
Then

$$\begin{aligned} A \cup B &= \{ a, c, d, e, g, f \} \, , \\ A \cap B &= \{ e, g \} \, , \\ A \setminus B &= \{ a, c, \} \, , \\ B \setminus A &= \{ d, f \} \, . \end{aligned}$$

Example 11.5. For each $i \in \mathbb{Z}^+$, set

$$A_i := \left\{ x \in \mathbb{R} \mid -\frac{1}{i} < x < \frac{1}{i} \right\} = (-\frac{1}{i}, \frac{1}{i}) \, .$$

Compute:

1. $A_1 \cup A_2 \cup A_3$
2. $A_1 \cap A_2 \cap A_3$
3. $\bigcup_{i \in \mathbb{Z}^+} A_i$
4. $\bigcap_{i \in \mathbb{Z}^+} A_i$

Proposition 11.3. *For any A and B, $A \subseteq A \cup B$.*

Proof. Let A and B be arbitrary. Fix any $x \in A$. As $x \in A$, $x \in A$ or $x \in B$. Thus, $x \in A \cup B$. But, x was arbitrary, so $A \subseteq A \cup B$. □

Proposition 11.4. *For any A and B, $A \cap B \subseteq B$.*

Proof. Let A and B be arbitrary. Fix any $x \in A \cap B$. As $x \in A \cap B$, $x \in A$ and $x \in B$. Thus, $x \in A \cap B$. But, x was arbitrary, so $A \cap B \subseteq B$. □

Proposition 11.5. *For any A, $A \cap \emptyset = \emptyset$.*

Proof. Let A be arbitrary. Applying Proposition 11.4, we have that $A \cap \emptyset \subseteq \emptyset$. Further, Proposition 11.1, we have that $\emptyset \subseteq A \cap \emptyset$. Thus, $A \cap \emptyset = \emptyset$. □

Proposition 11.6. *For any A and B. If $A \subseteq B$, then*

1. *$A \cap B = A$ and*
2. *$A \cup B = B$.*

Proof. Fix A and B. Suppose that $A \subseteq B$.

1. By Proposition 11.4, $A \cap B \subseteq A$. It remains to show that $A \subseteq A \cap B$. Fix any $a \in A$. As $a \in A$ and $A \subseteq B$, $a \in B$. Thus, $a \in A$ and $a \in B$. So, $a \in A \cap B$, showing that $A \subseteq A \cap B$.
2. By Proposition 11.3, $B \subseteq A \cup B$. It remains to show that $A \cup B \subseteq B$. Fix any $b \in A \cup B$. By the Definition 11.5, $b \in A$ or $b \in B$. If $b \in A$, then as $A \subseteq B$ $b \in B$. So, in either case we have that $b \in B$. Whence, $A \cap B \subseteq B$. Showing that $A \cap B = B$

□

Proposition 11.7. *For any A, B, and C,*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Proof. Let A, B, and C be arbitrary.

($\subseteq$) Fix $x \in A \cup (B \cap C)$. By Definition 11.5, $x \in A$ pr $x \in (B \cap C)$.

If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$. Thus, $x \in (A \cup B) \cap (A \cup C)$.

If $x \in B \cap C$, then $x \in B$ and $x \in C$. As $x \in B$ and $x \in C$, $x \in A \cup B$ and $x \in A \cup C$. So, $x \in (A \cup B) \cap (A \cup C)$.

But, $x \in A \cup (B \cap C)$ was arbitrary, so

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C).$$

($\supseteq$) Fix $x \in (A \cup B) \cap (A \cup B)$. Then, $x \in A \cup B$ and $x \in A \cup C$. Either x is in A or it is not.

If x is in A, when $x \in A \cup (B \cap C)$, and we are done.

Suppose x is not in A. As $x \in A \cup B$ and x is not in A, $x \in B$. Similarly, as $x \in A \cup B$ and $x \notin A$, $x \in C$. Thus, $x \in B \cap C$. Whence, $x \in A \cup (B \cap C)$. □

Definition 11.8. Sets A and B are said to be *disjoint* when $A \cap B = \emptyset$

Example 11.6. Let E and O be the set of even and odd integers respectively. E and O are disjoint.

To show this, consider any $n \in \mathbb{Z}$. Using Proposition 5.9, n is either even or odd, but not both. In the case that n is even, $n \in E$ and $n \notin O$. Similarly, if n is odd, then $n \in O$ and $n \notin O$. Thus

$$E \cap O = \{\, n \in \mathbb{Z} \mid n \in O \wedge n \in E \,\} = \emptyset\,.$$

So, E and O are disjoint.

Definition 11.9. $\mathcal{A}$ is said to be a *mutually disjoint* collection provided $\forall A, B \in \mathcal{A}$ A and B are disjoint.

Definition 11.10. $\mathcal{A}$ is said to be a *partition* of a set X provided $\bigcup_{A \in \mathcal{A}} A = X$ and $\mathcal{A}$ is a mutually disjoint collection.

Proposition 11.8. *For any A and B, $A \cup B = B \cup A$.*

Proof.

$$\begin{aligned} A \cup B &= \{\, x \mid x \in A \vee x \in B \,\} \\ &= \{\, x \mid x \in B \vee x \in A \,\} \\ &= B \cup A \end{aligned}$$

□

Example 11.7. Let $A = \{\,1, 2, 3, 4, 5, 6\,\}$, $A_1 = \{\,1, 2\,\}$, $A_2 = \{\,3, 4\,\}$, and $A_3 = \{\,5, 6\,\}$. Note, as $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$ $\{\,A_1, A_2, A_3\,\}$ is a mutually disjoint collection. Finally as $A_1 \cup A_2 \cup A_3 = A$, $\{\,A_1, A_2, A_3\,\}$ is a partition of X.

Exercise 11.1. Let

$$\begin{aligned} T_0 &= \{\, n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}(n = 3k) \,\} \\ T_1 &= \{\, n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}(n = 3k + 1) \,\} \\ T_2 &= \{\, n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}(n = 3k + 2) \,\}\ . \end{aligned}$$

Show that $\{\,T_0, T_1, T_2\,\}$ is a partition of $\mathbb{Z}$.

Definition 11.11. Let $n \in \mathbb{Z}^+$ and $x_1, x_2, \ldots, x_n$ be given. Then, the *n-tuple*, often just *tuple*, $(x_1, x_2, \ldots, x_n)$ is the collection containing $x_1, x_2, \ldots, x_n$ together with their order. A 2-tuple is called an *ordered pair*. A 3-tuple is called an *ordered triple*.

Definition 11.12. Let A and B be given. The *caresian product* of A and B, written $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

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

Example 11.8.

$$\{\, 1, 2 \,\} \times \{\, a, b \,\} := \{\, (1, a), (1, b), (2, a), (2, b) \,\} .$$

Definition 11.13. Let A be a set. The set of all subsets of A, $\mathcal{P}$, is called the *power set* of A.

$$\mathcal{P}(A) := \{\, B \mid B \subseteq A \,\} .$$

Example 11.9.

$$\mathcal{P}(\{\, a, b \,\}) = \{\, \{\ \}, \{\, a \,\}, \{\, b \,\}, \{\, a, b \,\} \,\} .$$

Note, $a, b \notin \mathcal{P}$, though $a, b \in A$.

Proposition 11.9. *For all $n \in \mathbb{N}$, if X is a set with n elements, then $\mathcal{P}$ has 2^n elements.*

Proof. We prove this by induction on n.

In the case where $n = 0$. Then, the only set with 0 elements is the emptyset. We now see

$$\mathcal{P}(\emptyset) = \{\, \emptyset \,\}$$

has $2^0 = 1$ elements.

Now, suppose $n \in \mathbb{N}$ and the power set of any set with n elements has 2^n elements. Let X be a set with $n + 1$ many elements. As X has $n + 1$ many elements, there exists some $x \in X$. Fix any $x \in X$.

Note, $X \backslash \{\, x \,\}$ has n elements. So, by our inductive hypothesis $\mathcal{P}(X \backslash \{\, x \,\})$ has 2^n elements.

$\mathcal{P}(X \setminus \{\, x \,\})$ contains half of the elements in $\mathcal{P}(X)$. In particular, it is missing all the subsets of X which contain x. Note

$$\mathcal{P}(X) = \mathcal{P}(X \setminus \{\, x \,\}) \cup \{\, A \cup \{\, x \,\} \mid A \in \mathcal{P}(X \setminus \{\, x \,\}) \,\} .$$

As $\mathcal{P}(X \setminus \{ x \})$ has 2^n elements, $\{ A \cup \{ x \} \mid A \in \mathcal{P}(X \setminus \{ x \}) \}$ has 2^n many elements. Further, as each element of $\mathcal{P}(X \setminus \{ x \})$ does not contain x and each element of $\{ A \cup \{ x \} \mid A \in \mathcal{P}(X \setminus \{ x \}) \}$ does, those two sets are disjoint. This, $\mathcal{P}(X)$ has $2 \cdot 2^n = 2^{n+1}$ elements. $\square$

12 Functions

Definition 12.1. Let X and Y be sets. We say that $f \subseteq X \times Y$ is a *function* from a set X to a set Y, denoted $f : X \to Y$, is a relation from X to Y such that every element of x is related to exactly one element in Y. For $x \in X$ and $y \in Y$, y is the unique value related to x if, and only if, $(x, y) \in f$. In this case, we say that $f(x) = y$ or $f : x \mapsto y$.

In some contexts, the symbol $f(x)$ refers to the function itself and not the value of the function. This can lead to confusion. We will use f to refer to the function itself and $f(x)$ to refer to the value of the function at some value x.

Sometimes, an object presented as a function is not a function at all!

Example 12.1. Define $f : \mathbb{R} \to \mathbb{R}$ by for each $x \in X$, $f(x) = y$ where $x^2 + y^2 = 1$. Note, this described f is not a function as for almost all $x \in \mathbb{R}$ there either does not exist such a y or there exists 2 such y. In fact, the described f is a function precisely on the set $\{ -1, 1 \}$ as is not particularly interesting at those values.

Exercise 12.1. Define $f : \mathbb{Q} \to \mathbb{Z}$ by $f(\frac{n}{m}) = n$. Is f well-defined? That is, is the described object a function?

Definition 12.2. For a given function $f : X \to Y$, we call X the *domain* of f, written $\operatorname{dom}(f)$.

Definition 12.3. For a given function $f : X \to Y$, we call the set

$$\{ y \in Y \mid \exists x \in X (f(x) = y) \}$$

the *range* of f, and denote this set $\operatorname{ran}(f)$. We call the set Y to *codomain* of f.

Proposition 12.1. *Given functions $f, g : X \to Y$, we say that $f = g$ if, and only if, $\forall x \in X (f(x) = g(x))$.*

Proof. Let$f, g : X \to Y$ be arbitrary functions. As f and g share domain and co-domain, $f, g \subseteq X \times Y$.

Suppose $\forall x \in X (f(x) = g(x))$. Then for any $(x, y) \in X \times Y$,

$$\begin{aligned} (x, y) \in f &\iff f(x) = y \\ &\iff g(x) = y \\ &\iff (x, y) \in g\,. \end{aligned}$$

Thus, $f = g$ as sets.

For the converse, suppose $f = g$ as sets. Fix any $x \in X$. Then, for any $y \in Y$

$$\begin{aligned} f(x) = y &\iff (x, y) \in f \\ &\iff (x, y) \in g \\ &\iff g(x) = y\,. \end{aligned}$$

Thus $f(x) = y$ if, and only if, $g(x) = y$.

Though, for any $x \in X$, there is a unique y such that $f(x) = y$. Thus $\forall x \in X(f(x) = g(x))$. □

Example 12.2. Set $X = 0, 1, 2$ and defin $f, g : X \to Y$ as

$$f(x) = (x^2 + x + 1) \mod 3\,,$$

and

$$g(x) = (x + 2)^2 \mod 3\,.$$

Does $f = g$?

As

$$\begin{aligned} f(0) = 1 && = g(0) \\ f(1) = 0 && = g(1) \\ f(2) = 1 && = g(2) \end{aligned}$$

Proposition 12.1 gives that $f = g$.

For any function $a, b : \mathbb{R} \to \mathbb{R}$, define $(a + b) : \mathbb{R} \to \mathbb{R}$ as $\forall x \in \mathbb{R}$ $(a+b)(x) := a(x)+b(x)$. Let $f, g : \mathbb{R} \to \mathbb{R}$ be arbitrary. Does $f + g = g + f$.

Again, yes. As $\forall x \in \mathbb{R}$

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ &= g(x) + f(x) \\ &= (g + f)(x)\,. \end{aligned}$$

So, using the same proposition as before, we have that $f = g$.

Definition 12.4. Let $f : X \to Y$ be a function For any $A \subseteq X$, the *image* of A under f, written $f''A$ or sometimes $f(A)$, is

$$\{\, y \in Y \mid \exists x \in A(f(x) = y) \,\}\ .$$

For any $C \subseteq Y$, the *pre-image* of C under f, written $f''A$ or sometimes $f(A)$, is

$$\{ y \in Y \mid \exists x \in A(f(x) = y) \} .$$

Proposition 12.2. *If $f : X \to Y$ is a function and $A, B \subseteq X$, then*

$$f[A \cup B] \subseteq f[A] \cup f[B] .$$

Proof. Left as an exercise to the reader. □

Exercise 12.2. Prove Proposition 12.2.

Definition 12.5. A function $f : X \to Y$ is said to be *injective* (or *one-to-one*) provided $\forall x, y \in X$ if $x \neq y$, then $f(x) \neq f(y)$.

Example 12.3.

1. Show that $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = 4x - 1$ is injective.
   Like many proofs of infectivity, we will show the contrapositive of Definition 12.5. Fix $x, y \in \mathbb{R}$ and suppose that $f(x) = f(y)$. Then,

   $$\begin{aligned} & f(x) = f(y) \\ \Rightarrow \quad & 4x - 1 = 4y - 1 \\ \Rightarrow \quad & 4x = 4y \\ \Rightarrow \quad & x = y . \end{aligned}$$

   Thus, $\forall x, y \in \mathbb{R}(f(x) = f(y) \to x = y)$.

2. Show that $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ is not injective.
   To do this, we need only show that there exists distinct $x, y \in \mathbb{R}$ such that $g(x) = g(y)$. Note that $-1, 1 \in \mathbb{R}$ and $-1 \neq 1$, but $g(1) = g(-1)$.

   Note, we can change the domain of g to make the function injective. How?

Definition 12.6. A function $f : X \to Y$ is said to be *surjective* (or *onto*) provided $\forall y \in Y \exists x \in X \ f(x) = y$.

Example 12.4.

1. Show that $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = 4x - 1$ is surjective.

Fix any $y \in \mathbb{R}$. Our job is to find some $x \in \mathbb{R}$ such that $f(x) = y$. Given our selection of y, set $x = \frac{y+1}{4}$. We claim that this x works,

$$\begin{aligned} f(x) &= 4x - 1 \\ &= 4\frac{y+1}{4} - 1 \\ &= y + 1 - 1 \\ &= y\,. \end{aligned}$$

Thus, for each $y \in \mathbb{R}$ we can find some $x \in \mathbb{R}$ such that $f(x) = y$. Thus, f is surjective.

2. Show that $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ is not surjective.
   To do this, we need only produce some $y \in \mathbb{R}$ such that there does not exist a $x \in \mathbb{R}$ such that $g(x) = y$. Consider $y = -1$. Note, $\forall x \in \mathbb{R}$ $x^2 \geq 0$, thus there does not exist an $x \in \mathbb{R}$ such that $g(x) = -1$. Thus, g is not surjective.

   Note, we can change the codomain of g to make the function surjective. How?

Definition 12.7. A function $f : X \to Y$ is said to be *bijection* provided f is injective and surjective.

Example 12.5. 1. Show that $f(x) = 4x - 1$ is a bijection.

In Examples 12.3 and 12.4 respectively, we showed that f is injective and surjective. So, as f is both an injection and a surjection, f is a bijection.

2. Show that $g : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$g(x, y) = (x + y, x - y)$$

is a bijection.

First, we show that g is injective. Fix $x, y, a, b \in \mathbb{R}$ such that $g(x, y) = g(a, b)$. Then by definiton of g, we have that

$$\begin{aligned} & g(x,y) = g(a,b) \\ \Rightarrow \quad & (x+y, x-y) = (a+b, a-b) \\ \Rightarrow \quad & (x+y = a+b) \wedge (x-y = a-b)\,. \end{aligned}$$

Adding these two equalities gives that $2x = 2a$. So, $x = a$. Now, as $x = a$ and $x + y = a + b$, we have that $y = b$. Thus, $(x, y) = (a, b)$. So g is injective.

Now, to show that g is surjective. Fix $u, v \in \mathbb{R}$. Let $x = \frac{u+v}{2}$ and $y = \frac{u-v}{2}$. Then, we can note that

$$\begin{aligned} g(x,y) &= \left(\frac{u+v}{2} + \frac{u-v}{2}, \frac{u+v}{2} - \frac{u-v}{2}\right) \\ &= \left(\frac{u+v+u-v}{2}, \frac{u+v-u+v}{2}\right) \\ &= \left(\frac{2u}{2}, \frac{2v}{2}\right) \\ &= (u,v) \end{aligned}$$

So, g is injective.

Proposition 12.3. *Let $f : X \to Y$ be a bijection. Then, there exists a unique function $f^{-1} : Y \to X$ defined by $\forall y \in Y$ $f^{-1}(y) = x$ where x is the unique element of X such that $f(x) = y$. That is, $\forall x \in X \forall y \in Y$*

$$f^{-1}(y) = x \qquad \Longleftrightarrow \qquad f(x) = y\,.$$

Proof. □

Definition 12.8. f^{-1} in Proposition 12.3 is called the *inverse* of f.

Example 12.6. 1. Compute f^{-1} given $f(x) = 4x - 1$.

First, we performa sanity check and ask if f^{-1} makes sense given our function f. As we showed in Example 12.5, f as above is a bijection. So, this by Proposition 12.3 f^{-1} does exists. In fact, we have computed the inverse already, in Example 12.4, it is

$$f^{-1}(y) = \frac{y+1}{4}\,.$$

2. Compute the inverse of the function $g(x, y) = (x + y, x - y)$.

Again, we have already shown that this g is a bijection. Further, in Example 12.5, while showing that g was a surjection, we nearly computed the inverse of g. Putting together the work we did there, it is not difficult to see that

$$g^{-1}(u,v) = \left(\frac{u+v}{2}, \frac{u-v}{2}\right).$$

Proposition 12.4. *If $f : X \to Y$ is a bijections, then f^{-1} is a bijection.*

Proof. Fix $f : X \to Y$ a bijection. We must show that f^{-1} is an injection and a surjection.

To show that $f^{-1} : Y \to X$ is an injection, fix $y_1, y_2 \in Y$. Suppose that $f^{-1}(y_1) = f^{-1}(y_2)$. Set $x = f^{-1}(y_1) \in X$. By definition of f^{-1}, $f(x) = y_1$ Further, as $f^{-1}(y_1) = f^{-1}(y_2)$, $x = f^{-1}(y_2)$. Whence, $f(x) = y_2$. So, as $f(x) = y_1$ and $f(x) = y_2$, $y_1 = y_2$.

To show that f^{-1} is a surjection, fix some $x \in X$. Now, set $y = f(x)$. Then, by definition of f^{-1}, $f^{-1}(y) = x$. □

Definition 12.9. Let $f : X \to Y$ and $g : Y \to Z$. The *composition* of f and g, written $g \circ f : X \to Z$, is defined by $(g \circ f)(x) := g(f(x))$ for each $x \in X$.

Definition 12.10. Given a set X, the *identity* function on X, $\mathtt{id}_X : X \to X$, is defined as $\mathtt{id}_X(x) = x$ for all $x \in X$.

Proposition 12.5. *Let $f : X \to Y$ and $\mathtt{id}_X$, $\mathtt{id}_Y$ the identity functions on X and Y respectively. Then $f \circ \mathtt{id}_X = f$ and $\mathtt{id}_Y \circ f = f$.*

Proof. Fix any $x \in X$. Then,

$$\begin{aligned}(f \circ \mathtt{id}_X)(x) &= f(\mathtt{id}_X(x)) \\ &= f(x)\end{aligned}$$

So, $\forall x \in X(\,(f \circ \mathtt{id}_X)(x) = f(x)\,)$. Thus, by Proposition 12.1, $f \circ \mathtt{id}_X = f$.

$\mathtt{id}_Y \circ f = f$ is similar. Fix any $x \in X$. Then,

$$\begin{aligned}(\mathtt{id}_Y \circ f)(x) &= \mathtt{id}_Y(f(x)) \\ &= f(x)\end{aligned}$$

So, again by Proposition 12.1, we have that $\mathtt{id}_Y \circ f = f$. □

Proposition 12.6. *If $f : X \to Y$ is a bijection with inverse $f^{-1} : Y \to X$, then $f^{-1} \circ f = \boldsymbol{\mathtt{id}}_X$.*

Proof. Fix $f : X \to Y$ a bijection. Fix $x \in X$. Set $y = f(x)$. By definition of f^{-1}, $f^{-1}(y) = x$. So, we have that

$$\begin{aligned}(f^{-1} \circ f)(x) &= f^{-1}(f(x)) \\ &= f^{-1}(y) \\ &= x\,.\end{aligned}$$

Though, as $x \in X$ was arbitrary, we have that $\forall x \in X(f^{-1} \circ f = \mathtt{id}_X)$. Thus, by Proposition 12.1, $f^{-1} \circ f = \mathtt{id}_X$. □

Proposition 12.7. *If $f : X \to Y$ and $g : Y \to Z$ are both injective, then $g \circ f$ is injective.*

Proof. Fix any $x, y \in X$ and suppose that $x \neq y$. As f is injective and $x \neq y$, $f(x) \neq f(y)$. As g is injective, and $f(x), f(y) \in Y$ are distinct, $g(f(x)) \neq g(f(y))$. Thus, $g \circ f$ is injective. □

Proposition 12.8. *If $f : X \to Y$ and $g : Y \to Z$ are both surjective, then $g \circ f$ is surjective.*

Proof. Fix any $z \in Z$. As g is surjective, there exists some $y \in Y$ such that $g(y) = z$. As f is surjective, there exists some $x \in X$ such that $f(x) = z$. Now, we note that

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(y) \\ &= z\,.\end{aligned}$$

Showing that $g \circ f$ is surjective. □

Proposition 12.9. *If $f : X \to Y$ and $g : Y \to Z$ are both bijective, then $g \circ f$ is bijective.*

Proof. As f and g are bijections, they are both surjective and injective. Thus, by applying Propositions 12.8 and 12.7, we have that $g \circ f$ is a surjective and injective. Thus, as $g \circ f$ is a bijection. □

13 Cardinality

Definition 13.1. For sets A and B, A is said to have *cardinality no larger than* than B, written $|A| \leq |B|$, provided there exists an injection from A to B.

Definition 13.2. For sets A and B, A is said to have the *same cardinality* as B, written $|A| = |B|$, provided there exists a bijection from A to B.

Example 13.1. The set of even integers, $2\mathbb{Z} = \{\, 2z \mid z \in \mathbb{Z} \,\}$, has the same cardinality as $\mathbb{Z}$.

That is, $|2\mathbb{Z}| = |\mathbb{Z}|$. To show this, we must produce a bijection from $2\mathbb{Z}$ to $\mathbb{Z}$. Note that the function $f : 2\mathbb{Z} \to \mathbb{Z}$ defined by $f(z) = \frac{z}{2}$ for each $z \in \mathbb{Z}$ is a bijection.

Proposition 13.1. *For any set A, A has the same cardinality as itself.*

Proof. The identity map $\mathtt{id}_A$ is trivially a bijection from A to A which see that A has the same cardinality of A. □

Proposition 13.2. *For any sets A and B if A has the same cardinality as B, then B has the same cardinality as A.*

Proof. Fix sets A and B, and suppose that A has the same cardinality as B. As A has the same cardinality as B, there exists a bijection f from A to B. As f is a bijection, Proposition 12.4 gives that f^{-1} is a bijection from B to A. Whence, B has the same cardinality as A. □

Proposition 13.3. *For any sets A, B, and C if A has the same cardinality as B and B has the same cardinality as C, then A has the same cardinality as C.*

Proof. Fix sets A, B, and C, and suppose that A has the same cardinality as B and B has the same cardinality as C. As A has the same cardinality as B, there exists a bijection f from A to B. As B has the same cardinality as C, there exists a bijection g from B to C. As f and g are bijections, applying Proposition 12.9, $g \circ f$ is a bijection. Thus, $g \circ f$ sees that A has the same cardinality as B. □

Definition 13.3. A sets $S \subseteq \mathbb{N}$ is said to be an *initial segment of the naturals* provided there exists some $n \in \mathbb{N}$ such that $S = \{\, m \in \mathbb{N} \mid m < n \,\}$.

Definition 13.4. A sets A is said to be *finite* provided A has the same cardinality as an initials segment of the naturals. Suppose A is finite and has the same cardinality as $\{\, m \in \mathbb{N} \mid m < n \,\}$ for some $n \in \mathbb{N}$, then we say that $|A| = n$.

Definition 13.5. A sets A is said to be *infinite* provided A is not finite.

Definition 13.6. A sets A is said to be *countably infinite* provided A has the same cardinality as $\mathbb{N}$.

Definition 13.7. A sets A is said to be *countable* provided A has the same cardinality as $\mathbb{N}$ or is finite.

Example 13.2. The set of positive integers, $\mathbb{Z}^+$ is countable.

To show that $\mathbb{Z}^+$ is countable, we must show that either $\mathbb{Z}^+$ is finite or $|\mathbb{Z}^+| = |\mathbb{N}|$.

Clearly, $\mathbb{Z}^+$ is not finite.

To show that $|\mathbb{Z}^+| = |\mathbb{N}|$, we must produce a bijection from $\mathbb{N}$ to $\mathbb{Z}^+$ (the order doesn't really matter here, see Lemma 13.2). Certainly, the mapping $x \mapsto x + 1$ suffices.

Proposition 13.4. *The set of integers, $\mathbb{Z}$, is countable.*

Proof. To show that $\mathbb{Z}$ is countable, we must show that either $\mathbb{Z}$ is finite or $|\mathbb{Z}| = |\mathbb{N}|$. To show that $|\mathbb{Z}| = |\mathbb{N}|$ we will produce, explicitly, a bijection from $\mathbb{Z}$ to $\mathbb{N}$. To do this, we will keep 0 where it is, map the negative integers to the even natural numbers, and the positive integers to the odd natural numbers.

One such mapping is $f : \mathbb{Z} \to \mathbb{N}$ defined be

$$f(z) = \begin{cases} 0 & z = 0 \\ -2z & z < 0 \\ 2z - 1 & z > 0 \end{cases} .$$

It remains to show that this mapping has the desired properties. This is left as an exercise to the reader. □

Exercise 13.1. Show that the map described in the proof of Proposition 13.4 is a bijection which

- has 0 as a fixed point,

- maps the negative integers to the even natural numbers, and
- the positive integers to the odd natural numbers.

Theorem 13.5. *If $f : X \to Y$ and $g : Y \to X$ are injective, then there exists a bijection $h : X \to Y$.*

Proposition 13.6. *The set $\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. Define a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as $f(n, m) = 2^n 3^m$ for each $(n, m) \in \mathbb{N}$. We claim that f is an injection. Fix $(a, b), (n, m) \in \mathbb{N} \times \mathbb{N}$ and suppose that $f(a, b) = f(n, m)$. Let $z = f(a, b) = f(n, m)$. So, $2^a 3^b = z = 2^n 3^m$. Using the Fundamental Theorem Of Arithmetic, Theorem 5.7, z has a unique prime factorization. Thus, $a = n$ and $b = m$ So, $(a, b) = (n, m)$. Thus, f is injective.

Finally, the map $n \mapsto (n, 1)$ is an injection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$. Thus, Theorem 13.5 gives that there exists a bijection between $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$. Thus, $\mathbb{N} \times \mathbb{N}$ is countable. □

Proposition 13.7. *The set of rationals, $\mathbb{Q}$, is countable.*

Proof. We will show this in steps. Assume that we have constructed a bijection $f : \mathbb{Z}^+ \to \mathbb{Q}^+$. Note this map, after multiplying by -1, sees that negative rationals are have the same cardinality as $\mathbb{Z}$ as well. Now, with this bijection, we can form a bijection $g : \mathbb{Z} \to \mathbb{Q}$ defined as as

$$g(z) = \begin{cases} 0 & z = 0 \\ -f(-z) & z < 0 \\ f(z) & z > 0 \end{cases}$$

for each $z \in \mathbb{Z}$. With this bijection in hand, we use the fact that $\mathbb{Z}$ is countable, Proposition 13.4, together with Proposition 13.3 to obtain that $\mathbb{Q}$ is countable.

So, it remains to show that there is a bijection $f : \mathbb{Z}^+ \to \mathbb{Q}^+$. (There is a classic zig-zag argument which informally describes such a bijection. This zig-zagging can be made formal, and a closed form of that description can be written. I will present that in lecture, but for the notes I will show a different way.) As $\mathbb{Z}^+ \subset \mathbb{Q}^+$, there exists, trivially, an injection $\mathbb{Z}^+ \to \mathbb{Q}^+$, say $z \mapsto \frac{z}{1}$. Though, as $|\mathbb{Z}^+| = |\mathbb{N}|$, we can produce an injection from $\mathbb{N}$ to $\mathbb{Q}$, say $n \mapsto \frac{n+1}{1}$.

Define an injection from $\mathbb{Q}^+$ to $\mathbb{N}$ as follows First, we define $h : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$. For each $r \in \mathbb{Q}$, write $r = \frac{a}{b}$ where $\frac{a}{b}$ is completely reduced. Define $h(r) = (a, b)$. Certainly, this map is an injection. We use the fact that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ to obtain a bijection $i : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Then $i \circ h$ is the desired injection.

Finally, applying Schroder-Bernstein Theorem, we have that there exists a bijection $f' : \mathbb{N} \to \mathbb{Q}^+$. Set $f : \mathbb{Z}^+ \to \mathbb{Q}^+$ to be $f'(n + 1)$. □

Index