Calculus
and other higher level mathamatics

Dedicated to Shane Carey, who showed me the beauty of mathematics

Contents

1 Introduction

1.1 Thinking Mathematically

Despite this being a calculus textbook I will actually start off by teaching something normally taught in a *Discrete Mathematics* course. The first few sections of a discrete course usually go over mathematical logic and proof writing, and here I intended to give you a brief overview (a sparknotes version, if you will) of that. Why you may ask? Simply put, I think that logic (the mathematical sort in specific) is necessary, if not vital, for success not just in math, but also in life.

1.2 Introduction to Logic

Before we begin with the basics, there first something even more basic we must cover. Often times in logic we will create statements full of symbols and it's important to note that the end goal is usually to evaluate if the statement is true or false given a certain set of inputs. In order to abstractly represent this we will use *statement variables*. Statement variables are simply placeholder variables in a statement that can represent either a value of **true** or **false**. Now, let's begin with the basics:

Definition 1.2.1: Logical AND

Logical AND ($\wedge$)

Logical AND works exactly how you might expect it to: given two inputs, p and q, both p AND q must be true for the output to also be true. Logical AND is symbolized using the wedge: $\wedge$[a]. Thus, we can write $p \wedge q$ which is read as "p and q". The truth table[b] for AND looks like the following:

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

[a] In other texts, AND may also be symbolized through multiplication: $p * q \equiv pq \equiv p \wedge q$
[b] A truth table is a way to represent all possible truth values for a given statement

Definition 1.2.2: Logical OR

Logical OR ($\vee$)

Logical OR works, again, how you would probably expect it, given a statement $p \vee q$ (read "p or q"), *either* p OR q must be true for the output to be true. Logical OR is symbolized using the upside-down wedge: $\vee$[a]. Thus, we can write $p \vee q$ which is read "p or q". Using the truth table for AND and the above information about logical or, fill out the below truth table for OR:

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

[a] Similar to AND, OR might be represented through addition: $p + q \equiv p \vee q$

Definition 1.2.3: Logical NOT

LOGICAL NOT

Logical NOT, is very easy to understand. Simply put, the not operator just negates the current value of a variable. If the current value is true then the negated value is false, and vice versa. Logical NOT can be symbolized using $\sim$ or $\neg$[a]. Thus, we can write $\neg p$ which is read "not p". Once again, the truth table for NOT is left as an exercise to the reader:

p	$\neg p$
T	
T	
F	
F	

[a]NOT, may also be symbolized through an exclamation point: $!p \equiv \neg p$

Now, before we work some examples, let's quick take note of the logical order of operations:

Note 1.2.1: Logical Order of Operations

1. NOT gets evaluated first
2. AND second
3. OR is the last evaluated

Just like in normal algebra, parenthesis can be used to override the order of operations. For example, in the statement: $(p \vee q) \wedge r$, the parenthesis are used to show that $p \vee q$ should be evaluated first.

Examples: Use a truth table to evaluate the truth values of each statement

1. $\neg(p \vee q)$

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

2. $p \wedge \neg q$

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

3. $(p \wedge q) \wedge r$

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

1.3 Quantifers

As well as conditional operators, we have quantifiers which we can use to represent general statements about a certain set of objects. It's best to get right into it:

Definition 1.3.1: Universal Quantifier

The universal quantifer, $\forall$, is used to represent a shared truth value amongst *all* values in a given domain. For example, we could say $\forall x \in \mathbb{R}, x * 0 = 0$[ab], this statement would read "*for all* real numbers x, $x * 0 = 0$". The formal defintion of the universal quantifer looks something similar to the following:

Given a statement $Q(x)$ and the domain of x to be D, the **universal statement** $\forall x \in D, Q(x)$[c] is said to be true if, and only if, $Q(x)$ is true for *every* x in D. The statement is said to be false if $Q(x)$ is false for *at least one* x in D.

[a]The $\in$ symbol means 'contained in'
[b]$\mathbb{R}$ is the set of all real numbers
[c]Note that the $Q(x)$ on its own after the comma is implied to mean that $Q(x)$ is true

Definition 1.3.2: Existential Quantifier

The existential quantifer, $\exists$, is used to represent a truth value for *at least* ***one*** value in a given domain. For example, we could say $\exists x \in \mathbb{R}$ such that $\mathbf{e}^x = 1$[a], which reads "*there exists* a real number, x such that $\mathbf{e}^x = 1$". A more formal definiton can be found below:

Given a statement $Q(x)$, and the domain of x to be D, the **existential statement** $\exists x \in D$ such that $Q(x)$ is said to be true if, and only if, $Q(x)$ is true for *at least* one x contained in D. The statement is said to be false if, and only if, $Q(x)$ is false *for every* x in D.

[a]The abbriviation 's.t.' is often used in place of 'such that' and will be used going forwards

For each question, rewrite the statement using the universal or existential quantifier
Let $\mathbb{R}$ be the set of real numbers, $\mathbb{N}$ be the set of natural numbers, and $\mathbb{Q}$ be the set of rational numbers

1. Every real number times 1 equals itself
2. There exists a natural number that is both even and prime
3. Every rational number times it's reciprocal equals 1
4. For all real numbers x, there exists another real number, y, such that $x + y = 0$

Definition 1.3.3: Combining Quantifiers

As you saw, the final exercise on the previous page required the use of both the universal and the existential quantifier, which is not an uncommon occurence. When we combine two quantifers in a statement they are intepreted **in the order they occur**. Thus the statements $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ s.t. $P(x, y)$ and $\exists x \in \mathbb{Z}$ s.t. $\forall y \in \mathbb{Z}$, $P(x, y)$ have very different meanings. This leads us to the following: *switching the order of different quantifers may (and often will) change the meaning of a statement.* However, if two quantifers are of the same type, then switching the order **will not** change the value of the statement: $\forall x \in \mathbb{Z}$, $\forall y \in \mathbb{Q}, P(x, y) \equiv \forall y \in \mathbb{Q}$, $\forall x \in \mathbb{Z}, P(x, y)$ and $\exists x \in \mathbb{Q}$ s.t. $\exists y \in \mathbb{A}$ s.t. $P(x, y) \equiv \exists y \in \mathbb{A}$ s.t. $\exists x \in \mathbb{Q}$ s.t. $P(x, y)$[a].
** Note that in these examples $P(x, y)$ is a predicate, which contains variables and becomes a statement when specific values are subsituted for the variables*

[a] $\mathbb{A}$ is the set of algebraic numbers, for more information see this link or this link

Before we begin our calculus journey, there is one final logic topic I would like to cover: implication.

Definition 1.3.4: Implication

Implications are used for conditional statements and is represented by an arrow: $\rightarrow$. For example: if it it snowing, then it is below 32°F[a]. We can rewrite this symbolically by representing the statement 'it is snowing' with 'S' and the statement 'it is raining' with 'R'. Thus we get: $S \rightarrow R$ which would be read as "If S then R". The general conditional statement is $H \rightarrow C$ or "if hypothesis, then conclusion". The conditional statement is true if, and only if, both the hypothesis and the conclusion are true, or if the hypothesis is false. The second part may throw some for a loop, but consider the earlier example. If it is *not* snowing, then it must also not be below 32°F, which is another true statement. Or consider a different perspective: if it *is* snowing, but it *is not* below 32°F, then we have a contradiction, and so our statement must be false. With all this in mind, see the truth table for the conditional statement:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

[a] Assume, in this case, that in order for it be snowing it *must* be below 32°F

For the following examples, rewrite the statement without using any symbols:
Recall that $\mathbb{R}$ is the set of all real numbers, $\mathbb{Q}$ is the set of all rational numbers, and $\mathbb{N}$ is the set of all natural numbers

1. $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ s.t. $x * y = x$

2. $\exists a \in \mathbb{R}$ s.t. $\forall b \in \mathbb{R}$, $a * b = a$

3. $p \in \mathbb{N} \rightarrow p \in \mathbb{Q}$

2 Basic Group Theory

2.1 Group Axioms

Definition 2.1.1: Group axioms

Let $G = (G, *)$ be a group where G is a set and $*$ the group operation. Then, the following are true:

1. There exists an identity element $1_G \in G$ such that $g * 1_G = 1_G * g = g$ for all $g \in G$.
2. Every element $g \in G$ has an inverse $g^{-1} \in G$ such that $g * g^{-1} = 1_G$
3. The product elements in G is associative such that for $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
4. The product of two elements in G is commutative if and only if the group is abelian. (Ie. if a group G is abelian then $g * q = q * g$ for all $g, q \in G$)

Example 2.1.1: $(\mathbb{Z}, +)$

Let $G = (\mathbb{Z}, +)$ be the group of integers under addition. Then the identity element is 0 and the inverse of an integer $g \in G$ is $-g$. The group operation is associative since addition is associative. The group is abelian since addition is commutative. This group is called $\mathbb{Z}$.

Definition 2.1.2: The set of Rational Numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$$

Question 2.1.1: Group of Rational Numbers

Is $H = (\mathbb{Q}, *)$ a group? Why or why not?

2.2 Isomorphisms

2.2.1 Bijective functions

Definition 2.2.1: Bijective Functions

A bijective function is a function that is both injective and surjective. This means that the function is both one-to-one (ie. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$) and onto (ie. if $F : X \to Y$ is our function, then for every $y \in Y$ $\exists x \in X : F(x) = y$)

Definition 2.2.2: Domain, Codomain, and Range

Let $f : X \to Y$ be a function. Then,

- X is the **domain**
- Y is the **codomain**
- Let $Z = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}$. Then, Z is the **range** of f.

2.2.2 Isomorphic Groups

For two groups to isomorphic essentially means for them to be the same while also being different! Let's start with an example before going to a formal defintion. Consider the two groups $\mathbb{Z} = (\mathbb{Z}, +)$ and $10\mathbb{Z} = (10\mathbb{Z}, +)$ where $10\mathbb{Z} = \{\ldots, -20, -10, 0, 10, 20, \ldots\}$ and $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Now, take a look at the two groups and realize that they're pretty much the exact same except in the names of the elements. Notice that we can create a *bijective*

function $\phi : \mathbb{Z} \to 10\mathbb{Z}$ by the map $x \mapsto 10x$. One extremely interesting property of ϕ is that it respects the group operation from $\mathbb{Z}$ to $10\mathbb{Z}$:

$$\phi(x + y) = \phi(x) + \phi(y)$$

So, we've created a function that simply just re-assigns the elements without actually changing the structure of the group.

Definition 2.2.3: Isomorphisms

Let $G = (G, \star)$ and $H = (H, \times)$. G is **isomorphic** to H if, and only if, there exists a *bijective* function $\phi : G \to H$ such that $\forall g_1, g_2 \in G$:

$$\phi(g_1 \star g_2) = \phi(g_1) \times \phi(g_2)$$

ϕ is called an **isomorphism**. It's important to note that the left hand side uses the group operation of G and the right hand side uses the group operation of H. Note that we can rephrase this to say: If there exists an isomorphism from G to H then, G and H are isomorphic, denoted $G \cong H$.

Example 2.2.1: Integers mod 6 to multaplicative integers mod 7

I claim that $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$ where $\mathbb{Z}/6\mathbb{Z}$ is the group of integers modulo 6 under addition and $(\mathbb{Z}/7\mathbb{Z})^\times$ is the group of integers modulo 7 under **multiplication**. In order to prove isomorphism we must find a function $\phi : \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^\times$ such that $\phi(x + y) = \phi(x)\phi(y)$. The bijection is

$$\phi(a \bmod 6) = 3^a \bmod 7$$

We can see this to be bijective by direct proof

$$(3^0, 3^1, 3^2, 3^3, 3^4, 3^5) \equiv (1, 3, 2, 6, 4, 5) \pmod 7$$

Note that it's techincally $3^{0 \bmod 6}$, but since $a \bmod b = a \Leftrightarrow a < b$ it can be omitted here. Now to verify that ϕ respects the group operation we must show that

$$\phi(x + y \bmod 6) = \phi(x \bmod 6)\phi(y \bmod 6)$$

However, this is just the same as saying that $3^{a+b \bmod 6} \equiv 3^{a \bmod 6} 3^{b \bmod 6} \pmod 7$ which we know to be true through properties of exponents.

2.3 Orders

Definition 2.3.1: Order of a Group

The order of a group G is the the number of elements in G, denoted $|G|$. $|G|$ may be finite or infinite. If G is a **finite group** then $|G| < \infty$.

Definition 2.3.2: Order of an Element

The order of an element $g \in G$ is the smallest integer n such that $g^n = 1_G$, denoted $|g|$. If there is no value of n such that $g^n = 1_G$ then $|G| = \infty$.

Example 2.3.1: Example Orders of Groups

- The order of the group $\mathbb{Z}$ is $|G| = \infty$.
- The order of the group $\mathbb{Z}/6\mathbb{Z}$ is $|G| = 6$.
- The order of the group $(\mathbb{Z}/7\mathbb{Z})^\times$ is $|G| = 6$.

2.4 Homomorphisms

Definition 2.4.1: Homomorphisms

Let $G = (G, \star)$ and $H = (H, \times)$. A function $\phi : G \to H$ is a **homomorphism** if, and only if, $\forall g_1, g_2 \in G$:

$$\phi(g_1 \star g_2) = \phi(g_1) \times \phi(g_2)$$

Now its important to notice the difference between an isomorphism and a homomorphism: an isomorphism is a homomorphism that is also bijective. This makes sense as isomorphism is a stricter sense of equality so it must have stricter rules. Thus, every isomorphism is a homomorphism, but not every homomorphism is an isomorphism. As well, note that a homomorphism does not need to be surjective or injective, it just needs to preseve the group operation.

Example 2.4.1: Examples of homomorphisms

- The identity map $G \to G$ is a homomorphism
- There exists **the trivial homomorphism** $\phi : G \to H$ such that $\phi(g) = 1_H$ for all $g \in G$. This is a homomorphism since $\phi(g_1 \star g_2) = 1_H = 1_H \times 1_H = \phi(g_1) \times \phi(g_2)$.
- There is homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/100\mathbb{Z}$ given by the rule $x \mapsto x \bmod 100$.
- There is a homomorphism from $\mathbb{Z}$ to itself given by $x \mapsto 2x$. Note that this is injective but not surjective but is still a homomorphism.

Before moving on I encourge you to verify for yourself that the last two examples are indeed homomorphisms.

Fact 2.4.1: Properties of Homomorphisms

Let ϕ be a homomorphism from G to H. Then,

$$\phi(1_G) = 1_H \text{ and } \phi(g^{-1}) = \phi(g)^{-1}$$

Proof. To prove the first property, we can use the fact that 1_G is the identity element of G. Thus, for any $g \in G$, we have:

$$\phi(1_G) = \phi(1_G * 1_G) = \phi(1_G)\phi(1_G) \Rightarrow \phi(1_G)\phi(1_G)^{-1} = \phi(1_G)\phi(1_G)\phi(1_G)^{-1} \Rightarrow \phi(1_G) = 1_H$$

Recall that $\phi(g) \in H$ so $\phi(g)\phi(g)^{-1} = 1_H$ for all $g \in G$. To prove the second property, we can start with the first property and build from there:

$$\phi(g * g^{-1}) = \phi(1_G) = 1_H \Rightarrow \phi(g)\phi(g^{-1}) = 1_H \Rightarrow \phi(g)\phi(g^{-1})\phi(g)^{-1} = \phi(g)^{-1} \Rightarrow \phi(g^{-1}) = \phi(g)^{-1}$$

□

Definition 2.4.2: Kernel of a Homomorphism

Let $\phi : G \to H$ be a homomorphism. The **kernel** of ϕ, denoted $\ker(\phi)$, is the set of all elements in G that map to the identity element in H:

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_H\}$$

$\ker \phi$ is a subgroup of G (at the very least $1_G \in \ker \phi$)

Example 2.4.2: Example Kernels

- The kernel of the trivial homomorphism $\phi : G \to H$ by $x \mapsto 1_H$ is the entire group G itself, $\ker(\phi) = G$.
- The kernel of the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$ given by $x \mapsto x \bmod 100$ is the set of all integers that are multiples of 100, $\ker(\phi) = 100\mathbb{Z} = \{\ldots, -200, -100, 0, 100, 200, \ldots\}$.
- The kernel of the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto 2x$ is the set of all integers that are multiples of 0, which is just $\ker(\phi) = \{0\}$.

Question 2.4.1: Kernel of an Isomorphism

What is the kernel of an isomorphism and why?

2.5 Quotient Groups

The goal of this section is to define groups in the form G/N such as $\mathbb{Z}/100\mathbb{Z}$. First we have to talk about the kernel and one of its important properties. Recall that the kernel of a homomorphism, $\ker\phi$ is defined as

$$\{g \in G \mid \phi(g) = 1_H\} \tag{1}$$

Also recall that for any homomorphism $\phi : G \to H$ for $G = (G, \star)$ and $H = (H, \times)$

$$\phi(x \star y) = \phi(x) \times \phi(y) \tag{2}$$

Now if we combine **1** and **2** it should be evident that for any $g \in \ker\phi$ we have the following,

$$\phi(g \star x) = \phi(g) \times \phi(x) = 1_H \times \phi(x) = \phi(x) \tag{3}$$

So, interestingly enough, it seems as if for any $g \in \ker\phi$ our homomorphism can completely ignore it! Now what does this mean for us in our journey to define a quotient group? Well, lets work with a concrete example to start. Consider the integers modulo 100, $\mathbb{Z}/100\mathbb{Z}$, which we know to be the set

$$\mathbb{Z}/100\mathbb{Z} = \{0, 1, 2, 3, \dots, 97, 98, 99\} \tag{4}$$

Now, lets try to define this as a quotient group. We'll begin by taking a look at a homomorphism $\phi : \mathbb{Z} to \mathbb{Z}/100\mathbb{Z}$. It should be clear that $\ker\phi = 100\mathbb{Z}$ as $\forall g \in 100\mathbb{Z},\ g \bmod 100 = 0$. Now, let $N = 100\mathbb{Z}$ and consider the following

$$\begin{aligned}
N &= \{\dots, -200, -100, 0, 100, 200, \dots\} \\
N+1 &= \{\dots, -199, -99, 1, 101, 201, \dots\} \\
N+2 &= \{\dots, -198, -98, 2, 102, 202, \dots\} \\
&\vdots \\
N+97 &= \{\dots, -103, -3, 97, 197, 297, \dots\} \\
N+98 &= \{\dots, -102, -2, 98, 198, 298, \dots\} \\
N+99 &= \{\dots, -101, -1, 99, 199, 299, \dots\}
\end{aligned}$$

Now we can notice that for $n \in [0, 99]$ if we hold n constant then the image of $\phi(N + n)$ is the same and no two values of n produce the same image. Now I put forth the idea that our quotient group, Q, can be thought of the set whose elements are the above sets:

$$Q = \mathbb{Z}/100\mathbb{Z} = \{N, N+1, N+2, \dots, N+97, N+98, N+99\} \tag{5}$$

This allows us to construct an equivalence relation on G by saying $x \sim_N y \Leftrightarrow \phi(x) = \phi(y)$ and then think of Q as the equivalence classes of $\sim_N$. Regardless of how you decide to view it, most people find it easier to simply choose on element from each set and use that to represent the different sets. For example,

$$\mathbb{Z}/2\mathbb{Z} = \{\{\dots, -2, 0, 2, \dots\}, \{\dots, -3, -1, 1, \dots\}\} = \{0, 1\}$$

This idea is analgous to taking each 'fiber' and collapsing it onto a single element. So, what does this all mean? In short, if we have a quotient group $Q \cong G/N$ we can construct Q by using the left cosets of N where N is a normal subgroup of G.

Definition 2.5.1: Normal Subgroup

Let G be a group. A subgroug N of G is a **normal subgroup** of G if it is the kernel of some homomorphism. This is denoted as $N \trianglelefteq G$.

Definition 2.5.2: Left Cosets

Consider a group N such that N is a subgroup of G. Any get in the form gN is a **left coset** of N. Note that N can be *any* subgroup of G.

So, to put it all together,

Definition 2.5.3: Quotient Groups

Let $N \trianglelefteq G$. Then the quotient group G/N will be the group whose elements are the left cosets of N. We must also define the product of two elements in G/N, or the product of two cosets $C_1, C_2 \in G/N$.

- If c_1 is the value associated with C_1 and c_2 is the value associated with C_2 then the product C_1C_2 will be the coset that contains c_1c_2
- We can also defing C_1C_2 through the representations of C_1 and C_2. By definition of cosets we know that

  $$C_1 = g_1N \qquad \text{and} \qquad C_2 = g_2N$$

  for $g_1, g_2 \in G$. Thus, by the same logic above, C_1C_2 contains is the coset that contains g_1g_2. This definition is equivalent to the one above since $\phi(g_1g_2) = \phi(g_1)\,\phi(g_2) = c_1c_2$. So, its important to note how we can define this product both in terms of elements in G as well as elements in H.

3 Discrete Mathematics

3.1 Basic Number Theory

3.1.1 Basics and Definitions

Lets begin with the basics.

Definition 3.1.1: The Integers

The set of integers, represented $\mathbb{Z}$, contains all whole numbers, positive and negative. Symbolically, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

Definition 3.1.2: The Rational Numbers

The set of integers, represented $\mathbb{Q}$, contains all numbers that can be represented as fractions. Symbolically, $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}\,(n \neq 0)\}$

Theorem 3.1. *Every integer is a rational number.*

Proof. Trivial. □

Definition 3.1.3: Even and Odd Numbers

A number is **even** if, and only if, it is some multiple of 2. Symbolically, n is even $\Leftrightarrow n = 2k$ for some $k \in \mathbb{Z}$. A number if **odd** if, and only if, it is some multiple of 2 plus 1. Symbolically, n is odd $\Leftrightarrow n = 2k + 1$ for $k \in \mathbb{Z}$.

Theorem 3.2. *All integers are either even or odd*

Proof. Theorem (3.2) will be proved later in the section. □

Definition 3.1.4: Prime and Composite Numbers

A number is **prime** if, and only if, its only divisors are 1 and itself. In other words, n is prime $\Leftrightarrow \forall p, q \in \mathbb{Z},\ n = pq \Rightarrow p = n \vee q = n$. A number is **composite** if, and only if, it has more divisors than 1 and itself. Symbolically, n is composite $\Leftrightarrow \exists\ pq \in \mathbb{Z}$ such that $n = pq$ and neither p nor q equal n.

Theorem 3.3. 1 *is neither prime nor composite.*

Proof. Trivial. □

Lemma 3.4. *Every integer except* 1 *is either prime or composite.*

Proof. The proof is left as an exercise to the reader. □

Question 3.1.1: Sum of two rational numbers

Is the sum of two rational numbers also a rational number? Prove or give a counter example.

Fact 3.1.1: Closure

For those who are familiar with abstract algebra and set theory, given by the results of the previous question. Since the sum of two rational numbers is also rational we can say that the rational numbers are **closed** under the operation of addition. Symbolically: $\forall m, n \in \mathbb{Q},\ m+n \in \mathbb{Q}$. All this means is that for every two rational numbers, their sum is also a rational number.

Theorem 3.5. *The set of integers is closed under addition, subtraction, and multiplication.*

Proof. Trivial □

Theorem 3.6. *The set of rational numbers is closed under addition, multiplication, subtraction.*

Proof. Let $m, n \in \mathbb{Q}$. Then $m = \frac{a}{b}$ and $n = \frac{c}{d}$ for $a, b, c, d \in ZZ$ with $b, d \neq 0$.

Closure under addition: It follows that,

$$\begin{aligned} m+n &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{a}{b}\left(\frac{d}{d}\right) + \frac{c}{d}\left(\frac{b}{b}\right) \\ &= \frac{ad}{bd} + \frac{bc}{bd} \\ &= \frac{ad+bd}{bd} \end{aligned}$$

Since, $b \neq 0$ and $d \neq 0$, $bd \neq$. It follows from Theorem (3.5) that $ad + bd \in ZZ$ and $bd \in ZZ$ so by definition of $\mathbb{Q}$, $m + n \in \mathbb{Q}$.

Closure under subtraction: It follows that,

$$m - n = \frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$$

Following the logic as above, $\frac{ad-bc}{bd} \in \mathbb{Q} \Rightarrow m - n \in \mathbb{Q}$

Closure under multiplication: It follows that,

$$mn = \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$$

Since, $ac \in \mathbb{Z}$ and $bd \in \mathbb{Z} \setminus 0$, we have that $\frac{ac}{bd} = mn \in \mathbb{Q}$ by definition of $\mathbb{Q}$.
Thus we have shown that $\mathbb{Q}$ is closed under addition, subtraction, and multiplication. □

Note 3.1.1: $\mathbb{Q}$ closed under division

Eagle eyed readers might have noticed that Theorem (3.6) does not mention division. This obviously because $0 \in \mathbb{Q}$ and you cannot divide by 0. Thus, in order for the rational numbers to be closed under all four operations we must exclude 0 to create the set $\mathbb{Q} \setminus \{0\}$.

3.1.2 Divisibility

Definition 3.1.5: Divisibility

Let m and n be integers. Then m divides n if, and only if, $n = md$ for some $d \in \mathbb{Z}$. Symbolically, $m \mid n \Leftrightarrow n = md$, which is read '$m$ divides n'. The notation $\nmid$ means 'does not divide'.

Example 3.1.1: Basic Divisibility Examples

1. $2 \mid 4$ since $4 = 2k$ for $k \in \mathbb{Z}$ (obviously $k = 2$)
2. $3 \mid 9$ since $9 = 3k$ for $k \in \mathbb{Z}$
3. $2 \mid n \Leftrightarrow n$ is even
4. $2 \nmid n \Leftrightarrow n$ is odd

Question 3.1.2: Divisibility Proofs

Prove the final two statements from example (3.1.1)

Theorem 3.7 (Quotient-Remainder Theorem)**.** *Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then*

$$n = qd + r$$

where $0 \leq r < d$ for unique integers q and r.

Question 3.1.3: Application of the Quotient Remainder Theorem

Given the following values of n and d, find unique integers q and r such that $n = qd + r$ where $0 \leq r < d$:

1. $n = 56$ and $d = 3$
2. $n = 100$ and $d = 7$
3. $n = 3$ and $d = 2$

Definition 3.1.6: mod **and** div

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ such that $n = qd + r$ where q and r are unique integers and $0 \leq r < d$. Then $n \operatorname{div} d = q$ and $n \bmod d = r$.

Note 3.1.2

Note that the following is true:

$$m \bmod n = r \Leftrightarrow m \equiv r \pmod{n}$$

If you've ever programmed before the div should remind you an awful lot of the idea of integer division in programming languages. As well, another easy connection to draw should be that mod simply just returns the remainder of n/d which is why r must be bounded between $0 \leq r < d$. With these new ideas (mainly mod) we can extend our definition of divisibility to look like the following:

$$m \mid n \Leftrightarrow n = md \Leftrightarrow m \bmod n = 0 \Leftrightarrow m \equiv 0 \pmod{n}$$

Given $m, n, d \in \mathbb{Z}$ such that $n = md$

3.1.3 Theorems and such

Due to the structuring of this section and my lack of planning I've decided that this is the perfect section to talk about and prove some interesting theorems related to basic number theory. For more advanced readers I encourage you to try to write out your own proof before looking at the written one.
Before getting into the first theorem we must start with a new definition:

Definition 3.1.7: Parity

The **parity** of an integer refers to wether it is even or odd. 5 has an odd parity while 90 has an even parity. The fact that any integer is either even or odd is known as the **parity property**

Theorem 3.8. *Consecutive integers have opposite parity.*

Proof. Let $x \in \mathbb{Z}$. Then by the parity property, x is either even or odd.

x is even: Assume x is even. Then by definition of even numbers, $x = 2n$ for some $n \in \mathbb{Z}$. Then $x + 1 = 2n + 1$ which is odd by defintion of odd numbers. It follows that x and $x + 1$ have opposite parities.

x is odd: Assume x is odd. Then by defintion of odd numbers, $x = 2n + 1$ for some $n \in \mathbb{Z}$. Then, $x + 1 = (2n + 1) + 1 = 2n + 2 = 2(n + 1)$. Since the integers are closed under addition and multiplication (see 3.5), $n + 1$ is an integers, and thus $x + 1$ is even since it is of the form $2k$ where $k \in \mathbb{Z}$. It follows that x and $x + 1$ has opposite parities.

Thus, regardless of if any given integer is even or odd, the next consecutive integer will be of opposite parity. □

Theorem 3.9 (The Triangle Inequality)**.** *The $x, y \in \mathbb{R}$. Then,*

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

Proof. □

3.2 Relations

Definition 3.2.1: Relations

Let X and Y be sets. A relation R from X to Y is a subset of $X \times Y$. An ordered pair (x, y) is contained in R if, and only if, x is related to y, denoted $x \ R \ y$ or $x \sim_R y$ where $x \in X$ and $y \in Y$. If $X = Y$ then it is simply a relation on X.

Example 3.2.1: Example relations

- Define a relation E from $\mathbb{Z}$ to $\mathbb{R}$ such that $x \sim_E y \Leftrightarrow x - y > 0$.
  - $5 \sim_E 3$ since $5 - 3 = 2 > 0$
  - $5 \sim_E \pi$ since $5 - \pi > 0$
  - $\pi \not\sim_E 5$ since $\pi - 5 < 0$
- Define a relation T from $A = \{0, 1, 2, 3\}$ to $B = \{4, 5, 6, 7\}$ by the rule $x \sim_T y \Leftrightarrow x \mid y$
  - $1 \sim_T y \ \ \forall y \in B$ since $y = 1k$ has solutions, namely $k = y$
  - $0 \not\sim_T y \ \ \forall y \in B$ since $y = 0k$ has no solutions besides 0 and $0 \notin B$

Question 3.2.1: Finding relations

Find every element in B that is related to $2 \in A$ for the relation defined in the above example.

3.3 Equivalence Relations

Definition 3.3.1: Equivalence Relations

Let R be a relation on X. R is an equivalence relation if, and only if, it is *symmetric*, *transative*, and *reflexive*.

- A relation is *symmetric* if $a \sim_R b \Rightarrow b \sim_R a$ for $a, b \in X$.
- A relation is *transative* if $a \sim_R b$ and $b \sim_R c \Rightarrow a \sim_R c$ for $a, b, c \in X$
- A relation is *reflexive* if $a \sim_R a$ for $a \in X$.

To prove that a relation is an equivalence relation you must show that it is reflexive, symmetric, and transitive.

Question 3.3.1: Relation between Circuits

Let C be the set of all digital circuits that can be created using basic logic gates such as AND, OR, NOT, NOR, NAND, and XOR. Define a relation $\sim_E$ such that for any two circuits $a, b \in C$, $a \sim_E b$ if, and only if, a and b have the same truth/output tables. Prove that $\sim_E$ is an equivalence relation.

Theorem 3.10. *$\sim_E$, as defined in (3.3.1) is an Equivalence Relation*

Proof. Let C and $\sim_E$ be defined as in (3.3.1).

Proof of Reflexivity: Let $a \in C$. Then $a \sim_E a$ since a must have the same truth table as itself.

Proof of Symmetry: Let $a, b \in C$. Then $a \sim_E b$ and $b \sim_E a$ since if a and b have the same truth tables then b and a must have the same truth tables.

Proof of Transativity: Let $a, b, c \in C$ such that $a \sim_E b$ and $b \sim_E c$. Then, $a \sim_E c$ since if a and b have the same truth tables and b and c have the same truth tables, a and c must also have the same truth tables.

Therefore, since $\sim_E$ is reflexive, symmetric, and transitive, $\sim_E$ is an equivalence relation on C. □

3.3.1 Equivalence Classes

There may be times when we want to consider the set of all items that are related to a single item. Luckily for us, we have something that does exactly this.

Definition 3.3.2: Equivalence Classes

Let $\sim_R$ be a relation on a set X. Define the an equivalence class as the following set:

$$[a] = \{x \in X \mid x \sim_R a\}$$

This is the set of all elements in X that are related to a.

Lemma 3.11. *If $b \sim_R a$ then $[a] = [b]$*

Proof. To show that any two sets, A and B, are equivalent we must show that $A \subseteq B$ and $B \subseteq A$
Proof that $[a] \subseteq [b]$: Let $x \in [a]$. Then, by definition of equivalence classes $x \sim_R a$. But $a \sim_R b$ so $x \sim_R b$ since $\sim_R$ is transitive. Thus, $x \in [b]$.
Proof that $[b] \subseteq [a]$: Trivial and left as an exercise to the reader.
Thus, since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, $[a] = [b]$. □

Now following (3.11) it shouldn't be much of a surprise that when we wish to discuss the equivalence classes of a relation we often don't want to talk about *all* of them. Instead we talk about the **distinct** equivalence classes of a relation.

Definition 3.3.3: Distinct Equivalence Classes

The **distinct equivalence classes** of a relation are the first n equivalence classes such that no two equivalence classes are equivalent. Standardly we start with 0 and work our way up to n.

Example 3.3.1: Equivalence Classes of mod 2

Let $\sim_R$ be a relation on $\mathbb{Z}$ such that $m \sim_R n \Leftrightarrow 2 \mid (m-n)$. We can find the distinct equivalence classes of $\sim_R$ by noticing that $2 \mid (m-n) \Leftrightarrow m \equiv n \pmod 2$. With this in mind,

$$\begin{aligned}[a] &= \{x \in \mathbb{Z} \mid x \sim_R a\} \\ &= \{x \in \mathbb{Z} \mid 2 \mid (x-a)\} \\ &= \{x \in \mathbb{Z} \mid x \equiv a \pmod 2\}\end{aligned}$$

Hopefully, from here it should be pretty clear what our two distinct equivalence classes are:

$$\begin{aligned}[0] &= \{\dots, -4, -2, 0, 2, 4, \dots\} \\ [1] &= \{\dots, -3, -1, 1, 3, 5 \dots\}\end{aligned}$$

Question 3.3.2: Equivalence classes of congruence modulo n

What are the equivalence classes for the relation $\sim_T$ on $\mathbb{Z}$ where $m \sim_T n \Leftrightarrow 3 \mid (m-n)$? What about $m \sim_G n \Leftrightarrow 4 \mid (m-n)$? Can you generalize for $x \sim_C y \Leftrightarrow n \mid (x-y)$?

Theorem 3.12 (Equivalence Classes of Congruence modulo n relation)**.** *Let $\sim_R$ be a relation on $\mathbb{Z}$ such that $a \sim_R b \Leftrightarrow n \mid (a-b) \Leftrightarrow a \equiv b \pmod{n}$. The distinct equivalence classes of $\sim_R$ will be*

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{n}\} = \{x \in \mathbb{Z} \mid x = nk, \ \ k \in \mathbb{Z}\} \\
[1] &= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{n}\} = \{x \in \mathbb{Z} \mid x = nk+1, \ \ k \in \mathbb{Z}\} \\
&\vdots \\
[n-1] &= \{x \in \mathbb{Z} \mid x \equiv n-1 \pmod{n}\} = \{x \in \mathbb{Z} \mid x = nk+(n-1), \ \ k \in \mathbb{Z}\}
\end{aligned}$$

Proof. Left as an exercise to the reader. *(Hint: Use the quotient remainder theorem)* □