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. Oftentimesin 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 $\forall x \in \mathbb{R}, x * 0 = 0$[a][b], 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 $10\mathbb{Z} = \{\dots, -20, -10, 0, 10, 20, \dots\}$ and $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. 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?