Math Notes

Tyler Wilson

Contents

1 Mathematical Proof

A proof is defined as a verification of a proposition by a chain of logical deductions by a set of axioms.
A proposition is a statement that is true/false
A predicate is a proposition whose truth depends on the value of a variable. For example, the truth of $x = 2$ will depend on the value of x
An axiom is a proposition that is assumed to be true. Ex: if $a = b$ and $b = c$ then $a = c$.

1.1 Logic

1.1.1 Statement Types and Definitions

A statement is a sentance that is either true or false and will have exactly one of those truth values. They are fact and lack subjectvity.
Types of Statements:

- Axiom: statements we accept as true without proof
  Ex: let $m, n \in \mathbb{Z}$ then $m + n$ is also an integer
- Fact: statements we accept as true without proof
  Ex: let $x \in \mathbb{R}$ then $x^2 \geq 0$
- Theorem: an important true statement
- Collary: a statement that follows from a previous theorem
- Lemma: a true statement that helps us prove a more important result

- Result/Proposition: true statements that we will prove are called results (or propositions if more important)

Even/odd numbers:

- An integer is even if it can be written as $n = 2k$ for some $k \in \mathbb{Z}$
- An integer is odd if it can be written as $n = 2l + 1$ for some $l \in \mathbb{Z}$

Divisibility:

- Let $n, k \in \mathbb{Z}$. We say that k divides n if there is $l \in \mathbb{Z}$ so that $n = lk$. We write this as $k|n$ and say that k is a divisor of n and that n is a multiple of k
- Let $n \in \mathbb{N}$. We say that n is a prime when it has exactly two positive divisors (1 and itself). If n has more than two positive divisors then we say it is composite
  Finally, the number 1 is neither prime nor composite
- The greatest common divisor of a and b is the largest positive integer that divides both a and b.
  Ex: $\text{GCD}(4, 6) = 2$
- The least common multiple of a and b is the smallest positive integer divisible by both a and b.
  Ex: $\text{LCM}(8, 6) = 24$
- Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say that a is congruent to b modulo n when $n|(a - b)$. The n is referred to as the *modulus* and we write the congruence as $a \equiv b (\text{mod}\, n)$
  When $n \nmid (a - b)$ we say that a is not congruent to b modulo n and write $a \not\equiv b (\text{mod}\, n)$
  Ex: $5 \equiv 1 (\text{mod}\, 4)$
  Ex2: $17 \equiv 1 (\text{mod}\, 4)$
  Ex3: $3 \not\equiv 9 (\text{mod}\, 4)$

1.1.2 Set Notation

A set is defined as a collection of objects.
The objects are referred to as elements or members of the set.
Common notation uses capital letters for sets and lowercase numbers for elements.
The only question we can ask a set is "is this object in the set"
If a is an element of the set A, we write $a \in A$. If not, we write $a \notin A$.
The empty set is defined by $\varnothing = \{\}$
For small sets, we can define them by listing the elements. i.e. $B = \{1, 2, 3, 4\}$. However, for larger sets, we may make use of ellipses to represent skipped elements or using set builder notation.
Set builder notation is defined as:

$$S = \{\text{expression} \mid \text{rule}\}$$

Ex: $A = \left\{n^2 | n \text{ is a whole number}\right\} = \{0, 1, 4, 9, 36, \ldots\}$
Ex2: Rational Numbers: $\mathbb{Q} = \left\{\frac{a}{b} | a \in \mathbb{Z}, b \in \mathbb{N}\right\}$
The number of elements in a set S is called the cardinality of the set and is represented by $|S|$.

Ex: $|\varnothing| = 0$
Ex2: $|\{1, 2, 3\}| = 3$
Ex3: $|\{\varnothing, \{1, 2\}\}| = 2$

1.1.3 Logical Statements

A big part of math is proving that statements are true. We do this by starting from know facts (axioms, lemmas, theorems) and combining these facts using logic to build new facts.

An *open sentence* is a sentence whose truth value depends on the variable(s) that it contains (denoted by $P(x)$). i.e. the statement $x > 3$ is open as its truth value is dependent on the value of x.

Negation:
Given P, we can form a new statement with the opposite truth value. This is typically denoted with either $\sim P$, $\neg P$, or $!P$
Ex: The negation of "It is Tuesday" would be "It is not Tuesday".
Truth table:

P	$\sim P$
T	F
F	T

It also follows that the negation of a negation is the original statement: $\sim (\sim P) = P$.

Conjunction and Disjunction:
This is analogous to "and" and "or".
The *conjunction* of P and Q is defined to be "P and Q", denoted by $P \wedge Q$
The *disjunction* of P and Q is defined to be "P or Q inclusive", denoted by $P \vee Q$
This can be represented in the following truth table:

P	Q	$P \wedge Q$	$P \vee Q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

The conditional:
The *conditional* (or implication) is defined as "If P then Q", where the hypothesis is P and the conclusion is Q. This is denoted by $P \Rightarrow Q$
So, if P is true, and $P \Rightarrow Q$ is true then Q must also be true. In the case where P is false, this tells us nothing about Q. This can be summarized in the truth table:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

When formulating a proof, we want to prove that $P \Rightarrow Q$ is always true and can then use *modus ponens* to prove the truth of Q.
Modus ponens is typically a proof with the following structure:

- Assume that hypothesis P is true
- We see that P implies P_1
- From this we know that P_1 implies P_2

  $\vdots$
- From P_n we know that Q must be true $\square$

With implications, we can also define the converse, contrapositive, and biconditional
Given $P \Rightarrow Q$, the *converse* is defined to be $Q \Rightarrow P$ and the *contrapositive* is defined to be $(\sim Q) \Rightarrow (\sim P)$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(\sim Q) \Rightarrow (\sim P)$
F	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

It is worth noting that the contrapositive is identical to the implication. This can be very useful in proofs because in some cases, the contrapositive may be easier to prove.
One more logical statement is the *biconditional* which is when $P \Rightarrow Q$ and $Q \Rightarrow P$ are both true. It is defined as "P if and only if Q", denoted by $P \Leftrightarrow Q$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
F	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

1.2 Introduction to Proofs

1.2.1 A First Proof

The general method of writing a proof is to first write out some scratch work to solve the problem and then write a neat and structured proof which the reader will see.
Ex: Let n be an integer. If n is even then n^2 is even.
Scratch work:
We want to show that this implication is always true $(P \Rightarrow Q)$
We assume the hypothesis, n is even, is true (the false case doesn't tell us anything)
By the definition of even, $n = 2k,\ k \in \mathbb{Z}$
$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
Since $k \in \mathbb{Z}$ we know by an axiom that $2k^2 \in \mathbb{Z}$ so, by the definition of even we know that n^2 is even.
We can rewrite this using modus ponens as

- n is even $\Rightarrow n = 2k$ for some integer k
- $n = 2k$ for some integer $k \Rightarrow n^2 = 4k^2$
- $n = 4k^2 \Rightarrow n^2$ is two times an integer

- n^2 is two times and integer $\Rightarrow$ n^2 is even

Then the final proof would be written as follows:

Proof: Let n be an integer. If n is even then n^2 is even
Assume that n is an even number.
Hence we know that $n = 2k$ for some $k \in \mathbb{Z}$
If follows that $n^2 = 4k^2 = 2(2k^2)$
Since $2k^2$ is an integer, it follows that n^2 is even $\square$
Ex2: Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$ then $a|c$
Proof:
By definition of divisibility, $b = ka$ and $c = lb$ for $k, l \in \mathbb{Z}$.
We want to show $a|c$. That is $c = na$ for $n \in \mathbb{Z}$
Since $c = lb$ and $b = ka$, we know $c = lka$
Since $k, l \in \mathbb{Z}$ we know $kl \in \mathbb{Z}$ so we are done $\square$

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$ then $a|c$
Proof:
We start by assuming the hypothesis to be true
Assume that $a|b$ and $b|c$, so that $b = ka$ and $c = lb$ for some $k, l \in \mathbb{Z}$
It follows that $c = kla$
Since $kl \in \mathbb{Z}$, we know that $a|c$ as required $\square$