# Math 71: Preliminaries and Proof Writing

Lily McBeath*

September 15, 2023



*This LaTeX template is courtesy of Lucy Knight.

# 1 Some Set Theory

In mathematics we think of a **set** as a collection of mathematical objects. The objects in a set are not ordered, so it does not make sense to talk about where an object is in a set, or how many times it occurs. All that matters is whether or not the object is in the set.

Common examples of sets that you may already be familiar with are

- the natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$,
- the integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, and
- the real numbers $\mathbb{R}$.

Notice that all of the natural numbers are integers, and all of the integers are real numbers. These kinds of relationships between sets are crucial to the study of algebra, so we begin by defining some notation and conventions about sets and how they relate to one another.

## 1.1 Notation

Let $S$ be a set.

**Definition 1.1.** If $x$ is an object in $S$, we write $x \in S$ and say that $x$ is an **element** of $S$. If $x$ is not an element of $S$, we write $x \notin S$.

Further, we say that two sets $S$ and $S'$ are **equal**, and we write $S = S'$, if they have exactly the same elements.

**Example 1.2.** Let $S$ be the set of integers with absolute value less than 4. In **roster notation**, we can write this set as

$$S = \{-3, -2, -1, 0, 1, 2, 3\}.$$

Alternately, we can use **set-builder notation** to more concisely describe $S$, using the property satisfied by its elements:

$$S = \{x \in \mathbb{Z} : |x| < 4\}.$$

The symbol : in this notation means "such that," i.e., "the set of elements $x$ in $\mathbb{Z}$ such that $|x| < 4$."

Notice that in the example above, all of the elements of $S$ are contained in the larger set $\mathbb{Z}$. We formalize this phenomenon as follows.

**Definition 1.3.** A **subset** $A$ of a set $S$ is a set such that every element of $A$ is an element of $S$. That is, if $a \in A$ is an element of $A$, then $a \in S$. In this case, we write $A \subseteq S$. We say that $A$ is a **proper subset** of $S$ if $A \subseteq S$ and $A \neq S$, and we write $A \subsetneq S$.[1]

So $S \subsetneq \mathbb{Z}$ in Example 1.2. We also have $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{R}$.

[1] Some authors use the notation $A \subset S$ to mean that $A$ is a proper subset of $S$, but others use $A \subset S$ to simply mean $A$ is a subset of $S$, where $A$ may or may not equal $S$. Beware!

It is now clear that some sets are larger than others. How can we compare the sizes of sets? This is a fairly deep question in general.

**Definition 1.4.** We say that a set $S$ is a **finite set** if it contains a finite number of elements. This number is called the **cardinality** of the set and is written $|S|$. Otherwise, if $S$ contains infinitely many elements, we say that $S$ is an **infinite set**.

One special example is the **empty set**, the set with no elements. It has cardinality zero and is denoted by $\emptyset$ or $\{\}$.

**Proposition 1.5.** *Let $A$, $B$, and $C$ be sets.*

1. *$\emptyset \subseteq A$ and $A \subseteq A$.*
2. *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

*Proof.* Exercise. □

The objects in a set do not have to be numbers. They can even be other sets!

**Example 1.6.** Consider the set

$$E = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

The elements of $E$ are

- $\emptyset \in E$,
- $\{\emptyset\} \in E$, and
- $\{\emptyset, \{\emptyset\}\} \in E$.

Since $E$ has 3 elements, the cardinality is $|E| = 3$. Exercise for the reader: write out all of the subsets of $E$.

There is much more that can be said about cardinality in a real analysis or measure theory course, such as Math 73.

## 1.2 Unions, Intersections, and Differences

How do we compare two sets that are not necessarily subsets of one another? Say that

$$A = \{2, 4, 5, 7\} \subseteq \mathbb{Z}$$

and

$$B = \{1, 4, 5, 6\} \subseteq \mathbb{Z}.$$

$A$ is not a subset of $B$, and $B$ is not a subset of $A$, but they do share elements in common. Unions, intersections, and differences allow us to construct new sets from $A$ and $B$ that can help us understand more about them.

**Definition 1.7.** Let $S$ be a set, and let $A \subseteq S$ be a subset. The **complement** of $A$ (in $S$) is the set

$$A^c = \{x \in S : x \notin A\}.$$

If $B \subseteq S$ is some other set, the **difference** of $A$ and $B$, denoted $A \setminus B$ or $A - B$, is the set

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

It is important to note that the complement of a set $A$ is implicitly referencing some larger set $S$. In fact, in the definition above, $A^c = S \setminus A$ can be written as a set difference for clarity.

**Definition 1.8.** Let $S$ be a set, $A \subseteq S$, and $B \subseteq S$. The **union** of $A$ and $B$ is the set

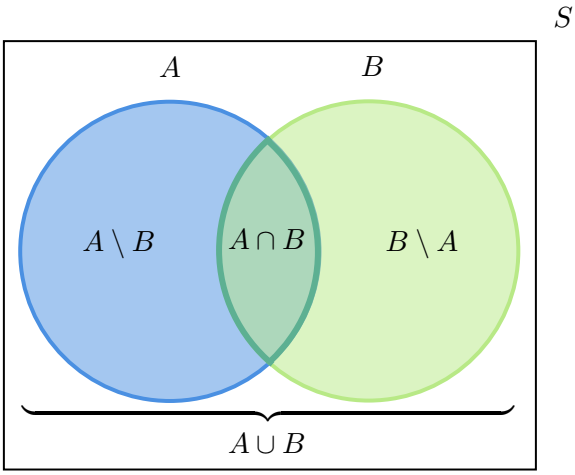
$$A \cup B = \{x \in S : x \in A \text{ or } x \in B\}.$$

The **intersection** of $A$ and $B$ is the set

$$A \cap B = \{x \in S : x \in A \text{ and } x \in B\}.$$

We say that $A$ and $B$ are **disjoint** if $A \cap B = \emptyset$.

The figure depicts these sets using a Venn diagram.




**Proposition 1.9.** *Let $S$ be a set, $A \subseteq S$, $B \subseteq S$, and $C \subseteq S$. Then*

1. $\emptyset \cup A = A$ *and* $\emptyset \cap A = \emptyset$.
2. $A \cap B \subseteq A \subseteq A \cup B$.
3. $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$ *(commutativity).*
4. $A \cup (B \cup C) = (A \cup B) \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C$ *(associativity).*
5. $A \cup A = A \cap A = A$.
6. *If* $A \subseteq B$ *then* $A \cup C \subseteq B \cup C$ *and* $A \cap C \subseteq B \cap C$.
7. $A \setminus B = A \cap B^c$.
8. $A = (A \setminus B) \cup (A \cap B)$.
9. $B = (B \setminus A) \cup (A \cap B)$.

*10.* $(A^c)^c = A$.

*11.* $(A \cap B)^c = A^c \cup B^c$.

*12.* $(A \cup B)^c = A^c \cap B^c$.

*Proof.* Exercise (Hint: the statement $A = B$ is equivalent to $A \subseteq B$ and $B \subseteq A$). □

The last two statements of Proposition 1.9 are known as **De Morgan's laws for sets**.

**Example 1.10.** Here are some common sets, written in set-builder notation.

1. The rational numbers
$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

2. The complex numbers
$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\}.$$

3. The real Hamiltonian quaternions
$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1,\\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j\}.$$

**Example 1.11.** Let $S$ denote the set of squares, $R$ the set of rectangles, $P$ the set of regular polygons, and $\mathcal{S}$ the set of shapes. Then $S \subsetneq R$, $S \subsetneq P$, $R \subsetneq \mathcal{S}$, and $P \subsetneq \mathcal{S}$. What is $R \cap P$?

Here is another important set to consider.

**Definition 1.12.** Let $S$ be a set. The **power set** of $S$, written $\mathcal{P}(S)$, is the set of all subsets of $S$.

For example, to answer the question posed at the end of Example 1.6, the power set of $E$ is
$$\mathcal{P}(E) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, E\}.$$

Remember that any set has the empty set and itself as subsets!

We will finish with one more important definition.

**Definition 1.13.** Let $A$ and $B$ be sets. The **cartesian product** of $A$ and $B$, denoted $A \times B$, is the set of ordered pairs of elements from $A$ and $B$. That is, in set-builder notation,
$$A \times B = \{(a, b) : a \in A,\ b \in B\}.$$

For example, the familiar Cartesian plane from calculus, denoted $\mathbb{R}^2$, is the set
$$\mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}.$$

# 2 Maps and Relations

Let $A$ and $B$ be sets. A **mapping** $f$ from $A$ to $B$, denoted $f : A \to B$ or $A \xrightarrow{f} B$, is an assignment of an element $f(a) \in B$ to each $a \in A$. It must be **well-defined**, which means that if $a_1, a_2 \in A$ and $a_1 = a_2$, then we must have $f(a_1) = f(a_2)$ (you may have seen the "vertical line test" in calculus, which tests well-definedness). A mapping may also be called a **map** or **function**, and we call the set $A$ the **domain** of $f$, and the set $B$ the **codomain**. The **image** of $f$, written $\text{im}(f)$ or $f(A)$, is the subset of $B$ consisting of all of the outputs of $f$. That is,

$$\text{im}(f) = \{f(a) \in B : a \in A\}.$$

For some subset $S \subseteq A$ of the domain $A$ of $f$, the **image of $S$** under $f$ is

$$f(S) = \{f(s) \in B : s \in S\} \subseteq \text{im}(f).$$

If $S = A$, then the image of $A$ under $f$ is precisely the image of $f$. On the other hand, for each subset $C \subseteq B$ the **preimage** or **inverse image** of $C$ under $f$ is the set

$$f^{-1}(C) = \{a \in A : f(a) \in C\}.$$

If $C$ consists of a single element, say $C = \{b\}$, then we call the preimage of $\{b\}$ under $f$ the **fiber** of $f$ over $b$.[2]

**Example 2.1.** The mapping $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is the familiar parabola. Note that authors sometimes write $x \mapsto x^2$ instead of $f(x) = x^2$ to define a mapping on elements.

**Example 2.2.** Let $A$ be the set of students enrolled in Math 71, and define a mapping

$$g : A \to \mathbb{Z}$$

as follows: if $a \in A$ denotes a student, then $g(a)$ is the student's age (in years).

We will explore the mappings in these examples further in the next section.

## 2.1 Injections, Surjections, and Bijections

We begin by defining some possible properties of mappings.

**Definition 2.3.** A mapping $f : A \to B$ is **injective** or **one-to-one** if distinct inputs are mapped to distinct outputs. That is, if $a_1, a_2 \in A$ and $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$. Or, equivalently, if $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$ then $a_1 = a_2$.[3]

In Example 2.1, $f$ is not injective: $-1 \neq 1$ but $f(-1) = f(1) = 1$. In Example 2.2, the function $g$ is injective if no two students have the same age, and otherwise not injective. In our case, $g$ is probably not injective.

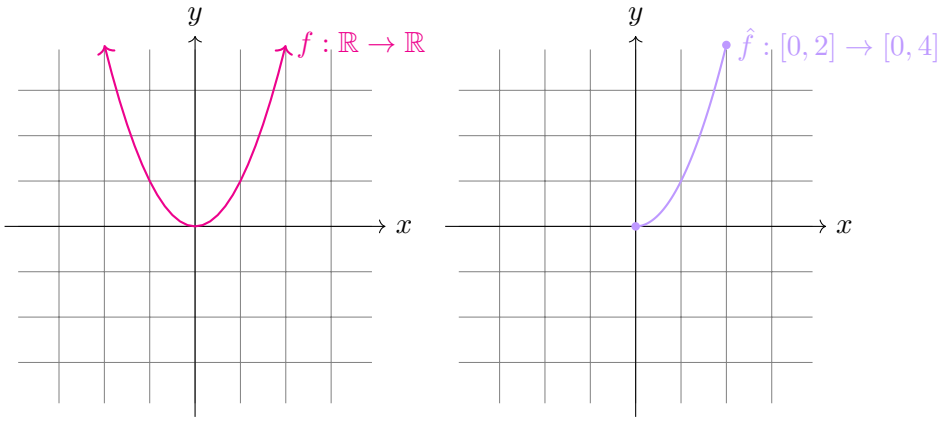
[2] Note that a fiber of $f$ over $b \in B$ may contain more than one element of $A$ (or no elements of $A$), so $f^{-1}$ is not necessarily a mapping.

[3] The latter definition of injective is much easier to prove in general.

**Definition 2.4.** A mapping $f : A \to B$ is **surjective** or **onto** if every element of $B$ is the output of some element of $A$. That is, for all $b \in B$ there exists $a \in A$ such that $f(a) = b$. Equivalently, this means that $B \subseteq \text{im}(f)$ (note that $\text{im}(f) \subseteq B$ for any mapping).

In Example 2.1, $f$ is not surjective since there is no $x \in \mathbb{R}$ such that $f(x) = x^2 = -1 \in \mathbb{R}$. The function $g$ from Example 2.2 certainly isn't surjective either, since it is impossible for a student to have age, say, $-100$.

That being said, changing the domain or codomain of a mapping that is not injective (or not surjective) can create a new mapping that *is* injective (or surjective). We denote the **restriction** of a function $f : A \to B$ to a subset $S \subseteq A$ of its domain as $f|_S : S \to B$. Exercise for the reader: show that although the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ from Example 2.1 is neither injective nor surjective, the restriction $f|_{[0,2]} : [0, 2] \to \mathbb{R}$ is injective (but not surjective). Further, by shrinking the codomain to match the image, we can get a function $\hat{f} : [0, 2] \to [0, 4]$ with $\hat{f}(x) = x^2$ that is both injective and surjective.




**Definition 2.5.** A mapping $f : A \to B$ is **bijective** or **invertible** if it is both injective and surjective.

So the mapping $\hat{f}$ described above is bijective.

Bijective mappings are sometimes called invertible because they indeed have inverses. If $f : A \to B$ is bijective, then $B = \text{im}(f)$ (surjectivity) so every element of $B$ has the form $f(a)$ for some $a \in A$, and moreover, this $a$ is unique (injectivity). So we can define a new function $f^{-1} : B \to A$ such that $f(a) \mapsto a$. That is, if $f(a) = b$, then $f^{-1}(b) = a$. For example, the bijective function $\hat{f}$ has inverse $\hat{f}^{-1} : [0, 4] \to [0, 2]$ defined by $\hat{f}^{-1}(y) = \sqrt{y}$.

## 2.2 Relations, Equivalence Relations and Equivalence Classes

We can also think of mappings within the more general language of relations.

**Definition 2.6.** Let $A$ and $B$ be (nonempty) sets. A **binary relation** $\mathcal{R}$ from $A$ to $B$ is a set of ordered pairs $\mathcal{R} \subseteq A \times B$. A **binary relation on** $A$ is a binary relation from $A$ to itself.

We will write $a \sim b$ and say $a$ is **related** to $b$ if $(a, b) \in \mathcal{R}$ for some $a \in A$ and $b \in B$, with $\mathcal{R}$ a binary relation from $A$ to $B$.

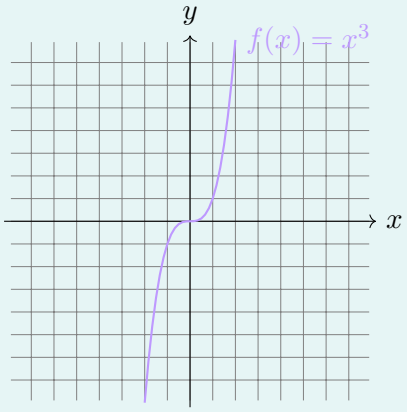
**Example 2.7.** Let $f : A \to B$ be a mapping. Then we can define a binary relation from $A$ to $B$ by the rule that $a \sim b$ if $b = f(a)$. Equivalently,

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

If $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = x^3$ for all $x \in \mathbb{R}$, then we have

$$\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y = x^3\},$$

which is the familiar graph below.




In fact, we could redefine a mapping $f : A \to B$ as a binary relation $f$ from $A$ to $B$ such that

$$A = \{a \in A : (a, b) \in f \text{ for some } b \in B\}$$

and for any $(a, b_1), (a, b_2) \in f$, $b_1 = b_2$. That is, every element of $A$ is related to *at least one* element of $B$, and every element of $A$ is related to *at most one* element of $B$.

Finally, we give some desirable properties that a binary relation on a set $A$ could have.

**Definition 2.8.** Let $\mathcal{R}$ be a binary relation on $A$. Then we say $\mathcal{R}$ is

1. **reflexive** if $a \sim a$ for all $a \in A$,
2. **symmetric** if $a \sim b$ implies $b \sim a$ for all $a, b \in A$, and
3. **transitive** if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.

If $\mathcal{R}$ is reflexive, symmetric, and transitive, then we say that $\mathcal{R}$ is an **equivalence relation**.

**Example 2.9.** Let $n \in \mathbb{N}$. We can define a binary relation on the set of integers $\mathbb{Z}$ as

$$\mathcal{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \mid (b - a)\},$$

where $n \mid (b - a)$ means "$n$ divides $b - a$," or in other words, there exists $q \in \mathbb{Z}$ such that $b - a = qn$.

Exercise for the reader: check that this is an equivalence relation.

The equivalence relation in Example 2.9 is so important in algebra and number theory that we give it its own definition.

**Definition 2.10.** Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $n \mid (b-a)$, we write

$$a \equiv b \bmod n$$

and say that $a$ is **congruent** to $b$ mod $n$.

We claim that the statement $a \equiv b \bmod n$ is closely related to the remainders of $a$ and $b$ upon division by $n$. Let $r$ be the remainder from dividing $a$ by $n$, and let $r'$ be the remainder for $b$, so that in particular we know that $0 \leqslant r < n$ and $0 \leqslant r' < n$, and there are integers $q, q'$ such that

$$a = qn + r \quad \text{and} \quad b = q'n + r'.$$

Assume that $n \mid (b-a)$, then $n$ divides

$$q'n + r' - (qn + r) = (q - q')n + (r' - r),$$

so that $n$ divides $r' - r$. But $0 \leqslant |r' - r| < n$, so $r - r' = 0$, and therefore $r = r'$. We conclude that the remainders of $a$ and $b$ upon division by $n$ are equal.

On the other hand, assume $r = r'$ in the representation of $a$ and $b$ above, then

$$b - a = q'n + r' - (qn + r) = (q - q')n + (r' - r) = (q - q')n,$$

so certainly $n \mid (b-a)$.

So we have shown that two integers being congruent mod $n$ is equivalent to two integers having the same remainder upon division by $n$, by proving that the first statement implies the second, and then that the second statement implies the first.[4] Moreover, if $a = qn + r$, then certainly $n \mid (a - r)$ so that an integer is congruent to its remainder mod $n$. We may deduce that all integers $a \in \mathbb{Z}$ can be classified via this equivalence relation by which of the possible remainders $\{0, 1, \ldots, n-1\}$ $a$ is congruent to mod $n$. This idea motivates the following definition.

**Definition 2.11.** Let $\mathcal{R}$ be an equivalence relation on $A$. The **equivalence class** of $a \in A$ is the set

$$\{x \in A : x \sim a\},$$

and we say that any element of the equivalence class of $a$ is **equivalent** to $a$. If $C$ is an equivalence class, then any element of $C$ is called a **representative** of the class.

So in the case of Example 2.9, denote the equivalence class of some $a \in \mathbb{Z}$ with respect to the equivalence relation by $\overline{a}$. Then $\overline{a}$ consists of integers that differ from $a$ by some integer multiple of $n$, and there are exactly $n$ different equivalence classes, up to choice of representative: $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. We say that the equivalence class of $a \in \mathbb{Z}$ with respect to the equivalence relation in Example 2.9 is a **congruence class** or **residue class** of $a$ mod $n$. The set of congruence classes of integers mod $n$ is called the **integers mod n** and is denoted by $\mathbb{Z}/n\mathbb{Z}$.

[4] This is a proof writing strategy that algebra students will use over and over again. We will discuss logic and proof writing more in Section 3.

# 3 Logic

Mathematical proofs are written in the language of logic. In order to write, read, and understand proofs, it is essential to understand their basic structure, and to avoid the pitfalls of logical fallacies.

## 3.1 Propositions

We begin with a simple definition.

**Definition 3.1.** A **proposition** is a sentence that is either true or false.

In order to make sense, propositions must clearly define each concept they contain. Opinions or vague statements about the future, such as "artificial intelligence will destroy the world," are not propositions.

**Example 3.2.** Examples of propositions:

1. $34 - 65 = 8$.
2. $34 - 65 = -31$.
3. The moon is made of cheese.
4. The Math 71 x-hour is at 3:30pm on Fridays.

To analyze propositions more abstractly, one can use a **truth table**, which displays some set of combinations of propositions in a tabular format. Here is a simple truth table representing the possible combinations of truth and falsehood of two propositions, which we denote by $P$ and $Q$:

| $P$ | $Q$ |
|---|---|
| $T$ | $T$ |
| $T$ | $F$ |
| $F$ | $T$ |
| $F$ | $F$ |

We can use truth tables to define the logical operations of AND, OR, and NOT.

**Definition 3.3.** Let $P$ and $Q$ be propositions. The **conjunction** (AND, $\wedge$) of $P$ and $Q$, the **disjunction** (OR, $\vee$) of $P$ and $Q$, and the **negation** (NOT, $\neg$) of $P$ are defined by the following truth tables.

| $P$ | $Q$ | $P \wedge Q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $F$ |

| $P$ | $Q$ | $P \vee Q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $F$ |

| $P$ | $\neg P$ |
|---|---|
| $T$ | $F$ |
| $F$ | $T$ |

Observe that disjunction (OR) refers to the inclusive or, which is sometimes called and/or in English, as opposed to the exclusive or which refers to "this or that but not both." Exercise to the reader: write the truth table for exclusive or.

We can use these logical operations to compute the truth value of propositions built out of other propositions in a more straightforward way.

**Example 3.4.** Let $P$, $Q$, and $R$ be the following propositions:

$P$: Dartmouth College is located in Hanover, New Hampshire.

$Q$: Dartmouth is a town in Massachusetts.

$R$: Dartmouth has eight letters.

$P$ is certainly true, and $R$ is false. It turns out that $Q$ is also true. Using this, we can compute the following:

| $P \wedge Q$ | $P \vee Q$ | $P \wedge R$ | $\neg R$ | $(\neg R) \wedge P$ | $\neg(R \vee P)$ | $(\neg P) \vee (((\neg R) \vee P) \wedge Q)$ |
|---|---|---|---|---|---|---|
| $T$ | $T$ | $F$ | $T$ | $T$ | $F$ | $T$ |

Exercise for the reader: does $P \vee (Q \wedge R)$ have the same truth value as $(P \vee Q) \wedge R$?

The process of proving a theorem involves evaluating how propositions lead to other propositions.

**Definition 3.5.** Let $P$ and $Q$ be propositions. The **conditional connective** ($\Longrightarrow$) and **biconditional connective** ($\Longleftrightarrow$) are defined by the following truth tables.

| $P$ | $Q$ | $P \Longrightarrow Q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $T$ |

| $P$ | $Q$ | $P \Longleftrightarrow Q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $T$ |

So, as the truth table shows, $P \Longleftrightarrow Q$ is true precisely when $P$ and $Q$ have the same truth states.

The truth table for the conditional connective $P \Longrightarrow Q$ seems a little more strange at first. The first row is reasonable: certainly $Q$ is true if $P$ is true if both $P$ and $Q$ were already true. In the second row, we see that it is impossible for a true statement to imply a false one. $P \Longrightarrow Q$ being false means that there is no way to assume $P$, and conclude $Q$. The third and fourth rows are perhaps the most strange: why are $F \Longrightarrow T$ and $F \Longrightarrow F$ considered true? Say that we assume $0 = 1$. Then this implies that $0 \cdot 0 = 0 \cdot 1$, so that $0 = 0$. We have shown that a false statement $P$ $(0 = 1)$ can imply a true statement $Q$ $(0 = 0)$, so logically speaking $P \Longrightarrow Q$ is true. On the other hand, assuming that $0 = 1$, we have $1+0 = 1+1$, so that $1 = 2$, another false statement.[5] Therefore one could say that a false proposition implies everything. You can learn more about these kinds of issues in a logic or mathematical philosophy course. Hopefully we will not be assuming false statements in Math 71 :)

There are various ways that the conditional and biconditional connectives are written in words. For example, $P \Longrightarrow Q$ can be written as any of the following:

- $P$ implies $Q$,
- if $P$ then $Q$,

[5] Or further, see this story about the mathematician and philosopher Bertrand Russell.

- $P$ only if $Q$,
- $P$ is sufficient for $Q$, or
- $Q$ is necessary for $P$.

On the other hand, $P \iff Q$ can be written as any of the following:

- $P$ if and only if $Q$,
- $P$ iff $Q$,
- $P$ and $Q$ are equivalent, or
- $P$ is necessary and sufficient for $Q$.

It is an important skill in mathematics to be able to clearly and concisely describe any mathematical statements you are making. This comes with practice!

## 3.2 Proofs and Methods of Proof

Mathematics is built on theorems.

**Definition 3.6.** A **theorem** is a justified assertion that a statement of the form $P \implies Q$ is true. A **proof** is an argument that serves as justification for a theorem.

One can think about a theorem as being in the first row of the truth table for $P \implies Q$. That is, if $P$ is true, then $Q$ is also true.

Here is a small example.

**Theorem 3.7.** *The sum of two odd integers is even.*

First, recall that everything in a proposition must be clearly defined. What does it mean mathematically for an integer to be odd or even? Let us make this precise.

**Definition 3.8.** Let $x$ be an integer. Then $x$ is **odd** if it can be written in the form $2n + 1$ for some $n \in \mathbb{Z}$. On the other hand, $x$ is **even** if it can be written in the form $2m$ for some $m \in \mathbb{Z}$.

How can we write Theorem 3.7 in the form $P \implies Q$? This involves separating our assumption from what we are trying to prove. In this case, $P$ is "$a$ and $b$ are odd integers," with odd defined as in Definition 3.8. We are trying to prove that their sum is even, so $Q$ is "$a + b$ is even," with even defined in Definition 3.8.

Here is a proof of Theorem 3.7.

*Proof.* Let $a, b \in \mathbb{Z}$ be odd. Then there exist integers $n, m \in \mathbb{Z}$ such that

$$a = 2n + 1 \quad \text{and} \quad b = 2m + 1.$$

Using the properties of the integers, we compute

$$a + b = (2n + 1) + (2m + 1) = 2(n + m) + 2 = 2(n + m + 1).$$

Since $n$ and $m$ are integers, $n + m + 1$ is an integer. So by definition, $a + b$ is even. □

Here is a question: if $P \implies Q$, does $Q \implies P$? The answer is no in general. For example, if it is raining, then I wear a jacket. But if I am wearing a jacket, that does not imply that it is raining (I might just be cold, or maybe it is snowing!). However, there is another construction that is logically equivalent to $P \implies Q$ that is used continually in mathematics.

**Definition 3.9.** The **converse** of $P \implies Q$ is $Q \implies P$. The **contrapositive** of $P \implies Q$ is $\neg Q \implies \neg P$.

**Theorem 3.10.** *The contrapositive of an implication is logically equivalent to the original implication.*

*Proof.* Exercise (Hint: compute the truth tables to see that they are identical). □

The contrapositive is a powerful tool in mathematics. Depending on $P$ and $Q$, it may be easier to prove $\neg Q \implies \neg P$ than $P \implies Q$ in some cases. Since the two are logically equivalent, proving $\neg Q \implies \neg P$ is necessary and sufficient to prove $P \implies Q$. This method is called **proof by contrapositive**.

**Example 3.11.** Let $a, b \in \mathbb{Z}$. Consider the following statement:

*"If $a + b$ is odd, then exactly one of $a$ or $b$ is odd."*

If we write this statement in the form $P \implies Q$, $P$ is "$a + b$ is odd for $a, b \in \mathbb{Z}$" and $Q$ is "exactly one of $a$ or $b$ is odd." Then the contrapositive of the statement is:

*"If the integers $a$ and $b$ are either both even or both odd, then $a + b$ is even."*

Thus, we can prove the statement $P \implies Q$ in Example 3.11 by proving its contrapositive. Since the hypothesis $\neg Q$ is "the integers $a$ and $b$ are either both even or both odd," when we prove this statement it makes sense to consider these two cases separately. This is often called a **proof by cases**.[6]

*Proof.* Let $a$ and $b$ be integers, and assume that $a$ and $b$ are either both even or both odd.

*Case 1:* Assume $a$ and $b$ are both even, then by definition there exist $n, m \in \mathbb{Z}$ such that $a = 2n$ and $b = 2m$. Then $a + b = 2n + 2m = 2(n + m)$ is even by definition.

*Case 2:* Assume $a$ and $b$ are both odd, then by definition there exist $k, \ell \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2\ell+1$. Then $a+b = (2k+1)+(2\ell+1) = 2(k+\ell+1)$ is even by definition.

In both cases $a + b$ is even, so we are done. □

Computing negations of propositions can be complicated, if the propositions are themselves built from combinations of other propositions. The general **De Morgan's laws** for logic are helpful here.

**Theorem 3.12.** *De Morgan's laws Let $P$ and $Q$ be propositions. Then*

1. $\neg(P \wedge Q) \iff \neg P \vee \neg Q$, *and*
2. $\neg(P \vee Q) \iff \neg P \wedge \neg Q$.

*Proof.* Exercise. □

[6] Note that it is essential to consider *all possible cases* in your argument.

Compare Theorem 3.12 to the De Morgan's laws for sets from Proposition 1.9.

## 3.3 Quantifiers

When performing more complicated proofs, it can be cumbersome to write out everything in full sentences. In fact, writing proofs concisely and using symbols such as $\implies$ and $\iff$ tend to make a proof more clear to the reader. Quantifiers are symbols that can be used to further clarify proofs.

**Definition 3.13.** The **universal quantifier** $\forall$ means "for all." The **existential quantifier** $\exists$ means "there exists."

For instance, we can rewrite the definition of a surjective mapping $f : A \to B$ as: $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$. Here are a few more examples.

| English | Logic |
|---|---|
| Every cloud has a silver lining. | $\forall$ clouds, $\exists$ a silver lining. |
| For every pair of positive real numbers, there is an integer whose product with the first is greater than the second. | $\forall x, y \in \mathbb{R}_{>0}$, $\exists n \in \mathbb{Z}$ such that $nx > y$. |
| Every positive integer can be written as the sum of the squares of four integers. | $\forall n \in \mathbb{N}$, $\exists a, b, c, d \in \mathbb{Z}$ such that $n = a^2 + b^2 + c^2 + d^2$. |

In some cases, the English version of a statement might be more clear than the version written with quantifiers. Regardless of how you choose to write your proofs on problem sets, the most important thing is that the reader can understand your proof fully from what is written (or typed) on the page.

# Index