[MA276] Intro to Proofs Notes

Rose-Hulman Institute of Technology

David Sachmanyan
February 25, 2026

Contents

1. Definitions

For the entire course, we can use and reference the following definitions:

1. An integer n is *even* if there exists an integer k such that $n = 2k$.
2. An integer n is *odd* if there exists an integer k such that $n = 2k + 1$.
3. For integers a, b, we say "a divides b", abbreviated as $a|b$, if there exists an integer k such that $ka = b$. In other words, a is a multiple of b.
4. A real number r is *rational* if there exists integers m, n where $n \neq 0$ so that $r = \frac{m}{n}$. Note that the set of rational numbers is denoted by $\mathbb{Q}$.
5. A real number r is *irrational* if r is not rational.
6. Recall that for rational numbers, $r = \frac{a}{b}$ and $q = \frac{c}{d}$ we know $r + q = \frac{ad+bc}{db}$.

When referencing these definitions, it is often helpful to restate the definition in the proof.

2. Proofs Practice

Problem 1. Proof by Contradiction. Prove if a and b are real numbers such that $ab = 0$, then $a = 0$ or $b = 0$. Note that we need to prove that $(a = 0) \vee (b = 0)$. So if we want to prove this by *contradiction*, we can say that $\neg(a = 0 \wedge b = 0) \equiv (a \neq 0 \vee b \neq 0)$.

Proof. Assume $a, b \in \mathbb{R}$ and $ab = 0$. To prove by contradiction, assume $a, b \neq 0$. Since $b \neq 0$ there exists some inverse of b, $b^{-1} \in R$ such that $bb^{-1} = 1$. We can conclude

$$(a \cdot b)b^{-1} = 0 \cdot b^{-1} \implies a\left(bb^{-1}\right) = 0 \tag{2.1}$$

by *associative law*. Since $0 \cdot b^{-1} = 0$, $a \cdot 1 = 0$ therefore $a = 0$. As this contradicts $a \neq 0$, it must be the case that $a = 0$ or $b = 0$. □

Problem 2. Show that for any integers m, n, if m and n are even, then $m + n$ is even.

Proof. For some $m, n \in \mathbb{Z}$, by the definition of even numbers, an integer c is even if $c = 2k$ for some $k \in \mathbb{Z}$. Since m, n are both even, it is the case that

$$m = 2k_1, \qquad n = 2k_2 \tag{2.2}$$

where $k_i \in \mathbb{Z}$ which means by substitution, we can say that $m + n = 2k_1 + 2k_2 = 2(k_1 + k_2)$. Since k_1, k_2 are integers and integers are closed under addition, $k_1 + k_2$ is also an integer. So, there exists some $k_3 = k_1 + k_2$ such that $2k_3 = 2(k_1 + k_2) = m + n$. Thus, for any $m, n \in \mathbb{Z}$, if m and n are both even, then the sum $m + n$ is also even. □

Problem 3. Show that if $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ where A, B are arbitrary sets.

Proof. First, we define the *power set* of an arbitrary set X, $\mathcal{P}(X)$ as the set of all subsets of X. We can also consider the definition of a subset which states that for the arbitrary sets X and Y, $X \subseteq Y$ if $\forall c \in X, c \in Y$. Since $A \subseteq B$, if we let $a \in A$ and $b \in B$, we can say that for all $a \in A$, $a \in B$. By the definition of a subset, we can also say that $\forall x \in \mathcal{P}(A), x \in \mathcal{P}(B)$. So by the definitions defined above, it must be that if $A \subseteq B$, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. □

Problem 4. Prove that $\overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}$ where I is an index set such that for each $i \in I$, A_i is a set. Note that this is a generalized form of DeMorgan's Theorem.

Proof. Not sure how to prove this lol. □

Problem 5. Prove that if the integers m, n are both odd, then $m + n$ is even.

Proof. By the definition of odd numbers, we can write an odd integer $c \in \mathbb{Z}$ as $c = 2k + 1$ where $k \in \mathbb{Z}$. Meaning, we can rewrite m, n as

$$m = 2k_1 + 1, \qquad n = 2k_2 + 1 \tag{2.3}$$

where $k_i \in \mathbb{Z}$. We are now free to say

$$\begin{aligned} m + n &= (2k_1 + 1) + (2k_2 + 1) && (2.4)\\ &= 2k_1 + 2k_2 + 2 && (2.5)\\ &= 2(k_1 + k_2 + 1). && (2.6) \end{aligned}$$

Since integers are closed under addition, we can name another integer $k_3 = k_1 + k_2 + 1$. We can now rewrite the sum as $m + n = 2k_3$. An integer c is considered to be even if it can be rewritten as $c = 2k$ where $k \in \mathbb{Z}$. Since our sum $m + n$ directly matches this form, it must be the case that if both m, n are odd, $m + n$ is even. □

Problem 6. Prove that for an real numbers r, q, if r and q are rational, then $r + q$ is rational.

Proof. A real number c is considered to be rational if there exists integers n, m such that $c = \frac{m}{n}$ where $n \neq 0$. Meaning, we can rewrite r, q as

$$r = \frac{m_1}{n_1}, \qquad q = \frac{m_2}{n_2} \tag{2.7}$$

where $m_i, n_i \in \mathbb{R}$ and $n_i \neq 0$. We know that the sum of two rational numbers $k_1 = \frac{a}{b}, k_2 = \frac{c}{d}$ can be written as

$$k_1 + k_2 = \frac{ad + bc}{db}. \tag{2.8}$$

If we write the sum of our two rational numbers r, q, we have

$$r + q = \frac{m_1}{n_1} + \frac{m_2}{n_1} = \frac{m_1 n_2 + m_2 n_1}{n_2 n_1} \tag{2.9}$$

which follows the form described in **??**. Therefore, if there exists two rational numbers r, q, their sum $r + q$ is also rational. □

Problem 7. Show that if any sets A, B, C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. By the definition of a subset, if there exists two sets X, Y, $X \subseteq Y$ if $\forall x \in X, x \in Y$. So by saying $A \subseteq B$, $\forall a \in A, a \in B$. Similarly, by saying $B \subseteq C$, we imply that $\forall b \in B, b \in C$. Therefore, $\forall a \in A, a \in C$ which means $A \subseteq C$. □

Problem 8. Prove that for any sets A, B, we know $B \cap A = A$ if and only if $A \subseteq B$.

Proof. If we assume that $B \cap A = A$ is true and let $x \in A$, we can say that $x \in B \cap A$. Thus, by the definition of *set intersection*, $x \in B$. Since $x \in A$ and $x \in B$, $A \subseteq B$. □

Problem 9. For some arbitrary set A, show that $\bigcup \mathcal{P}(A) = A$.

Proof. First we must show that $\bigcup \mathcal{P}(A) \subseteq A$. Assume $x \in \bigcup \mathcal{P}(A)$. By the definition of the union operator, there is $B \in \mathcal{P}(A)$ such that $x \in B$. Since $B \in \mathcal{P}(A)$, we know $B \subseteq A$. So, $x \in B$ and $B \subseteq A$ let us conclude that $x \in A$. So for any x, if $x \in \bigcup \mathcal{P}(A)$, then $x \in A$, making $\bigcup \mathcal{P}(A) \subseteq A$. Now, assume $x \in A$. Then $\{x\} \in \mathcal{P}(A)$ by the definition of the power set and clearly $x \in \{x\}$. Thus, there is $\{x\}$ in the $\mathcal{P}(A)$ with $x \in B$. □

3. Relation Definitions

Recall the following definitions:

- *Reflexive* iff. every element of A is related to itself: $\forall x \in A, (x, x) \in \mathbb{R}$.
- *Symmetric* iff. whenever xRy, we also have yRx: $\forall x \in A, \forall y \in A, (x, y) \in R \to (y, x) \in \mathbb{R}$.
- *Transitive* iff. xRy and yRz, then xRz: $\forall x, y, z \in A, [(x, y) \in \mathbb{R} \wedge (y, z) \in \mathbb{R} \to (x, z) \in \mathbb{R}]$.

We need to discuss another similar property known as *antisymmetric*. R is considered to be antisymmetric on A iff. for any $x, y \in A$, if xRy and yRx, then $x = y$. Basically, no distinct elements ($x \neq y$) are related in both directions.

Definition 3.1 (Partial Order)**.** A relation R on some set A to be a partial order if and only if R if reflexive, antisymmetric, and transitive.

Definition 3.2 (Poset)**.** An arbitrary set A with a partial order R together make a "partially ordered set" (A, R), often called a poset.

Some other useful definitions and terms are as follows: Given a poset (A, R), that is, a set with partial ordering R on A, and given a subset B of A, we define

(a) An element $b \in B$ is *R-smallest* (least) in B is for all $x \in B, bRx$. And $b \in B$ is *R-largest* (greatest) in B if for all $x \in B, xRb$.

(b) An element $b \in B$ is a *R-minimal* element of B if there does not exist some $x \in B$ such that bRx and $x \neq b$.

(c) Note: Smallest/largest elements of a set $B \subseteq A$ are unique if they exist (can you prove it?) Maximal/minimal elements may not be unique. If the partial order R is clear from context, we just say "smallest" instead of "R-smallest", etc.

(d) An element $u \in A$ is *upper bound* for the set B if for all $b \in B$, bRq. (Note, u is not necessarily in B). An element $l \in A$ is a *lower bound* for the set B if for all $b \in B$, lRb (Note, l is not necessarily in B).

(e) Let $\mathcal{U}$ be the set of upper bounds for B. The smallest element of $\mathcal{U}$ (if it exists) is the *least upper bound* ("lub" or "supremum") of B. Let $\mathcal{L}$ be the set of of lower bounds for B. The largest element of $\mathcal{L}$ (if it exists), is the *greatest lower bound* ("glb") of B.

Definition 3.3 (Identity Relation)**.** We define the identity relation i_A on the set A as

$$i_A = \{(x, x) \mid x \in A\}. \tag{3.1}$$

In essence, every element in the set is only related to itself, technically making it the "smallest" reflexive relation. In some cases, it is also known as the identity function where $f(x) = x$.

4. Relations Cheat Sheet

Below is a list of properties that a relation R may have in this course.

1. **Reflexive**. R is reflexive if $\forall a \in A, (a, a) \in R$.
   Meaning: Every element in R is related to itself.

2. **Irreflexive**. R is irreflexive if $\forall a \in A, (a, a) \notin R$.
   Meaning: No element is related to itself.

3. **Symmetric**. R is symmetric if $(a, b) \in R \implies (b, a) \in R$.
   Meaning: Relations go both ways, if (a, b), then (b, a).

4. **Antisymmetric**. R is antisymmetric if $(a, b) \in R \wedge (b, a) \in R \implies a = b$.
   Meaning: Distinct elements cannot point to each other, if they do, they are the same elements $(a = b)$.

5. **Asymmetric**. R is asymmetric if $(a, b) \in R \implies (b, a) \notin R$.
   Meaning: No elements are related in both directions (antisymmetric) and nothing relates to itself (irreflexive).

6. **Transitive**. R is transitive if $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$.
   Meaning: If (a, b) and (b, c), then (a, c).

7. **Equivalence relation**. R is considered to be an equivalence relation if it is
   (a) Reflexive
   (b) Symmetric
   (c) Transitive

8. **Partial order**. R is considered to be partial order if it is
   (a) Reflexive
   (b) Antisymmetric
   (c) Transitive

A relation R may also have the following:

1. **Minimal element**. An element $m \in A$ is minimal if $\forall x \in A, x \leq m \implies x = m$. *Meaning:* There is nothing that comes before m.

2. **Minimum element**. An element $m \in A$ is a minimum element if $\forall x \in A, m \leq x$.
   Meaning: m comes before everything.

3. **Maximal element**. An element $m \in A$ is maximal if $\forall x \in A, (m \leq x \implies x = m)$. *Meaning:* Nothing comes after m.

4. **Maximum element**. An element $m \in A$ is a maximum if $\forall x \in R, x \leq M$.
   Meaning: m comes after everything.

5. Relations Practice

Example 5.1. Consider the real numbers $\mathbb{R}$ with the $\leq$ order. $(\mathbb{R}, \leq)$ is a poset, and in fact, $\leq$ is considered to be total order.

(a) Find any minimal elements and maximal elements of $[0, 1)$.
Solution: No maximal, the only minimal element is 0.

(b) Does $[0, 1)$ have a smallest element? A largest element? If so, what are they?
Solution: No largest, the smallest element is 0.

In the previous example, especially (a) and (b), the reason why the answer is no for some of them might be a bit confusing. However, if we have some interval (a, b), it does not have a smallest. largest, minimal, or maximal. The reason for this is because in $\mathbb{R}$, has infinitely many numbers between its elements. So, for example, if we do not include b in the interval, then what is the greatest number in the set? It is hard to say.

Example 5.2 (Equivalence Relations)**.** Define the relation $\equiv_2$ on $\mathbb{Z}$ by

$$a \equiv_2 b \iff 2|(a - b). \tag{5.1}$$

That is, $a \equiv_2 b \iff (a - b)$ is even, or equivalently, $a \equiv_2 b$ if and only if a and b have the same remainder when we divide by 2. This relation is called the *congruence of integers mod 2*. We will prove some properties below:

1. *Reflexive*: Assume that $a \in \mathbb{Z}$. Since $a - a = 0$ and $0 = 0 \cdot 2$, we see $2|0$. So $2|a - a$ and therefore $a \equiv_2 a$.

2. *Symmetric*: Let $a, b \in \mathbb{Z}$. Assume $a \equiv_2 b$. Since $a \equiv_2 b$, we know $2|a - b$. So, $(a - b) = 2k$ for some $k \in \mathbb{Z}$. Then

$$(b - a) = (-1)(a - b) = 2(-1)k = 2(-k). \tag{5.2}$$

   So, $2|(b - a)$ by definition divides. Thus, $b \equiv_2 a$.

3. *Transitive*: Let $a, b, c \in \mathbb{Z}$ and assume that $a \equiv_2 b$ and $b \equiv_2 c$. So, $2|(a - b)$ and $z|(b - c)$. Thus, $a - b = 2k$ and $b - c2l$ for some $k, l \in \mathbb{Z}$. Now, since

$$\begin{aligned} a - c &= (a - b) + (b - c) && (5.3)\\ &= 2k + 2l && (5.4)\\ &= 2(k + l) && (5.5) \end{aligned}$$

   where $k + l \in \mathbb{Z}$. Therefore, $2|(a - c)$, so it must be the case that $a \equiv_2 c$.

Remark 5.1. Equivalence relations tend to "split up" our universe into what we call *partitions*.

Definition 5.1 (Equivalence Class)**.** For an equivalence relation E on the set A the *equivalence class* of $x \in A$ is the set of all elements of A that are related to x, in other words:

$$[x]_E = \{y \in A \mid yEx\}. \tag{5.6}$$

Example 5.3 (Equivalence Classes)**.** Come up with two equivalence relations on for the set $\{a, b, c, d\}$. Write down the family of equivalence classes for your equivalence relation.

6. Functions

Consider the function $f(x) = \frac{1}{x}$. We can write this formally as

$$f = \left\{ \left(x, \frac{1}{x} \right) \;\middle|\; x \in \mathbb{R} \setminus \{0\} \right\} \subseteq \mathbb{R} \setminus \{0\} \times \mathbb{R} \tag{6.1}$$

which we can express in the form $f : A \to B$ as $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ where A is the *domain* and B is the *codomain*. Actually, a function is just relation f from A to B is a function from A to B exactly when for all $a \in A$ there exists a unique $b \in B$ such that $(a, b) \in f$, written as $f : A \to B$.

Definition 6.1 (Injective)**.** A function $f : A \to B$ is injective (or "one to one") when every $b \in B$ appears as a second coordinate. Or more formally, $\forall b \in B, \exists a \in A$ so that $(a, b) \in f$. A common way of way of saying this is that every input gives a different output.

Definition 6.2 (Surjective)**.** A function $f : A \to B$ is surjective (or "onto")...

Definition 6.3 (Bijective)**.** A function is bijective if it is both injective and surjective.

Example 6.1. Is $g_1 = \{(m, n) \in \mathbb{R} \times \mathbb{R} \mid 2n = m\}$ a function from $\mathbb{R}$ to $\mathbb{R}$?
Solution: Yes, $g_1 : \mathbb{R} \to \mathbb{R}$.

Example 6.2. Consider the following examples functions:

(a) Is $g_1 = \{(m, n) \in \mathbb{R} \times \mathbb{R} \mid 2n = m\}$ a function from $\mathbb{R}$ to $\mathbb{R}$?
Solution: Yes, $g_1 : \mathbb{R} \to \mathbb{R}$.

(b) Is $g_2 = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid 2n = m\}$ a function from $\mathbb{Z}$ to $\mathbb{Z}$?
Solution: No, since, for example, $m = 1 \in \mathbb{Z}$ so $n = \frac{1}{2} \notin \mathbb{Z}$.

Proposition 6.1. *Given some function $f : A \to B$ and $g : A \to B$, $f = g$ if and only if for all $x \in A$, $f(x) = g(x)$.*

Theorem 6.1 (Composition of functions)**.** *If $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$. Moreover, for $a \in A$ we have $(g \circ f)(a) = g(f(a))$.*

Proof. Assume $f : A \to B$ and $g : B \to C$. Then, by definition, $g \circ f$ is a relation from A to C. Now, assume that $a \in A$. Since, $f : A \to B$, there exists a unique $b \in B$ such that $(a, b) \in f$ $(f(a) = b)$. Since g is a function from B to C, there is a unique $c \in C$ so that $(b, c) \in g$ or in more traditional function notation, $g(b) = c = g(f(a))$. By the definition of composition, $(a, c) \in g \circ f$. So for any $a \in A$, there exists some $c \in C$ such that $(a, c) \in g \circ f$. We will now prove the idea of uniqueness of $g \circ f$.

Assume $c_1, c_2 \in C$ and $(a, c_1), (a, c_2) \in g \circ f$. By the definition of composition of $g \circ f$, there are $b_1, b_2 \in B$ so that $(a, b_1) \in f$ and $(b_1, c_1) \in g$, $(a, b_2) \in f$, and $(b_2, c_2) \in g$. And since f is a function, $b_1 = b_2$. Since $b_1 = b_2$ and g is a function, we have $c_1 = c_2$. So, for any $a \in A$, there is a unique $c \in C$ such that $(a, c) \in g \circ f$. □

Remark 6.1. Functions are often called *maps* since they tend to map information from the set A to some other set B. We knew this though.

Theorem 6.2. *If $f : A \to B$ and $g : B \to C$ are both injective, then so is $g \circ f$.*

Proof. Assume $f : A \to B$ and $g : B \to C$ are both injective. We know that by definition, for all $x_1, x_2 \in A$, if

$$(g \circ f)(x_1) = (g \circ f)(x_2) \tag{6.2}$$

then $x_1 = x_2$. So, we will assume (6.2) is true. So, $g(f(x_1)) = g(f(x_2))$. Since g is injective, $f(x_1) = f(x_2)$. Now, since f is injective, $x_1 = x_2$. Therefore, $g \circ f$ is injective. □

Theorem 6.3. *If $f : A \to B$ is injective and surjective, then $f^{-1} : B \to A$.*

Proof. Let $b \in B$. Since f is surjective, there is $a \in A$ such that $f(a) = b$. Then, $(a, b) \in f$, so $(b, a) \in f^{-1}$ by the definition of inverse relations, showing existence.

Now, we must prove uniqueness. Assume $a_1, a_2 \in A$ such that $(b, a_1), (b, a_2) \in f^{-1}$. Then, $(a_1, b), (a_2, b) \in f$. This leads us to

$$f(a_1) = b, \quad f(a_2) = b, \quad f(a_1) = f(a_2) \tag{6.3}$$

and since f is injective, $a_1 = a_2$. Therefore, for any $b \in B$, there is a unique $a \in A$ where $(b, a) \in f^{-1}$, meaning f^{-1} is indeed a function from B to A. □

Theorem 6.4. *Suppose $f : A \to B$ and $f^{-1} : B \to A$. Then, $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_b$.*

Proof. For some arbitrary $a \in A$, then $(a, f(a)) \in f$ where $f(a) \in B$ is the unique element of B paired with a by f. Then, $(f(a), a) \in f^{-1}$. Since we know $(f^{-1} \circ f)(a) = f^{-1}(f(a))$, it follows that

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a = i_A \tag{6.4}$$

is true for all $a \in A$. Thus, $f^{-1} \circ f = i_A$. □

Often times in a class like pre-calculus, we learn that a function is invertible if it is injective, but this is not actually the whole story. Let $g : A \to \mathbb{R}$ where $A \subseteq \mathbb{R}$ be a one-to-one function. For example, $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = e^x$ is injective, but not surjective. Meaning, g^{-1} is not a function $\mathbb{R} \to \mathbb{R}$. For a function to have an inverse, it must be bijective.

Theorem 6.5. *Suppose $f : A \to B$. Then the following statements are all equivalent;*

(a) f is injective and surjective (f is a bijection)

(b) $f^{-1} : B \to A$.

(c) There exists a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$.

We have actually already established all the tools we need to prove the theorem above, but for the sake of time, we will not prove it in class.

7. Functions Practice

Problem 10. Given $f : A \to B$

(a) The function f is surjective ("onto") if:
Solution: $\forall b \in B, \exists a \in A,\ f(a) = b$.

(b) The function f is injective ("one to one") if:
Solution: $\forall a_1, a_2 \in A$ if $f(a_1) = f(a_2)$, then $a_1 = a_2$.

Problem 11. Is the function injective, surjective, or bijective: $h = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = 2m\}$ from $\mathbb{Z}$ to $\mathbb{Z}$.
Solution: We can clearly see that h is a function since each input gets paired with an output. We can also see via drawing a graph that the function is injective but not surjective.

Problem 12. Let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(n) = 6n - 5$. Prove that h is injective ("one to one") and surjective ("onto").

Proof. We are given that $n \in \mathbb{R}$ and $(n, a) \in h$. We can write h more formally as

$$h = \{n \in \mathbb{R} \mid (n, 6n - 5)\}. \tag{7.1}$$

Assume $r \in \mathbb{R}$ and let $n = \frac{r+5}{6}$. Then,

$$h(n) = 6\left(\frac{r+5}{6}\right) - 5 = r + 5 - 5 = r. \tag{7.2}$$

Thus, for any $r \in \mathbb{R}$, there is $n \in \mathbb{R}$ so that $h(n) = r$, making h surjective. Now, we must prove that h is also injective. Let $x_1, x_2 \in \mathbb{R}$ and assume $h(x_1) = h(x_2)$ by the definition of injective functions. Attempt to complete the rest of this proof. □

Problem 13. Let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(n) = 6n - 5$. What is h^{-1} and is it a function? *Solution:* Let $k = 6n - 5$, meaning $h(n) = k$. We now solve for n in terms of k,

$$k = 6n - 5 \implies 6n = k + 5 \implies n = \frac{k+5}{6}. \tag{7.3}$$

So, if we rephrase our inverse function back in terms of our original variables, $h^{-1}(n) = \frac{n+5}{6}$ which we can write as

$$h^{-1} = \{(6n - 5, n) \mid n \in \mathbb{R}\} = \left\{\left(n, \frac{n+5}{6}\right) \,\middle|\, n \in \mathbb{R}\right\} \tag{7.4}$$

for fun I guess? So yes, h^{-1} is indeed a function.

8. Proofs by Induction

The *Principle of Mathematical Induction* states that to prove a statement in the form $\forall n \in \mathbb{N} P(n)$, it suffices to prove the following two statements:

1. $P(0)$
2. $\forall n \in \mathbb{N}(P(n) \to P(n+1))$.

Likewise, for proving the statement of form $\forall n \in \mathbb{Z}^+ P(n)$, or a statement of the form $\forall n \in \mathbb{N}$ such that $n \geq n_0 P(n)$.

Proposition 8.1 (Well-Ordering Principle of $\mathbb{N}$)**.** *Any non-empty subset of* $\mathbb{N}$ *has a least element (in the standard* $\leq$ *order on* $\mathbb{N}$*).*

Some other examples of sets that are well-ordered is $\mathbb{Z}^+$, where the least element is 1. We also sets that are not well-ordered such as $\mathbb{R}$ or $\leq$.

Example 8.1 (Proof by Induction)**.** Show that for any $n \in \mathbb{N}$,

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{8.1}$$

Proof. To prove that our equality holds by induction, we will consider the following base case $n = 0$ where $0 + \cdots + n = 0$. We now plug n into the right side of the equation,

$$\frac{n(n+1)}{2} = \frac{0(1)}{2} = 0. \tag{8.2}$$

Thus, $0 + \cdots + n = \frac{n(n+1)}{2}$ for $n = 0$. We can now move forward with our inductive step. Let $n \in \mathbb{N}$ and assume (8.1) is true. We are going to prove that

$$0 + 1 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2} \tag{8.3}$$

is also true. In fact, we can rewrite the previous equation as

$$\begin{aligned}
[0 + 1 + \cdots + n] + (n+1) &= \left[\frac{n(n+1)}{2}\right] + (n+1) && (8.4)\\
&= \frac{n(n+1) + 2(n+1)}{2} && (8.5)\\
&= \frac{(n+1)(n+2)}{2} && (8.6)\\
&= \frac{(n+1)((n+1)+1)}{2} && (8.7)
\end{aligned}$$

which is in the form of $\frac{n(n+1)}{2}$ with $n = n+1$. Thus, by the principle of mathematical induction, for all $n \in \mathbb{N}$,

$$0 + 1 + \cdots + n = \frac{n(n+1)}{2}. \tag{8.8}$$

□

Remark 8.1. For the previous example, we are able to use $\sum_{k=0}^{n}$ instead of $0 + 1 + \cdots + n$.

Example 8.2. Prove by induction that for all $n \geq 10, 2^n > n^3$.

Proof. Let our base case be $n = 10$. Then, $2^n = 2^{10} = 1024$ and $n^3 = 1000$. We will now proceed with our inductive step. Let $n \in \mathbb{N}$ such that $n \geq 10$ and assume $2^n > n^3$. Now, we will show

$$2^{n+1} > (n+1)^3 \implies 2^{n+1} = 2 \cdot 2^n > (n+1)^3 = n^3 + \underbrace{3n^2 + 3n + 1}_{\leq n^3}. \tag{8.9}$$

For the polynomial $3n^2 + 3n + 1$ where $n \geq 10$, we must show

$$3n^2 + 3n + 1 \leq 3n^2 + 3n^2 + n^2 = 7n^2 \leq 10n^2 \leq n \cdot n^2 = n^3. \tag{8.10}$$

To restate our work in a cleaner way,

$$2^{n+1} = 2 \cdot 2^n > 2n^3 \tag{8.11}$$

$$= n^3 + n^3. \tag{8.12}$$

So, we have

$$n^3 + n^3 \geq n^3 + (3n^2 + 3n + 1) \tag{8.13}$$

$$= (n+1)^3. \tag{8.14}$$

Therefore, $n^{n+1} > (n+1)^3$ and $2^n > n^3$ is true for all $n \geq 10$ by proof by induction. □

Problem 14. Assume a chocolate consists of n squares arranged in a rectangular pattern. The bar, and any smaller rectangular pieces of the bar can be broken along a vertical or horizontal line separating the squares. Assuming that only one piece can be broken at a time, determine how many breaks you must successively make to break the bar into n separate squares.

Consider the following examples where $B(n)$ is how many breaks it takes,

$$B(1) = 0,\ B(2) = 1,\ B(3) = 2,\ B(4) = 3. \tag{8.15}$$

As we can see, $B(n) = n - 1$ for any $n \in \mathbb{Z}^+$. Now, we can start our proof.

Proof. Consider the base case $n = 1$ where $B(1) = 1 - 1 = 0$. Now, let $n \in \mathbb{Z}^+$ and assume for any $1 \leq k < n$ we can break a bar of k squares using $k - 1$ breaks. Take the rectangular bar of n squares and break it once into two rectangular pieces of sizes k and $n - k$ respectively. Since $1 \leq k < n$ and $1 \leq n - k < n$, our inductive hypothesis tells us that this statement applies to both pieces. To break a piece of size k, it takes $k - 1$ breaks, and for the other piece, it takes $n - k - 1$ breaks. So in total, we do

$$1 + (k - 1) + (n - k - 1) = n - 1 \tag{8.16}$$

breaks we must successively make to break the bar into n separate squares. □

Definition 8.1 (Recursively Defined Set)**.** There are some sets that are *recursively* defined. For example, if we define a set X by giving some "base" examples of elements, and then giving rules to generate further examples, and define X to contain no elements except that get into X by these rules, we call that a recursive definition of the set X.

Remark 8.2. An important part of this definition is that X is the $\subseteq$-smallest set that follows the given rules.

Example 8.3. Define the set $S \subseteq \mathbb{Z} \times \mathbb{Z}$ by

- $(3, 5) \in S$
- If $(x, y) \in S$ then $(x + 2, y) \in S$
- If $(x, y) \in S$ then $(-x, y) \in S$
- If $(x, y) \in S$ then $(y, x) \in S$

Prove that both coordinates are odd for any elements of $p \in S$.

To show that the statement $P(z)$ is true for every element z of a recursively defined set X:

i. Show $P(z)$ is true for all elements z in the base case.

ii. For each recursive step rule, show that if $P(z)$ is true for the "input" elements in the rule, then $P(z)$ is true of the resulting "new" elements of X as well. We say that property P is *preserved* by these rules.

Proof. We can begin our inductive step and assume $(x, y) \in S$, and x, y are both odd. Since x is odd, $x = 2k + 1$ for some $k \in \mathbb{Z}$ so

$$x + 2 = 2k + 1 + 2 = 2(k + 1) + 1 \tag{8.17}$$

which is also odd. So, both coordinates of $(x + z, y)$ are odd. Next, since

$$-x = -(2k + 1) = -2k - 1 + 1 - 1 = 2(-k - 1) + 1 \tag{8.18}$$

and $-k - 1 \in \mathbb{Z}$ so $-x$ is odd. Thus, both coordinates of $(-x, y)$ are odd. Lastly, both coordinates of (y, x) are odd. So, for every $p \in S$, both coordinates are odd. □

9. Cardinality of a Set

We will be revisiting sets to discuss their size. Sounds pretty simple but there is more to discuss than one might think. We will use these ideas to later discuss properties of infinity and infinite sets. We will begin with this motivating example.

Consider the sets $A = \{a, b, c, d\}$ and $I_4 = \{1, 2, 3, 4\}$. It should be obvious that both sets have 4 elements. However, what tells us that they have the name number of elements? Well, we *could* form a bijection in which we construct a function that is both injective and surjective and map each element of A to an element of I_4.

Definition 9.1 (Equinumerous)**.** A set is considered to be equinumerous if and only if there exists a bijection from the sets A to B, making them sets of the same size. If A and B are equinumerous, $A \sim B$.

Example 9.1 (Equinumerous Infinite Sets)**.** We will show that the sets $\mathbb{Z}$ and $\mathbb{Z}^+$ are equinumerous. From the set $\mathbb{Z}^+$, we will match each odd integer with a positive integer from $\mathbb{Z}$ and each even integer from $\mathbb{Z}^+$ to a negative integer from $\mathbb{Z}$. We can describe this function as

$$f(n) = \begin{cases} -\frac{n}{2}, & n \equiv 0 \pmod 2 \\ \frac{n-1}{2}, & n \not\equiv 0 \pmod 2 \end{cases} \tag{9.1}$$

where $f : \mathbb{Z}^+ \to \mathbb{Z}$. This may be a sketchy example / proof but it might make sense later.

Definition 9.2 ("Identity Set")**.** For $n \in \mathbb{N}$, we define $I_n = \{k \in \mathbb{Z}^+ \mid k \leq n\}$.

Definition 9.3 (Finite)**.** A set A is finite if $A \neq \emptyset$ or there is $n \in \mathbb{Z}^+$ such that $A \sim I_n$.

Definition 9.4 (Denumerable)**.** The set A is denumerable if $\mathbb{Z}^+ \sim B$, meaning it is *countably infinite*.

Definition 9.5 (Countable)**.** A set A is countable if it is finite or denumerable.

Definition 9.6 (Uncountable)**.** The set A is not countable (not finite and not denumerable).

An interesting idea that stems from this is that we can actually prove by induction, that for some $n \in \mathbb{Z}$ where $n = |B|$, for any finite set B, if $A \subset B$, then $A \not\sim B$. We might end up proving this later.

Theorem 9.1. *Suppose that $A \sim B$ and $C \sim D$. Then, the following hold:*

(1) $A \times C \sim B \times D$

(2) If $A \cap C = \emptyset$ and $B \cap D = \emptyset$ then $A \cup C \sim B \cup D$.

Say $A = \{u, v\}, B = \{1, 2\}, C = \{w, x, y\}$, and $D = \{4, 5, 6\}$. Then, it must be that $A \sim B$ and $C \sim D$...

Following from the previous theorem, what do we know about $\mathbb{Z}^+ \times \mathbb{Z}^+$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}^+$? First, consider $\mathbb{Z}^+ \times \mathbb{Z}^+$ defined via

$$\mathbb{Z}^+ \times \mathbb{Z}^+ = \{(m, n) \mid m, n \in \mathbb{Z}^+\} \tag{9.2}$$

which is denumerable. Actually, to show that $\mathbb{Q}$ is denumerable, we can define a function

$$f : \mathbb{Z} \times \mathbb{Z}^+ \to \mathbb{Q},\ f((m, n)) = \frac{m}{n}. \tag{9.3}$$

This function is well-defined and we can also say that for some arbitrary $q \in \mathbb{Q}$, we can write that $q = \frac{m}{n}$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

Theorem 9.2. *For any arbitrary set A, the following statements are equivalent:*

(1) A is a countable set.

(2) $A = \emptyset$ or there exists a surjective function $f : \mathbb{Z}^+ \to A$.

(3) There exists an injective function $g : A \to \mathbb{Z}^+$.

Proof. This justification will have two parts showing why each statement is equivalent to each other.

(1) $\iff$ *(2).* Assume A is countable, finite set. If $A = \emptyset$, then $A = \emptyset$ or there exists a surjective $f : \mathbb{Z}^+ \to A$. If $A \neq \emptyset$ there is $n \in \mathbb{Z}^+$ such that $A \sim I_n$ where $I_n = \{1, 2, 3, \ldots, n\}$. There is a bijection $h : I_n \to A$ defined via

$$\hat{h}(k) = \begin{cases} h(k), & 1 \leq k \leq n \\ h(n), & k \geq n+1 \end{cases}. \tag{9.4}$$

Therefore, $\hat{h}$ is surjective. Now, we assume that A is countable and infinite. By definition, this must mean that A is denumerable, so there is a bijection $f : \mathbb{Z}^+ \to A$. Therefore, f is surjective. Thus, we have shown that statements *(1)* and *(2)* are equivalent.

(2) $\iff$ *(3).* Assume $A = \emptyset$ or there exists a surjective function $f : \mathbb{Z}^+ \to A$. If $A = \emptyset$, then $\emptyset : \emptyset \to Z^+$ (we have not discussed the empty function in detail but imagine we have). Now, if $A \neq \emptyset$, we define a function g where

$$g(b) = \min\{k \in \mathbb{Z}^+ \mid f(k) = b\}. \tag{9.5}$$

The function g is injective since f is a function. Therefore, *(2)* and *(3)* are equivalent. □

Proposition 9.1. *A union of a countable family of countable sets is countable.*

Proposition 9.2. *The set of real numbers* $\mathbb{R}$ *is uncountable.*

Proof. We will not really do this proof, but this is shown by *Cantor's diagonal argument.* □

Proposition 9.3. *The subset* $(0, 1) \subseteq \mathbb{R}$ *is uncountable.*

Proposition 9.4. *The set of irrational numbers,* $\mathbb{R} \setminus \mathbb{Q}$*, is uncountable since* $\mathbb{R}$ *is not a countable set.*