Contents

Preface

It is, I think, safe to assume that everyone who has dealt with math at an undergraduate level to some capacity knows some naive set theory, and knows how to work with sets at some level, for example I suppose that the reader of this blog will not protest if I were to define a *set* A as $A = \{x \in \mathbb{N} | x \text{ is odd}\}$, and then say that A is the set of odd natural numbers. The reader is probably familiar with function notations $f : A \to B$, which states that f maps elements from the set A (the domain) to the set B (the co-domain), and with the notion of union and intersection of sets. I have even explicitly presented some elementary definitions in naive set theory in Graph Theory Part 1. And yet, I have not yet properly stretched the importance of set theory (formal and naive) as the *foundation* of all of math, on top of which we model theories such as number theory, group theory, etc. The goal of this entry is to provide an introduction to formal set theory and show how we can construct familiar mathematical objects only from formal set theory. As such, our goal in this entry is to construct the real line from first principles.

This entry serves as a semi-follow-up to my writings in Introduction to Mathematical Logic, and as such assumes familiarity with formal logic, but someone unfamiliar with formal logic can still follow along for the most part. Since I am unsatisfied with my writings on set theory in Graph Theory Part 1, I will not assume familiarity with any of the definitions and results from that entry.

This discussion is based on the first half of Math 135 by Berkley University's Prof. Antonio Montalban.

A Brief History of Set Theory

Formal set theory, as it is studied today, is a one-sorted first-order logic (where "one-sorted" means that we only allow for one domain of discourse in the structure interpreting statements written in the language of first-order logic with the vocabulary of set-theory, which intuitively means that set theory studies *sets* and is not to be interpreted as a theory that studies other objects). This means that

it is a first-order logic with its own vocabulary and axioms, and all of set theory is built upon those axioms (with definitions being, for the most part, just shorthands for WFFs in the first-order language). However, the roots of set theory are not in such formalism, but rather in a more informal setting, which to this day is still widely beneficial (while keeping in mind formal set theory). Due to this duality, it is useful to learn about the history of set theory.

Set theory finds its roots in Cantor's writings at the end of the 19th century, in his 1874 paper "Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen" ("On a Property of the Collection of All Real Algebraic Numbers"), where, to prove that there exists more than one kind of infinity (e.g. there is an infinite amount of natural numbers and of real numbers, however there are more real numbers than natural numbers) and to prove properties on these transfinite ("beyond" finite, for our purposes it is synonymous for infinite) quantities, Cantor came up with set theory. Set theory, then, was created as a mathematical tool for defining and analyzing infinite "collections", which in set theory are infinite sets. The key set theoretic developments in his paper (outside of the obvious introduction of set theory) that he used to deal with infinite sets are *cardinal numbers*, which measures the number of elements in a set and can also measure the size of infinite sets, and *ordinal numbers* that lets one enumerate infinite sets even after one has reached a type of infinity.

Cantor's work was criticized by mathematicians and philosophers alike due to his (rarely precedented) discussion of infinity and due to a lack of formalism in the foundations of set theory itself. Set theory, at that time, was expressed using natural, informal language. We call such formulation *naive set theory*. For example, a set would be described as "a collection of objects", and one could define a set via a membership set as "the set of all algebraic numbers greater than the number 2". This definition led to many paradoxes, most famous of which are Russell's paradox, which argues the following:

1. Let B be the set of all sets that are not members of themselves (i.e. $B = \{A | A \notin A\}$)
2. Suppose $B \notin B$, then B is a set which is not a member of itself, but then by definition of B as the set of all sets which are not members of themselves, then $B \in B$, a contradicition.
3. Suppose $B \in B$, then B is a member of itself, so by definition it is not in B, so $B \notin B$, a contradiction.

Russell's paradox is often worded as the *barber paradox* - in a town with one barber who shaves all the people who don't shave themselves, does the barber shave himself?

Russell's paradox shows that set theory, defined informally, is *inconsistent*, and as we have shown in our discussion of formal logic an inconsistent theory is subject to the principle of explosion - anything can be proven from such theory. Clearly, this is a problem that needs to be addressed if we still wish to use set theory.

The paradox can still be resolved within naive set theory - we simply prohibit sets from being members of themselves, which motivates the idea of a *hierarchy* of sets. While this does solve Russell's paradox, it is still easy to construct similar contradictions in naive set theory. Consider the following argument:

1. Let A be the set of all numbers which can be described in over 15 words in the English language, i.e. $A = \{x | x \text{ is described using over } 15 \text{ words}\}$.
2. N is the least natural number that can't be described in under 15 words.
3. $N \in A$ by definition of N, A
4. N is described using 14 words (in 2)
5. $N \notin A$ by definition of A

Which again shows that naive set theory is inconsistent, and removing these type of paradoxes from our language is trickier than removing Russell's paradox - we need to restrict the *language* we used to define sets, and those familiar with formal languages should be able to see where this is headed.

Finally, the assertion of the *existence* of some sets also led to discourse, mathematical and philosophical alike. As an example, consider Platonism, which is a philosophical view that asserts that mathematical objects (and any other object or "form" or "idea") are representation of some *objective, timeless* object - this is the key idea behind the theory of forms, which is central to Platonism. What, then, justifies the existence of the *empty set*, a set with no elements? And on a purely mathematical standpoint, what justifies taking the set of all real numbers?

These issues in naive set theory, as well as other issues in mathematics which bothered mathematicians in the early 20th century, motivated David Hilbert to suggest his program in the early 1920s to solve this crisis. The goal of Hilbert's program was to provide secure, formal foundations for all of mathematics. Namely, the goal was to provide a theory expressed in *formal language* which would be *complete, consistent* and *decidable*, and which would preserve all results in math that appeal to informal ideas, such as those involving Cantor's uncountable sets.

Hilbert's program received a massive blow in the form of Godel's incompleteness theorems in 1931, which led Hilbert to relax the goals of his program - instead of providing a singular theory for all of math, a singular theory for all of math that is actually used by mathematicians would be desired, and weaker forms of completeness, consistency and decidability would be required.

Over a decade before Hilbert suggested his program, mathematicians attempted to formulate set theory as a first-order theory in an attempt to solve the paradoxes described earlier in this section. Among these attempts was Ernst Zermelo and Abraham Fraenkel's axiomatization of set theory, which is known today as ZF set theory, which together with the axiom of choice forms ZFC set theory. It can be shown that ZFC provides a strong foundation virtually all of mathematics, and so it is a reasonable answer to Hilbert's program, and indeed ZFC is, formally, used as the foundation of mathematics today, alongside mathematical logic which provides a foundation for ZFC to operate in. The axiom of choice and equivalent statements of it the cause for contention among mathematicians, which we may discuss at a different time. Other constructions, such as *type theory*, do exist, but such constructions are outside the scope of this discussion.

While naive set theory (i.e. set theory described using natural language) is inconsistent, it is still widely

used by mathematicians to this day due to it being much easier to use and much less error prone (when used by humans) than ZFC. Naive set theory, as it is used today, is an informal description of ZFC. As such, it is customary to explicitly reference an axiom that is not considered trivial, so the axiom of choice is often explicitly referenced when used.

It is important to stretch that this is by no means close to a complete account of meaningful events in the development of set theory, but it should provide enough motivation for us to start our discussion of set theory with a brief overview of naive set theory followed by an introduction of the ZFC axioms, now that we are properly motivated that such axiomatization is necessary.

Naive Set Theory

DEFINITION 0.1 ⟨**set**⟩

A set is a collection of elements and may not contain itself.

Note that this definition, while intuitive, is not particularly formal - where do these elements come from? And is it the case that every element that is not the set itself can be a member of a set? These will be answered when we introduce ZFC.

DEFINITION 0.2 ⟨**member of a set**⟩

Let A be a set and let x be some element. If A contains x, we say that x is a member *of A, and denote this by $x \in A$ (read: x belongs to A). Otherwise, we say x does not belong to A and denote this by $x \notin A$.*

DEFINITION 0.3 ⟨**equivalence of sets**⟩

Two sets A and B are equal*, denoted by $A = B$, if and only if they contain the same elements, i.e. $\forall x(x \in A \iff x \in B)$.*

We will later formalize this statement as an axiom of ZF, called the *axiom of extensionality*. From this definition, it follows that there are two ways to uniquely define a set:

COROLLARY 0.1 ⟨**set builder notation**⟩

A set A may be uniquely defined by:
1. Specifying all elements of A. For example, $\{1, 2, 3\}$ uniquely defines a set whose members are $1, 2, 3$.
2. Specifying a domain from which elements are taken and a predicate such that elements that satisfy the predicate belong to the set, for example $\{x \in \mathbb{N} | n$ is odd$\}$ uniquely defines the set of all odd natural numbers. We call the predicate a membership test*.*

Proof. Immediate from 0.3 equivalence of sets . When we present ZF, form 2 will be an axiom schema known as the *axiom schema of specification* or the *subset axiom* □

COROLLARY 0.2

Multiplication of elements and order of elements in a set do not matter.

Proof. Let A, B be two sets such that $\forall x(x \in A \iff x \in B)$, then by definition $A = B$. Suppose some elements in B occur multiple times, i.e. B is of the form $\{a, \dots, a, \dots\}$, but since $a \in A \iff a \in B$ by construction, it still follows that $A = B$ by definition, so multiplication of elements doesn't matter. Now suppose the order of elements in the sets is different, but still $\forall x(x \in A \iff x \in B)$, so order doesn't matter as well. □

This result motivates us to ignore multiplicative elements in sets, so when discussing the *elements* of a set we implicitly mean the *unique* elements of the set.

DEFINITION 0.4 ⟨**cardinality of a set**⟩

The cardinality *of a set A is the number of (unique) elements in A, and is denoted $|A|$.*

DEFINITION 0.5 ⟨**empty set**⟩

There exists a set with no elements, denoted $\emptyset$, which is called the empty set*.*

PROPOSITION 1 ⟨**uniqueness of the empty set**⟩

The empty set is unique.

Proof. Immediate from 0.3 equivalence of sets - take any two sets with no elements, then they share the same elements, then they are the same set □

DEFINITION 0.6 ⟨**inclusion**⟩

Let A, B be sets. If $\forall x \in B(x \in A)$, we say that B is included *in A, and call B a* subset *of A and A a* superset *of B. We denote this relation by $B \subseteq A$.*

PROPOSITION 2

$\emptyset \subseteq A$ for every set A.

Proof. Vacuously true by 0.6 inclusion □

PROPOSITION 3 ⟨**mutual inclusion**⟩

$$A \subseteq B \wedge B \subseteq A \iff A = B$$

Proof. $\implies$ By 0.6 inclusion it follows that $\forall x \in B(x \in A)$ and also $\forall x \in A(x \in B)$, so it follows that $\forall x(x \in B \iff x \in A)$, so by definition $A = B$. To prove the other direction, we argue the same in the opposite direction □

DEFINITION 0.7 ⟨**power set**⟩

Let A be a set, then the power set *of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.*

EXAMPLE 0.1 ⟨**power set**⟩

Let $A = \{1, 2\}$, then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

PROPOSITION 4 ⟨**cardinality of the power set**⟩

The power set of A contains exactly $2^{|A|}$ *distinct elements, with $2^0 = 1$ as per the usual definition.*

Proof. We prove by induction on $|A|$. If $|A| = 0$, then $A = \emptyset$ so its only subset is itself, so $\mathcal{P}(A) = \{\emptyset\}$ so $|\mathcal{P}(A)| = 1$. Suppose the theorem holds for sets with cardinality n, and let $|A| = n + 1$, then A without some element x has cardinality n and by the induction hypothesis has 2^n subsets. Now, introduce x to A, then by combinatorical considerations half the subsets of A include x, and the other half do not, so $|A| = 2k$ where k is the number of subsets of A that do not include x, but this is exactly the number of subsets of A without x, so $k = 2^n$, so $|A| = 2^{n+1}$, which completes the proof □

It is not immediately obvious that a power set can always be constructed for a given set. This will be axiomatized in ZF by the axiom of power set.

We also define the following basic operations on sets:

DEFINITION 0.8 ⟨**union**⟩

Let A be a set of sets, then $\cup A$ is defined as the set called the union *of A whose elements are the elements of the elements of A, i.e. $\cup A := \{x | \exists X \in A(x \in X)\}$. We also similarly define the* union *of two sets as $A \cup B = \{x | x \in A \vee x \in B\}$, i.e. the set of all elements of A or B.*

DEFINITION 0.9 ⟨**intersection**⟩

Let A be a set of sets, then $\cap A$ called the intersection *of A is a set whose elements are the shared elements of the elements of A, i.e. $\cap A = \{x | \forall X \in A(x \in X)\}$. The* intersection *of two sets $A \cap B$ is the set of all elements that are in both sets, i.e. $A \cap B = \{x | x \in A \wedge x \in B\}$. If $A \cap B = \emptyset$ we say that A and B are* disjoint*.*

Immediately from the definition of equality of sets, we can show the following:

PROPOSITION 5 ⟨**uniqueness of union and intersection**⟩

$\cup A$ and $\cap A$ are unique, as well as the case where A consists of just two sets as elements.

Another trivial and useful property is

LEMMA 0.1 ⟨**the intersection is a subset of the union**⟩

$$\cap A \subseteq \cup A$$

Proof. Let $x \in \cap A$, then by definition $\forall X \in A(x \in X)$, so $\exists X \in A(x \in X)$, so by definition $x \in \cup A$, so all elements of $\cap A$ are in $\cup A$, so by definition $\cap A \subseteq \cup A$ □

Finally, given A, B s.t. A is a subset of B, we can define the *complement* of A with respect to B as follows:

DEFINITION 0.10 ⟨**complement**⟩

Given sets A, B s.t. $A \subseteq B$, we define the complement *of A with respect to B as the set of all members of B which are not members of A, and denote it via $B \setminus A$ or $\overline{A}$ if B is unambiguous.*

In this overview of the elementary definitions of naive set theory we have pointed multiple times that, since sets are themselves mathematical objects and can be elements of other sets, we should concern ourselves with *where* sets come from. In formal logic, this is the *universe* or *domain of discourse* of set theory (those familiar with formal logic may recall that a domain of discourse is associated to a *structure* of a first-order (or higher-order) logic and not to the theory itself, however as we have briefly mentioned in the beginning of the post, set theory is a *one-sorted logic*, i.e. it has only one intended domain of discourse, so discussing the universe of sets is well-defined). Formal set theory provides a framework for constructing this universe from axioms, without any elements foreign to set theory.

Zermelo-Fraenkel Set Theory

DEFINITION 0.1 ⟨**language of ZF set theory**⟩

The formal language of ZF set theory is a first-order language with equality*, whose vocabulary* π *consists of only one symbol:* $\pi = \{\in\}$*, where* $\in$ *is a relation symbol.*

Of note here is the absence of the empty set and of the inclusion relation from the vocabulary, both of which we defined above. We build these as extensions by definitions in the formal language or from axioms. For example:

DEFINITION 0.2 ⟨**inclusion**⟩

We define inclusion in the formal language as the WFF $\forall x(x \in A \implies x \in B)$*, and denote it by* $A \subseteq B$*.*

DEFINITION 0.3 ⟨**not contained**⟩

We use $A \notin B$ *as a shorthand for* $\neg(A \in B)$*.*

DEFINITION 0.4 ⟨**universe of ZF**⟩

ZF set theory is a one-sorted logic, and as such its domain is always the universe of sets*.*

First Axioms

The axioms of ZF set theory provide the foundations upon which we can build all of mathematics. The exact wording of the axioms differs from writer to writer, but all formulations of the axioms are equivalent. *ZFC* refers to a system which has both the ZF axioms and the axioms of choice (hence *C*) as

axioms. It can be shown that ZF and C are independent of each other, so the distinction is important. We will present the axiom of choice at a later point.

Recall that the axioms are expressed in the formal language of set theory, so quantifiers quantify over the universe of sets. We will show that, using these axioms, we can arrive at the results and definitions from our brief discussion of naive set theory.

DEFINITION 0.5 ⟨**axiom of extensionality (ZF1)**⟩

$$\forall A \forall B (\forall x (x \in A \iff x \in B)) \implies A = B)$$

Observe that this axiom is simply 0.3 equivalence of sets expressed as a logical axiom: two sets are equal if they have the same elements. In fact, we can immediately prove the following expected result:

LEMMA 0.2 ⟨**equivalence of sets in ZF**⟩

Two sets are equivalent if and only if *they share the same elements.*

Proof. $\implies$ is simply 0.5 axiom of extensionality (ZF1) . $\impliedby$ We wish to show $\forall A \forall B (A = B \implies \forall x (x \in A \iff x \in B))$. We show this using results from mathematical logic:

1. $A = B \implies (\forall x (x \in A \iff x \in A) \implies \forall x (x \in A \iff x \in B))$ ($E3$, i.e. equality susbtitution axiom for formulas)
2. $\forall x (x \in A \iff x \in A)$ (tautology, so deducible by rule T)
3. $A = B \implies \forall x (x \in A \iff x \in B)$ (tautologically implied by $1, 2$)
4. $\forall A \forall B (A = B \implies \forall x (x \in A \iff x \in B))$ (by generalization lemma)

□

Using this axiom (and the regular axioms of a FOL deductive system) and the formal definition of inclusion, we can prove 3 mutual inclusion formally. This is left as an exercise.

DEFINITION 0.6 ⟨**axiom of empty set (ZF2)**⟩

$$\exists B \forall x (x \notin B)$$

This axiom asserts the existence of the empty set, which we denote by $\emptyset$ as an extension to our language. It should be noted that the existence of an empty set is not always taken as an axiom. As we will soon see, there exists another axiom which asserts the existence of subsets of a given set, and (as one would

expect from naive set theory) since every set has the empty set as a subset, we can use that axiom to prove $\exists B \forall x (x \notin B)$, however that argument only applies if we suppose that there are sets, i.e. the universe of sets is not empty. While this can be argued, either via the axiom of infinity which we will soon present which asserts that there exists an infinite set, or by taking the existence of some set as an axiom, we choose to follow the school which explicitly asserts the axiom of empty set as a part of the ZF axioms.

From 0.5 axiom of extensionality (ZF1) and 0.6 axiom of empty set (ZF2) , it can be shown that the empty set is unique. The proof looks much like 1 uniqueness of the empty set, only expressed as a formal proof.

DEFINITION 0.7 ⟨**axiom of pairing (ZF3)**⟩

$$\forall A \forall B \exists C (\forall x (x \in C \iff ((x = A) \vee (x = B)))$$

Informally, this axiom states that for every two sets A, B, there exists a set C which has A, B as its only elements, i.e. $C = \{A, B\}$ (hence "pairing"). It is trivial to show formally that such C is unique: take two witnesses C_1, C_2 that satisfy this axioms for some instantiation of A, B in $ZF3$, then
1. $\forall x (x \in C_1 \iff ((x = A) \vee (x = B))$ (hypothesis)
2. $\forall x (x \in C_2 \iff ((x = A) \vee (x = B))$ (hypothesis)
3. $\forall x (x \in C_1 \iff x \in C_2)$ (tautologically implied by $1, 2$ since $(A \iff B) \wedge (C \iff B)$ tautologically implies $A \iff C$ so deducible by rule T)
4. $\forall x (x \in C_1 \iff x \in C_2) \implies C_1 = C_2$ (instantiation of axiom of extensionality with $A = C_1, B = C_3$)
5. $C_1 = C_2$ (MP)

DEFINITION 0.8 ⟨**axiom of union (ZF4)**⟩

$$\forall A \exists B (\forall x (x \in B \iff (\exists C (C \in A \wedge x \in C))))$$

Informally, the axiom states that for every set A, its union $\cup A$ exists, i.e. there exists some set B whose elements are exactly the elements of the elements of A. This is exactly 0.8 union, so we denote such B as $\cup A$.

From this definition and the axiom of pairing, we can retrieve the definition of the union of two sets:

COROLLARY 0.3 ⟨**union of two sets**⟩

Let A, B be sets, then their union as defined in 0.8 union exists.

Proof. By $ZF3$ (the pairing axiom) there exists a set whose elements are A, B, i.e. $\exists C$ such that $C = \{A, B\}$, then by $ZF4$ (union axiom) there exists a set D whose elements are the elements of elements C, i.e. the elements of A, B, so it follows that $\forall x(x \in C \iff (x \in A \vee x \in B))$, so C corresponds to $A \cup B$ as previously defined □

DEFINITION 0.9 ⟨**axiom schema of specification (ZF5)**⟩

$$\exists B \forall x(x \in B \iff (x \in A \wedge \varphi(x)))$$

Note that this is an axiom schema*: all free variables, including the WFF $\varphi(x)$ (which is a WFF formula with x as its free variable) can be replaced in an* instantiation*.*
This axiom schema is also known as the subset axiom schema*.*

Informally, the axiom schema states that for every set A, we can define a *subset* B of A (and we denote this relation by $B \subseteq A$) based on a well-formed condition (i.e., that x satisfies the formula $\varphi(x)$).

EXAMPLE 0.2 ⟨**subsets using schema of specification**⟩

Suppose we have a set of the natural numbers $\mathbb{N}$ (we have not yet formally constructed the natural numbers within set theory so this is an appeal to the informal notion of the set of natural numbers).
We extend the vocabulary of set theory with a unary relation symbol IsOdd and interpret it as true if and only if its argument is odd (it is not necessary to extend our vocabulary with this relation symbol, we do this to avoid defining parity in terms of equivalence classes, which we have not yet introduced in this formalism of set theory). Then IsOdd(x) is a WFF, so by the axiom schema of specification, there exists a set B whose elements are all the elements of $\mathbb{N}$ that satisfy IsOdd, which corresponds to our naive notion of "the set of odd natural numbers".

Now we can consider Russell's paradox within ZF set theory: Russell's paradox works by taking a set B such that $B = \{x | x \notin x\}$. $x \notin x$ is, of course, a WFF, but by the axiom schema of specification, sets *cannot* be constructed that way - we need to take x from some superset A. Russell's paradox works by specifying A as the set of all sets, let's call it the universal set. Note that its existence is *not* guaranteed by any of the ZF axioms we have shown so far, and will not be guaranteed by any other axioms, including the axiom of choice. But, suppose A exists and is a set, i.e. we add $\exists A(\forall x(x \in A))$ to our theory, then:

1. $\exists A(\forall x(x \in A))$ (hypothesis)
2. $\exists B \forall x(x \in B \iff (x \in A \wedge x \notin x))$ (instantiation of $ZF5$)

3. $B \in B \iff (B \in A \wedge B \notin B)$ (instantiation of 2 with $x = B$)
4. $B \in B \iff B \notin B$ (By 1 we know that $B \in A$ is always satisfied so 3 tautologically implies 4)
5. $B \in B \iff B \in B$ (tautology)

A contradiction, which means

PROPOSITION 6 ⟨**the universe is not a set**⟩

The more nuanced paradoxes we have shown, cannot be translated to WFFs, so they are also do not apply to our formal treatment of set theory.

DEFINITION 0.10 ⟨**set builder notation in ZF**⟩

Since a set can be uniquely described by its elements (by 0.5 axiom of extensionality (ZF1)), and since we can uniquely describe subsets using the axiom schema of specification via a condition on the element of the superset, we can introduce the set builder notation as a shorthand for declaring sets. Set builder notation use $\{,\}$ to describe the set either by explicitly listing all its elements (for example, $\emptyset$, the set with no elements, is simply $\{\}$), or by specifying a membership test on the elements of a superset A, as follows: $\{x \in A | \textit{predicate}(x)\}$. We will use this notation as shorthand in the future.

Using the schema of specification, we can prove that the *intersection* of a set of sets, i.e. $\cap A$, as defined in 0.9 intersection , exists:

PROPOSITION 7 ⟨**intersection exists**⟩

Let A be a set, then there exists a set B that is the intersection of A as defined in 0.9 intersection, i.e.

$$\exists B(x \in B \iff (\forall a \in A(x \in a)))$$

And for any two sets A, C, there exists a set D such that D is the intersection of A, C, i.e. $D = A \cap C$.

Proof. Let A be a set, and consider the formula $\forall a \in A(x \in a)$, which is a WFF with x free, denote it $\varphi(x)$. Now, consider $\cup A$ which exists by 0.8 axiom of union (ZF4). By the axiom schema of specification, $\exists B \forall x(x \in B \iff (x \in \cup A \wedge \varphi(x)))$, then B is in exact correspondence to our definition of the intersection of a set $\cap A$. Given two sets A, C, we first used the axiom of pairing to produce a set whose elements are A, C, then use the same argument as above to produce $A \cap C$ □

DEFINITION 0.11 ⟨**axiom of power set (ZF6)**⟩

$$\forall A \exists B \forall x (x \in B \iff x \subseteq A)$$

Where $\subseteq$ is the shorthand defined in 0.2 inclusion .

Informally, the axiom asserts the existence of the power set $\mathcal{P}(A)$, since it states that for every set A there exists a set B whose members are exactly the subsets of A.

EXAMPLE 0.3 ⟨**power set and set builder notation**⟩

By 0.6 axiom of empty set (ZF2), we know that a set with no elements exists. We denoted this set by $\emptyset$, and using set builder notation identified it with $\{\}$. Now, by 0.11 axiom of power set (ZF6), the power set of the empty set also exists, which is just $\{\{\}\}$, or $\{\emptyset\}$. Taking it a step further, by 0.7 axiom of pairing (ZF3), there exists a set whose elements are $\emptyset, \{\emptyset\}$, which in set builder notation is $\{\{\}, \{\{\}\}\}$.

In fact, we make a stronger claim

LEMMA 0.3 ⟨**expressive power of set builder notation**⟩

Using set builder notation, we can construct all sets which are constructible by all ZF axioms presented so far (i.e. ZF1-6).

Proof. We prove by induction on the number of elements of the set, $|A|$. First, if $|A| = 0$ then by existence and uniqueness of the empty set, $A = \emptyset$ so $A = \{\}$. Suppose $n0$, then either:
1. A is constructed using the union axiom, so it is the union of two sets each with less than n elements so by the induction hypothesis they are expressible using set builder notation, then A is simply $\{s_1, s_2\}$ where s_1, s_2 is the concatenation of the elements of those sets expressed in set builder notation (with the outermost brackets omitted).
2. A is constructed using the power set axiom, so a similar argument applies since for every set B, $|\mathcal{P}(B)| = 2^{|B|}|B|$.
3. A is constructed using the axiom of pairing, so similarly A can be represented as $\{S_1, S_2\}$ where S_1, S_2 is the set builder notation representation of the sets paired to create A.
4. A is constructed using the axiom schema of specification, then $A = \{x \in B | \text{predicate}(B)\}$ for some B and some predicate, which we have defined as a valid set builder notation for A.

□

We will introduce 3 more axioms, not including the axiom of choice, at later points to assist us in our construction of fundamental mathematical objects such as functions and the natural numbers. For now, we will use these six axioms to begin our formal construction of mathematical objects within set theory.

Functions and Relations

The reader should be familiar with the notion $f : A \to B, x \mapsto f(x)$ to define functions. We read this as follows: A is the domain of f, B is the co-domain of f, and that f takes $x \in A$ to $f(x)$. We say that the *graph* of a function is given by the *set* of *ordered pairs* $\langle x, f(x)\rangle$ for all $x \in A$, and we *plot* the graph of a function in a *cartesian* coordinate system when feasible to gain a better understanding of the function.

All of these objects, with the exception of the domain and co-domain A and B which are sets, are foreign to formal set theory. For example, an ordered pair, while similar to a a set, is not a set since order *matters*: $\langle x, f(x)\rangle \neq \langle f(x), x\rangle$, while $\{x, f(x)\} = \{f(x), x\}$. In this section, we will build these objects within formal set theory and formalize the construction of functions and relations within set theory.

Ordered Pairs

DEFINITION 0.1 $\langle$**ordered pair**$\rangle$

An ordered pair *is a pair of objects where order matters, i.e. given two ordered pairs* $\langle x_1, y_1\rangle$ *and* $\langle x_2, y_2\rangle$*, they are* equal *if and only if* $x_1 = x_2$ *and* $y_1 = y_2$*. We denote ordered pairs using angular brackets.*

DEFINITION 0.2 $\langle$**Kuratwoski's ordered pair**$\rangle$

We call the set $\{\{x\}, \{x, y\}\}$ *the* ordered set $\langle x, y\rangle$*.*

PROPOSITION 8

The above definitions are equivalent.

Proof. To show equivalence, we need to show that

$$(\{\{x_1\}, \{x_1, y_1\}\} = \{\{x_2\}, \{x_2, y_2\}\}) \iff (x_1 = x_2 \wedge y_1 = y_2)$$

$\Longleftarrow$ If $x_1 = x_2$ and $y_1 = y_2$ then both sets in the LHS reduce to two sets with the same element so by the axiom of extensionality they are equivalent.

$\Longrightarrow$ Suppose $\{\{x_1\}, \{x_1, y_1\}\} = \{\{x_2\}, \{x_2, y_2\}\}$. Consider the following cases:
1. $x_1 = y_1$, then $\{\{x_1\}, \{x_1, y_1\}\}$ reduces to $\{\{x_1\}, \{x_1\}\} = \{\{x_1\}\}$, so by the equivalent it follows that $\{x_2, y_2\}$ must also have one unique element (otherwise there would be an element of that set that is not in $\{x_1, y_1\}$, contradicting the equality of the sets), then $x_2 = y_2$, so we have $\{\{x_1\}\} = \{\{x_2\}\}$ which is true only if $\{x_1\} = \{x_2\}$ so it follows that $x_1 = x_2$ by the converse of the axiom of extensionality.
2. $x_1 \neq y_1$, then it must be that $\{x_1\} = \{x_2\}$ and $\{x_1, y_1\} = \{x_2, y_2\}$, so $x_1 = x_2$ and $y_1 = y_2$.

□

DEFINITION 0.3 ⟨**cartesian product**⟩

The cartesian product *of two sets A, B, denoted by $A \times B$, is the set of all ordered pairs where the first element is from A and the second elements is from B, i.e.:*

$$A \times B = \{\langle a, b\rangle | a \in A \wedge b \in B\}$$

The cartesian product of a set with itself, i.e. $A \times A$, is often denoted using power notation as A^2, and call it the second cartesian power *of A.*

PROPOSITION 9

The cartesian product $A \times B$ of two sets A, B exists.

Proof. First we note that by 0.3 union of two sets $A \cup B$ exists, and by applying 0.11 axiom of power set (ZF6) twice it follows that $\mathcal{P}(\mathcal{P}(A \cup B))$ exists. Now, consider some ordered pair $\langle a, b\rangle$ such that $a \in A, b \in B$. By definition, it is the set $\{\{a\}, \{a, b\}\}$, which itself is a subset of $\mathcal{P}(\{a, b\})$, but $\{a, b\}$ is a subset of $A \cup B$, so $\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(\{a, b\}) \subseteq \mathcal{P}(A \cup B)$, or that $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Since this applies to every ordered pair from A, B, it follows that $A \times B$ exists. Formally, we can use the axiom schema of specification on the set $\mathcal{P}(\mathcal{P}(A \cup B))$ to assert that

$$\exists B(x \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge (\exists a, b(a \in A \wedge b \in B \wedge (x = \{\{a\}, \{a, b\}\}))))$$

□

n-Tuples

Ordered pairs let us assign meaning to the order in a collection of two elements. It is trivial to generalize this idea to arbitrarily large collections, called n-tuples where n is the number of elements, as follows:

DEFINITION 0.4 ⟨**n-tuple**⟩

An n-tuple $\langle x_1, x_2, \ldots, x_n\rangle$ is a set of n elements where order matters, i.e. two ordered tuples $\langle x_1, \ldots, x_n\rangle$ and $\langle y_1, \ldots, y_n\rangle$ are equal if and only if $x_i = y_i$ for every natural i in $[1, n]$.

DEFINITION 0.5 ⟨**n-tuple in ZF set theory**⟩

An n-tuple is defined as follows:
1. If $n = 2$, then the 2-tuple is an ordered pair as defined in 0.2 Kuratwoski's ordered pair
2. If $n2$, then the n-tuple is $\langle x_1, \ldots, x_n\rangle$ the ordered pair $\langle\langle x_1, \ldots, x_{n-1}\rangle, x_n\rangle$ where $\langle x_1, \ldots, x_{n-1}\rangle$ is an $(n-1)$-tuple.

EXAMPLE 0.4 ⟨**3-tuple**⟩

Consider a 3-tuple $\langle x, y, z\rangle$, then by definition $\langle x, y, z\rangle = \langle\langle x, y\rangle, z\rangle$ which is an ordered pair. Now, $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$ by definition, so $\langle\langle x, y\rangle, z\rangle = \{\langle x, y\rangle, \{\langle x, y\rangle, z\}\}$, which expands to

$$\left\{\left\{\{\{x\}, \{x, y\}\}\right\}, \left\{\{\{x\}, \{x, y\}\}, z\right\}\right\}$$

It is trivial to observe that the set of n-tuples is freely generated so the recursive definition is well-defined, and it can be argued by induction based on 8 that both definitions are equivalent.
Relations

DEFINITION 0.6 ⟨**relation on two sets**⟩

Given two sets A, B, a relation *R from A to B is a subset of the cartesian product $A \times B$, i.e. it is a set of* ordered pairs *with first element from A and second element from B.*

Consider the function $f(x) = x^2$ in $\mathbb{R}$, it is nothing but a relation R where $A = B = \mathbb{R}$ given by the set of ordered pairs $\langle x, x^2\rangle$ with the restriction that given $x \in A$ there *exists* a *unique* ordered pair whose first element is x (we say that f is *well-defined*). We will formalize this idea shortly.

More generally, we can define a relation independent of the cartesian product of two sets as follows

DEFINITION 0.7 ⟨**relation**⟩

A relation R is a set of ordered pairs.

When the ordered pairs are taken from $A \times B$, this reduces to the definition of a relation on two sets.

Relations can also be defined on n-tuples as follows

DEFINITION 0.8 $\langle$**n-ary relation**$\rangle$

A n-ary relation is a set of n tuples.

When $n = 2$, we retrieve the definition for a relation. Such relation is called a *binary* relation.

DEFINITION 0.9 $\langle$**domain, range and field of a relation**$\rangle$

Let R be a relation, then:
1. The domain *of R, denoted domain(R), is given by domain$(R) = \{a|\exists b\langle a, b\rangle \in R\}$*
2. The range *of R, donated range(R), is given by range$(R) = \{b|\exists a\langle a, b\rangle \in R\}$*
3. The field *of R, denoted field(R), is given by field(R) = domain$(R) \cup$ range(R).*
Where a, b in definitions $1, 2$ are taken from field(R) (recall that we need to specify where elements are taken from in formal set theory).

Informally, given a relation, the *domain* is the set of all first elements, the range is the set of all second elements, and the field is the union of the domain and range. Note that given a relation on two sets A, B, it follows that the domain of the relation is R, the range of the relation is B, and the field is $A \cup B$.

The definition for the domain, range and field, as currently presented, is circular - the filed is constructed from the domain and the range, but the domain (and range) are constructed by elements from the field. This issue can be resolved by showing that the field can be constructed without reference to the domain or the range. The following lemma shows such construction:

LEMMA 0.4

The field of a relation R, field(R), is $\cup(\cup R)$.

Proof. Consider an element of R, it is an ordered pair of the form $\langle a, b\rangle$, i.e. $\{a, \{a, b\}\}$, so $\{a, \{a, b\}\} \in R$, which means that $\{a, b\} \in \cup R$ (here we mean that the *set* $\{a, b\}$ is an element of $\cup R$), so $a, b \in \cup\cup R$ (here we mean that the *elements* a, b are elements of $\cup \cup R$), but the domain of R is simply the set of all such a and the range of R is the set of all such b, so the *field* of R is the set of all such a, b, so field$(R) = \cup \cup R$ □

If R is a binary relation, then we usually write aRb as a shorthand for $\langle a, b\rangle \in R$, as is customary with binary opreators.

We define a special relation which will be especially important in the context of functions, the identity relation

DEFINITION 0.10 ⟨**identity**⟩

The identity relation *is a relation where domain*(R) = *range*(R) *and* $\langle x, y\rangle \in R \iff x = y$. *We represent the identity relation by* id_A, *where* A *is the domain of* R.

Equivalence Relations

We classify binary relations based on their properties. We define the following properties:

DEFINITION 0.11 ⟨**properties of a binary relation**⟩

Let R *be a binary relation with field* A, *then:*
1. R *is* reflexive *if* $\forall x \in A(xRx)$
2. R *is* irreflexive *if* $\forall x \in A(\neg xRx)$
3. R *is* symmetric *if* $\forall x, y \in A(xRy \iff yRx)$
4. R *is* assymetric *if* $\forall x, y \in A(xRy \implies \neg yRx)$
5. R *is* antisymmetric *if* $\forall x, y \in A((xRy \wedge yRx) \implies x = y)$ *(as an example, consider inclusion of sets)*
6. R *is* transitive *if* $\forall x, y, z \in A((xRy \wedge yRz) \implies xRz)$
7. R *is* complete *or* connected *if* $\forall x, y \in A(xRy \vee yRx \vee x = y)$
8. R *is* strongly complete *or* strongly connected *or* total *if* R *satisfies* $\forall x, y \in A(xRy \vee yRx)$

DEFINITION 0.12 ⟨**equivalence relation**⟩

A binary relation R *is an* equivalence relation *if it is reflexive, symmetric and transitive.*

DEFINITION 0.13 ⟨**equivalence class**⟩

Let R *be a relation and let* $x \in$ *field*(R), *then the* equivalence class *of* x *under* R, *denoted* $[x]_R$ *is given by*

$$[x]_R = \{y \in \textit{field}(R) | xRy\}$$

Note that while equivalence classes as we have defined here are sets, there are equivalence classes that are collection which are not sets. Such collection are called *proper classes*. We have already seen such proper class - the “set” of all sets.

In our case, $[x]_R$ is still a set, and its existence is guaranteed by the axiom schema of specification and from the existence of field(R).

LEMMA 0.5

$$([x]_R = [y]_R) \iff xRy$$

Proof. $\implies$ Suppose $[x]_R = [y]_R$ and denote the field of R by A. By definition $[x]_R = \{a \in A | xRa\}$ and $[y]_R = \{a \in A | yRa\}$, so if a is a member of both equivalence classes it follows that $xRa \wedge yRa$, and due to the symmetry of the equivalence relation R we have $yRa \implies aRy$, so we have $xRa \wedge aRy$, so due to transitivity xRy. $\impliedby$ Suppose xRy, then similarly for any $a \in A$ such that aRx (i.e. $a \in [x]_R$) it follows aRy, so $a \in [y]_R$, so $[x]_R \subseteq [y]_R$, similarly we find $[y]_R \subseteq [x]_R$, so we conclude that $[x]_R = [y]_R$ □

DEFINITION 0.14 ⟨**partition**⟩

Let A be a set, then a partition *of A is a set Π of subsets of A such that:*
1. $\forall x, y \in \Pi(x \cap y = \emptyset)$, i.e. any two elements of a partition are disjoint.
2. $\cup\Pi = A$, i.e. the union of a partition is the partitioned set.

THEOREM 1 ⟨**partition-equivalence relation duality**⟩

1. Let Π be a partition of a set A, then Π defines an equivalence relation on A given by $R = \{\langle x, y\rangle \in A \times A | \exists \pi \in \Pi(x \in \pi \wedge y \in \pi)\}$
2. Let R be an equivalence relation on A, then R defines a partition on R given by $\Pi = \{[x]_R | x \in A\}$

Proof. 1. Consider the relation as defined in the statement of the theorem, and let $x, y, z \in A$. Consider $\langle x, x\rangle \in A^2$, since Π is a partition of A, $x \in \cup\Pi$, so $\exists \pi \in \Pi$ such that $x \in \pi$, so xRx, i.e. R is reflexive. Now consider $\langle x, y\rangle$: if $\exists \pi \in \Pi$ such that $x \in \pi \wedge y \in \pi$, then obviously the formula $y \in \pi \wedge x \in \pi$ is also satisfied, so $xRy \implies yRx$, similarly $yRx \implies xRy$, thus R is symmetric. Finally, consider $\langle x, y\rangle$ and $\langle y, z\rangle$ - if xRy then it follows that $\exists \pi_1 \in \Pi$ such that $x, y \in \pi_1$, similarly if yRz then it follows that $\exists \pi_2 \in \Pi$ such that $y, z \in \pi_2$, but since Π is a partition then all its elements must be distinct, so if $\pi_1 \neq \pi_2$ it follows that $\pi_1 \cup \pi_2 = \emptyset$, but clearly $y \in \pi_1 \cup \pi_2$, a contradiction, so $\pi_1 = \pi_2$, but then $x, y, z \in \pi$ so in particular $x, z \in \pi$ so $\langle x, z\rangle \in A^2$ is in R, so R is transitive, so R is an equivalence relation.

2. First, we show that given two distinct equivalence classes, they are disjoint: suppose not, then $\exists [x]_R, [y]_R, [x]_R \neq [y]_R$ such that $[x]_R \cup [y]_R \neq \emptyset$, in particular there exists some a such that $a \in [x]_R$ and also $a \in [y]_R$, but then by definition aRx and aRy, so by symmetry and transitivity xRy, so $[x]_R = [y]_R$ by definition, a contradiction, so all equivalence classes are distinct. Now, consider the union of all equivalence classes: since the equivalence relation is symmetric, i.e. $\forall a \in A(aRa)$, it follows that $\forall a \in A \exists [a]_R \in \Pi$ (by definition of an equivalence class), so then $\cup \Pi = A$. In conclusion, Π is a partition of A.

□

DEFINITION 0.15 ⟨**quotient set**⟩

Let R be an equivalence relation on a set A, the the quotient set *on A under R, denoted A/R, is given by $A/R = \{[x]_R | x \in A\}$.*

Note that the quotient set is simply the partition described in part 2 of Theorem 1 partition-equivalence relation duality.

EXAMPLE 1.1 ⟨**modular arithemetics**⟩

Suppose we have the set of natural numbers $\mathbb{N}$, and we have defined addition, subtraction and multiplication on $\mathbb{N}$. Fix some $n \in \mathbb{N}$, then given any $a \in \mathbb{N}$, it can be shown that there exists $m, r \in \mathbb{N}, rn$ such that $a = mn + r$. We define the relation mod(n) as follows: given $a, b \in \mathbb{N}$, we say $a \equiv_{mod(n)} b$ if and only if $r_a = r_b$ (equivalently, if division is defined, we can use the more elegant definition that $a \equiv_{mod(n)} b$ if and only if $(b - a)$ divides n). First, we verify that it is an equivalent relation:

1. $a = a \Rightarrow r_a = r_a \Rightarrow a \equiv_{\mod(n)} a$ *(reflexivity)*
2. $a \equiv_{\mod(n)} b \implies r_a = r_b \implies r_b = r_a \implies b \equiv_{\mod(n)} b$ *(symmetry)*
3. $a \equiv_{mod(n)} b \wedge b \equiv_{mod(n)} c \implies r_a = r_b = r_c \implies r_a = r_c \implies a \equiv_{mod(n)} c$ *(transitivity)*

Thus we conclude that mod(n) is an equivalence relation. We further claim that there are exactly n *distinct equivalence classes of n. This trivially follows from the fact that rn and $r \in \mathbb{N}$ so r takes exactly n distinct values, and since the relation is defined by equivalence of corresponding r terms, it follows that there are exactly n equivalence classes, so the quotient sets can be identified with $A/$mod$(n) = \{[0], [1], \ldots, [n-1]\}$, where $[i]$ is the equivalence class of i, i.e. the set of all natural numbers with term $r = i$.*

Functions

DEFINITION 0.16 ⟨**function**⟩

A function is a relation F such that for every x in the domain of F, there exists a unique y in the range of F such that $\langle x, y\rangle$ is in F. Expressed formally, a function is a relation F which satisfies:

$$\forall x \in \textit{dom}(F) \exists! y \in \textit{range}(F)(\langle x, y\rangle \in F)$$

We write $F : A \to B$ (F is a function from A to B) if $A = \textit{dom}(F)$ and $\textit{range}(F) \subseteq B$, and we call B the co-domain *of F. We use the notation $F(x)$ for $x \in A$ to refer to the value $y \in B$ such that $\langle x, y\rangle \in F$.*

The identity relation is an example of a function.

We define the following properties on functions:

DEFINITION 0.17 ⟨**properties of a function**⟩

Given a function $F : A \to B$, we say F is:
1. surjective *or* onto *if $\textit{range}(F) = B$, i.e. if its range is its co-domain.*
2. injective *or* one-to-one *if $\forall a, b(F(a) = F(b) \implies (a = b))$, i.e. if each element in the range of F uniquely corresponds to an element in the domain of F.*
3. bijective *if it is* injective *and* surjective*.*

We define the following *operations* on *relations*, although we usually associate them with functions, hence why the definitions are presented here.

DEFINITION 0.18 ⟨**inverse**⟩

Given a relation R, we define its inverse R^{-1} *as* $R^{-1} = \{\langle y, x\rangle \in \textit{range}(F) \times \textit{domain}(F) | \langle x, y\rangle \in R\}$

PROPOSITION 10

The inverse is an involution, i.e. $(R^{-1})^{-1} = R$.

Proof. Let R be a relation with range B and domain A, then $R^{-1} = \{\langle y, x\rangle \in B \times A | \langle x, y\rangle \in R\}$, and $(R^{-1})^{-1} = \{\langle x, y\rangle \in A \times B | \langle y, x\rangle \in R^{-1}\}$, which is just R. (if the reader remains unconvinced, the reader can take any pair from R and show that it must also be in $(R^{-1})^{-1}$ and vice versa, and conclude by mutual inclusion that $R = (R^{-1})^{-1}$) □

DEFINITION 0.19 ⟨**restriction**⟩

Given a relation R and a set A, we define its restriction *to A as $R_{|A} = \{\langle x, y\rangle \in R | x \in A\}$*

DEFINITION 0.20 ⟨**image**⟩

Given a relation R and a set A, we define the image *of R under A, denoted $Im_R(A)$ or $R[A]$, as the set $\{y \in range(R) | \exists x \in A(\langle x, y\rangle \in R)\}$.*

Given two relations, we define their *composition* as follows:

DEFINITION 0.21 ⟨**composition**⟩

Given two relations F, G, we define their composition *$F \circ G$ as the set*

$$F \circ G = \{\langle x, z\rangle \in dom(G) \times range(F) | (\exists y(\langle x, y) \in G \wedge (\langle y, z\rangle \in F)\}$$

It is easier to remember the order of operations in a composition by reading the composition $F \circ G$ as F after G. If $F : B \to C$ and $G : A \to B$ are functions, then $F \circ G : A \to C, (F \circ G)(x) = F(G(x))$.

PROPOSITION 11 ⟨**compositon of bijections is a bijection**⟩

Let $f : A \to B$ and $g : B \to C$ by bijective functions, then their composition $g \circ f : A \to C$ is a bijection.

Proof. Let $c \in C$. Since g is bijective, there exists a unique $b \in B$ s.t. $g(b) = c$. Since f is bijective, there exits a unique $a \in A$ for every $b \in B$ s.t. $f(a) = b$, so given $c \in C$ there exists a unique $a \in A$ s.t. $g(f(a)) = c$, so $g \circ f$ is a bijection □

PROPOSITION 12 ⟨**composition with inverse**⟩

Given a relation F with domain A and range B and its inverse F^{-1}, it follows that $F^{-1} \circ F = id_A$

Proof. By definition $F^{-1} = \{\langle y, x\rangle \in B \times A | \langle x, y\rangle \in F\}$, so by definition of composition $F^{-1} \circ F$ is the set of all $\langle x, z\rangle$ such that there exists some $y \in B$ such that $\langle x, y\rangle \in F$ and $\langle y, z\rangle \in F^{-1}$, but since $\langle x, y\rangle \in F$ then it follows that $\langle y, x\rangle \in F^{-1}$, so $z = x$, so $F^{-1} \circ F = \{\langle x, x\rangle | x \in A\} = \text{id}_A$ □

DEFINITION 0.22 ⟨**left inverse**⟩

Given a function $f : A \to B$, we say that a function $g : B \to A$ is a left inverse *of f if $g \circ f = id_A$.*

PROPOSITION 13 ⟨**left inverse-injective equivalence**⟩

Given a function $f : A \to B$ where A is not empty, f has a left inverse if and only if f is injective.

Proof. $\implies$ Suppose f has a left inverse, then $\exists g : B \to A$ such that g is a function and $g \circ f = \text{id}_A$, i.e. $g(f(x)) = x$, which is only possible if g is well-defined (i.e. for every element in its domain it matches a single element in its range), which is only possible if $\forall a, b \in A((f(a) = f(b)) \implies (a = b))$, otherwise for some a, b such that $y = f(a) = f(b)$ and $a \neq b$, g would have two ordered pairs $\langle y, a\rangle$ and $\langle y, b\rangle$, so g would not be a function, so it follows that f is injective.

$\impliedby$ Suppose f is injective, i.e. $\forall a, b \in A((f(a) = f(b) \implies (a = b))$, and take $g = f^{-1}$, which exists as the inverse of a relation, so all that is left is to show that g is a function. Suppose not, i.e. $\exists y \in \text{domain}(f^{-1})(\exists x_1, x_2 \in A((x_1 \neq x_2) \wedge (\langle y, x_1\rangle \in f^{-1} \wedge \langle y, x_2\rangle \in f^{-1})))$, but then by definition of the inverse it follows that both $\langle x_1, y\rangle$ and $\langle x_2, y\rangle$ are in f, so $f(x_1) = f(x_2)$ but $x_1 \neq x_2$, contradicting the fact that f is injective, so g is a left inverse of f since it is a function and $g = f^{-1}$.

□

DEFINITION 0.23 ⟨**right inverse**⟩

Given a function $f : A \to B$, we say that a function $g : B \to A$ is a left inverse *of f if $f \circ g = id_B$.*

PROPOSITION 14 ⟨**right inverse implies surjectivity**⟩

If $f : A \to B$ has a right inverse, then f is surjective.

Proof. Suppose $g : B \to A$ is a left inverse of f, i.e. g is function such that $f \circ g = \text{id}_B$, then $\forall y \in B, f(g(y)) = y$, so $\forall y \in B \exists x \in A$ such that $f(x) = y$, so it follows that range$(f) = B$, so f is surjective □

To prove the converse, we introduce the *axiom of choice*.

DEFINITION 0.24 ⟨**axiom of choice (AC)**⟩

Given a set A of nonempty sets, there exists a choice function *f from A to the union of the union of A (informally the flattened set of elements of A, or the set of the elements of the elements of A), such that f maps elements of $X \in A$ to one of their elements (i.e.* chooses *an element of x for every set X in A)*

$$\forall A(\emptyset \notin A \implies (\exists f : A \to \cup \cup A(\forall X \in A(f(X) \in X))))$$

EXAMPLE 1.2 ⟨**axiom of choice**⟩

Consider the power set of the natural numbers $\mathcal{P}(\mathbb{N})$. The axiom of choice asserts that there exists a function $f : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$, such that given a subset N of the natural numbers, $f(N)$ is an element of that subset, i.e. f chooses *an element of the subset.*

While in trivial cases it is possible to explicitly construct such choice function, in general it is non-trivial, non-trivial enough to make the axiom of choice equivalent to more perplexing theorems, which make the axiom of choice controversial. We will explicitly state when AC is used.

Now that we have introduced AC, we can prove the converse of 14 right inverse implies surjectivity:

PROPOSITION 15 ⟨**surjectivity implies right inverse**⟩

Let $f : A \to B$ be a surjective function, then f has a right inverse.

Proof. Suppose f is surjective, then $\forall y \in B \exists x \in A$ s.t. $f(x) = y$, with x not necessarily unique. Now consider for each y the set $Y_y = \{x \in A | f(x) = y\}$. Since f is surjective each such set Y_y is nonempty. Take the union $Y = \bigcup_{y \in B} Y_y$, it is a set of nonempty sets. By AC, there exists a choice function $g : Y \to \cup \cup Y$ such that $\forall Y_y \in Y, g(Y_y) \in Y_y$, but $g(Y_y)$ is a value x such that $f(x) = y$, so $(f \circ g)(y) = f(g(y)) = y$, so $f \circ g = \mathrm{id}_B$, so g is a *right inverse* of f □

DEFINITION 0.25 ⟨**two-sided inverse**⟩

Given a function $f : A \to B$, a two-sided inverse *of f is a function $g : B \to A$ such that g is both a right inverse and a left inverse, i.e. $f \circ g = id_B$ and $g \circ f = id_A$.*

PROPOSITION 16 ⟨**two-sided inverse-bijection equivalence**⟩

Let $f : A \to B$. f has a two sided inverse if and only if f is a bijection.

Proof. $\implies$ Suppose g is a two-sided inverse of f, then by 13 left inverse-injective equivalence f is injective and by 14 right inverse implies surjectivity f is surjective, so by definition f is injective.

$\impliedby$ Suppose f is a bijection, and consider the inverse relation f^{-1} (which always exists as per 0.18 inverse given by $\{\langle y, x\rangle | \langle x, y\rangle \in f\}$. To show that f^{-1} is a function, suppose it isn't, i.e. there exists some $y \in B$ for which $\exists x_1, x_2 \in A, x_1 \neq x_2$ and $yf^{-1}x_1$ and $yf^{-1}x_2$, but that means $f(x_1) = y$ and $f(x_2) = y$, and since f is bijective it is injective so $x_1 = x_2$, a contradiction, so f^{-1} is a function. Now, by 12 composition with inverse we already know that f^{-1} is the left-inverse of f.

Consider $f \circ f^{-1}$: by 10 it follows that f is the inverse of f^{-1} so by the previous argument f is the left-inverse on f^{-1}, so $f \circ f^{-1} = \mathrm{id}_B$, so f^{-1} is also the right-inverse on f, so it is a two-sided inverse on f.

□

PROPOSITION 17 ⟨**uniqueness of the two-sided inverse**⟩

If the two-sided inverse of $f : A \to B$ exists, then it is unique, and we call it the inverse *of f.*

Proof. Suppose by contradiction that a two-sided inverse exists but isn't unique, then $\exists g, h : B \to A, g \neq h$ such that $f \circ g = f \circ h = \mathrm{id}_B$ and $g \circ f = h \circ f = \mathrm{id}_A$, then f is also the two-sided inverse of g, h and all f, g, h are bijections by 16 two-sided inverse-bijection equivalence. Since $g \neq h$, there exists some $y \in B$ such that $g(y) \neq h(y)$, but since $f \circ g = \mathrm{id}_B$ and $f \circ h = \mathrm{id}_B$ it follows that $f(g(y)) = f(h(y)) = y$, and since f is a bijection and in particular an injection it follows that $g(y) = h(y)$, a contradiction, so it must be that $g = h$.

□

Suppose $f : A \to B$ and R is an equivalence relation on A and consider some equivalence class $[a]_R$. Sometimes, functions preserve equivalence classes, for example if $A = \mathbb{N}$ and f maps $a \in A$ to its remainder with respect to some $n \in \mathbb{N}$, it is clear that $\forall a_1, a_2 \in [a]_R(f_(a_1) = f(a_2))$, i.e. f maps all elements of the equivalence class $[a]_R$ to the same element in its range. In such case, we can choose any *representative element* $a \in [a]_R$, evaluate $f(a)$, and determine $\forall b \in [a]_R(f(b) = f(a))$, thus it makes sense to define a function $\hat{f}$ on the *quotient set* of A under R (i.e. the set of all equivalence classes of A under R) such that $\hat{f}([a]_R) = f(a)$. Obviously, for $\hat{f}$ to be a function, it needs to be well-defined, i.e. there can't be two distinct $b_1, b_2 \in B$ such that $\langle [a]_R, b_1\rangle$ and $\langle [a]_R, b_2\rangle \in B$. This holds only when f truly maps all elements of an equivalence class to the same element in its range. We formalize this result in the following theorem:

THEOREM 2 ⟨**function on quotient set**⟩

Given a function $f : A \to B$ and an equivalence relation R, then there exists a function $\hat{f} : A/R \to B$ such that $\hat{f}([a]_R) = f(a)$ if and only if $\forall x, y \in A(xRy \implies (f(x) = f(y)))$.

Proof. $\implies$ This direction is trivial since if xRy then $[x]_R = [y]_R$ and by definition of $\hat{f}$ we have $\hat{f}([x]_R) = f(x)$ and $\hat{f}([y]_R) = f(y)$ and since $\hat{f}$ is a function it follows that since $\hat{f}([x]_R) = \hat{f}([y]_R)$ (since $[x]_R = [y]_R$) so $f(x) = f(y)$. $\impliedby$ Consider the relation $\hat{f} : A/R \to B$ defined as $\{\langle [a]_R, f(a)\rangle \in (A/R) \times B \,|a \in A\}$ (the reader is invited to verify that such set exists by the subset axiom and by previous results). Suppose $\hat{f}$ isn't a function, then $\exists x, y \in A$ such that $[x]_R = [y]_R$ and $f(x) \neq f(y)$, but since $[x]_R = [y]_R$ it follows that xRy so by assumption $f(x) = f(y)$, a contradiction, so $\hat{f}$ is a function □

Infinite Cartesian Product

We define the cartesian product of two sets A, B, as the set of all ordered pairs $\{\langle x, y\rangle | x \in A \wedge y \in B\}$ (whose existence is guaranteed since, as we have argued, $\langle x, y\rangle \in \mathcal{P}(\mathcal{P}(A \cup B))$). Consider the cartesian product of *three* sets A, B, C. One can trivially extend the definition to three sets by defining $A \times B \times C$ to be the set of 3-tuples $\langle a, b, c\rangle$ where $a \in A, b \in B, c \in C$:

$$A \times B \times C = \{\langle a, b, c\rangle | a \in A \wedge b \in B \wedge c \in C\}$$

Consider $\langle a, b, c\rangle$. Recall by 0.4 3-tuple that this is simply $\langle\langle a, b\rangle, c\rangle$ so it is a set from $\mathcal{P}(\mathcal{P}((A \times B) \cup C))$ as per 9 . Clearly if any of A, B, C is empty then there exists no such 3-tuple so $A \times B \times C$ is empty, so suppose all are nonempty sets. We can extend this definition to any finite cartesian product, but given an infinite cartesian product, it is not guaranteed that we can construct the set of elements of the cartesian product, or indeed that it is a set at all and not a formal class, so this notion of a cartesian product breaks down when dealing with infinite products.

Consider an alternative definition of the cartesian product, in terms of functions:

DEFINITION 0.26 ⟨**cartesian product as a set of functions**⟩

Let X be a function with domain I where $\forall i \in I$, $X(i)$ is a set (note that this is a redundant restriction since in the setting of formal set theory, everything is a set - we have not introduced any foreign ideas), then the cartesian product *on all $X(i)$ is given by the set of* all functions *$f : I \to \bigcup_{i\in I} X(i)$ such that $\forall i \in I(f(i) \in X(i))$. We denote this product as $\prod_{i\in I} X(i)$. Formally, we write:*

$$\prod_{i\in I} X(i) = \{f : I \to \bigcup_{i\in I} X(i) | \forall i \in I(f(i) \in X(i))\}$$

EXAMPLE 2.1 ⟨**cartesian product of 3 sets as a set of functions**⟩

Given 3 sets A, B, C and a set I with 3 elements $I = \{1, 2, 3\}$ (taken as numerals, not as numbers - we have not defined the natural numbers yet nor do we need to for this definition), we define a function X as the set $\{\{1, A\}, \{2, B\}, \{3, C\}\}$, then their cartesian product as a set of functions is given by

$$(A \times B) \times C = \{f : I \to (A \cup B) \cup C | f(1) \in A \wedge f(2) \in B \wedge f(3) \in C\}$$

Since functions are relations which are themselves sets of ordered pairs, the above formula is in fact just shorthand for

$$(A \times B) \times C = \{\langle 1, f(1)\rangle, \langle 2, f(2)\rangle, \langle 3, f(3)\rangle | f(1) \in A \wedge f(2) \in B \wedge f(3) \in C\}$$

Note that this is the set of all *such functions f.*

PROPOSITION 18 ⟨**isomorphism of definition for the cartesian product**⟩

There exists a natural isomorphism between 0.26 cartesian product as a set of functions and 0.3 cartesian product (in the finite case).

Proof. One should observe that n-tuples can be defined as sets of n ordered pairs $\langle i, x_i\rangle$ where $i \in I$ with I being some index set, and that there exists an isomorphism between this definition and 0.4 n-tuple. The isomorphism of the definitions for the cartesian product in the finite case quickly follows □

PROPOSITION 19

In the general (non necessarily finite) case, the cartesian product as defined in 0.26 cartesian product as a set of functions of a set of non-empty sets is non-empty if and only if the axiom of choice holds.

Proof. The cartesian product of a set of non-empty sets X is non-empty if and only if there exists a function $f : I \to \cup X$ such that $f(i) \in X_i$, which is exactly the definition of a choice function on X, which is exactly the axiom of choice □

Numbers

When discussing numbers, it is important to distinguish between *numbers*, which are abstract mathematical objects, and *numerals*, which are used to represent numbers. IX, $9_{10}, 1001_2, 100_3$ are all *numerical representations* using *numerals* of the *number* 9. While we usually use decimal numerals in base 10 to represent numbers, it is important to remember that this is just a *representation*. In this section, we will deal with the introduction of *numbers*, not *numerals*, to ZF set theory. We will use decimal numerals for convenience, but it is important the remember that what we are constructing are *numbers*.
Natural Numbers

Introduction

The *natural numbers*, or *counting numbers*, are, informally, numbers we used for *counting*. We denote the set of natural numbers by $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ (with 0 being a much later addition to number theory, controversial at first).

Were we pressed to provide a more concise definition of the set of natural numbers, we would say that $\mathbb{N}$ is a set where every element, except for 0, is the *successor* of another element, which encapsulates the idea of counting - suppose you are counting sheep: when you start counting, you have counted 0 sheep, then you count the first sheep, so you have counted 1 sheep - the successor of 0, then you count the second sheep - your count grows to 2, the successor of 1, etc, each time producing a different element of the natural numbers from the last. We can formalize this idea by definition a *successor function* $s : \mathbb{N} \to \mathbb{N}$ which maps a number to its successor, then we may define $\mathbb{N}$ as follows

$$\mathbb{N} = \{x | x = 0 \vee (\exists y \in \mathbb{N}(x = s(y)))\}$$

i.e. the set of all numbers which are 0 or successors of other numbers in the set. However, this definition is not without issues: first, it is *informal* - where does x come from? Recall that by 0.9 axiom schema of specification (ZF5), the elements must be taken from some set. Second, this definition does not prohibit the case where $\exists x_1, x_2 \in \mathbb{N}(s(x_1) = s(x_2) \wedge x_1 \neq x_2)$, i.e. it can still be the cases that there exists two different numbers such that their successors are the same, which is counter intuitive in counting as we normally think of it (but natural when we think, for example, of modular arithemetics), so we should further restrict s to be *injective*, but still the definition remains informal due to the first issue. Finally, what is 0? And what is s? How do we know that such s exists? All of these questions must be answered if we were to formally establish the natural numbers, without appealing to intuition or to some platonic ideal.

Our goal for this section then is to construct $\mathbb{N}$ purely within ZF set theory in a way that models our intuitive understanding and usage of numbers in mathematics.

Constructing Natural Numbers

One way to construct the natural numbers within set theory is as follows. First, we define 0:

DEFINITION 0.1 ⟨**0**⟩

The natural number 0 is the empty set, i.e. $0 = \emptyset$. We will define what it means to be a natural number *at a later point.*

DEFINITION 0.2 ⟨**successor**⟩

Given a set A, its successor A^+ *is the set $A \cup \{A\}$.*

The existence of the successor is guaranteed by 0.8 union and 0.11 axiom of power set (ZF6) (since $\{A\} \in \mathcal{P}(A)$).

EXAMPLE 2.2 ⟨**first few numbers**⟩

Using the above definition, we will construct the numbers $1, 2, 3$ such that 1 is the successor of 0, 2 is the successor of 1 and 3 is the successor of 2:

$1 = 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset, \{\emptyset\}\}$

$2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\} \cup \{\emptyset, \{\emptyset\}\} = \Big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\Big\}$

$3 = 2 \cup \{2\} = \left\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \Big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\Big\}\right\}$

Note that the successor of a set is a property of any set and not just of sets of natural numbers (which we haven't yet defined)

Recall from our informal discussion that given any natural number, we expect that there exists a natural number that is its successor, i.e. $\forall n \in \mathbb{N}$ (whose existence we haven't yet asserted), we expect that its successor n^+ exists and is also in $\mathbb{N}$ (since it is also a natural number). We formalize this notion when defining an *inductive set*.

DEFINITION 0.3 $\langle$**inductive set**$\rangle$

An inductive set is a set A such that:
1. $\emptyset \in A$
2. $\forall a \in A(a^+ \in A)$ (i.e. $a \cup \{a\} \in A$), meaning A is closed under succession

I have discussed inductive sets in a more general sense before when discussing introductory mathematical logic, so the reader can find all theorems involving inductive sets (and soon, recursion) in a more general form with proofs in that discussion. However, since the specialized forms of these definitions we deal with here are simpler to state and prove, I will not refer to that discussion for the most part in favor of keeping this discussion more self-contained.

In the formal theory we have constructed so far, the existence of an inductive set is undecided - we cannot prove or disprove that such set exists. However, if the natural numbers exist as a set in our theory, then it follows that the set of natural numbers is an inductive set since, as per our informal discussion, it must be that $0 \in \mathbb{N}$ and $\forall n \in \mathbb{N}((n+1) \in \mathbb{N})$ and $n+1$ is the successor of n i.e. n^+ so $\mathbb{N}$ is closed under succession, so we assert the existence of such set as an axiom:

DEFINITION 0.4 $\langle$**axiom of infinity (ZF7)**$\rangle$

$$\exists I(\emptyset \in I \wedge \forall x(x \in I \implies (x^+ \in I))$$

Where x^+ is the successor of x. If we wish to state the axiom without referring to x^+, it can be replaced with $(x \cup \{x\}) \in I$.

The axiom asserts the existence of an inductive set. As we will soon see, it is implied from the definition of the successor that such inductive set I is infinite, hence the name of the axiom.

Once we know that there exists some inductive set, we can start talking about the *set* of inductive sets (since at least one inductive set exists this set is non-empty).

PROPOSITION 20 ⟨**intersection of inductive sets**⟩

The intersection of two inductive sets is an inductive set.

Proof. Take A, B inductive sets. Since both are inductive then $\emptyset \in A, \emptyset \in B$ so $\emptyset \in A \cap B$. Now take some $x \in A \cap B$. Since $x \in A \cap B$ then $x \in A$ and $x \in B$, and both are inductive so $x^+ \in A$ and $x^+ \in B$, so $x^+ \in A \cap B$, so $A \cap B$ is inductive □

PROPOSITION 21 ⟨**minimal inductive set**⟩

The intersection of the set of all inductive sets is the smallest inductive set.
We denote this set by ω.

Proof. Take A as the set of all inductive sets. By 20 intersection of inductive sets we can argue that $\cap A$ is is inductive. To show that it is minimal, suppose not, then $\exists B \in A$ such that B has less elements than $\cap A$, but then there must be that $\exists a(a \in \cap A \wedge a \notin B)$, but $B \in A$ since it is inductive and $\cap A$ is the intersection of all inductive sets so $\forall a(a \in \cap A \implies a \in B)$, a contradiction, so $\cap A$ is minimal □

Now we are primed to define natural numbers:

DEFINITION 0.5 ⟨**natural number**⟩

A natural number is an element of all inductive sets, i.e. a member of ω.

Which immediately leads to

DEFINITION 0.6 ⟨**the set of natural numbers**⟩

The set of natural numbers $\mathbb{N}$ is the intersection of all inductive sets ($\mathbb{N} = \omega$).

The existence of this set follows immediately from the axiom of infinity.

THEOREM 3 ⟨**induction principle**⟩

Given an inductive set $A \subseteq \omega$, then it follows $A = \omega$.

Proof. Follows from the fact that ω is the smallest inductive set □

By the induction principle we can perform *induction* on the natural numbers as defined within set theory.

PROPOSITION 22

Every natural number except for 0 is a successor of some other natural number.

Proof. Let $A = \{n \in \mathbb{N} | n = 0 \vee (\exists x \in \mathbb{N}(n = x^+))\}$, i.e. the set of all natural numbers that are successors of other natural numbers, and 0. Clearly $0 \in A$, now take some $a \in A$. Since $a \in A$ then $a \in \mathbb{N}$ and since $\mathbb{N}$ is inductive then $a^+ \in \mathbb{N}$ so by the specification of A, $a^+ \in A$ since it is the successor of $a \in \mathbb{N}$, so A is inductive, then by the induction principle $A = \omega = \mathbb{N}$, so all natural numbers are either successors of some natural number, or 0 □

The natural numbers can be constructed from the bottom-up by starting with 0 and taking the successor, then taking the successor of the newly produced number, ad infinitum. This is called a *bottom-up* construction of the set, since we incrementally build our set starting from a small subset ("basis") and an operator under which the larger set is closed (the successor operation). It can be shown that this process generates the minimal inductive set. This is asserted by Theorem 53 in Introduction to Mathematical Logic

PROPOSITION 23

the members of a natural number are natural numbers.

Proof. Let $A = \{n \in \mathbb{N} | n = 0 \vee \forall m(m \in a \implies m \in \mathbb{N})\}$, which is a valid definition as per the axiom schema of specification. This is the set of all natural numbers whose members are also natural numbers. To prove the proposition, we shall show that the set is inductive. Clearly $0 \in A$ by definition. Take some $n \in A$, and consider $n^+ \in \mathbb{N}$. By definition, $n^+ = n \cup \{n\}$. Take some $m \in n^+$, either $m = n$, in which case $m \in \mathbb{N}$ since $n \in A$ and A is a subset of $\mathbb{N}$, or $m \in n$, but since $n \in A$ it follows that $\forall m(m \in a \implies m \in \mathbb{N})$, so in conclusion $\forall m(m \in n^+ \implies m \in \mathbb{N})$, so $n^+ \in A$, so A is inductive □

Reaching Infinity

We wish to show that $\mathbb{N}$ is indeed infinite, which would justify the name of the axiom of infinity. To do that, we need to define the successor *function*, and show that it is injective, i.e. $\nexists n_1, n_2 \in \mathbb{N}$ such that $n_1 \neq n_2 \wedge f(n_1) = f(n_2)$. By proving this, it immediately follows that $\mathbb{N}$ is infinite (a formal definition for an infinite set within formal set theory will soon follow, for now we use the term informally).

DEFINITION 0.7 ⟨**successor function**⟩

The successor function is the function $s : \mathbb{N} \to \mathbb{N}, n \mapsto n^+$.

Note that we can define a more general successor function $\hat{s} : \cup U \to \cup U, a \mapsto a^+$ where U is the set of all inductive sets. The benefit of this definition is that it lets us do away with the restriction to the set of natural numbers. However, this definition is not particularly useful within this discussion so we will not use it.

DEFINITION 0.8 ⟨**transitive set**⟩

A set A is transitive *if* $\forall a(a \in A \implies \forall x(x \in a \implies x \in A))$. *More concisely, a set is transitive if* $\forall x(x \in a \in A \implies x \in A)$.

THEOREM 4 ⟨**transitive set definitions**⟩

For a given set A, the following are equivalent:
1. A is transitive.
2. $\cup A \subseteq A$
3. $a \in A \implies a \subseteq A$
4. $A \subseteq \mathcal{P}(A)$

Proof. $1 \implies 2:$ Suppose A is transitive and consider $\cup A$. Take some $x \in \cup A$, then $\exists a \in A$ such that $x \in a$ so by transitivity of A, $x \in A$, but this holds for every $x \in \cup A$, so $\cup A \subseteq A$.

$2 \implies 3:$ Suppose $\cup A \subseteq A$ and take some $a \in A$, then by the union axiom $\forall x(x \in a \implies x \in \cup A)$, so $a \subseteq \cup A$, so by transitivity of inclusion $a \subseteq A$.

$3 \implies 4:$ Suppose (3) and consider $\mathcal{P}(A)$. By definition it is the set of all subsets of A. By 3, $\forall a(a \in A \implies a \subseteq A)$ so $a \in \mathcal{P}(A)$, which means $\forall a(a \in A \implies a \in \mathcal{P}(A))$, so $A \subseteq \mathcal{P}(A)$.

$4 \implies 1:$ Suppose 4 and consider some $a \in A$ and some $x \in a$. Since $A \subseteq \mathcal{P}(A)$, it follows that $a \in \mathcal{P}(A)$, so $a \subseteq A$, so $x \in A$, so A is transitive.

□

PROPOSITION 24

Natural numbers are transitive sets.

Proof. We prove this by applying the induction principle on $\mathbb{N}$. For 0, which is the set with no elements, it is vacuously true. For any natural number n which is transitive, its successor, given by, $n^+ = n \cup \{n\}$, is also transitive, since if $x \in n^+$ then either

1. $x \in n$ which is transitive by the induction hypothesis (formally using the induction principle, this holds because we choose n such that it is already transitive) so $\forall a \in x \in n, a \in n$ but since $n \subseteq n^+$ it follows that $a \in x \in n \implies a \in n^+$.

2. $x = n$, and again $\forall a(a \in x \implies a \in n)$ by the induction hypothesis, but again $n^+ = n \cup \{n\}$ so $\forall a(a \in n \implies a \in n^+)$, so $a \in n \implies a \in n^+$.

So we conclude by induction that the natural numbers are transitive numbers □

Note that this result means that for every natural number n, that number is a transitive set (as per our definition of natural numbers via sets), and *not* that the *set* of all natural numbers $\mathbb{N}$ is a transitive set, which we assert in the following theorem:

PROPOSITION 25

The set of all natural numbers is transitive.

Proof. Let $n \in \mathbb{N}$, then by 23 $\forall m(m \in n \implies m \in \mathbb{N})$ so $\mathbb{N}$ is transitive by definition □

THEOREM 5

If A is a transitive set, then $\cup A^+ = A$.

Proof. We prove by mutual inclusion. By definition $A^+ = A \cup \{A\}$ so $A \subseteq \cup A^+$. To show $\cup A^+ \subseteq A$, take some $a \in \cup A^+$, so $a \in \cup\{A, \{A\}\}$, so either $a \in A$ or $\exists b \in A$ such that $a \in b$, but since A is transitive $\forall a(a \in b \wedge b \in A \implies a \in A)$, so $a \in A$ in both cases, so $\cup A^+ \subseteq A$, so in conclusion $\cup A^+ = A$ □

COROLLARY 5.1 ⟨**injectivity of the successor function**⟩

The successor function on $\mathbb{N}$ is injective.

Proof. Take $n, m \in \mathbb{N}$ such that $s(m) = s(n)$, i.e. $m^+ = n^+$, then $\cup m^+ = \cup n^+$, so by the theorem $m = n$, so s is injective □

The injectivity of the successor function implies that $\mathbb{N}$ - the set whose existence is asserted by the axiom of infinity - is infinite, since for any $n \in \mathbb{N}$ we can find a successor $n^+ \in \mathbb{N}$ that is *unique* (by the injectivity of the successor function), so given any finite set of natural numbers we can always find a successor to one of the numbers that is outside of that set but still in $\mathbb{N}$.

Total Order

DEFINITION 0.9 ⟨**partial order**⟩

A partial order *is a binary relation* $\leq$ *such that it is* reflexive*,* antisymmetric *and* transitive*.*

DEFINITION 0.10 ⟨**total order**⟩

A total order *is a* partial order $\leq$ *that is also* total *(strongly complete).*

THEOREM 6 ⟨**total order of N**⟩

The total order $\leq$ *on* $\mathbb{N}$ *is defined as follows:*

$$a \leq b \iff (a \in b) \vee (a = a)$$

Proof. We will show that this is a total order:

1. *Reflexive*: Given $a \in \mathbb{N}$, since $a = a$ then $a \leq a$ by definition.
2. *Antisymmetric*: Given $a, b \in \mathbb{N}$, if $a \leq b \wedge b \leq a$ then by definition it follows that either $a = b$ or $b \in a \wedge a \in b$, but the latter is impossible since either $a \in b$ or $b \in a$, so $a = b$.
3. *Transitive*: Given $a, b, c \in \mathbb{N}$ such that $a \leq b \wedge b \leq c$, by definition it follows that either $a = b \wedge b = c$ so $a = c$ which, by reflexivity, implies $a \leq c$, or $a \in b \wedge b \in c$. Since natural numbers are *transitive*, it follows that $a \in c$, so $a \leq c$ by definition.
4. *Total*: Given $a, b \in \mathbb{N}$, then either $a = b$, in which case $a \leq b$ by definition, or at least one of a, b is the successor of some natural number. By 5.1 injectivity of the successor function it follows that either $a \in b$ or $b \in a$, so either $a \leq b$ or $b \leq a$.

□

Similarly, we can define a *strict total order* on $\mathbb{N}$:

DEFINITION 0.11 ⟨**strict partial order**⟩

A strict partial order *is a binary relation that is* irreflexive*,* assymetric *and* transitive*.*

DEFINITION 0.12 ⟨**strict total order**⟩

A strict total order *is a* strict partial order *that is* total*.*

THEOREM 7 ⟨**strict total order on N**⟩

The strict total order on $\mathbb{N}$ *is defined as follows:*

$$ab \iff a \in b$$

Proof. 1. *Irreflexive*: Take $a \in \mathbb{N}$, then clearly $a \notin a$, so $\neg(aa)$.
2. *Assymetric*: Take $a, b \in \mathbb{N}$ such that ab, then $a \in b$, which implies $\neg(b \in a)$, so $\neg(ba)$.

The rest of the proof is identical to Theorem 6 total order of N □

Given an order relation, we can start talking about the *predecessors* of a number:

DEFINITION 0.13 ⟨**predecessors of a number**⟩

Given a natural number n*, its* predecessors *are all numbers* m *such that* mn*.*
The singular form predecessor *is reserved for the unique* $m \in \mathbb{N}$ *such that* $n = m^+$*.*

PROPOSITION 26

A natural number n *is the set of its predecessors.*

Proof. When $n = 0$ this is vacuously true, so we suppose n is nonempty. Let M_n be the set of predecessors of n, i.e. $M_n = \{m \in \mathbb{N} | m \in n\}$. It immediately follows that $\forall m(m \in M_n \implies mn)$ since $mn \iff m \in n$, so $M_n \subseteq n$. Now take some $k \in n$. By 23 it follows that $\forall n(n \in \mathbb{N} \implies \forall k(k \in n \implies k \in \mathbb{N}))$, so $k \in \mathbb{N}$, so $k \in M_n$, so $n \subseteq M_n$, so we conclude $n = M_n$ □

Arithemetics

At the moment, our set of natural numbers has the following properties:
1. $0 \in \mathbb{N}$
2. $\forall n(n \in \mathbb{N} \implies n^+ \in \mathbb{N})$
3. $\forall n, m \in \mathbb{N}(nm \iff n \in m)$

By defining operations on $\mathbb{N}$, such as addition and multiplication, we construct the *arithemetic* of the natural numbers. For the operations to properly model those naturally defined on the natural numbers, they should model certain axioms.

Suppose we have defined binary operations $+ : \mathbb{N}^2, \cdot : \mathbb{N}^2$, then the following axioms specify the formal axioms (stated in a first-order language) that these operations, and $\mathbb{N}$ itself, should satisfy so that $(\mathbb{N}, s, 0, +, \cdot)$ (where s is the successor function) will be a model of the natural numbers.

DEFINITION 0.14 ⟨**Peano arithmetic**⟩

A tuple $(\mathbb{N}, s, 0, +, \cdot)$ *models Peano arithmetic if the following axioms are satisfied:*
1. $0 \in \mathbb{N}$ *(*0 *is a natural number)*
2. $\forall n \in \mathbb{N}(0 \neq s(n))$ *(*0 *is not the successor to any number)*
3. $\forall m, n \in \mathbb{N}(s(n) = s(m) \implies (n = m))$ *(the successor function is injective)*
4. $\forall n \in \mathbb{N}(n + 0 = n)$ *(*0 *is the additive identity)*
5. $\forall m, n \in \mathbb{N}(m + s(n) = s(m + n))$
6. $\forall n \in \mathbb{N}(n \cdot 0 = 0)$
7. $\forall m, n \in \mathbb{N}(m \cdot s(n) = m \cdot n + m)$ *(implies distributivity of multiplication over addition)*

The reader is invited to convince themselves that their understanding of natural number arithemetic models the Peano axioms. Our goal in this section is to introduce addition and multiplication to formal set theory such that $(\mathbb{N}, s, 0, +, \cdot)$ will satisfy these axioms, thus we will conclude that we have a model of the natural numbers and their arithmetic.

Our definitions will be recursive, so first we introduce the recursion theorem as it applies to the natural numbers (a more general form is discussion in Introduction to Mathematical Logic):

THEOREM 8 ⟨**recursion theorem**⟩

Let A *be a set, let* $a_0 \in A$ *and let* $f : A \to A$ *be a unary operator on* A*, then there* exists *a* unique *function* $h : \mathbb{N} \to A$ *such that:*
1. $h(0) = a_0$
2. $h(n^+) = f(h(n))$

Proof. Define

$$h = \{\langle n, a\rangle \in \mathbb{N} \times A | \exists g : n^+ \to A(g(0) = a_0 \wedge g(n) = a \wedge \forall i \in n(g(i^+) = f(g(i)))\}$$

i.e. h is the set of all ordered pairs $\langle n, a\rangle$ in the cartesian product $\mathbb{N} \times A$ such that for each pair there exists a function $g : n^+ \to A$ which acts as h (as defined in the theorem), restricted to n^+, and $g(n) = a$.

We will show that there always exists such a function g: let $n \in \mathbb{N}$, then we define $g : n^+ \to A$ as follows:
1. $g(0) = a_0$
2. $\forall i \in n^+, g(i^+) = f(g(i))$

Clearly g is a relation and its existence is obvious from the existence of a_0, n^+, f. To show that it is a function, take some $i \in n^+$, either $i = 0$ in which case it is not the successor to any function so it is

sent to a_0 according to rule 1, or $i \neq 0$ in which case it is the successor to some number so it is sent to A *uniquely* by g according to rule 2 (uniqueness follows from f being a function), so g is a function.

To show uniqueness of g, suppose by contradiction that $\exists g_1, g_2$ for some n that satisfy both properties such that $g_1 \neq g_2$, so $\exists i \in n^+$ such that $g_1(i) \neq g_2(i)$, but clearly this i is not 0 since they must agree on 0. Now note that if $i \neq 0$ then i is the successor of some number, so $\exists i_1 \in n^+$ such that $i = i_1^+$, so by property 2 it follows that $g_1(i) = f(g_1(i_1))$. Now, i_1 is either 0 or the successor of some $i_2 \in n^+$, so $g_1(i_i) = f(g_1(i_2))$, so $g_1(i) = f(f(g_1(i_2)))$. We can repeat this argument until we get to 0 (this process must terminate after a finite number of steps since the domain of g_1 is n^+ which is finite), so $g_1(i) = f(f(\dots f(g_1(0))\dots))$, and similarly for $g_2(i)$, but then $g_1(i) = g_2(i)$ since $g_1(0) = g_2(0)$, a contradiction, so g is unique.

Since g exists and is unique, it follows that h is a function (since g is unique) whose domain is $\mathbb{N}$ (since we can find a g for every $n \in \mathbb{N}$).

□

This is a specialization of the more general theorem that deals with any set B in place of $\mathbb{N}$ such that B is *freely-generated* by the operations under which it is closed and are considered by the homomorphism, and some base (in this case, $\mathbb{N}$ is *freely-generated* by the successor operation and 0, which serves as the base).

We can now define precursors to addition and multiplication recursively, knowing by the recursion theorem that these definitions are indeed well-defined as functions.

DEFINITION 0.15 ⟨**addition operator**⟩

Given some $k \in \mathbb{N}$, we define the addition on k *as a function $A_k : \mathbb{N} \to \mathbb{N}$ as follows:*
1. $A_k(0) = k$
2. $\forall n \in \mathbb{N}$, $A_k(n^+) = A_k(n)^+$

This definition satisfies the above theorem since $A_k(n)^+ = s(A_k(n))$, so s takes the place of f in the theorem.

PROPOSITION 27

The addition operator on a fixed $k \in \mathbb{N}$ is injective.

Proof. Consider $A_k : \mathbb{N} \to \mathbb{N}$. Suppose it is not injective, then $\exists m, n \in \mathbb{N}, m \neq n$ such that $A_k(m) = A_k(n)$. Either one is zero, or both are non-zero. In the former case, w.l.o.g suppose $m = 0$, then $A_k(m) = k$, then $A_k(n) = k$ but since n is non-zero then it is the successor of some number n_1, and this argument can be repeated finitely many times until we get n represented in terms of successors to 0, in a similar fashion to how we argued this in the proof of the recursion theorem,

then $A_k(n) = A_k(\ldots(0^+)\ldots^+)$ which by definition is $(\ldots(A_k(0)^+)\ldots^+ = (k^+)\ldots^+$, but since the successor function on $\mathbb{N}$ is itself injective by 5.1 injectivity of the successor function it follows that it cannot be that $(k^+)\ldots^+ = k$, a contradiction, so A_k is injective □

DEFINITION 0.16 ⟨**multiplication operator**⟩

Given some $k \in \mathbb{N}$, we define the multiplication by k *as a function $M_k : \mathbb{N} \to \mathbb{N}$ as follows:*
1. $M_k(0) = 0$
2. $M_k(n^+) = A_k(M_k(n))$

DEFINITION 0.17 ⟨**addition and multiplication**⟩

Let $k, n \in \mathbb{N}$, then we define:
1. $k + n = A_k(n)$ *(addition)*
2. $k \cdot n = M_k(n)$ *(multiplication)*

EXAMPLE 8.1 ⟨**addition and multiplication**⟩

We will calculate, by definition, the following expressions:
1. $2 + 3$*, which expands to*

$$A_2(3) = A_2(2)^+ = (A_2(1)^+)^+ = ((A_2(0)^+)^+)^+ = ((2^+)^+)^+ = 5$$

2. $3 \cdot 2$ *which expands to*

$$M_3(2) = A_3(M_3(1)) = A_3(A_3(M_3(0))) = A_3(A_3(0)) = A_3(3) = ((3^+)^+)^+ = 6$$

DEFINITION 0.18 ⟨**parity of a number**⟩

The parity *of a number n is defined as follows:*
1.n is even *if it can be written as $2 \cdot m$ for some number m.*
2. n is odd *if it is not even.*

PROPOSITION 28

$(\mathbb{N}, s, 0, +, \cdot)$ *models Peano arithemtic.*

Proof. We have already shown that the first three axioms are satisfied, so we start from 4.

4. by definition $n + 0 = A_n(0) = n$.

5. $m + s(n) = A_m(s(n)) = (A_m(n))^+ = (m + n)^+ = s(m + n)$
6. $n \cdot 0 = M_n(0) = 0$ by definition.
7. $m \cdot s(n) = M_m(s(n)) = A_m(M_m(n)) = m + m \cdot n$. By commutativity of addition (which can be shown by induction), it follows that $m + m \cdot n = m \cdot n + m$.

□

THEOREM 9 ⟨**arithemetic properties of the natural numbers**⟩

Let $a, b, c \in \mathbb{N}$, then:
1. addition is associative*, i.e. $(a + b) + c = a + (b + c)$, and* commutative*, i.e. $a + b = b + a$.*
2. multiplication is associate and commutative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $a \cdot b = b \cdot a$.
3. multiplication is distributive over addition, i.e. $a \cdot (b + c) = a \cdot b + a \cdot c$.
And given the strict order $<$ and order $\leq$ on $\mathbb{N}$ as previously defined:
1. strict order is preserved by addition, i.e. if ab then $a + cb + c$
2. order is preserved under multiplication, i.e. $a \leq b \implies a \cdot c \leq b \cdot c$

The proof for each of these propositions is by induction, and is left as an exercise.

The structure $(\mathbb{N}, 0, +)$ is our first example of a *monoid*, which is one of the structures studied in abstract algebra:

DEFINITION 0.19 ⟨**monoid**⟩

A monoid *is a non-empty set A equipped with a binary operation $\cdot : A^2 \to A$ that satisfies:*
1. Associativity*: $\forall a, b, c \in A, (a \cdot b) \cdot c = b \cdot (a \cdot c)$*
2. Identity*: $\exists e \in A, a \cdot e = a$*
A monoid where $\cdot$ commutes is called a commutateive *monoid.*

The identity of $+$ in $\mathbb{N}$ is 0, and associativity follows from Theorem 9 arithemetic properties of the natural numbers. The identity of $\cdot$ is 1, and its associativity also follows from that theorem, so $(\mathbb{N}, 1, \cdot)$ is also a monoid.

PROPOSITION 29

1. Addition of odd numbers results in an even number.
2. Addition of even numbers results in an even number.
3. Addition of an odd number with an even number results in an odd number.
4. Multiplication of odd numbers results in an odd number.
5. Multiplication of even numbers results in an even number.
6. Multiplication of an odd number with an even number results in an even number.

The reader is invited to verify the proposition by considering $\mathbb{N}/\sim$ where $\sim$ is an equivalence relation defined as follows: $n \sim m \iff \text{parity}(n) = \text{parity}(m)$, which forms two equivalence classes - odd and even numbers. The proof makes use of Theorem 9 arithemetic properties of the natural numbers.

Integers

Introduction

Informally, the natural numbers are extended to the integers, denoted $\mathbb{Z}$, by associating a negative number with every natural number, where negative numbers are the *additive inverse* of a natural number $n \in \mathbb{N}$ greater than 0. An *additive inverse* of a number n is a number $-n$ such that $n+(-n) = 0$, the additive identity. Given the set of integers, which extends the natural numbers with their additive inverses, we can define *subtraction* as addition of an additive inverse, for example $a - b$ is nothing but $a + (-b)$ where $-b$ is the additive inverse of b which is an integer. A first attempt at formalizing this yields the following

$$\mathbb{Z} = \mathbb{N} \cup \{z | \exists n \in \mathbb{N}(n + z = 0)\}$$

This definition suffers from many of the same issues as our first attempts at defining the natural numbers. First, what is addition on $\mathbb{Z}$? Is it the same as addition on $\mathbb{N}$? The condition $n + z = 0$ must be clarified. But a far more pressing issue is, again, that of the improper use of the axiom schema of specification: where do we take z from? In which set does it reside? Clearly not in $\mathbb{N}$ or any of its subsets.

In this section, we will present a formal construction of the integers within set theory, define addition and multiplication on integers and a total order (strict and non-strict), and show that the resulting structure satisfies the arithemetic and algebraic properties we expect from the integers, namely that the set is an ordered commutative ring, a term which will be defined later.

Constructing Integers

We will construct the integers as a quotient set on the natural numbers.

DEFINITION 0.20 ⟨**integers**⟩

Let $\sim$ be an equivalence relation on $\mathbb{N}^2$ defined as follows:

$$\langle a, b\rangle \sim \langle c, d\rangle \iff a + d = b + c$$

Then the set of integers $\mathbb{Z}$ is given by the quotient set *of $\mathbb{N}^2$ under $\sim$, i.e. $\mathbb{Z} = \mathbb{N}^2 / \sim$.*

PROPOSITION 30

$\mathbb{Z}$ exists and is a set.

Proof. By 0.15 quotient set it suffices to show that $\sim$ is indeed an equivalence relation on $\mathbb{N}^2$, then $\mathbb{Z}$ exists as defined as a quotient set. Reflexivity is trivial. As for symmetry, take $\langle a, b\rangle, \langle c, d\rangle \in \mathbb{N}^2$ such that $\langle a, b\rangle \sim \langle c, d\rangle$, so $a + d = b + c$, but since equality is symmetric (this is a property of first-order logic with equality) then $b + c = a + d$, so $\langle c, d\rangle \sim \langle a, b\rangle$, so $\sim$ is symmetric.

For transitivity, take $\langle e, f\rangle \in \mathbb{N}^2$ in addition to the previous pairs, and suppose $\langle a, b\rangle \sim \langle c, d\rangle$ and $\langle c, d\rangle \sim \langle e, f\rangle$, then $a + d = b + c$ and $c + f = d + e$. Consider the semi-formal argument:
1. $a + d = b + c$ (hypothesis)
2. $(a + d) = (b + c) \implies ((a + d) + f = (b + c) + f))$ (by properties of equality, the two terms on the RHS differ only by the equivalent terms, for further details see Introduction to Mathematical Logic)
3. $(a + d) + f = (b + c) + f$ (MP on $1, 2$)
4. $(a + f) + d = b + (c + f)$ (associativity and commutativity of addition)
5. $c + f = d + e$ (hypothesis)
6. $(c + f = d + e) \implies ((a + f) + d = b + (c + f) \implies (a + f) + d = b + (d + e))$ (properties of equality)
7. $(a + f) + d = b + (d + e)$ (MP two times on $4, 5, 6$)
8. $d + (a + f) + d = d + (b + e)$ (associativity and commutativity of addition)
9. $A_d(a + f) = A_d(b + e)$ (explicit form of 8 as per 0.17 addition and multiplication)
10. $a + f = b + e$ (by the injectivity of A_d established in 27)
11. $\langle a, b\rangle \sim \langle e, f\rangle$ (from 10 by definition of $\sim$)

In conclusion, $\sim$ is an equivalence relation on $\mathbb{N}^2$, so $\mathbb{Z}$ exists and is well-defined.

□

Consider the rational for this definition: with our knowledge of subtraction, we know that $a + d = b + c \iff a - b = c - d$, i.e. $\langle a, b\rangle \sim \langle c, d\rangle$ if and only if the signed difference of the terms in each pair is the same, however since to define the difference using subtraction we first need to define the

integers, we cannot use this definition and instead use the more obscure definition provided above. From this, it quickly follows why $\mathbb{Z}$ indeed looks like the integers as we think of them: consider its elements, which are equivalent classes on $\mathbb{N}^2$ under $\sim$. Given some $z \in \mathbb{Z}$, all $\langle a, b\rangle \in z$ must satisfy $a - b = k$ for some k, and similarly by our knowledge of subtraction, $b - a = -k$, so it belongs to the equivalence class which represents the *additive inverse* of k. This way, we can identify each equivalence class with an *integer*, either zero (whose equivalence class is that of all ordered pairs of the form $\langle a, a\rangle$ as we will soon show), positive or negative (depending on whether ab or not with being the strict order on $\mathbb{N}$ since $a, b \in \mathbb{N}$), and build the set of integers.

To illustrate this idea, consider the following representation of 4×4 (the cartesian product of the set 4 with itself):

$$\begin{pmatrix} \langle 0,3\rangle & \langle 1,3\rangle & \langle 2,3\rangle & \langle 3,3\rangle \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 2,2\rangle & \langle 3,2\rangle \\ \langle 0,1\rangle & \langle 1,1\rangle & \langle 2,1\rangle & \langle 3,1\rangle \\ \langle 0,0\rangle & \langle 1,0\rangle & \langle 2,0\rangle & \langle 3,0\rangle \end{pmatrix}$$

The equivalence classes on the set under $\sim$ that consist of more than one member have been colored. Consider how the structure of the matrix relates to the elements of $(4 \times 4)/\sim$:
1. The *secondary diagonal* (in red) consists of all the ordered pairs where the elements are the same, i.e. the difference between the elements is 0.
2. Above the secondary diagonal, all ordered pairs are of the form $\langle a, b\rangle$ such that ab, while below it they are of the form ba.
4. One diagonal below it (in green), the difference of elements in the ordered pairs between the first and second is 1. Going on diagonal below that (in brown) we have a difference of 2, and finally we have a single element at the bottom-right corner where the difference is 3.
5. One diagonal above the secondary (in violet), the difference is -1, going one below (in purple) the difference is -2, and at the top-left corner where the difference is -3.

This kind of construction is called a *diagonal* construction. Hopefully the example makes it clear why that is the case. Now consider $\mathbb{N}^2$ again - since $\mathbb{N}$ is infinite, the rows and columns of the matrix extend infinitely, so intuitively it should be obvious that these construction creates a set of equivalence classes such that the set looks like the integers. This motivates *defining* the integers as those equivalence classes.

EXAMPLE 9.1 ⟨**integers in set theory**⟩

We identify the integer 0 *with the equivalence class* $[\langle 0,0\rangle]$*, which is the equivalence class of all pairs where both elements are the same. It is important to note that* 0_z*, the* 0 *of the integers, is* not 0_n*, the* 0 *of the natural numbers, sine* $0_z = [\langle 0_n, 0_n\rangle] \neq 0_n$*.*
The integer 1 *is identified with the equivalence class of* $[\langle 1,0\rangle]$*, and the integer* -1 *is identified with the equivalence class of* $[\langle 0,1\rangle]$*.*

We will now formalize our observation regarding the equivalence classes formed under $\sim$:

PROPOSITION 31

Given $a, b \in \mathbb{N}$*, when* $a \neq b$ *the equivalence classes of* $\langle a,b\rangle, \langle b,a\rangle$ *are distinct, i.e. they belong to different members of* $\mathbb{Z}$*, and when* $a = b$ *they belong to a different equivalence class where all members are of the form* $\langle a,a\rangle$*.*

Proof. Since $\mathbb{Z}$ is a quotient set on $\mathbb{N}^2$, it is a partition on $\mathbb{N}^2$, so every ordered pair in that set belongs to some element of $\mathbb{Z}$ and the elements of $\mathbb{Z}$ are distinct, so it suffices to show that $\langle a,b\rangle \not\sim \langle b,a\rangle$ when $a \neq b$, and that $\langle a,a\rangle \sim \langle b,b\rangle$ and $\langle a,a\rangle \not\sim \langle a,b\rangle$ when $a \neq b$. We show both by definition: $a + a = b + b \iff a = b$, so by definition of $\sim$, $\langle a,b\rangle \not\sim \langle b,a\rangle$ when $a \neq b$. In the latter, we have $a+b = a+b$ which is always true so $\langle a,a\rangle \sim \langle b,b\rangle$ for all $a, b \in \mathbb{N}$, and further $a+b = a+a \iff a = b$, so $\langle a,a\rangle \not\sim \langle a,b\rangle$ when $a \neq b$ □

Arithmetic

DEFINITION 0.21 ⟨**integer arithemetic**⟩

Given any two integers $[\langle a,b\rangle], [\langle c,d\rangle]$ *we define* addition *and* multiplication *as follows:*
1. $[\langle a,b\rangle] + [\langle c,d\rangle] = [\langle a+c, b+d\rangle]$ *(the addition on the RHS is addition on* $\mathbb{N}$*)*
2. $[\langle a,b\rangle] \cdot [\langle c,d\rangle] = [\langle a\cdot c + b\cdot d, a\cdot d + b\cdot c\rangle]$ *(multiplication on the RHS is multiplication on* $\mathbb{N}$*)*

The motivation behind those definitions is that, since we wish to identify each ordered pair $\langle a,b\rangle$ with $a-b$, we can calculate $(a-b)+(c-d) = (a+c)-(b+d)$ which we identify with $\langle a+c, b+d\rangle$ and retrieve the definition for addition. Similarly, $(a-b)(c-d) = ac-ad-bc+bd = (ac+bd)-(ad+bc)$, which motivates the definition for multiplication.

PROPOSITION 32

Integer arithmetic is well-defined.

Proof. We only present the proof for addition, the proof for multiplication follows the same structure. By Theorem 2 function on quotient set it suffices to show that $[\langle a,b\rangle]+[\langle c,d\rangle]=[\langle a',b'\rangle]+[\langle c',d'\rangle]$ if $\langle a,b\rangle \sim \langle a',b'\rangle$ and $\langle c,d\rangle \sim \langle c',d'\rangle$. By definition, the sum on the LHS is $[\langle a+c,b+d\rangle]$ and on the RHS the sum is $[\langle a'+c',b'+d'\rangle]$. By a previous result both classes are equivalent if and only if $\langle a+c,b+d\rangle \sim \langle a'+c',b'+d'\rangle$, i.e. $(a+c)+(b'+d')=(b+d)+(a'+c')$, reordering this expression (due to properties of addition on $\mathbb{N}$), we get $(a+b')+(c+d')=(b+a')+(d+c')$, which is the equality we need to satisfy. From the hypothesis it follows that $a+b'=b+a'$ and $c+d'=d+c$. By addition of these two formulas (a more formal argument was provided in 30) we retrieve the equality we wish to prove, so we conclude that addition as a function on $\mathbb{Z}$ is well=defined □

From this definition and the properties of $\mathbb{Z}$, we can show that each element in $\mathbb{Z}$ has an *additive inverse*.

DEFINITION 0.22 ⟨**additive inverse**⟩

The additive inverse *of some number n is a number m such that $n+m=0$, with 0 being the additive identity of the set. We denote the additive inverse of n as $-n$.*

Note that being an additive inverse is symmetric - i.e. $n, -n$ are each other's additive inverse.

PROPOSITION 33

For every $z\in\mathbb{Z}$, there exists an additive inverse $-z\in\mathbb{Z}$.

Proof. Recall that $0_z=[\langle 0,0\rangle]$, and that $z=[\langle a,b\rangle]$. Consider $z'=[\langle b,a\rangle]$. By a previous proposition we know that z,z' are distinct equivalent classes. Now, consider $z+z'$ by defintion: $z+z'=[\langle a+b,b+a\rangle]=[\langle a+b,a+b\rangle]$, which again by a previous proposition is the same as the equivalence class $[\langle 0,0\rangle]$, so $z+z'=0_z$, so z' is the additive inverse of z □

We can now define *subtraction*:

DEFINITION 0.23 ⟨**subtraction**⟩

Subtraction *is a binary operator $-:\mathbb{Z}^2\to\mathbb{Z}$ defined as*

$$a-b=a+(-b)$$

Where $-b$ is the additive inverse of $b\in\mathbb{Z}$.

Since subtraction is simply addition of two elements in $\mathbb{Z}$, it is well-defined on $\mathbb{Z}$ since addition is well-defined.

In fact, $(\mathbb{Z}, 0_z, +)$ is our first example of a (abelian) *group*, which is one of the objects of study in abstract algebra.

DEFINITION 0.24 ⟨**group**⟩

A group *is a* monoid *that satisfies the* inverse *property:* $\forall a \in A \exists b \in A$ *s.t.* $a \cdot b = e$

DEFINITION 0.25 ⟨**abelain group**⟩

A group is called abelian *if it the operator* $\cdot$ *commutes, i.e* $\forall a, b \in A, a \cdot b = b \cdot a$*. Equivalently, an abelian group is a commutative monoid that satisfies the inverse property.*

We have already shown that $(\mathbb{Z}, 0_z, +)$ satisfies identity and inverse. Associativity can be proven by explicitly expressing each element as an equivalence class with a representative element and working from definition, using the associativity of addition in $\mathbb{N}$.

The structure $(\mathbb{Z}, 0_z, +, 1_z, \cdot)$ is our first example of a (commutative) *ring*.

DEFINITION 0.26 ⟨**ring**⟩

A ring *is a set* A *equipped with two binary operations which are called* addition *and* multiplication*, denoted* $(+, \cdot)$ *that satisfies:*
1. A *is an abelian group under addition.*
2. A *is a* monoid *under multiplication.*
3. Multiplication is distributive under addition, i.e. $\forall a, b, c \in A$*,* $a \cdot (b + c) = a \cdot b + b \cdot c$ *(left-distributive) and* $(a + b) \cdot c = a \cdot c + b \cdot c$ *(right-distributive).*

DEFINITION 0.27 ⟨**commutative ring**⟩

A commutative ring *is a ring where* multiplication *is also commutative.*

Note that, in a commutative ring, it suffices to show that multiplication is left-distributive (or right-distributive). It can be verified, and left as an exercise, that $(\mathbb{Z}, 0_z, +, 1_z, \cdot)$ is indeed a commutative ring.

Order

We also naturally define order on $\mathbb{Z}$ as an extension of order on $\mathbb{N}$:

DEFINITION 0.28 ⟨**order on Z**⟩

We define strict order and order on $\mathbb{Z}$ *as follows (on the RHS is strict order on* $\mathbb{N}$*):*
1. $[\langle a,b\rangle][\langle c,d\rangle] \iff (a+d)(b+c)$
2. $[\langle a,b\rangle] \leq [\langle c,d\rangle] \iff ([\langle a,b\rangle][\langle c,d\rangle] \vee [\langle a,b\rangle] = [\langle c,d\rangle]$

PROPOSITION 34

order on $\mathbb{Z}$ *is well-defined.*

Proof. Let $\langle a,b\rangle \sim \langle a',b'\rangle$ and $\langle c,d\rangle \sim \langle c',d'\rangle$. We will show that strict-order as defined in 0.28 order on Z is well-defined. Suppose $[\langle a,b\rangle][\langle c,d\rangle]$, i.e. $a+db+c$. By definition of the equivalence relation, we have $a+b'=b+a'$ and $c+d'=d+c'$. We wish to show $[\langle a',b'\rangle][\langle c',d'\rangle]$, i.e. $a'+d'b'+c'$.
1. $a+db+c$ (by hypothesis)
2. $(a+d)+(c'+b')(b+c)+(c'+b')$ (addition preserves order in $\mathbb{N}$)
3. $(a+b')+(d+c')(b'+c')+(b+c)$ (properties of addition in $\mathbb{N}$)
4. $a+b'=b+a'$ (by hypothesis)
5. $c+d'=d+c'$ (by hypothesis)
6. $(b+a')+(d'+c)(b'+c')+(b+c)$ (from $3,4,5$ by substitution)
7. $(a'+d')+(b+c)(b'+c')+(b+c)$ (properties of addition in $\mathbb{N}$)
8. $a'+d'b'+c'$ (addition preserves order in $\mathbb{N}$)

Hence strict-order in $\mathbb{Z}$ is well-defined. In the case of non-strict order, we need to consider the case wehere $[\langle a,b\rangle] = [\langle c,d\rangle]$. Clearly in this case all 4 ordered pairs we considered belong to the same equivalence class, so immediately we get $[\langle a',b'\rangle] = [\langle c',d'\rangle]$, so non-strict order is well-defined as well.

□

Once order is defined, we can define the *sign* of a number:

DEFINITION 0.29 ⟨**sign**⟩

The sign *of a number* $z \in \mathbb{Z}$ *is:*
1. $+$ *(positive) if* $0_{\mathbb{Z}} z$
2. $-$ *(negative) if* $z 0_{\mathbb{Z}}$
3. 0 *is* $0_{\mathbb{Z}} = 0$

It is trivial to show that these are indeed strict order and order relations, and that both are total, based on the definition of on $\mathbb{N}$. We will only show transitivity as an example:

Suppose $[\langle a, b\rangle][\langle c, d\rangle]$ and $[\langle c, d\rangle][\langle e, f\rangle]$, so by definition $(a+d)(b+c)$ and $c+fd+e$. Since addition preserves order on $\mathbb{N}$, then $(a+d)+f(b+c)+f$, and from the commutative and associative properties of addition on $\mathbb{N}$ it follows that $(a+f)+db+(c+f)$. Adding b to both sides of the second relation, we get $b+(c+f)b+(d+e)$. Recall that ab implies $a \in b$, and that natural numbers are transitive sets, so ab and bc implies ac, so it follows that $(a+f)+db+(d+e)$, which can be reordered as $(a+f)+d(b+e)+d$, which from injectivity of addition on $\mathbb{N}$ is true if and only if $a+fb+e$, which is exactly the same as $[\langle a, b\rangle][\langle e, f\rangle]$, so strict order on $\mathbb{Z}$ is transitive (order is transitive as well by a similar argument).

PROPOSITION 35

Addition preserves order in $\mathbb{Z}$.

Proof. We prove for strict-order only. Take $z_1 = [\langle a, b\rangle], z_2 = [\langle c, d\rangle], z_3 = [\langle e, f\rangle], z_4 = [\langle g, h\rangle]$ such that $z_1 z_2$ and $z_3 z_4$. Now consider $z_1 + z_3$. By definition of addition in $\mathbb{Z}$ it follows that $z_1 + z_3 = [\langle a+e, b+f\rangle]$. Similarly, $z_2 + z_4 = [\langle c+g, d+h\rangle]$. By definition, $z_1 + z_3 z_2 + z_4$ if and only if

$$(a+e)+(d+h)(b+f)+(c+g)$$

Since $z_1 z_2$ we have $a+db+c$, and since $z_3 z_4$ we have $e+hf+g$. Since addition preserves order in $\mathbb{N}$ (by Theorem 9 arithemetic properties of the natural numbers which we haven't proven) it follows that $(a+d)+(e+h)(b+c)+(f+g)$. Reordering both sides by commutativity and associativity of addition in $\mathbb{N}$, we retrieve the inequality we set to prove.

□

PROPOSITION 36

Multiplication of non-negative values preserves sign, i.e.

$$\forall a, b \in \mathbb{Z}, (0 \leq a \wedge 0 \leq b \implies 0 \leq a \cdot b)$$

Proof. In the case where $0 = a$ or $0 = b$ it follows that $a \cdot b = 0$ since $\mathbb{Z}$ is a ring, so $0 \leq a \cdot b$. Otherwise suppose $0a$ and $0b$ and write a, b explicitly as $a = [\langle a_1, a_2\rangle], b = [\langle b_1, b_2\rangle]$, then it follows that $a_1 \neq a_2$ and $b_1 \neq b_2$, otherwise they would be equal to 0_z by a previous result. Since $0a, 0b$ then $a_2 a_1, b_2 b_1$. Now consider $a \cdot b$. By definition, this is $[\langle a_1 b_1 + a_2 b_2, a_2 b_1 + a_1 b_2\rangle]$.

Since $a_2 a_1$ then since multiplication preserves order in $\mathbb{N}$ it follows that $a_2 b_1 a_1 b_1$. Similarly, $b_2 b_1 \implies a_1 b_2 a_2 b_2$. Consider the equivalence classes $c = [\langle a_1 b_1, a_2 b_1\rangle]$ and $d = [\langle a_2 b_2, a_1 b_2\rangle]$, and we have just

shown by definition that $0c$ and $0d$, so since addition preserves order in $\mathbb{Z}$ by the previous proposition it follows that $0c + d$, but $c + d$ is simply $[\langle a_1b_1 + a_2b_2, a_2b_1 + a_1b_2] = a \cdot b$, so $0a \cdot b$.

□

PROPOSITION 37 ⟨**product of negative numbers**⟩

The product of negative numbers $a, b \in \mathbb{Z}$ is positive and equal to the product of their additive inverses, i.e. $\forall a, b \in \mathbb{Z}((a0 \wedge b0) \implies a \cdot b = (-a) \cdot (-b) \wedge 00 \cdot b))$.

Proof. Take $a, b \in \mathbb{Z}$ s.t. $a0$ and $b0$. Write a, b in terms of equivalence classes: $a = [\langle a_1, a_2\rangle], b = [\langle b_1, b_2\rangle]$. Consider $a \cdot b$. By definition, $a \cdot b = [\langle a_1b_1 + a_2b_2, a_2b_1 + a_1b_2\rangle]$. It suffices to show that $a \cdot b = (-a) \cdot (-b)$ then by the previous proposition we will have $0a \cdot b$. Work from definition:

$$(-a) \cdot (-b) = [\langle a_2, a_1\rangle] \cdot [\langle b_2, b_1\rangle] = [\langle a_2b_2 + a_1b_1, a_2b_1 + a_1b_2\rangle] = a \cdot b$$

□

DEFINITION 0.30 ⟨**ordered commutative ring**⟩

An ordered commutative ring *is a commutative ring where order is preserved under addition, and if $0 \leq a$ and $0 \leq b$ then $0 \leq a \cdot b$.*

PROPOSITION 38

The structure $(\mathbb{Z}, 0_z, 1_z, +, \cdot,)$ is an ordered commutative ring*.*

Proof. We already know that $(\mathbb{Z}, 0_z, 1_z, +, \cdot)$ is a commutative ring, and we have just shown that the order on $\mathbb{Z}$ satisfies both new properties of an ordered commutative ring, so the structure $(\mathbb{Z}, 0_z, 1_z, +, \cdot,)$ is an ordered commutative ring □

Homomorphism of $\mathbb{N} \to \mathbb{Z}$

It is common to treat the natural numbers as a subset of the integers, i.e. say that $\mathbb{N} \subseteq \mathbb{Z}$. However, in our construction provided above, this is strictly untrue: in fact, $\forall n \in \mathbb{N}, n \notin \mathbb{Z}$, since $\mathbb{Z}$ is the quotient set of $\mathbb{N}^2$ under an equivalence relation $\sim$. We can, however, identify elements of $\mathbb{N}$ with elements of $\mathbb{Z}$ in a way which would preserve the structure of $\mathbb{N}$, i.e. be a *homomorphism* $\mathbb{N} \to \mathbb{Z}$. Once we have such homomorphism, we can forget that $\mathbb{N} \not\subseteq \mathbb{Z}$ as both sets were constructed since we would have a

homomorphism $E : \mathbb{N} \to \mathbb{Z}$ so by abuse of notation we could think of $\mathbb{N}$ as E$[\mathbb{N}]$ when we are dealing with the integers.

DEFINITION 0.31 $\langle$**homomorphism of N** $\to \mathbb{Z}>$

We define $E : \mathbb{N} \to \mathbb{Z}$*, given by* $E(n) = [\langle n, 0\rangle]$.

PROPOSITION 39

E *is a homomorphism with respect to the structure* $(\mathbb{N}, +, \cdot,)$*, i.e.* $\forall m, n \in \mathbb{N}$
1. $E(n + m) = E(n) + E(m)$
2. $E(n \cdot m) = E(n) \cdot E(m)$
3. $nm \iff E(n)E(m)$

Proof. Let $m, n \in \mathbb{N}$.

1. By definition $E(n + m) = [\langle n + m, 0\rangle] = [\langle n + m, 0 + 0\rangle]$, which be definition of addition on $\mathbb{Z}$ is the same as $[\langle n, 0\rangle] + [\langle m, 0\rangle]$, which is $E(n) + E(m)$.
2. By definition $E(n) \cdot E(m) = [\langle n, 0\rangle] \cdot [\langle m, 0\rangle]$, which by definition of multiplication on $\mathbb{Z}$ is $[\langle n \cdot m + 0 \cdot 0, n \cdot 0 + 0 \cdot m\rangle] = [\langle n \cdot m, 0\rangle]$, which is $E(n \cdot m)$ by definition.
3. $E(n)E(m)$ means by definition $[\langle n, 0\rangle]E[\langle m, 0\rangle]$ which is true if and only if $n + 00 + m$, i.e. nm.

□

Rational Numbers

Introduction

In elementary school the introduction of the rational numbers is often motivated by fractions: suppose you have one box of pizza with 8 slices, and you and your friend share the box, each getting 4 slices. How much of the pizza did each of you get? The respective part of 4 from 8, which is the fraction $\frac{4}{8}$, which reduces to $\frac{1}{2}$. Appreciate that this is non-trivial and widely different than how we usually treat the integers: here, $\frac{4}{8} = \frac{1}{2}$, despite the fact that both are clearly different. By now, you probably intuitively guess that to formally construct the rationals, we will define another equivalence relation, in which our representation of $\frac{4}{8}$ and $\frac{1}{2}$ will fall under the same equivalence class, so in that sense it will be no different than stating that $2 - 1 = 3 - 2$, both terms correspond to elements in $\mathbb{N}^2$ belonging to the same equivalent class under the relation we used to define $\mathbb{Z}$.

Now, suppose you add together 8 slices, then you have a whole bow: $8 \cdot \frac{1}{8} = 1$. Recall that a group is a monoid where every element has an inverse, and that $\mathbb{Z}$ is a group under addition, but *not* under

multiplication (for example, given $2 \in \mathbb{Z}$ there is no $z \in \mathbb{Z}$ such that $2 \cdot z = 1$), however now we see that by introducing fractional quantities, we *can* find a multiplicative inverse, so we can form a group under multiplication, and a field under addition and multiplication (we will formally define *field* at a later point).

We then say that *rational numbers* $\mathbb{Q}$ are *all* numbers which can be expressed as fractions, i.e. $q \in \mathbb{Q} \iff \exists n, m \in \mathbb{Z}, q = \frac{n}{m}$, but what is $\frac{n}{m}$, if not some way to denote an ordered pair $\langle n, m \rangle \in \mathbb{Z}^2$? We may be tempted, then, to define $\mathbb{Q}$ as follows:

$$\mathbb{Q} = \{\langle n, m \rangle \in \mathbb{Z}^2 | n, m \in \mathbb{Z}\}$$

While this is a (shorthand for a) WFF in FOL and a valid application of the axiom of schema specification, so $\mathbb{Q}$ is indeed a set, closer inspection reveals that it does not satisfy an elementary property of $\mathbb{Q}$. Namely, by this definition $\langle 4, 8 \rangle$ and $\langle 1, 2 \rangle$, which we identified with $\frac{4}{8}$ and $\frac{1}{2}$, are *distinct* elements. This is no good. But why do we say that they are equal? Can we express this equivalence in terms of operations defined on $\mathbb{Z}$, namely addition, subtraction and multiplication? From middle school, we know that

$$\frac{a}{b} = \frac{c}{d} \iff a \cdot d = b \cdot c$$

This can be reworked to an equivalence relation on $\mathbb{Z}^2$: $\langle a, b \rangle \sim \langle c, d \rangle \iff a \cdot d = b \cdot c$. Then, by taking $\mathbb{Q} = \mathbb{Z} / \sim$, we find that $\langle 4, 8 \rangle \sim \langle 1, 2 \rangle$ so are elements of the same member of $\mathbb{Q}$, so they are *equivalent* in that sense. However, now we have an issue with any $\langle z, 0 \rangle \in \mathbb{Z}^2$: by definition of multiplication, $\forall \langle a, b \rangle \in \mathbb{Z}^2, \langle z, 0 \rangle \sim \langle a, b \rangle$, but then $\mathbb{Z}^2$ is reduced to a single equivalence class. This, also, is no good, and motivates leaving $\frac{z}{0}$ undefined - we do not represent it in $\mathbb{Q}$. Instead, we consider $\mathbb{Z} \times \mathbb{Z}^+$, where $\mathbb{Z}^+$ is the set of all elements $z \in \mathbb{Z}$ such that $0z$.

Observe that this construction *immediately* lets us define division: $a \div b$ is given by *any* element of the equivalence class $[\langle a, b \rangle]$. We can then define addition and multiplication on $\mathbb{Q}$ in a way that would correspond to our expected behavior of those operations on fractions.

Let's formalize this discussion.

Constructing Rational Numbers

DEFINITION 0.32 ⟨**rational numbers**⟩

Define an equivalence relation $\sim$ *on* $\mathbb{Z} \times \mathbb{Z}^+$ *such that* $\langle a, b\rangle \sim \langle c, d\rangle \iff a \cdot d = b \cdot c$ *(this is multiplication on the* integers*, not on the natural numbers).*
The set of rational numbers*,* $\mathbb{Q}$*, is given by* $\mathbb{Q} = \mathbb{Z}^2 / \sim$*.*

The reader can verify that $\sim$ is indeed an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^+$.

DEFINITION 0.33 ⟨**identity elements of Q**⟩

We define 0_Q *(which will serve as the additive identity) as* $0_Q = [\langle 0, 1\rangle]$*, and* 1_Q *(multiplicative identity) as* $1_Q = [\langle 1, 1\rangle]$*.*

DEFINITION 0.34 ⟨**fraction**⟩

Given $\langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}^+$*, we call* $\langle a, b\rangle$ *a* fraction *and express it as* $\frac{a}{b}$*, with the property that* $\frac{a}{b} = \frac{c}{d} \iff [\langle a, b\rangle] = [\langle c, d\rangle]$*, i.e. if both belong to the same element of* $\mathbb{Q}$*.*

We define addition and multiplication on elements of $\mathbb{Q}$ as we would expect addition and multiplication of fractions to behave, namely that $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot}{b \cdot d}$:

DEFINITION 0.35 ⟨**rational arithemetic**⟩

We define addition $+ : \mathbb{Q}^2 \to \mathbb{Q}$ *and multiplication* $\cdot : \mathbb{Q}^2 \to \mathbb{Q}$ *as follows*
1. $[\langle a, b\rangle] + [\langle c, d\rangle] = [\langle a \cdot d + b \cdot c, b \cdot d\rangle]$
2. $[\langle a, b\rangle] \cdot [\langle c, d\rangle] = [\langle a \cdot c, b \cdot d\rangle]$

PROPOSITION 40

Addition and multiplication on $\mathbb{Q}$ *is well defined.*

Proof. We start with addition: suppose $[\langle a, b\rangle] \sim [\langle a', b'\rangle]$ and $[\langle c, d\rangle] \sim [\langle c', d'\rangle]$, then $a \cdot b' = b \cdot a'$ and $c \cdot d' = d \cdot c'$. Now consider $[\langle a, b\rangle] + [\langle c, d\rangle]$ and $[\langle a', b'\rangle] + [\langle c', d'\rangle]$. By definition they evaluate to $[\langle a \cdot d + b \cdot c, b \cdot d\rangle]$ and $[\langle a' \cdot d' + b' \cdot c', b' \cdot d'\rangle]$. To show both are equivalent under $\sim$, we need to show that

$$(a \cdot d + b \cdot c) \cdot (b' \cdot d') = (b \cdot d) \cdot (a' \cdot d' + b' \cdot c')$$

We will show that his equation holds using the properties of addition and multiplication on $\mathbb{Z}$ (since a, b, c, d are all elements of $\mathbb{Z}$). Namely, recall that $\mathbb{Z}$ is a commutative field under addition and multiplication. Then,

$(a \cdot d + b \cdot c) \cdot (b'$ $adb'd' + bcb'd' =$

$\cdot d') =$

So addition is well-defined. As for multiplication, we need to show that $(a \cdot c) \cdot (b' \cdot d') = (a' \cdot c') \cdot (b \cdot d)$. Reordering the LHS, we get $(ab')(cd') = (ba')(dc') = (a' \cdot c') \cdot (b \cdot d)$, so multiplication is well-defined as well.

□

DEFINITION 0.36 ⟨**multiplicative inverse**⟩

A multiplicative inverse *of an element a is an element b such that $a \cdot b = e_\times$, where $e_\times$ is the multiplicative identity. We denote such b as a^{-1} or $\frac{1}{a}$.*

Note that being a multiplicative inverse is symmetric - i.e. a, a^{-1} are each other's multiplicative inverse.

PROPOSITION 41

For any $q \in \mathbb{Q}$ such that $q \neq 0_Q$, $\exists p \in \mathbb{Q}$ s.t. p is the multiplicative inverse of q, i.e. $q \cdot p = 1_Q$, and if $q = [\langle a, b \rangle]$ such that $a \neq 0_Z$ (i.e. $q \neq 0_Q$), then that q is given by $[\langle b, a \rangle]$.

Proof. Take $a, b \in \mathbb{Z}$ s.t. $a \neq 0$, then $[\langle a, b \rangle] \cdot [\langle b, a \rangle] = [\langle a \cdot b, a \cdot b \rangle]$. To show that this is the same equivalence class as that of 1_Q, we need to show that $\langle ab, ab \rangle \sim \langle 1, 1 \rangle$ under the equivalence relation, and indeed since 1_Z is the multiplicative identity on $\mathbb{Z}$ it follows that $(ab) \cdot 1 = ab$ and $1 \cdot (ab) = ab$ (since multiplication is commutative in $\mathbb{Z}$ as a commutative field), so $[\langle a, b \rangle] \cdot [\langle b, a \rangle] = [\langle 1, 1 \rangle] = 1_Q$, so $[\langle b, a \rangle]$ is the multiplicative inverse of $[\langle a, b \rangle]$ □

Using this property we can define *division* on $\mathbb{Q}$:

DEFINITION 0.37 ⟨**division**⟩

Division on $\mathbb{Q}$ *is a binary operator* $\div : \mathbb{Q}^2 \to \mathbb{Q}$ *defined as*

$$a \div b = a \cdot b^{-1}$$

Where b^{-1} *is the multiplicative inverse of* b*.*

Since division is defined in terms of multiplication, it is well-defined as a function since multiplication is well-defined on $\mathbb{Q}$ as we have shown.

To re-introduce subtraction, we use 0.23 subtraction adjusted for $\mathbb{Q}$. To show that it is well-defined, it suffices to show that $\forall q \in \mathbb{Q} \exists p \in \mathbb{Q}$ s.t. $q + p = 0$, which we prove in the following lemma.

LEMMA 9.1

$\forall q \in \mathbb{Q}$ *there exists an additive inverse* $p \in \mathbb{Q}$ *such that* $q + p = 0_Q$*.*

Proof. Recall that $0_Q = [\langle 0, 1\rangle]$. Take some $q \in \mathbb{Q}$, so $\exists a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$ s.t. $q = [\langle a, b\rangle]$. Now, take $-a \in \mathbb{Z}$, the additive inverse of a, which exists since $\mathbb{Z}$ is a ring, and denote $p = [\langle -a, b\rangle]$. Now, work $q + p$ by definition: $q + p = [\langle ab - ab, b \cdot b\rangle] = [\langle 0, b \cdot b\rangle]$. Now since $0 = 0 \implies 0 \cdot (b \cdot b) = 1 \cdot 0$, it follows that $\langle 0, 1\rangle \sim \langle 0, b \cdot b\rangle$, so $[\langle 0, b \cdot b\rangle] = [\langle 0, 1\rangle] = 0_Q$, so p is the additive inverse of p. □

$\mathbb{Q}$ is our first example of a *field*.

DEFINITION 0.38 ⟨**field**⟩

A field *is a structure* $(A, 0, 1, +, \cdot)$ *where* A *is a set,* $+, \cdot$ *are binary operations on* A *called addition and multiplication,* 0 *is the additive identity and* 1 *is the multiplicative identity, such that the structure is a* commutative ring *and also* all nonzero elements *of* A *have a multiplicative inverse in* A*.*

To verify that $(\mathbb{Q}, 0_Q, 1_Q, +, \cdot)$ is a field, one needs to verify that $\mathbb{Q}$ satisfies all field axioms. We have already shown that $\mathbb{Q}$ has an additive inverse for every element and a multiplicative inverse for every nonzero element. Satisfying the rest of the axioms follows from properties of $\mathbb{Z}$ as a commutative ring, and is left as an exercise.

To make $\mathbb{Q}$ an *ordered* field, we need to introduce *order* on $\mathbb{Q}$.

DEFINITION 0.39 ⟨order on Q⟩

We define strict order and order on $\mathbb{Q}$ as follows:
1. $[\langle a,b\rangle][\langle c,d\rangle] \iff a\cdot db\cdot c$
2. $[\langle a,b\rangle]\leq[\langle c,d\rangle] \iff a\cdot db\cdot c\vee[\langle a,b\rangle]=[\langle c,d\rangle]$
Where $a,c\in\mathbb{Z}$ and $b,d\in\mathbb{Z}^+$.

We know the order show hold since

PROPOSITION 42

Order on $\mathbb{Q}$ is indeed an order, and total.

Proof. We only prove the proposition for strict order, the proof for non-strict order follows trivially as a corollary.

Irreflexive: take $[\langle a,b\rangle]$, then $[\langle a,b\rangle][\langle a,b\rangle]$ if and only if $a\cdot bb\cdot a$, which is impossible since multiplication commutes on $\mathbb{Z}$ and on $\mathbb{Z}$ is a strict order, hence irrefleixve.

Assymetric: Take $[\langle a,b\rangle]$ and $[\langle c,d\rangle]$ and suppose $[\langle a,b\rangle][\langle c,d\rangle]$, then it follows $a\cdot db\cdot c$, so from the assymetry of $_{\mathbb{Z}}$ as a strict order then it follows that $b\cdot c\not a\cdot d$.

Transitivity: Take $[\langle a,b\rangle],[\langle c,d\rangle],[\langle f,e\rangle]$ such that $a\cdot d_{\mathbb{Z}}b\cdot c$ and $c\cdot e_{\mathbb{Z}}d\cdot f$. To show $_{\mathbb{Q}}$ is transitive, we need to show that $a\cdot e_{\mathbb{Z}}b\cdot f$. Now, recall that $\mathbb{Q}$ is a quotient set of $\mathbb{Z}\times\mathbb{Z}^+$, i.e. $0b,0d,0e$, so by the properties of an ordered ring ($\mathbb{Z}$) it follows that $adbc \implies adebce$ and $cedf \implies bcebdf$, so by transitivity of $_{\mathbb{Z}}$ it follows that $adebdf$, and by the properties of multiplication we get $(ae)d(bf)d$, so $aebf$.

Total: Take $[\langle a,b\rangle],[\langle c,d\rangle]$. We wish to show that if $[\langle a,b\rangle]\neq[\langle c,d\rangle]$, either $[\langle a,b\rangle][\langle c,d\rangle]$ or $[\langle c,d\rangle][\langle a,b\rangle]$. Suppose $[\langle a,b\rangle]\not[\langle c,d\rangle]$, then $a\cdot d\not b\cdot c$, so by totality of strict order in $\mathbb{Z}$ it follows that $b\cdot ca\cdot d$, so $[\langle a,b\rangle]\not[\langle c,d\rangle]\implies[\langle c,d\rangle][\langle a,b\rangle]$.

□

It can be shown that the order on $\mathbb{Q}$ is preserved by addition and that if $0\leq q,0\leq p$ it follows that $0\leq q\cdot p$ by using the definitions of multiplication and addition on $\mathbb{Q}$ and the fact that $\mathbb{Z}$ was shown to be an ordered field, so we conclude that $(\mathbb{Q},0_Q,1_Q,+,\cdot,)$ is an *ordered field*.

Homomorphism $\mathbb{Z}\to\mathbb{Q}$

Similarly to our construction of $\mathbb{Z}$ where we ran into the issue that strictly speaking $\mathbb{N}\not\subseteq\mathbb{Z}$ as one would expect, and solved that issue via a homomorphism, we run into the same issue with $\mathbb{Z}$ and $\mathbb{Q}$

since, strictly speaking, $\mathbb{Z} \not\subseteq \mathbb{Q}$. Again, we solve this issue via a homomorphism:

DEFINITION 0.40 ⟨**homomorphism of Z** $\to \mathbb{Q}$⟩

Let $E : \mathbb{Z} \to \mathbb{Q}$ *be given by* $E(z) = [\langle z, 1\rangle]$*, then* E *is an ordered commutative ring homomorphism, i.e. the properties of* $\mathbb{Z}$ *as an ordered commutative ring are preserved by* E*.*

It needs to be shown that E is indeed an ordered commutative ring homomorphism. To do that, we need to verify that all properties of $\mathbb{Z}$ as an ordered commutative ring are preserved under E. We will show a few examples, and leave the rest to the reader:

1. $E(a \cdot b) = [\langle a \cdot b, 1\rangle] = [\langle a, 1\rangle] \cdot [\langle b, 1\rangle]$ (multiplication is preserved)
2. $E(a + b) = [\langle a + b, 1\rangle] = [\langle a, 1\rangle] + [\langle b, 1\rangle]$ (addition is preserved)
3. $a \leq b \implies a \cdot 1 \leq b \cdot 1 \implies [\langle a, 1\rangle] \leq [\langle b, 1\rangle] \implies E(a) \leq E(b)$ (order is preserved)

Real Numbers

Introduction

Consider $\mathbb{Q}$, which informally is the set of all numbers which can be expressed as $\frac{a}{b}$ where $a, b \in \mathbb{Z}, b \neq 0$. In $\mathbb{Q}$ we define a new term:

DEFINITION 0.41 ⟨**square root**⟩

A number a *is the* square root *of some number* n*, denoted* $\sqrt{n}$*, if* $\sqrt{n} \cdot \sqrt{n} = a$*.*

Consider the following proposition:

$$\forall x \in \mathbb{Q} \exists y \in \mathbb{Q} \text{ s.t. } y \cdot y = x$$

Is the proposition true? Let's try a few examples. Take $4 \in \mathbb{Q}$, then $2 \cdot 2 = 4$ (this is easy to verify by composition of $E_1 : \mathbb{N} \to \mathbb{Z}$ and $E_2 : \mathbb{Z} \to \mathbb{Q}$), so 2 is a square root of 4. But also $(-2) \cdot (-2) = 4$, so -2 is also a square root of 4. To have any hope of defining $\sqrt{}$ as a function, we need it to be well-defined for every value in its domain, so we can restrict the negative values which, when timed with themselves, equal to the value we wish to take the root of, by stating that we are only looking for y s.t. $0 \leq y$.

Let's take another example: $\frac{1}{4}$. It can be shown by definition of multiplication in $\mathbb{Q}$, then $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. In fact, it follows directly from the fact that the multiplicative inverse of a rational number $[\langle a, b\rangle]$ in $\mathbb{Q}$ is $[\langle b, a\rangle]$ and the fact that 2 is the square root of 4, and we map natural number to $\mathbb{Q}$ as $n \mapsto [\langle n, 1\rangle]$.

Now take 2.

THEOREM 10 $\langle \sqrt{2} is irrational >$

There exists no $q \in \mathbb{Q}$ *such that* $q \cdot q = 2$*, i.e.* $\sqrt{2}$ *is* irrational *(i.e. it is not in* $\mathbb{Q}$*).*

Proof. Suppose by contradiction that $\sqrt{2}$ is rational, so take $a \in \mathbb{Z}, b \in \mathbb{Z}^+$ with no common factors (i.e. $\nexists \alpha \in \mathbb{N}$ s.t. $\langle a, b\rangle \sim \langle \alpha c, \alpha d\rangle$ for some $c \in \mathbb{Z}, d \in \mathbb{Z}^+$, where $\sim$ is the equivalence relation used to defined $\mathbb{Q}$) such that $[\langle a, b\rangle] \cdot [\langle a, b\rangle] = [\langle a \cdot a, b \cdot b\rangle] = [\langle 2, 1\rangle]$, which means that $a^2 = 2b^2$, so a^2 is even. By 29 it follows that a^2 is even if and only if a is even, so $a = 2m$ for some m. Substituting $2m$ for a, we have $(2m)^2 = 2b^2 \Rightarrow 4m^2 = 2b^2 \Rightarrow b^2 = 2m^2$, so b is also even, but then a, b have a common factor, a contradiction, so 2 does not have a square root in $\mathbb{Q}$ □

.

But is this an issue? Do we have any reason to consider the construction of such numbers at all? The answer is yes, and I will present two reasons, one elementary and the other a bit more advanced.

The first reason is a geometric one: recall the Pythagorean theorem, which states that the length of the hypotenuse of a right triangle is equal to the square root of the sum of squares of its sides, i.e. $c = \sqrt{a^2 + b^2}$, where a, b are the measures of the sides and c is the measure of the hypotenuse. Clearly right triangles manifest in the real world, either naturally or by construction. Now consider the case where $a = b = 1$, we get $c = \sqrt{2}$, so $\sqrt{2}$ must have some form of existence since it is the measure of the hypotenuse!

Another reason, related to calculus, is the following: there exist Cauchy sequences which do not converge in the metric space $\mathbb{Q}$ with the common Euclidean metric, and it would be beneficial to complete $\mathbb{Q}$ to a metric space where all Cauchy sequences converge (we call such metric space a *Banach space*). I have discussed about Cauchy sequences and Banach spaces in Differential Calculus.

Hopefully this provides enough motivation for the *completion* of the rationals. By completing the rationals, we construct the *real numbers*, or the *real line*, denoted $\mathbb{R}$. We naturally extend all operations defined in $\mathbb{Q}$ to $\mathbb{R}$, and as should be expected $\mathbb{R}$ will also be an ordered field.

Constructing the Real Numbers

One way to construct the real numbers had essentially already been described in the previous section: take the metric space $(\mathbb{Q}, ||\cdot||_{\text{euclid}})$ and *complete* it by adding the limits of all Cauchy sequences to the set on which the metric is defined. However, this construction relies on definition of sequences, Cauchy sequences, limits and convergence, which, although they can already be established given the current collection of mathematical objects we know how to represent using ZF set theory, is a bit less

elegant in my opinion since it is a big shift from how we constructed the sets $\mathbb{N}, \mathbb{Z}$ and $\mathbb{Q}$. There is also the issue of where those elements, which we take as the limits of Cauchy sequences, come from.

Instead, we opt for a more set theoretic construction called *Dedekind cuts*. The idea of a Dedekind cut is to identify real numbers with subsets of $\mathbb{Q}$ (i.e. each Dedekind cut x is a member of the power set $\mathcal{P}(\mathbb{Q})$), such that each subset x is the subset of $\mathbb{Q}$ that contains all elements in $\mathbb{Q}$ that are strictly smaller than the number we wish x to represent. For example, consider $\frac{1}{2} \in \mathbb{Q}$, we identify its Dedekind cut as the set of all elements in $\mathbb{Q}$ that are strictly below $\frac{1}{2}$, and call this set $\frac{1}{2}_{\mathbb{R}}$, i.e. that set is identified with the *real* number $\frac{1}{2}$. This also lets us define $\sqrt{2}$: by definition we want $\sqrt{2}$ to satisfy $\sqrt{2} \cdot \sqrt{2} = 2$, so the Dedekind cut of $\sqrt{2}$ would be the set of all rational numbers $\mathbb{Q}$ such that $\sqrt{2} = \{q \in \mathbb{Q} | q^2 2 \vee q 0\}$. We call these *cuts* since the *cut* $\mathbb{Q}$ to two subsets, that of the cut and its complement (i.e the set $\mathbb{Q} \setminus \sqrt{2}$).

Imagine this construction as follows: draw a line, then pick one point and a direction which implies the order of points on the line, highlight all points along that direction except for the point that you picked, this is the Dedekind cut that uniquely identifies the point.

Formally, we define a Dedekind cut as follows:

DEFINITION 0.42 ⟨**Dedekind cut**⟩

A Dedekind cut is a set $X \subseteq \mathbb{Q}$ such that:
1. X is a proper subset of $\mathbb{Q}$, i.e. $X \neq \emptyset$ and $X \neq \mathbb{Q}$.
2. X is closed downwards under the order $_{\mathbb{Q}}$, i.e. $\forall p \in \mathbb{Q}(\exists q(q \in \mathbb{X} \wedge pq) \implies (p \in \mathbb{Q}))$ (if q is an element of X then all rational numbers that are strictly less than q are also in X)
3. X has no largest element, i.e. $\forall x \in X \exists y \in X$ s.t. xy.

We then take $\mathbb{R}$ to be the set of all Dedekind cuts, and call it the *real line* or the *set of real numbers*.

DEFINITION 0.43 ⟨**real line**⟩

The set of real numbers or the real line*, denoted $\mathbb{R}$, is the set of all Dedekind cuts on $\mathbb{Q}$.*

EXAMPLE 10.1 ⟨**Dedekind cut of $\sqrt{2}$**⟩

As we have stated before, the Dedekind cut of $\sqrt{2}$ is given by

$$\sqrt{2} = \{q \in \mathbb{Q} | q^2 2 \wedge q 0\}$$

In our construction of the real line, this set is $\sqrt{2}$.

Order

Since $\mathbb{R}$ is defined using Dedekind cuts that are themselves defined via the order $_{\mathbb{Q}}$, it is natural to define order in $\mathbb{R}$ before discussing arithmetic.

DEFINITION 0.44 ⟨**order on R**⟩

We define order *on* $\mathbb{R}$ *as follows:*
1. $a \leq b \iff a \subseteq b$
2. $ab \iff a \subset b$

PROPOSITION 43

Order relation on $\mathbb{R}$ *is total.*

Proof. First we note that 0.44 order on R indeed defines strict and non-strict order, this follows immediately from the properties of inclusion. To show that both orders are total, consider $a, b \in \mathbb{R}$. Suppose $a \neq b$, then we wish to show that $a \not\subset b \implies b \subset a$. Take some $x \in b$. Suppose by contradiction that $\nexists y \in a$ s.t. $x_{\mathbb{Q}}y$, then since order on $\mathbb{Q}$ is total it follows that $\forall y \in a, y \leq_{\mathbb{Q}} x$, and since $x \in b$ and b is closed down (since it is a Dedekind cut) it follows that $\forall y \in a, y \in b$, but then $a \subset b$, a contradiction, so $\forall x \in b \exists y \in a$ s.t. $x_{\mathbb{Q}}y$, but since a is also a Dedekind cut, it is also closed downwards, so $\forall x \in b, x \in a$, so $b \subset a$, so strict order is total. If $a = b$, we trivially have $a \leq b$, so non-strict order is also total.

□

Once order has been defined, we can define an *upper bound* of a subset of reals:

DEFINITION 0.45 ⟨**upper bound**⟩

Given a set of real numbers $X \subseteq \mathbb{R}$*, an* upper-bound *on* X *is a real number* $M \in \mathbb{R}$ *s.t.* $\forall x(x \in X \implies x \leq M)$*. i.e.* M *is greater than all numbers belonging to* X*. Equivalently using union notation, we write that* $(\cup X) \cup \{M\}$ *has* M *as its biggest element.*

Similarly, we define an upper bound on a set in $\mathbb{Q}$ as a rational number $q \in \mathbb{Q}$ s.t. it is greater than or equal to all numbers in that set.

To prove interesting properties on the upper bound, we need to define a homomorphism from $\mathbb{Q}$ to $\mathbb{R}$.

Homomorphism of $\mathbb{Q} \to \mathbb{R}$

By the construction of $\mathbb{R}$ via Dedekind cuts, it is tempting to define the homomorphism $\mathbb{Q} \to \mathbb{R}$ as follows:

DEFINITION 0.46 $\langle$**homomorphism of Q** $\to \mathbb{R}>$

$E : \mathbb{Q} \to \mathbb{R}$ *is given by* $E(q) = \{p \in \mathbb{Q} | pq\}$.

Verify that the $E(q)$ is indeed a Dedekink cut on $\mathbb{Q}$:
1. $q \in \mathbb{Q}$ and $q \notin E(q)$ so $E(q) \neq \mathbb{Q}$, and also since $\forall q \in \mathbb{Q}$ we can take $q - 1$ which by definition will satisfy $q - 1q$ so $E(q)$ is not empty, so it is a proper subset.
2. Take some $p_1 \in E(q)$, and consider $p_2 \in \mathbb{Q}$ such that $p_2 p_1$. Since $p_1 \in E(q)$ then $p_1 q$, by transitivity of the order on $\mathbb{Q}$ it follows that $p_2 q$, so $p_2 \in E(q)$, so $E(q)$ is closed downwards.
3. Suppose by contradiction that there exists a larger element $m \in E(q)$, so m also satisfies mq. Now, consider $m + \frac{q-m}{2}$. Clearly it is still less than q so it is in $E(q)$ by definition, but also $mm + \frac{q-m}{2}$, contradicting the maximallity of m, so $E(q)$ has no biggest element.

We haven't yet defined addition and multiplication on $\mathbb{R}$, so we still can't verify that E is indeed an ordered-field homomorphism, but for now we will show that it is well-behaved with respect to order, i.e. it preserves the order on $\mathbb{Q}$.

PROPOSITION 44

Order is preserved under E*, i.e.* $p \leq_{\mathbb{Q}} q \implies E(p) \leq_{\mathbb{R}} E(q)$.

Proof. Take $p, q \in \mathbb{Q}$ s.t. $p \leq_{\mathbb{Q}} q$. If $p =_{\mathbb{Q}} q$, then $E(p) = E(q)$ trivially, so consider the case when p is strictly smaller than q, i.e. $p_{\mathbb{Q}} q$. By definition $E(p) = \{a \in \mathbb{Q} | ap\}$ and $E(q) = \{a \in \mathbb{Q} | aq\}$. We wish to show that $E(p) E(q)$ by definition, which means we wish to show that $E(p) \subset E(q)$. Let $a \in E(p)$, then $a_{\mathbb{Q}} p$, so by transitivity $a_{\mathbb{Q}} q$, so since $E(q)$ is closed downwards, $a \in E(q)$, hence $E(p) \subseteq E(q)$. To show that $E(p)$ is a proper subset of $E(q)$, consider $p + \frac{q-p}{2}$, which is strictly greater than p and strictly smaller than q, so it is a member of $E(q)$ but not of $E(p)$, so $E(p) \subset E(q)$, which by definition means $E(p)_{\mathbb{R}} E(q)$.

□

Once we have define addition and multiplication, we can verify that E is an ordered-field homomorphism. Then we can forget about $\mathbb{Q}$ and consider the set of rational numbers to be the image $E[\mathbb{Q}]$.

Via the homomorphism we can prove a useful property on the rationals in the reals:

THEOREM 11 ⟨**density of the rationals in the reals**⟩

The rationals are dense in $\mathbb{R}$*, meaning that* $\forall x, y \in \mathbb{R}$ *such that* xy*,* $\exists q \in \mathbb{Q}$ *such that* $xE(q)y$*.*

Proof. Take $x, y \in \mathbb{R}$ such that xy, so by definition of strict order on $\mathbb{R}$, $xy \implies x \subset y$, so $\exists q \in y$ such that $q \notin x$ and $\forall p \in x, pq$ (otherwise we would have some $p \in x$ that is greater then q and since x is closed downwards it would follow that $q \in x$, contradicting $q \notin x$). This q is a rational number, i.e. $q \in \mathbb{Q}$, so it corresponds to a Dedekind cut $E(q) = \{p \in \mathbb{Q} | pq\}$. Clearly $xE(q)$ since $\forall p \in x, pq$ as we have shown. Similarly, since $q \in y$ and y is a Dedekind cut, q can't be the biggest element in y, so $\exists w \in y$ s.t. qw, so $E(q)y$. Putting everything together, we get $xE(q)y$ for some $q \in \mathbb{Q}$.

□

COROLLARY 11.1 ⟨**density of the rationals in themselves**⟩

The rationals are dense in $\mathbb{Q}$*, i.e.* $\forall x, y \in \mathbb{Q}$ *s.t.* xy*,* $\exists q \in \mathbb{Q}$ *s.t.* xqy*.*

Proof. Suppose xy. Since E preserves order, $E(x)E(y)$. By density of the rational in the reals, $\exists q \in \mathbb{Q}$ s.t. $E(x)E(q)E(y)$. Again since E preserves order, it follows that xq and qy.

□

The theorem can also be proven purely in $\mathbb{Q}$, by considering $x, y \in \mathbb{Q}$ s.t. xy and $x + \frac{y-x}{2}$. It needs to be shown that $x + \frac{y-x}{2}$ is greater than x and less than y. In fact, we have already used this property multiple times without proof. Let's prove it

PROPOSITION 45 ⟨**midpoint of rationals**⟩

Let $x, y \in \mathbb{Q}$ *s.t.* xy*, then* $\exists (x + \frac{y-x}{2}) \in \mathbb{Q}$ *s.t.* $x(x + \frac{y-x}{2})y$*. We call* $x + \frac{y-x}{2}$ *the* midpoint *of* x *and* y*.*

Proof. Start with xy. Consider $x + \frac{y-x}{2}$, which simplifies to $\frac{1}{2}(x + y)$. Since multiplication by non-negative numbers preserves order in $\mathbb{Q}$, we can write $xy \implies \frac{1}{2}x\frac{1}{2}y$. Also, since addition preserves order in $\mathbb{Q}$, we can write $\frac{1}{2}x + \frac{1}{2}x\frac{1}{2}y + \frac{1}{2}x \implies x\frac{1}{2}(x + y)$ (we used the distributive property of multiplication over addition in the last transition). Similarly, if we start from $\frac{1}{2}x\frac{1}{2}y$ and add $\frac{1}{2}y$ to both sides, we retrieve $\frac{1}{2}(x + y)y$, which completes the proof.

□

Supremum

In the section, we provide interesting properties on upper bounds in $\mathbb{R}$.

PROPOSITION 46 ⟨**existence of an upper bound for a Dedekind cut**⟩

For every Dedekind cut x, there exists an upper bound in $\mathbb{Q}$, and this upper bound q also satisfies $x \leq_{\mathbb{R}} E(q)$.

Proof. Since x is a Dedekind cut, it is a proper subset of $\mathbb{Q}$ and closed downwards so if $\nexists q \in \mathbb{Q}$ s.t. $\forall p \in x(p \leq q)$ then $\forall q \in \mathbb{Q} \exists p \in x(qp) \implies q \in x \implies x = \mathbb{Q}$ contradicting the properness of x. A stronger claim is also true: $\forall p \in x(pq)$: suppose $\exists p \in x$ s.t. $p = q$, then p is the biggest element in x, contradicting the property that x has no biggest element. In fact, this q satisfies $x \leq E(q)$ since $\forall p \in x, pq$ so by definition $x \subseteq E(q)$, so $x \leq E(q)$, this proves that for each Dedekind cut, we can find an upper bound for the cut. □

COROLLARY 11.2

For real number x, there exists a real number y s.t. xy.

Proof. By the theorem $\exists q \in \mathbb{Q}$ s.t. $x \leq E(q)$. Take $q + 1 \in \mathbb{Q}$. Since $qq + 1$ and E preserves order, it follows that $E(q)E(q + 1)$, so by transitivity $xE(q + 1)$, so $y = E(q + 1)$ is strictly greater than x □

PROPOSITION 47 ⟨**union of bounded Dedekind cuts is a Dedekind cut**⟩

Given $A \subset \mathbb{R}$ s.t. A has an upper bound, it follows that $\cup A$ is a real number, i.e. a Dedekind cut.

Proof. 1. Since Dedekind cuts are nonempty proper subsets of $\mathbb{Q}$, it follows that their union is also nonempty, so either $\cup A = \mathbb{Q}$ or $\cup A \subset \mathbb{Q}$. Since A has an upper bound then $\exists r \in \mathbb{R}$ s.t. $\forall a \in A, a \leq r$, which by definition gives $a \subseteq r$. By the corollary of 46 existence of an upper bound for a Dedekind cut it follows that $\exists q \in \mathbb{R}$ s.t. $q \notin r$ and $rE(q)$. Suppose $\exists a \in A, q \in a$. Since a is closed downwards, this would imply $E(q) \leq a$ and also $a \leq r$ so $E(q) \leq r$, but $rE(q + 1)$, a contradiction, so $(q + 1) \notin a$, which implies $E(q + 1) \notin \cup A$, so $\cup A$ is a proper subset.
3. $\cup A$ is closed downwards since otherwise some member of A would not be closed downwards so it would not be a Dedekind cut.
4. $\cup A$ has no largest element, since otherwise that element would belong to some $x \in A$, but then it would also be the largest element of x, and since x is a Dedekind cut it has no largest element, a

contradiction.

□

DEFINITION 0.47 ⟨**supremum**⟩

Given a subset $A \subset \mathbb{R}$, the supremum *on A, or the* least-upper-bound *on A, is a real number $M \in \mathbb{R}$ s.t. it is an upper bound on A (i.e. $\forall a \in A, a \leq M$)* and $\forall r \in \mathbb{R}$ *s.t. rM, r is not an upper bound on A (i.e. $\exists a \in A$ s.t. ra). We denote the supremum as sup(A).*

Similarly, the supremum of a Dedekind cut is the least upper bound on the Dedekind cut.

PROPOSITION 48

If $x \in \mathbb{R}$ is given by $E(q)$ for some $q \in \mathbb{Q}$, then $q =$ sup(x).

Proof. By definition $x = \{p \in \mathbb{Q} | pq\}$, so q is an upper bound on x and if $pq, p \in x$ and hence not a bound on x, so $q = \sup(x)$ □

PROPOSITION 49

The supremum of a Dedekind cut is not a member of the cut.

Proof. Let A be a cut and suppose $\sup(A) \in A$, then $\exists a \in A$ s.t. $\forall a' \in A, a' \leq \sup(A)$, contradicting that A has no biggest element. □

PROPOSITION 50 ⟨**supremum defines Dedekind cut**⟩

Given $x, y \in \mathbb{R}$ whose supremums are attained (i.e. exist), $x = y \iff$ sup$(x) =$ sup(y).

Proof. $\implies$ is immediate since $x = y$. $\impliedby$ Let $x, y \in \mathbb{R}$ and suppose $\sup(x) = \sup(y)$. Suppose $x \neq y$, so either $x \subset y$ or $y \subset x$ as we have seen before (since x, y are Dedekind cuts so this is implied by the fact that both are closed downwards). Suppose $x \subset y$, then $\exists y' \in y$ s.t. $y' \notin x$, so $\forall x' \in x, x'y'$, otherwise y' would be in x since x is closed downwards. Since $\sup(x)$ is the supremum on x', it follows that $\sup(x) \leq y'$. Since $\sup(y)$ is the supremum on y, it follows $y'\sup(y)$, but since $\sup(x) = \sup(y)$, we have $\sup(x) \leq y'\sup(y)$, which is impossible, so $x = y$. □

PROPOSITION 51 ⟨**existence of a supremum**⟩

If $A \subset \mathbb{R}$ has an upper bound, then it has a supremum, and the supremum is given by $\cup A$.

Proof. By 47 union of bounded Dedekind cuts is a Dedekind cut it follows that $\cup A \in \mathbb{R}$. Since $\cup A$ is the union on A it follows that $\forall a \in A, a \subseteq \cup A$ tautologically, which means $\forall a \in A, a \leq \cup A$, so $\cup A$ is an upper bound on A. It remains to show that $\cup A$ is the *least* upper bound.

Suppose not, then $\exists M \in \mathbb{R}$ s.t. $M \cup A$ and M is an upper-bound on $\mathbb{R}$. By Theorem 11 density of the rationals in the reals, $\exists q \in \mathbb{Q}$ s.t. $ME(q) \cup A$, but since $E(q) \cup A$ it follows that $q \in \cup A$, which means that $\exists a \in A$ s.t. $E(q) \leq a$, so by transitivity $M \leq a$, so M is not an upper bound on A, a contradiction, thus $\cup A$ is minimal.

□

Addition

We begin with a brief informal discussion on the question of how to define $x + y$ in $\mathbb{R}$. Since the elements of $\mathbb{R}$, our definition needs to send (x, y) to a Dedekind cut, in particular it needs to be closed downwards. We would also addition in $\mathbb{R}$ to be defined in terms of addition in $\mathbb{Q}$, since if x, y correspond to $E(q), E(p)$ we wish for $E(q + p)$ to be equal to $E(q) + E(p)$ since we want E to be a field homomorphism, but $E(q + p)$ is the set of all rationals that are smaller than $q + p$, where $q + p$ is the smallest combination of rationals not in $E(q), E(p)$. This motivates the following definition:

DEFINITION 0.48 ⟨addition on R⟩

Addition on $\mathbb{R}$ is defined as follows:

$$x +_{\mathbb{R}} y = \{q \in \mathbb{Q} | \exists t \in x \exists s \in y (qt + s)\}$$

i.e. addition results in the set of all rational numbers that are smaller than a sum of rational numbers that belong to x and y, one from each set.

PROPOSITION 52

Addition on $\mathbb{R}$ is well-defined.

Proof. To show that addition is well-defined, we need to show that $\forall x, y \in \mathbb{R}$, $\{q \in \mathbb{Q} | \exists t \in x \exists s \in y (qt + s)\}$ is indeed a Dedekind cut and hence in $\mathbb{R}$.

1. Since x, y are Dedekind cuts, they are non-empty, so $\exists t \in x \exists s \in y$. Consider $t + s - 1 \in \mathbb{Q}$: $t + s - 1 t + s$, so it is in $x + y$ as defined, so $x + y$ is non-empty. Since x, y are Dedekind cuts there exists m_x, m_y s.t. xm_x and ym_y by the corollary to 46 existence of an upper bound for a

Dedekind cut. Take $m_{xy} = \max\{m_x, m_y\}$, it follows that $x \subset m_{xy}$ and $y \subset m_{xy}$, so $x + y \neq \mathbb{Q}$, so it is a proper subset of $\mathbb{Q}$.

2. Take $a \in x + y$, and let ba. Since $a \in x + y$, $at + s$ for some $t \in x, s \in y$, so by transitivity $bt + s$, so by construction $b \in x + y$, so $x + y$ is closed downwards.
3. Suppose there exists a greatest element $a \in x + y$, then $\forall b \in (x + y), b \leq a$, and also $at + s$ for some $\langle t, s\rangle \in x \times y$. By 11.1 density of the rationals in themselves it follows that $\exists q \in \mathbb{Q}$ s.t. $aqt + s$, but then $q \in x + y$ by definition, in contradiction to a being the greatest element in $x + y$.

We conclude that $x + y$ is a Dedekind cut, so $x + y \in \mathbb{R}$.

□

PROPOSITION 53

Given $x, y \in \mathbb{R}$, the sum of every pair of elements from x, y is an element of the sum $x + y$:

$$\forall x, y \in \mathbb{R}(\forall a, b \in \mathbb{Q}((a \in x \wedge b \in y) \implies (a + b \in x + y))$$

Proof. Let $x, y \in \mathbb{R}$, since they are Dedekind cuts they are non-empty so take $a \in x, b \in y$. To show $a + b \in x + y$, we need to show that $\exists t \in x \exists s \in y$ s.t. $a + b_{\mathbb{Q}} t + s$. Since x, y are Dedekind cuts, a, b cannot be their greatest element (since no such element exists), so $\exists a' \in x, b' \in y$ s.t. aa', bb', so $a + b_{\mathbb{Q}} a' + b'$. Take $t = a', s = b'$ and we get $a + b_{\mathbb{Q}} t + s$, so $a + b \in x + y$.

□

PROPOSITION 54

All elements in $x + y$ is equal to the sum of a pair of elements from x, y:

$$\forall r \in (x + y) \exists a \in x \exists b \in y(r = a + b)$$

Proof. Let $x, y \in \mathbb{R}$ and let $r \in x + y$, then $\exists s \in x, t \in y$ s.t. $rs + t$. Define $\epsilon = s + t - r$, since $rs + t$, 0ϵ, so $s - \frac{\epsilon}{2} \in x$ and $t - \frac{\epsilon}{2} \in y$ since both are cuts so closed downwards. By summation we have $s - \frac{\epsilon}{2} + t - \frac{\epsilon}{2} = s + t - \epsilon = r$. □

We now introduce an equivalent, more intuitive definition of addition in $\mathbb{R}$, called *Minkowski addition*:

DEFINITION 0.49 ⟨Minkowski addition on R⟩

Let $x, y \in \mathbb{R}$, their sum using Minkowski addition is given by $x \oplus y = \{a+b \in \mathbb{Q} | a \in x \wedge b \in y\}$, i.e. it is the set of all the sums between elements of x and y. Note that a more formal definition would be $\{\langle q \in \mathbb{Q} | \exists a \in x \wedge \exists b \in y (q = a + b)\}$.

PROPOSITION 55

0.48 addition on R and 0.49 Minkowski addition on R are equivalent.

Proof. By 53 and 54 □

PROPOSITION 56

Addition preserves order.

Proof. Take $a, b, c, d \in \mathbb{R}$ s.t. ab and cd. Consider $a + c$ and $b + d$, we wish to show $a + cb + d$, i.e. $a + c \subset b + d$. Let $x \in a + c$, by definition $\exists t \in a \exists s \in c$ s.t. $xt + s$. Since ab and cd, by definition $a \subset b, c \subset d$, so $t \in a \implies t \in b$, and $s \in c \implies s \in d$, so $x \in b + d$ as well, so $a + c \subseteq b + d$, meaning $a + c \leq b + d$. This shows that addition preserves non-strict order.

Since ab, by Theorem 11 density of the rationals in the reals $\exists q_{ab} \in \mathbb{Q}$ s.t. $aE(q_{ab})b$, so $q_{ab} \in b$ and $\forall a' \in a, a' q_{ab}$. Similarly, $\exists q_{cd} \in \mathbb{Q}$ s.t. $cE(q_{cd})d$ so $q_{cd} \in d$ and $\forall c' \in c, c' q_{cd}$, so $q_{ab} + q_{cd} \notin a + c$ (since addition preserves order in $\mathbb{Q}$), and also by the previous proposition since $q_{ab} \in b, q_{cd} \in d$ then $q_{ab} + q_{cd} \in b + d$, so $a + cb + d$, so addition preserves strict order.

□

PROPOSITION 57

$E : \mathbb{Q} \to \mathbb{R}$ preserves addition.

Proof. Take $q, p \in \mathbb{Q}$ and consider $E(q + p)$. By definition $E(q + p) = \{x \in \mathbb{Q} | xq + p\}$. Now consider $E(q)$ and $E(p)$, which are given by $\{x \in \mathbb{Q} | xq\}$, $\{x \in \mathbb{Q} | xp\}$ respectively. By definition, $E(q) + E(p) = \{x \in \mathbb{Q} | \exists s \in E(q) \exists t \in E(p)(xs + t)\}$. We will show that $E(q + p) = E(q) + E(p)$ by mutual inclusion.

$E(q) + E(p) \subseteq E(q + p)$: Take $x \in E(q) + E(p)$, then $\exists s \in E(q), t \in E(p)$ s.t. $xs + t$. Since $s \in E(q), t \in E(p)$ it follows that sq, tp, so since addition preserves order in $\mathbb{Q}$ we have $s + tq + p$, so by transitivity $xq + p$, so $x \in E(q + p)$ by definition.

$E(q+p) \subseteq E(q) + E(p)$: Take $x \in E(q+p)$, so $xq + p$. Consider $\epsilon = q + p - x$, which is a strictly positive rational number (since $\mathbb{Q}$ is a field so it is closed under addition). Since 0ϵ, it follows that $q - \frac{\epsilon}{2}q, p - \frac{\epsilon}{2}p$, so they are in $E(q), E(p)$ respectively, then $q - \frac{\epsilon}{2} + p - \frac{\epsilon}{2} = q + p - \epsilon = x$. Since $E(q), E(p)$ are cuts, $q - \frac{\epsilon}{2}, p - \frac{\epsilon}{2}$ cannot be maximal, so $\exists s \in E(q), t \in E(p)$ s.t. $q - \frac{\epsilon}{2}s, p - \frac{\epsilon}{2}t$, so $xs + t$, so $x \in E(q) + E(p)$.

We conclude that $E(q+p) = E(q) + E(p)$.

□

PROPOSITION 58 ⟨**additive identity of R**⟩

$E(0)$ is the additive identity of $\mathbb{R}$. We denote it $0_{\mathbb{R}}$, or simply 0.

Proof. We probe by mutual inclusion.

Let $a \in \mathbb{R}$. By definition $a + E(0) = \{x \in \mathbb{Q} | \exists s \in a \exists t \in E(0)(xs + t)\}$. Since $E(0) = \{x \in \mathbb{Q} | x0\}$ it follows that $\forall s \in a, s + ts$, so $xs + t \implies xs$, so $\forall e \in a + E(0), e \in a$, i.e. $(a + E(0)) \subseteq a$.

To show $a \subseteq (a + E(0))$, let $x \in a$. Since a is a cut, $\exists s \in a$ s.t. xs. Consider $x - s \in \mathbb{Q}$: since xs, it is less than 0, so it belongs to $E(0)$ by definition Furthermore, it cannot be the greatest element of $E(0)$ since it too is a cut, so $\exists t \in E(0)$ s.t. $x - st$, adding s to both sides we have $xs + t$ with $s \in a, t \in E(0)$, so by definition $x \in (a + E(0))$, so $a \subseteq (a + E(0))$.

We conclude that $a = (a + E(0))$.

□

We turn our attention to additive inverses in $\mathbb{R}$. First we observe the following:

PROPOSITION 59 ⟨**E preserves additive inverse**⟩

$E(-q) = -E(q)$, where $-q$ is the additive inverse of q in $\mathbb{Q}$ and $-E(q)$ is the additive inverse of $E(q)$ in $\mathbb{R}$.

Proof. Let $q \in \mathbb{Q}$, then $q + (-q) = 0$, and since E preserves addition it follows that $E(q) + E(-q) = 0$, so $E(-q)$ is the inverse of $E(q)$ in $\mathbb{R}$, so $E(-q) = -E(q)$.

□

But what is $E(-q)$? It is simply the cut $\{x \in \mathbb{Q} | x - q\}$. Since We know $E(-q) = -E(q)$, i.e. the additive inverse of $E(q)$, we should consider how to express $E(-q)$ in terms of $E(q)$, and then attempt to generalize that for any $x \in \mathbb{R}$ to find the additive inverse of x.

By definition of E we know that $\forall y(y \in E(q) \iff yq)$, i.e. $\forall y(y \notin E(q) \iff q \leq y)$, and the last inequality is the same as $-y \leq -q$. Substituting y for $-x$, we have $\forall x(-x \notin E(q) \iff x \leq -q)$, which is *almost* the definition of $E(-q)$: we want $x - q$ and not just $x \leq -q$. This is simply one element that we wish to remove, so we can easily do this by the following trick: $E(-q) = \{x \in \mathbb{Q} | \exists s \notin E(q)(x - s)\}$. If $x = -q$, then clearly $\nexists s \notin E(q)$ s.t. $-q - s$ since q is the smallest element in $\mathbb{Q} \setminus E(q)$. This final definition can be generalized for any real number, and in the next proposition we will prove that it indeed represents the inverse:

PROPOSITION 60 ⟨**additive inverse in R**⟩

Given $x \in \mathbb{R}$, there exists an additive inverse $-x \in \mathbb{R}$, given by $-x = \{q \in \mathbb{Q} | \exists s \notin x(q - s)\}$, s.t. $x + (-x) = 0_{\mathbb{R}}$.

Proof. First we should agree that $-x$ is indeed a real number, i.e. a Dedekind cut. This follows from the definition of $-x$ and from the fact that x is a cut. The proof is immediate so it is omitted. To prove $-x$ is the additive inverse of x, we prove by mutual inclusion that $x + (-x) = 0_{\mathbb{R}}$ using 0.49 Minkowski addition on R

$0_{\mathbb{R}} \subseteq (x + (-x)) :$ Take $a \in 0_{\mathbb{R}}$, then $a0_{\mathbb{Q}}$.

First, we prove a lemma:

LEMMA 11.1 ⟨**sign of additive inverse**⟩

If $x \geq 0_{\mathbb{R}}$, then $0_{\mathbb{R}} \leq -x$.

Proof. Observe that if $x = 0$ and $y = 0$ then the proof is trivial. Suppose both have the same sign: if both are 0 then $\exists s \in x, \exists t \in (-x)$ s.t. $s0$ and $t0$, so $0s + t$, so $0_{\mathbb{R}}x + (-x)$, a contradiction. Similarly if both are negative, then we can find some $q0$ that is also not in $x + (-x)$, again a contradiction to $x, -x$ being inverses, so the only possible case is that $x \leq 0_{\mathbb{R}} \implies 0_{\mathbb{R}} \leq -x$, as we expect from middle school. □

COROLLARY 11.3 ⟨**0 is its own additive inverse**⟩

If $x = 0_{\mathbb{R}}$ then $-x = 0_{\mathbb{R}}$

Proof. Since $x \leq 0$ and $0 \leq x$ then by the lemma we have $0 \leq -x$ and $-x \leq 0$, so $x = 0$. □

Using the lemma, we know that when $x = 0_{\mathbb{R}}$ then the proof is immediate. If $-x$ is the inverse of x, then x is the inverse of $-x$, so suppose w.l.o.g that $x0$, then $-x0$. Take an upper bound $M \in \mathbb{Q}$ on

x s.t. $M + \frac{a}{2} \in x$ (since $a0$ it follows that $M + \frac{a}{2}M$ so we a tight enough M, one must exist). Since $M \notin x$ (since it is an upper bound on x and x has no greatest element), and since $-M + \frac{a}{2} - M$, it follows that $-M + \frac{a}{2} \in -x$. Taking the sum of both elements, we have $(M + \frac{a}{2}) + (-M + \frac{a}{2}) = a$, so $a \in (x + (-x))$, so $0_{\mathbb{R}} \subseteq (x + (-x))$.

$(x + (-x)) \subseteq 0_{\mathbb{R}}$: Take $a \in (x + (-x))$, then by definition $\exists s \in x \exists t \in (-x)$ s.t. $a = s + t$. Since $t \in (-x)$, it follows that $\exists k \notin x(t - k)$, which means that $s + ts - k$ for some $k \notin x$. If $k \notin x$, then k cannot be smaller than some $s \in x$, otherwise $k \in x$ since k is closed downwards, which implies sk, which implies $s - k0$, so $s + t0$, so $a0$, so by definition $a \in 0_{\mathbb{R}}$.

□

Once we have shown that for every element in $\mathbb{R}$ there exists an additive inverse, we can define *subtraction* as addition with the additive inverse of the subtrahend.

Other properties of addition, such as associativity and commutativity, follow from the definition and the properties of $\mathbb{Q}$.
Multiplication

Upon defining multiplication we again reflect on multiplication on $\mathbb{Q}$. At first we may wish to define $x \cdot_{\mathbb{R}} y$ as the set $\{q \in \mathbb{Q} | \exists a \in x \exists b \in y(q = a \cdot_{\mathbb{Q}} b)\}$, but this definition leads to several issues: since x, y are cuts, they are closed downwards, so they contain all negative numbers starting at some point, but by 37 product of negative numbers we know that if $a0$ and $b0$, their product is greater than 0. This means that if we try to multiply $1_{\mathbb{R}} \cdot 1_{\mathbb{R}}$, which we expect to be $1_{\mathbb{R}}$ since we expect E to be a homomorphism and $1_{\mathbb{R}} = E(1)$ so we expect it to be the multiplicative identity, we find ourselves with a set that is closed *upwards*, and does not contain any negative rational number! This is, of course, nonsense.

What if we instead define $x \cdot y$ as $\{q \in \mathbb{Q} | \exists s \in x \exists t \in y(qs \cdot t)\}$? While less intuitive, this is in line with 0.48 addition on R. This does not solve the issue since for any number $0q$ we could still find $s, t \in 1_{\mathbb{R}}$ s.t. $s0, t0$ and $q = s \cdot t$. This motivates restricting the choice of s, t s.t. $0 \leq s, 0 \leq t$ (on in the first definition, to ensure that $a \in x, b \in y$ are both non-negative).

Now, what about the case when $x0$ or $y0$? Since we restrict the choice of $s \in x, t \in y$ s.t. x, y must both be non-negative, in this case there exists no pair $\langle s, t \rangle$ that satisfies this condition, so multiplication on such elements cannot be defined using the same definition. This motivates restricting multiplication to $\mathbb{R}^+$ in our initial definition. We will then extend it to the handle the cases where one (or both) of the elements is negative.

DEFINITION 0.50 ⟨multiplication on $\mathbf{R}^+$⟩

We define multiplication $\mathbb{R}^+ + \times \mathbb{R}^+ \to \mathbb{R}^+$ as follows:

$$x \cdot y = \{q \in \mathbb{Q} | \exists s \in x \exists t \in y (0 \leq s \wedge 0 \leq t \wedge qs \cdot_{\mathbb{Q}} t)\}$$

PROPOSITION 61

Multiplication on $\mathbb{R}^+$ is well-defined.

Proof. Let $x, y \in \mathbb{R}^+$, i.e. $0_{\mathbb{R}} x$ and $0_{\mathbb{R}} y$. Consider $x \cdot y$, given by definition by $\{q \in \mathbb{Q} | \exists s \in x \exists t \in y (0 \leq s \wedge 0 \leq t \wedge qs \cdot t)\}$. We wish to show that $x \cdot y$ is indeed a Dedekind cut, and that it is in $\mathbb{R}^+$ i.e. $0_{\mathbb{R}} x \cdot y$.

First, we show it's a Dedekind cut.
1. *Properness*: Since $0x, 0y$, then by density of $\mathbb{Q}$ in $\mathbb{R}$, $\exists q_x, q_y \in \mathbb{Q}$ s.t. $0E(q_x)x$, $0E(q_y)y$, so $q_x \in x, q_y \in y$ by definition of order in $\mathbb{R}$. Since order is preserved under E, it follows that $0q_x, 0q_y$ so since $\mathbb{Q}$ is an ordered field, $0q_x q_y$. Again from density, this time of $\mathbb{Q}$ in itself, $\exists p \in \mathbb{Q}$ s.t. $0pq_x q_y$. Taking $s = q_x, t = q_y$, we have pst with $s \in x, 0s$ and $t \in x, 0t$, so $p \in x \cdot y$, which implies that $x \cdot y$ is not empty. By 46 existence of an upper bound for a Dedekind cut we know that $\exists m_x, m_y \in \mathbb{Q}$ s.t. m_x is an upper bound on x and m_y is an upper bound on y. Consider, so $\forall s \in x \forall t \in y, sm_x, tm_y$, and since all terms are non-negative, order is preserved under multiplication in $\mathbb{Q}$ as an ordered field, so we have $stm_x m_y$, which means that $m_x m_y \notin x \cdot y$, so $x \cdot y \neq \mathbb{Q}$.
2. *Closed downwards*: Take $a \in x \cdot y$. Since $a \in x \cdot y$, then $\exists s \in x \exists t \in y$, both positive, s.t. $as \cdot t$. Take any $q \in \mathbb{Q}$ s.t. qa, then $qs \cdot t$, so $q \in x \cdot y$, so $x \cdot y$ is closed downwards.
3. *No greatest element*: Proven by the usual argument: suppose there is, denote it m, so $ms \cdot t$ for some s, t, but then $\exists q \in \mathbb{Q}$ s.t. $mqs \cdot t$ by density of the rationals, so $q \in x \cdot y$ but mq, a contradiction.

Positivity follows from the proof of properness - we found that $\exists q \in \mathbb{Q}$ s.t. $0q$ and $q \in x \cdot y$, so since $x \cdot y$ is a Dedekind cut we have $E(q) \subset x \cdot y$, now since E preserves order we have $0_{\mathbb{R}} E(q)$, so $0_{\mathbb{R}} \subset E(q)$, so by transitivity $0x$.

□

We wish to extend multiplication to a binary operator on $\mathbb{R}$ (as opposed to on $\mathbb{R}^+$). We base our definition on $\mathbb{Q}$, which itself borrows properties of multiplication of numbers with different signs from $\mathbb{Z}$. Observe that $\forall q, p \in \mathbb{Q}$, the following holds (this can be developed from 37 product of negative numbers):

$$q \cdot p = -((-q) \cdot p) = -(q \cdot (-p)) = (-q) \cdot -p$$

If we want E to preserve multiplication, then we must define multiplication on $\mathbb{R}$ such that it satisfies those relations as well, so we really don't have much freedom in extending multiplication to $\mathbb{R}$.

DEFINITION 0.51 ⟨**multiplication on R**⟩

We extend multiplication on $\mathbb{R}^+$ to $\mathbb{R}$ as follows (we use $x \cdot_{\mathbb{R}^+} y$ to refer to multiplication on $\mathbb{R}^+$)

$$x \cdot y = \begin{cases} x \cdot_{\mathbb{R}^+} y & 0x, y \text{ or } x, y0 \\ 0 & x = 0 \text{ or } y = 0 \\ -(|x| \cdot_{\mathbb{R}^+} |y|) & 0 \text{otherwise} \end{cases}$$

Where $|x|$ is the absolute value on x - if $0x$, $|x| = -x$, otherwise $|x| = x$.

Since all cases are mutually exclusive and since $x \cdot_{\mathbb{R}^+} y$ is well defined, $x \cdot y$ is well-defined on $\mathbb{R}$.

PROPOSITION 62 ⟨**multiplicative identity of R**⟩

$E(1)$, denoted $1_{\mathbb{R}}$, is the multiplicative identity of $\mathbb{R}$, i.e. $\forall x \in \mathbb{R}$, $x \cdot E(1) = x$.

Proof. Let $x \in \mathbb{R}^+$. We will show $x \cdot E(1) = x$ by mutual inclusion.

$(x \cdot E(1)) \subseteq x$: Let $a \in (x \cdot E(1))$, then $\exists s \in x \exists t \in E(1)$ s.t. $as \cdot t$ where $0 \leq s, t$. Since $t \in E(1), t1$, so $s \cdot ts$ (since $0 \leq t$), so by transitivity as. Since as for some $s \in x$ and x is a cut, $a \in x$, so $(x \cdot E(1)) \subseteq x$.

$x \subseteq (x \cdot E(1))$: Let $a \in x$. Since x does not have a greatest element, $\exists k \in x$ s.t. ak. Since $0x$, there exists such an k that satisfies $0k$. Since $0ak$, it follows that $a \cdot k^{-1}1$ (multiplication of non-negative quantities preserves sign in an ordered field), so $a \cdot k^{-1} \in E(1)$ by definition, and since $E(1)$ is a cut there exists $t \in E(1)$ greater than $a \cdot k^{-1}$, so $0k \cdot (a \cdot k^{-1})k \cdot t$, and by commutativity and associativity of multiplication in $\mathbb{Q}$ we have $k \cdot (a \cdot k^{-1}) = a$, so $ak \cdot t$ for $k \in x, t \in E(1)$ with $0 \leq k, t$, so $a \in (x \cdot E(1))$ by definition, so $a \subseteq (x \cdot E(1))$.

All that's left is to generalize for the cases when $x \in \mathbb{R} \setminus R^+$. Suppose $x = 0$, then by definition $0 \cdot E(1) = 0$, so the theorem holds. If $x0$, then by definition $x \cdot E(1) = -(-x \cdot E(1)) = -(-x) = x$. □

PROPOSITION 63

$E : \mathbb{Q} \to \mathbb{R}$ preserves multiplication.

Proof. Let $q, p \in \mathbb{Q}$ s.t. $q, p0$. We wish to show $E(q) \cdot E(p) = E(q \cdot p)$. We show this by mutual inclusion.

$E(q) \cdot E(p) \subseteq E(q \cdot p)$: Let $x \in E(q) \cdot E(p)$, then $\exists s \in E(q) \exists t \in E(p)$ both non-negative s.t. $xs \cdot t$. By definition sq, tp, and since s, t, q, p are all non-negative, we have $s \cdot tq \cdot p$, so $xq \cdot p$, so by definition $x \in E(q \cdot p)$.

$E(q \cdot p) \subseteq E(q) \cdot E(p)$: Let $x \in E(q \cdot p)$, then $xq \cdot p$. Now consider the sequence $a_n = q - n^{-1}$, $b_n = p - n^{-1}$. Each a_n, b_n is in $E(q), E(p)$ respectively by definition. From analysis (see Differential Calculus), we know that $\lim_{n\to\infty} a_n b_n = q \cdot p$, so we can find some n s.t. $qp - a_n b_n qp - x$, which implies $x a_n b_n$ where $a_n \in E(q), b_n \in E(p)$, so $x \in E(q) \cdot E(p)$.

We conclude that $E(q) \cdot E(p) = E(q \cdot p)$ if $q, p0$.

Now suppose $q = 0$ or $p = 0$, w.l.o.g suppose $q = 0$, then $E(q) \cdot E(p) = 0 \cdot E(p) = 0$ by definition, and also $E(q \cdot p) = E(0) = 0$. When both $q, p0$, we use the identity $q \cdot p = (-q) \cdot (-p)$. Since $-q, -p$ are positive, the argument above holds and so $E(q \cdot p) = E((-q) \cdot (-p)) = E(-q) \cdot E(-p)$, now since $E(-q), E(-p)0$ (as E preserves order) by definition we have $E(-q) \cdot E(-p) = E(q) \cdot E(p)$. Finally, when only one of $q, p0$ we suppose w.l.o.g that $q0$, then $E(q \cdot p) = E(-((-q) \cdot p))$, since E preserves inverses it follows that $E(-((-q) \cdot p)) = -E((-q) \cdot p)$, for which the above argument applies, so we have $E(q \cdot p) = (-E(-q)) \cdot E(p)$, and finally from the properties of multiplication (which needs to be shown, but suppose $\mathbb{R}$ is an ordered field, which it is) $(-E(-q)) \cdot E(p) = E(q) \cdot E(p)$, which completes the proof for the general case.

□

Once multiplication has been defined, we can show that it is distributive over addition, commutative and associative. We will suppose those have been proven, and turn our attention to an important property of the real numbers:

THEOREM 12 ⟨**Archimedean property**⟩

Given $a \in \mathbb{R}^+, b \in \mathbb{R}$, there exists a real natural number n s.t. nab.

Proof. Note that n is a *real* natural number, i.e. a natural number as represented in $\mathbb{R}$, and not a natural number as defined in our initial definition of $\mathbb{N}$, which we can forget thanks to the homomorphism sequence $\mathbb{N} \to \mathbb{Z}, \mathbb{Z} \to \mathbb{Q}, \mathbb{Q} \to \mathbb{R}$. Now consider the set of all real numbers of the form $A = \{na | n \in \mathbb{N}\}$. Suppose $\forall x \in A, x \not b$, then b is an upper bound on A, then by 51 existence of a supremum it follows that A has a least upper bound $\sup(A)$. Since $0a$, we have $\sup(A) - a\sup(A)$, so $\sup(A) - a$ is not an upper bound on A, so $\exists m \in \mathbb{N}$ s.t. $\sup(A) - ama$ (since $ma \in A$), but now we have $\sup(A)(m+1)a$, and $m + 1 \in \mathbb{N}$ so $(m+1)a \in A$, so $\sup(A)$ is not an upper bound on A, a contradiction, so $\exists n \in \mathbb{N}$ s.t. nab. □

We turn our attention to multiplicative inverses in $\mathbb{R}$. First, we observe the following:

PROPOSITION 64 ⟨**E preserves multiplicative inverse**⟩

$$E(q^{-1}) = E(q)^{-1}$$

Proof. Since E preserves multiplication $E(q \cdot q^{-1}) = E(q) \cdot E(q^{-1})$, so $E(1) = E(q) \cdot E(q^{-1})$, so $E(q^{-1})$ is the inverse of $E(q)$, so $E(q^{-1}) = E(q)^{-1}$. □

We note that $E(q^{-1}) = \{x \in \mathbb{Q} | xq^{-1}\}$. First, we limit our discussion to $\mathbb{R}^+$, since generalizing to $\mathbb{R}$ is simple and it makes the discussion simpler. We then hypothesize, either because of a similar line of reasoning to that present when hypothesizing the derivation of the additive inverse of some $x \in \mathbb{R}$, or simply by good faith that the multiplicative inverse will mirror the definition of the additive inverse, that the multiplicative inverse of x is given by $x^{-1} = \{q \in \mathbb{Q} | \exists s \notin x(qs^{-1})\}$, and show that it is indeed the multiplicative inverse when $x \in \mathbb{R}^+$:

PROPOSITION 65 ⟨**multiplicative inverse in R$^+$**⟩

Given $x \in \mathbb{R}^+$, its multiplicative inverse, x^{-1}, is given by $\{q \in \mathbb{Q} | \exists s \notin x(qs^{-1}\}$.

Proof. First one needs to show that x^{-1} as defined is indeed in $\mathbb{R}$, i.e. it is indeed a Dedekind cut. This is trivial and left as an exercise. We then need to show that $x \cdot x^{-1} = 1_{\mathbb{R}}$ by definition. We show this via mutual inclusion.

$1_{\mathbb{R}} \subseteq (x \cdot x^{-1})$: Let $a \in 1_{\mathbb{R}}$, so $a1$, and we need to find $s \in x, t \in x^{-1}$, both ≥ 0, s.t. $as \cdot t$. There are three cases: $a \leq 0$, in which case any $s, t \geq 0$ will satisfy $as \cdot t$ so a is trivially in $x \cdot x^{-1}$, or $a0$. In the latter, we have $0a1$. Since $0a1$ it follows that $01 - a$, so by Theorem 12 Archimedean property it follows that there exists some $m \in \mathbb{N}$ s.t. $am(1 - a)$, so by arithemtic

$$am(1-a) \implies am - ma \implies a(m+1)m \implies$$

$$a\frac{m}{m+1}$$

If fact, since $0a$, it follows that the above inequality holds for every $n \in \mathbb{N}$ s.t. $m \leq n$.

We now take some $r \in x$ s.t. $r0$, and $q \in \mathbb{Q}$ s.t. $0q\frac{r}{m}$ (such q much exist due to 11.1 density of the rationals in themselves), and choose some n s.t. $nq \in x$ but $(n+1)q \notin x$ (such n must exist since x has an upper bound). Now, since $(n+1)q \notin x$, it implies that $r(n+1)q$ since $r \in x$, and since $0q\frac{r}{m}$

we have mqr, so $mqr(n+1)q$, so it must be that $n \geq m$, so n satisfies the above inequality. By that inequality and since $0nq$, we have $\frac{a}{nq}\frac{1}{(n+1)q} = ((n+1)q)^{-1}$, so by definition of x^{-1}, since $(n+1)q \notin x$, we have $\frac{a}{nq} \in x^{-1}$.

We now have $nq \in x, \frac{a}{nq} \in x^{-1}$. Their product is $nq \cdot \frac{a}{nq} = a$, and since both cannot be maximal in each set (since each set is a cut) we can take $s = nq + \epsilon \in x, t = \frac{a}{nq} + \epsilon \in x^{-1}$ with 0ϵ, which produces a product $s \cdot t$ such that $as \cdot t$, so by definition $a \in (x \cdot x^{-1})$, so $1_{\mathbb{R}} \subseteq (x \cdot x^{-1})$.

$(x \cdot x^{-1}) \subseteq 1_{\mathbb{R}}$: Let $a \in (x \cdot x^{-1})$, then $\exists s \in x \exists t \in x^{-1}$, both ≥ 0, such that $as \cdot t$, with tk^{-1} for some $k \notin x$ by definition of x^{-1}. Since $k \notin x$, it follows that sk since x is a cut. Since $0 \leq s, 0 \leq t$, it follows that $0k$, so we can multiply both sides by t while preserving order and get $s \cdot tk \cdot t$, and since tk^{-1} we have $s \cdot tk \cdot k^{-1} = 1$, so $s \cdot t1$, so by transitivity $a1$, so $a \in 1_{\mathbb{R}}$, so $(x \cdot x^{-1}) \subseteq 1_{\mathbb{R}}$.

We conclude $(x \cdot x^{-1}) = 1_{\mathbb{R}}$.

□

We can then generalize to $\mathbb{R}$:

PROPOSITION 66 ⟨**multiplicative inverse in R**⟩

Given $x \in \mathbb{R}$, its multiplicative inverse is given by:

$$x^{-1} = \begin{cases} \{q \in \mathbb{Q} | \exists s \notin x(sq^{-1})\} & 0x \\ 0 & 0 = x \\ -((-x)^{-1}) & x0 \end{cases}$$

Proof. If $0x$ then the definition is justified by 65 multiplicative inverse in R$^+$ If $x = 0$ then $x = E(0)$ whose inverse is $E(0) = 0$ by 64 E preserves multiplicative inverse, so $x^{-1} = 0$. Finally, when $x0$, then $0 - x$ by 11.1 sign of additive inverse, so we can take its multiplicative inverse $(-x)^{-1}$ by the previous proposition and get $(-x) \cdot (-x)^{-1} = 1$. By 0.51 multiplication on R we know that $(-x) \cdot (-x)^{-1} = (-(-x)) \cdot (-(-x)^{-1}) = x \cdot (-(-x)^{-1}) = 1$, so $(-(-x)^{-1})$ is the multiplicative inverse of x if $x0$, which completes the proof.

□

We define *division* on $\mathbb{R}$ same way as we did on $\mathbb{Q}$ - by multiplication with the inverse of the divisor. It is well defined since multiplication is well-defined (and preserved by E for the same reason).

Other properties of multiplication, such as commutativity, associativity, order preserving when both operands are non-negative and distributivity over addition are already satisfied by those definitions, so $(\mathbb{R}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, +, \cdot,)$ is an *ordered field*.

Since E preserves order, multiplication and addition and since $\mathbb{R}$ is an ordered ring with respect to these operations, and E takes identities of $\mathbb{Q}$ to identities of $\mathbb{R}$ and inverses in $\mathbb{Q}$ to inverses in $\mathbb{R}$, it follows that E is indeed an ordered ring homomorphism.

Cardinality

Recall that in 0.4 cardinality of a set we defined cardinality as the number of elements in the set. This definition is workable if the set is finite, but it is insufficient for sets like $\mathbb{N}$ or $\mathbb{Q}$ which are infinite. This definition is also insufficient within formal set theory since we do not yet have a formal notion of what it means for a set to be finite. In this section, we will present a formal discussion of cardinalities of sets and how to compare them, presenting unituitive results such as that the cardinality of the set of real numbers in the interval $(0,1)_{\mathbb{R}}$ is the same as the cardinality of the set of the real numbers.

Equinumerousity

DEFINITION 0.1 ⟨**equinumerousity**⟩

A set A is equinumerous *to a set B if there is a bijection $f : A \to B$. We denote this relation by $A \approx B$, or by $|A| = |B|$.*

PROPOSITION 67 ⟨**properties of equinumerousity**⟩

Given sets A, B, C, equinumerousity is:
1. Transitive: $A \approx A$
2. Symmetric: $A \approx B \implies B \approx A$
3. Transitive: $A \approx B \wedge B \approx C \implies A \approx C$
Note that equinumerousity is not *an equivalent relation, since it is defined on* sets*, and not on* elements of sets*.*

Proof. 1. Take the identity on A, id_A. It is a bijection, so $A \equiv A$.
2. Suppose $A \approx B$, then there exists some $f : A \to B$ that is bijective, then by 16 two-sided inverse-bijection equivalence it has a left and right sided inverse $f^{-1} : B \to A$, so it is also the two-sided inverse of f^{-1}, so f^{-1} is a bijection, so $B \approx A$.
3. Suppose $A \approx B$ and $B \approx C$, then there is a bijection $f : A \to B$ and a bijection $h : B \to C$. Consider $h \circ f : A \to C$, it is a composition of bijections so by 11 compositon of bijections is a bijection it is a bijection, so $A \approx C$.

□

Equinumerousity of Number Sets

PROPOSITION 68 $\langle \mathbf{Z} \approx \mathbb{N} \rangle$

The integers and the natural numbers are equinumerous.

Proof. Let $f : \mathbb{Z} \to \mathbb{N}$ be given by

$$f(z) = \begin{cases} 2z & 0 \leq z \\ -2z - 1 & z0 \end{cases}$$

To prove that it is a bijection, let $n \in \mathbb{N}$. Suppose $f(z) = n$ for some $z \in \mathbb{Z}$, then either $n = 2z$ or $n = -2z - 1$, i.e. either $z = \frac{n}{2}$, or $z = -\frac{n+1}{2}$. Since z is an integer, and n is a natural number, 2 must divide the dividend without reminder, so in the first case we have that $n = 2m$ for some $m \in \mathbb{N}$, i.e. n is even, and in the second case we have $n + 1 = 2m$ for some $m \in \mathbb{N}$, i.e. $n = 2m - 1$, i.e. n is odd, and since these are mutually exclusive we have that only one of the options may occur for a given n, so f is injective, and since n is always either odd or even, we can always solve for z, so f is surjective, so in conclusion f is a bijection, so $\mathbb{Z} \approx \mathbb{N}$. □

PROPOSITION 69 $\langle \mathbf{Q} \approx \mathbb{N} \rangle$

The rationals and the integers are equinumerous.

Recall that $\mathbb{Q}$ is defined as the quotient set of the cartesian product $\mathbb{Z} \times \mathbb{Z}^+$ under an equivalence relation $\sim$ as defined in 0.32 rational numbers. Consider the following visualization of $\mathbb{Z} \times \mathbb{Z}^+$, where elements from $\mathbb{Z}^+$ are used as the y axis and elements from $\mathbb{Z}$ are used as the x axis. (the visualization only displays a small subset of $\mathbb{Z} \times \mathbb{Z}^+$)

$$\begin{pmatrix} (-3,4) & (-2,4) & (-1,4) & (0,4) & (1,4) & (2,4) & (3,4) \\ (-3,3) & (-2,3) & (-1,3) & (0,3) & (1,3) & (2,3) & (3,4) \\ (-3,2) & (-2,2) & (-1,2) & (0,2) & (1,2) & (2,2) & (3,2) \\ (-3,1) & (-2,1) & (-1,1) & (0,1) & (1,1) & (2,1) & (3,2) \end{pmatrix}$$

Consider a walk along the elements of the set, performed as follows (it is suggested that you trace along the above matrix with your finger to understand this construction):
1. Start at $(0,1)$
2. Move one position to the right, to $(1,1)$
3. Move one position up, to $(1,2)$

4. Move one position to the left ($(0, 2)$), then move another position to the left ($(-1, 2)$)
5. Move one position down to $(-1, 1)$. You have now completed one half-loop around the origin $(0, 1)$, which is the shortest possible half-loop. We now set on another half-loop around the origin in the opposite direction, which is also going to be the shortest possible half-loop along unvisited elements of the cartesian product, as follows:
6. Move one position to the left to $(-2, 1)$
7. Move upwards until you reach $(-2, 3)$
8. Move to the right until you reach $(1, 3)$
9. Move downwards until you reach $(1, 1)$. You have now completed a second half-loop.
10. Continue indefinitely, each time starting the shortest possible half-loop of unvisited elements in the *opposite* direction of the previous.

It should be pretty convincing that this construction eventually reaches all of $\mathbb{Z} \times \mathbb{Z}^+$, i.e. given any $z \in \mathbb{Z} \times \mathbb{Z}^+$, it will eventually be reached via this walk. Since each step is associated with a single element of the cartesian product in a one-to-one correspondence, and since each element is eventually reached (assuming the thought-experiment above convinces you), then we have a bijection $g : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}^+$. It should be noted that formally, we haven't proven anything - we haven't even properly defined a relation, much less shown that it is a bijection $\mathbb{N} \to \mathbb{Z} \times \mathbb{Z}^+$, but it is easy enough to feel in the details of a formal proof, so it is left as an exercise. We now suppose that there exists such g, and continue with the rest of the proof, written formally.

Proof. We suppose a bijection $g : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}^+$ exists (that corresponds to the walk described above). We now define a function $f : \mathbb{N} \to \mathbb{Q}$ recursively as follows:
1. $f(0) = [g(0)]$
2. $f(n + 1) = [g(k)]$ where k is the smallest natural number such that $\forall i \in [0, n], [g(k)] \neq f(i)$

By the recursion theorem f is unique and well-defined. Now let $q \in \mathbb{Q}$. Since g is a bijection $\mathbb{N} \to \mathbb{Z} \times \mathbb{Z}^+$, there exists some $k \in \mathbb{N}$ for which $g(k) \in q$, so there exists a minimal such k. If $k = 0$, then $f(0) = [g(0)] = q$, so $q \in \text{Im}(f)$. Otherwise, $k \neq 0$, so it corresponds to some $n \in \mathbb{N}$ by the recursive step of the definition (suppose not, then $\forall n \in \mathbb{N}, f(n) \neq q \iff f(n) \neq [g(k)]$. Take nk, then we necessarily have at least one pair $n, m \in \mathbb{N}, n \neq m$ s.t. $f(n) = f(m)$, contradicting the recursive definition of f), so again $q \in \text{Im}(f)$ so we conclude that f is surjective. By the recursive step, it must be injective, so we conclude f is bijective, so $\mathbb{N} \approx \mathbb{Q}$.

□

PROPOSITION 70 $\langle (0, 1)_{\mathbb{R}} \approx \mathbb{R} \rangle$

The unit interval in $\mathbb{R}$ and $\mathbb{R}$ are equinumerous.

Proof. Recall from analysis that $\tan x$ is bijective in $(-\frac{\pi}{2}, \frac{\pi}{2})$. Consider the linear interpolation function $f(t) = (1-t)\frac{-\pi}{2} + t\frac{\pi}{2}$, which is linear and thus bijective on $[0,1]_{\mathbb{R}}$. The composition $\tan \circ f : (0,1)_{\mathbb{R}} \to \mathbb{R}$ is a composition of bijective functions and thus bijective, so we have a bijection $(0,1)_{\mathbb{R}} \to \mathbb{R}$, so $(0,1)_{\mathbb{R}} \approx \mathbb{R}$. □

Cantor's Diagonal Argument

Consider $\mathbb{R}$ vs $\mathbb{N}$, are they equinumerous? At first, our intuition would be that they are not, since $\mathbb{N}$ is contained (via homomorphisms) in $\mathbb{R}$. However, this same intuition is true for $\mathbb{Z}$ and $\mathbb{Q}$ as well, but as we have seen both are equinumerous to $\mathbb{N}$, so by now our intuition may suggest to expect the unexpected result, that $\mathbb{R} \approx \mathbb{N}$. However, that is not the case. We will prove this by Cantor's diagonal argument.

THEOREM 13 ⟨**Cantor's diagonal argument**⟩

$\mathbb{N} \not\approx \mathbb{R}$.

Proof. We prove the theorem in 3 steps:
1. We show $\mathbb{N} \not\approx S$ for a particular S, this is where the "diagonal argument" is.
2. We show that same S satisfies $S \approx (0,1)_{\mathbb{R}}$.
3. We conclude by transitivity that $\mathbb{N} \not\approx \mathbb{R}$.

Step 1: Consider the set S of all sequences of the form $s_n : \mathbb{N} \to \{0_{\mathbb{N}}, 1_{\mathbb{N}}\}$, i.e. the set of all sequences whose elements are either the natural number 0 or the natural number 1. This is a proper set, since each s_n is a function and functions are themselves relations which are themselves ordered pairs, i.e. elements of the cartesian product $\mathbb{N} \times \{0_{\mathbb{N}}, 1_{\mathbb{N}}\}$.

Suppose now that $\mathbb{N} \approx S$, so there exists a bijection $f : \mathbb{N} \to S$. We now construct a new sequence $a : \mathbb{N} \to \{0_{\mathbb{N}}, 1_{\mathbb{N}}\}$ as follows:

$$a(n) = \begin{cases} 0 & f(n)(n) = 1 \\ 1 & f(n)(n) = 0 \end{cases}$$

i.e. the n-th element of a is 0 when the n-th element of the sequence s_n corresponding to $f(n)$ is 1, otherwise it is 0 - it is always the opposite number.

As a finite example (note that the theorem will *not* hold for such example, it is here for illustrative purposes only), consider the following:
1. $s_0 = (0,1,0,0)$
2. $s_1 = (1,1,0,1)$

3. $s_2 = (1, 0, 1, 0)$
4. $s_3 = (1, 1, 1, 0)$

With $f : n \mapsto s_n$, so a_n would be constructed as follows: since $f(0)(0) = s_0(0) = 0$, $a_0 = 1$, similarly $s_1(1) = 1$ so $a_1 = 0$, $s_2(2) = 1$ so $a_2 = 0$, and finally $s_3(3) = 0$ so $a_3 = 1$ and we have $a = (1, 0, 0, 1)$.

Another way to think of this construction is that we take the *diagonal* of all s_n, and *invert* it via the rule that 0 becomes 1 and 1 becomes 0 (this is why why call it a *diagonal* argument).

Back to our proof, we have some $a : \mathbb{N} \to \{0_{\mathbb{N}}, 1_{\mathbb{N}}\}$, so $a \in S$, but by construction for each $n \in \mathbb{N}$ we have $f(n)(n) \neq a(n)$, $f(n) \neq a$, so $a \notin \text{range}(f)$, so f is not surjective, a contradiction, so we conclude that there does not exist a bijection $f : \mathbb{N} \to S$, so $\mathbb{N} \not\approx S$.

Step 2: This step relies on the fact that all numbers have a decimal representation in any base, not necessarily unique (for example $1 = 0.999\ldots$ in base 10 although both are distinct decimal representations). Proving this is outside the scope of this discussion, and it is assumed that the reader is aware of this fact. Then for each base we define a function $f_b : S \to [0, 1]_{\mathbb{R}}$ as follows: $f_b(s) = 0.s_0s_1s_2\ldots_b$, i.e. f_b takes a sequence S which consists only of 0s and 1s to the representation of a number in $[0, 1]_{\mathbb{R}}$ given by 0 followed by a decimal point and then the i-th digit after the decimal point is simply the i-th element of S.

Now consider the function f_2, i.e. the function which takes S to binary representations of numbers in $[0, 1]_{\mathbb{R}}$. Clearly f_2 is surjective, however:
1. The co-domain of f_2 is $[0, 1]_{\mathbb{R}}$, and we want to define a new function g based on f_2 s.t. its co-domain will be $(0, 1)_{\mathbb{R}}$, because we have shown $(0, 1)_{\mathbb{R}} \approx \mathbb{R}$.
2. Not all numbers in $[0, 1]_{\mathbb{R}}$ have a unique binary representation. These numbers are called *dyadic rationals*, and are the numbers that can also be finitely represented in binary (so they can be represented either via a finite representation, or by replacing the last digit with an infinite sequence of $111\ldots$), so f_2 is not injective.

Both problems can be solved when constructing a bijection $g : S \to (0, 1)_{\mathbb{R}}$ from f_2. The idea is to put the dyadic rationals in a sequence $r : \mathbb{N} \to \mathbb{R}$ such that 0 and 1 (both of which are dyadic rationals) are omitted and all elements are unique, and the sequences in S corresponding to dydic rationals in a sequence $s' : \mathbb{N} \to S$, and then define g as follows:

$$g(s) = \begin{cases} r(i) & \exists! i \in \mathbb{N} \text{ s.t. } s'(i) = s \\ f(s) & \text{otherwise} \end{cases}$$

Evidently since the pre-images of 0 and 1 are in the range of s', by construction of g, $\forall s \in S, g(s) \neq 0 \wedge g(s) \neq 1$, so $g : S \to (0, 1)_{\mathbb{R}}$ and g is surjective, and also since all sequences mapping to the same dyadic rational have been remapped by g to distinct dyadic rationals we have that g is injective, so in conclusion g is a bijection, so $S \approx (0, 1)_{\mathbb{R}}$.

Dyadic rationals and numerical representations are outside the scope of this discussion, so for a more in-depth discussion (which the reader can then use to fill in the gaps in this proof) the reader is referred to the Wikipedia entries on dyadic rationals and Cantor's diagonal argument.

Step 3: We have $S \approx (0,1)_{\mathbb{R}}$, so by 67 properties of equinumerousity and 70 $(0,1)_{\mathbb{R}} \approx \mathbb{R}$ it follows that $S \approx \mathbb{R}$. If $\mathbb{N} \approx \mathbb{R}$, then by transitivity we would have $\mathbb{N} \approx S$, but in step 1 we have shown $\mathbb{N} \not\approx S$, so it follows that $\mathbb{N} \not\approx \mathbb{R}$, which completes the proof.

□

THEOREM 14 ⟨**Cantor's theorem**⟩

For every set A, $A \not\approx \mathcal{P}(A)$.

Proof. Let f be any function $A \to \mathcal{P}(A)$, and let B be a subset of A defined as $B = \{a \in A | a \notin f(a)\}$, i.e. B is the set of all elements of A that are not elements of their image under f. Since B is a subset of A, we have $B \in \mathcal{P}(A)$, so if f is surjective we should have $B \in f[A]$. Suppose that is the case, then $\exists b \in A$ s.t. $f(b) = B$. There are two cases:

1. $b \in B$, but then we have $b \in f(b)$, so by specification of B, $b \notin B$, a contradiction.
2. $b \notin B$, but then we have $b \notin f(b)$, so by specification of B, $b \in B$, a contradiction.

We have reached a contradiction, so f is not surjective, so f cannot be bijective, so $A \not\approx \mathcal{P}(A)$.

□

These theorems present an unituitive result about infinite sets (which we have not yet properly defined, yet we know all sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are infinite): there are infinite sets of different sizes. Put in other words, there are different types of infinity, some larger than the others.

Finite Sets and Cardinality

We are now ready to define what it means for a set to be *finite* within our formal system.

DEFINITION 0.2 ⟨**finite set**⟩

A set is finite *if it is equinumerous with a natural number. Otherwise, it is* infinite*.*

Where natural numbers are defined as the elements of 0.6 the set of natural numbers.

We now introduce a very elementary result in counting and combinatorics:

THEOREM 15 ⟨**pigeonhole principle**⟩

Given $n \in \mathbb{N}$, it is not equinumerous to any proper subset of itself, i.e. $\forall m \in \mathcal{P}(n) \setminus \{n\}, n \not\approx m$.

Proof. We prove by induction. For $n = 0$ we have $n = \emptyset$ so $\mathcal{P}(n) = \{\emptyset\}$ so $\mathcal{P}(n) \setminus \{n\} = \emptyset$ so the proposition is vacuously true. Suppose it is true for some n, we will show it holds for $n+1$. We prove by contradiction: suppose there exists a proper subset $k \subset n+1$ s.t. $n+1 \approx k$, so there exists a bijection $f : n+1 \to k$. Recall that $n = \{0, 1, \ldots, n-1\}$ and $n+1 = \{0, 1, \ldots, n\}$. There are two cases:

1. $n \notin k$, in which case consider f restricted to n with co-domain restricted to $k \setminus \{f(n)\}$, i.e. $f_{|n} : n \to k \setminus \{f(n)\}$, which is clearly a bijection with $k \setminus \{f(n)\} \subset n$, which is a contradiction to the induction hypothesis.
2. $n \in k$, in which case since f is bijective there exists a single $x_0 \in k$ such that $f(x_0) = n$. Consider a remapping g of f such that $g(x) = f(x)$ if $x \neq x_0$, and $g(x_0) = f(n)$. Since $g(n) = f(n)$ and $g(x_0) = f(n)$, we can drop n from the domain and the co-domain (since x_0 is the only value of x for which $f(x_0) = n$) and get a new bijection $g : n \to k \setminus \{n\}$, but since k was already a proper subset of $n+1$, we now have a proper subset of n in $k \setminus \{n\}$, contradicting the induction hypothesis.

So we conclude that in both cases there cannot exist a bijection, which completes the proof □

COROLLARY 15.1 ⟨**pigeonhole principle corollaries**⟩

1. No finite set is equinumerous to a proper subset of itself.
2. $\mathbb{N}$ is not finite.
3. Every finite set is equinumerous to a unique natural number.

Proof. 1. Suppose by contradiction that there exists a finite set that is equnumerous to a proper subset of itself, denote the set A and the subset $B \subset A$. By definition of a finite set we have $A \approx n$ and $B \approx m$ where $n, m \in \mathbb{N}$ with $n \subset m$, and by our supposition we have $A \approx B$, so by transitivity we have $n \approx m$, contradicting Theorem 15 pigeonhole principle.

2. Given any natural number n, it is a proper subset of $\mathbb{N}$ since it is the set of all its predecessors, so by Theorem 15 pigeonhole principle $n \not\approx \mathbb{N}$ for all $n \in \mathbb{N}$, so by 0.2 finite set, $\mathbb{N}$ is not finite. Since $\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q}$, it follows that $\mathbb{Z}, \mathbb{Q}$ are infinite as well.

3. Let A be a finite set, then it is equinumerous to a natural number $n \in \mathbb{N}$. Suppose by contradiction there exists more than one distinct natural numbers in $\mathbb{N}$ equinumerous to A, and consider two of them $n, m \in \mathbb{N}, n \neq m$. Since $n \neq m$ either $n \subset m$ or $m \subset n$, and in both cases by Theorem 15 pigeonhole principle $n \not\approx m$, but by our supposition we have $A \approx n$ and $A \approx m$ so by transitivity

$n \approx m$, a contradiction, so n is unique.

□

By (3) in 15.1 pigeonhole principle corollaries, we can define the *cardinality* of a finite set within formal set theory as follows

DEFINITION 0.3 ⟨**cardinality of a finite set**⟩

The cardinality of a finite set A, denoted card(A) or $|A|$, is the unique natural number equinumerous to A.

What about the cases which are infinite? Clearly the above definition does not hold, but we still want to have a notion of the size of those sets, since by Theorem 13 Cantor's diagonal argument and Theorem 14 Cantor's theorem we know that not all of them are equinumerous, but by 69 Q $\approx \mathbb{N}$ and other propositions we know that some of them are. It would be tempting to classify these sets based on equinumerousity, since it is very similar to an equivalent relation in its properties, but since it is defined on sets we cannot specify "the set of all sets equinumerous to $\mathbb{N}$" for example, because by 0.9 axiom schema of specification (ZF5) we need to specify a set from which the sets are taken, and as we have seen the collection of all sets is not a set, but a proper class. To still be able to talk about cardinality of infinite sets, we need to generalize 0.3 cardinality of a finite set. For example, we would like to say that $\mathbb{N}$ is the *cardinality* of $\mathbb{Z}$ and $\mathbb{Q}$. To do this, we present the following definition:

DEFINITION 0.4 ⟨**cardinal set**⟩

A set A is cardinal *if:*
1. It is transitive
2. $\forall x, y \in A, x \neq y$, either $x \in y$ or $y \in x$
3. $\forall x \in A, x \not\approx A$.

EXAMPLE 15.1 ⟨**natural numbers are cardinal sets**⟩

We have seen that natural numbers are transitive, and since order in $\mathbb{N}$ is total and natural numbers consist of the set of all their predecessors we have that $\forall x, y \in n$ (where n is a natural number), either xy or yx, which implies $x \in y$ or $y \in x$. Finally, by proposition 1 of 15.1 pigeonhole principle corollaries we know that n is not equinumerous to any proper subset of itself, and since each natural number is a set of natural numbers, each $x \in n$ is also a subset of n, so $\forall x \in n, x \not\approx n$, so we conclude that all natural numbers are cardinal sets.

It can be shown that for any set, there exists a unique cardinal set equinumerous to that set. The proof for this is proposition is beyond the scope of this discussion, but presenting it is necessary to justify that the following definition is well defined:

DEFINITION 0.5 ⟨**cardinality of a set**⟩

The cardinality of a set A*, denoted card*(A) *or* $|A|$*, is the cardinal set equinumerous to* A*.*

By 15.1 natural numbers are cardinal sets we see that 0.5 cardinality of a set generalizes 0.3 cardinality of a finite set. It can also be verified that $\mathbb{N}$ is a cardinal set, and since equinumerousity is reflexive we know that $\mathbb{N} \approx \mathbb{N}$, so $\mathbb{N}$ is its own cardinal. We denote this cardinal by $\aleph_0$. Similarly, since $\mathbb{N} \approx \mathbb{Z}$ and $\mathbb{N} \approx \mathbb{Q}$, we know that card$(\mathbb{Z}) =$ card$(\mathbb{Q}) =$ card$(\mathbb{N}) = \aleph_0$. Cardinal arithmetic can be defined to allow considering the cardinality of a union, intersection, power set, product, etc.

DEFINITION 0.6 ⟨**countable set**⟩

A set A *is* countable *if any of the following conditions is met:*

1. *It is* finite *or it is equinumerous to* $\mathbb{N}$*.*
2. *It's cardinality is* $\leq \aleph_0$*.*

Otherwise we say that the set is uncountable*.*

PROPOSITION 71

The conditions in 0.6 countable set are equivalent.

Proof. $1 \implies 2:$ Suppose A is a set and is finite or equinumerous to $\mathbb{N}$. If it is finite, then it is equinumerous to some $n \in \mathbb{N}$ and clearly $n\aleph_0$ so its cardinality is $\aleph_0$. If it is equinumerous to $\mathbb{N}$, then its cardinality is $\aleph_0$. In conclusion we have that the cardinality of the set is$\leq \aleph_0$.

$2 \implies 1:$ Suppose A has cardinality $\leq \aleph_0$. If card$(A) = \aleph_0$ then $A \approx \mathbb{N}$, otherwise card$(A)\aleph_0$, so $A \approx n$ for some $n \in \mathbb{N}$, so A is finite.

□

PROPOSITION 72

If A *is countable, then there exists an injective function* $f : A \to \mathbb{N}$*.*

Proof. Suppose A is a countable set, so it has cardinality $\leq \aleph_0$. Since the cardinal of A is unique (we have asserted this proposition without proof), it follows that if card$(A) = \aleph_0$ then $A \approx \mathbb{N}$ so $\exists f : A \to \mathbb{N}$ that is a bijection, so in particular f is injective. If card$(A)\aleph_0$ then card$(A) = n$ for some $n \in \mathbb{N}$ so $A \approx n$, so $\exists f : A \to n$ that is bijective and in particular injective, so we can consider f with codomain $\mathbb{N}$ (since $n \subset \mathbb{N}$ as the set of all its predecessors), denote it $\hat{f}$, then that $\hat{f}$ is also injective

(but not bijective).

□

Once more interesting results regarding cardinals have been studied, one can show that the last proposition is in fact an if and only if proposition, but such study is beyond the scope of our discussion.

Conclusion

In this discussion, we presented a logistic construction of the real numbers and their properties within the formal language of set theory starting from first principles, using only the axioms and results of first-order logic and a set of axioms for set theory, along with the axiom of choice. Within this rather limited set of axioms, we managed to create a solid foundation for math. The reader can trivially extend $\mathbb{R}$ to complex number $\mathbb{C}$ by simply taking ordered pairs of reals. Thus it is possible to construct most of analysis inside set theory, and indeed most of mathematics. It should surprise the reader that there are still two ZF axioms we have not presented, since they were not necessary for our discussion. These are the *axiom of regularity* and the *axiom schema of replacement*, both of which are necessary for dealing with infinite sets and ordinals, the former of which we barely started discussing and the latter we haven't even properly mentioned.

The axioms presented in our discussion form *Zeremlo set theory*, which was originally proposed by Ernst Zermelo in a 1908 paper.

DEFINITION 0.1 ⟨**Zeremlo set theory**⟩

Zermelo set theory is a first-order language whose vocabulary consists of the symbol $\in$, and contains the following axioms:
1. 0.5 axiom of extensionality (ZF1)
2. 0.6 axiom of empty set (ZF2)
3. 0.7 axiom of pairing (ZF3)
4. 0.8 axiom of union (ZF4)
5. 0.9 axiom schema of specification (ZF5)
6. 0.11 axiom of power set (ZF6)
7. 0.4 axiom of infinity (ZF7)
8. 0.24 axiom of choice (AC)

The reader is invited to continue Math 135 to learn about infinite sets, ordinals, the two remaining axioms which form ZF set theory, and interesting equivalent propositions to the axiom of choice.