Set theory notes

Matthew Signorotti

Fall 2019

Contents

1 Axioms and operations

1.1 Zermelo-Fraenkel axioms (first 6)

Our axiomatic system of set theory consists of two "primitive notions": **sets** and **members** of sets. We only restrict their meaning in the following ways: members are in ($\in$) sets, only another set can be a member of a set, and certain basic, rigorous assumptions (**axioms**) hold for sets and members. Indeed, a common basis for set theory, and mathematics as a whole, are the following **Zermelo-Fraenkel axioms**. They avoid issues like Russell's paradox which arise in the more intuitive "naive" set theory. Each axiom can be stated more mathematically with the notation of predicate logic, including: variables (letters representing sets), the logical connectors $\wedge$ $\vee$ $\neg$ $\iff$ and $\implies$, the quantifiers $\forall$ and $\exists$, and perhaps the con-

stants 1 and 0. We hold each proposition/predicate logic statement to be either true or false (law of the excluded middle).

Ax1. **Extensionality**: If two sets have the same members, then they are equal:

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

Ax2. **Empty set**: There is a set, $\emptyset$, having no members:

$$\exists B\ \forall x\ x \notin B.$$

Ax3. **Pairing**: For any sets u and v, there exists a set, denoted $\{u, v\}$, whose members are exactly u and v:

$$\forall u\ \forall v\ \exists B\ \forall x\ (x \in B \iff x = u \vee x = v)$$

Ax4. **Union**: For any set A, there exists a set whose members are exactly the members of members of A:

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

Ax5. **Power set**: For any set a, there exists a set whose members are exactly the subsets of a:

$$\forall a\ \exists B\ \forall x\ (x \in B \iff x \subseteq a).$$

($x \subseteq a$ is taken to mean that $\forall t\ (t \in x \implies t \in a)$.)

Ax6. **Subset**: For each formula _ not containing B, the following is an axiom:

$$\forall t_1\ \cdots \forall t_k\ \forall c\ \exists B\ \forall x\ (x \in B \iff x \in c \wedge \_)$$

We require that _ be a logic formula built from expressions of the form $a \in B$ and $a = b$, joined (with clear parenthesization) by only the symbols $\forall$, $\exists$, $\neg$, $\wedge$, $\vee$, $\implies$, and $\iff$.

There are a few other axioms, to be introduced later.

1.2 A note on existence and predicate logic

Throughout this survey of set theory, when we show that some set exists, you can be assured that we have some way of phrasing it using the aforementioned predicate logic system. In practice, we may write something such as $\langle x, y \rangle$ in a predicate logic expression, which, strictly speaking, is not allowed in predicate logic. Yet since $\langle x, y \rangle$ exists, we can reasonably assume that we can insert the quantifier $\exists z$, replace instances of $\langle x, y \rangle$ with z, and thirdly impose that $\forall v \; v \in z \iff$ [$\langle x, y \rangle$'s predicate logic expression]. When we write a proof of a set S's existence, it may be useful to check this inductive hypothesis: that, if the component sets $\{s_i\}$ from which S is built can be written with valid predicate logic expressions, so can the S in consideration. But for purposes of abstraction and simple arguments, we neglect this standard of rigorous detail.

1.3 A universal set?

A universal set does not exist, by a contradiction argument: If A is a set, then the subset axiom tells us that $B = \{x \in A | x \notin x\}$ is also a set. Therefore, supposing there is some universal set A, we would have that $B \in B$ iff $B \in A$ and $B \notin B$. Having both $B \in B$ and $B \notin B$ poses a contradiction.

However, it is sometimes useful to discuss all sets which have a certain property, even if this collection of sets is not itself a set. In this case, we are discussing a **class** of sets.

1.4 Operations

The union axiom clearly defines a **union** operation ($\cup$), while the subset operation implies **intersection** ($\cap$), **set difference** ($\setminus$), and even **symmetric difference** ($\triangle$) operations. We can also discuss the **set complement**, A^c, which is really just $\Omega \setminus A$, with Ω typically implied by the context. These operations have many algebra-like properties (proofs can be an exercise):

- Pairwise union and intersection are *commutative*.
- Three-wise union and intersection are *associative*.
- *Distributive laws*: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Similarly for infinite union and intersection, $A \cap \bigcup \mathscr{B} = \bigcup_{X \in \mathscr{B}} (A \cap X)$ and $A \cup \bigcap \mathscr{B} = \bigcap_{X \in \mathscr{B}} (A \cup X)$, provided that $\mathscr{B} \neq \emptyset$.

- *De Morgan's laws*: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$. Likewise, for $\mathscr{A} \neq \emptyset$, $\left(\bigcup \mathscr{A}\right)^c = \bigcap_{X \in \mathscr{A}} X^c$ and $\left(\bigcap \mathscr{A}\right)^c = \bigcup_{X \in \mathscr{A}} X^c$.
- *Identities involving* $\emptyset$: $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$, and $A \cap (C \setminus A) = \emptyset$.

2 Relations and functions

2.1 Ordered pairs

Recall the **pair set** $\{x, y\}$ is the unique set containing exactly the two sets x and y. Also recall that by extensionality, whether we write $\{x, y\}$ or $\{y, x\}$, we are talking about the same set. For this section, we now want some way of representing order among sets, to obtain a set representation of some **ordered pair** $\langle x, y\rangle$, which does not equal $\langle y, x\rangle$. One way is to define $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$. It can be argued that with this definition, for all sets u v x and y, $\langle u, v\rangle = \langle x, y\rangle$ iff $u = x$ and $v = y$: The if direction is trivial by arguing you can substitute u and x interchangeably, while the only if direction is argued by cases. This justifies the definition of the **Cartesian product** $A \times B$: $A \times B = \{\langle x, y\rangle | x \in A \wedge y \in B\}$. $\langle x, y\rangle$ appears in the second power set of C if C contains both x and y; the subset axiom allows us to then construct a set containing exactly the pairs $\langle x, y\rangle$ with $x \in A$ and $y \in B$.

2.2 Relations

A **relation** is a set of ordered pairs (expressing this in predicate logic is left as an exercise to the reader). We proceed under the assumption that we know that some relation R is a set that exists, and hence can be expressed in predicate logic. For this relation R, we sometimes write xRy to denote $\langle x, y\rangle \in R$. One can use relations to encode information, such as the ordering of numbers, as we will see later on. We can define the **domain** (intuitively, the set of all x) and **range** (the set of all y) of a relation as one would expect, because for any $\langle x, y\rangle \in A$, we can find x and y in $\bigcup\bigcup A$, and use the subset axiom. We define the **field** to be the union of the domain and the range of a relation.

2.3 n-ary relations

We inductively define the ordered n-tuple[1] as follows:

$$\langle t_1, \ldots, t_n \rangle = \langle \langle t_1, \ldots, t_{n-1} \rangle t_n \rangle$$

The 1-tuple $\langle x \rangle$ is defined as x itself, for consistency. By an infinite, inductive argument, we can define n-ary relations, by taking more power sets and using subset.

2.4 Functions

A **function**, in set theory, is a relation F for which each $x \in \text{dom } F$ corresponds to only one $y \in \text{ran } F$ such that xFy. In a **single-rooted** relation, each $y \in \text{ran } F$ corresponds to only one x:

$$\forall x_1 \, \forall x_2 \, \forall y \, (\langle x_1, y \rangle \in F \wedge \langle x_2, y \rangle \in F) \implies x_1 = x_2$$

A single-rooted function is called **one-to-one**.

2.4.1 Definitions

To any sets A, F, and G (usually relations and, more strictly speaking, functions, but not necessarily), these definitions apply:

(a) The **inverse** of F is the set $F^{-1} = \{\langle u, v \rangle | vFu\}$.

(b) The **composition** of F and G is $F \circ G = \{\langle u, v \rangle | \exists t \, (uGt \wedge tFv)\}$.

(c) The **restriction** of F to A is $F \upharpoonright A = \{\langle u, v \rangle | uFv \wedge u \in A\}$.

(d) The **image** of A under F is $F[A] = \text{ran}(F \upharpoonright A)$.

The existence of these sets is established by the subset axiom. Try showing this for one of them!

[1] It's kind of puzzling that we are using n, a natural number, to define mathematical machinery with which we'll later define the naturals, reals, etc. For now, please don't read too much into the usage of numbers in set theory definitions; rather, think about quantity as an intuitive notion. I'd argue we don't need a formal number system, so long as our heads can think of counting and inductive arguments.

2.4.2 Theorems (proofs omitted)

E. For a set F, $\operatorname{dom} F^{-1} = \operatorname{ran} F$, and vice versa. If F is a relation, $(F^{-1})^{-1} = F$.

F. For any set F, F^{-1} is a function iff F is single-rooted. A relation F is a function iff F^{-1} is single-rooted.

G. For a one-to-one function F, if $x \in \operatorname{dom} F$, then $F^{-1}(F(x)) = x$; if $y \in \operatorname{ran} F$, then $F(F^{-1}(y)) = y$.

H. If F and G are functions, then the composition $F \circ G$ has domain $\{x \in \operatorname{dom} G | G(x) \in \operatorname{dom} F\}$.

I. For any sets F and G, $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$.

J. If $F : A \to B$ (F is a function from A to B: $\operatorname{dom} F = A$ and $\operatorname{ran} F \subseteq B$), with $A \neq \emptyset$,

   (a) there exists a function $G : B \to A$ such that $G \circ F = I_A$ iff F is one-to-one;

   (b) there exists a function $H : B \to A$ such that $F \circ H = I_B$ iff F maps A **onto** B (so that $\operatorname{ran} F = B$).

Proving the second part of this last theorem requires a new axiom, the **axiom of choice**.

Ax7. **Axiom of choice** (first form): For any relation R, there is a function $H \subseteq R$ with $\operatorname{dom} H = \operatorname{dom} R$.

We also have several more theorems:

K. For any sets F, A, B, and/or $\mathscr{A}$,

   (a) The image of the union is the union of the images: $F[A \cup B] = F[A] \cup F[B]$ and $F[\bigcup \mathscr{A}] = \bigcup_{A \in \mathscr{A}} F[A]$.

   (b) The image of an intersection is included in the intersection of the images: $F[A \cap B] \subseteq F[A] \cap F[B]$; $F[\bigcap \mathscr{A}] \subseteq \bigcap_{A \in \mathscr{A}} F[A]$.

   (c) The image of the difference includes the difference of the images: $F[A] \setminus F[B] \subseteq F[A \setminus B]$.

Equality holds in the last two if F is a single-rooted set, i.e. the tuples in F form a single-rooted relation.

- As a corollary, since a function G always has a single-rooted inverse, we have from this theorem that $G^{-1}[\bigcup \mathscr{A}] = \bigcup_{A \in \mathscr{A}} G^{-1}[A]$, $G^{-1}[\bigcap \mathscr{A}] = \bigcap_{A \in \mathscr{A}} G^{-1}[A]$, and $G^{-1}[A \setminus B] = G^{-1}[A] \setminus G^{-1}[B]$.

Several final notes, applicable to the notation used above: If I is a set called the index set, and F is a function whose domain includes I, then we can define the union over the index set as $\bigcup_{i \in I} F(i) = \bigcup \{F(i) | i \in I\} = \{x | (\exists i \in I) x \in F(i)\}$. Also, for any sets A and B, we can use power set, the existence of the Cartesian product $A \times B$, and subset to construct the set of all functions $F : A \to B$, denoted as ${}^{A}B$.

2.5 Infinite Cartesian products

Let I be some set and H some function whose domain includes I. $\bigtimes_{i \in I} H(i)$ is defined as set of all functions from I such that $\forall i \; i \in I \implies f(i) \in H(i)$. If we further impose that all $H(i) \neq \emptyset$, then we can re-write the axiom of choice:

Ax7. **Axiom of choice** (second form): For any set I and any function H with domain I, if $H(i) \neq \emptyset$ for all $i \in I$, then $\bigtimes_{i \in I} H(i) \neq \emptyset$.

2.6 Equivalence relations

A relation R is an **equivalence relation** on a set A if it is **reflexive** (xRx for all $x \in A$), **symmetric** (if xRy, then yRx also), and **transitive** (if xRy and yRz, then xRz) on A. Actually, symmetry and transitivity are sufficient to show a relation is an equivalence relation.

The set $[x]_R$ is the set of all t such that xRt. R here is a relation, but if it is also an equivalence relation, then $[x]_R$ is the **equivalence class** of x, modulo R. If R is an equivalence relation on A and $x, y \in A$, then $[x]_R = [y]_R$ iff xRy. Also, the set $\left\{[x]_R \,|\, x \in A\right\}$ exists. If R is an equivalence relation, then this set is called the **quotient set** A/R and pronounced "A modulo R."

The **partition** Π of a set A is a set of *nonempty* subsets of A that is disjoint and exhaustive, i.e. no two different sets in Π share common elements, and each element in A belongs to one set in Π. If R is an equivalence relation on A, then there is a unique partition $\left\{[x]_R \,|\, x \in A\right\}$, the set of all equivalence classes, over A.

For our last theorem on equivalence relations, we first define that a function $F : A \to A$ is compatible with an equivalence relation R on A if for all x and y in A, $xRy \implies F(x)RF(y)$. Under this assumption, there exists a unique function $\hat{F} : A/R \to A/R$ such that for all $x \in A$, $\hat{F}\left([x]_R\right) = [F(x)]_R$. If not, then no such $\hat{F}$ exists.

2.7 Ordering relations

Let A be any set. A **linear ordering** (**total ordering**) on A is a binary relation R on A ($R \subseteq A \times A$) which is transitive and satisfies **trichotomy** on A, in that exactly one of the following always holds: xRy, $x = y$, or yRx. If we have such a linear ordering, then we can be assured there is no x for which xRx, and for all sets $x \neq y$ which are both in A, either xRy or yRx, but not both.

3 Natural numbers

3.1 Inductive sets

Set theory takes a constructive, rather than axiomatic approach, to numbers, in that numbers are defined as sets rather than their own entities obeying certain axioms. We define the **successor** a^+ of a set a as $a^+ = a \cup \{a\}$; the number 0 is defined to be $\emptyset$. But before we continue, we write another axiom to help us:

Ax8. **Infinity axiom**: There exists an **inductive set**:

$$\exists A \ \left[\emptyset \in A \wedge (\forall a \in A)\ a^+ \in A\right]$$

Using this axiom and the subset axiom, we can construct a set, ω, containing the elements which appear in every inductive set. Let us call the elements of ω **natural numbers**, sets which belong to every inductive set. ω can be shown rigorously to be inductive, and a subset of every other inductive set, as our intuition tells us. The **induction principle** for ω observes that any inductive subset of ω is (coincides with) ω. This is a powerful, widely accepted proof idea which goes beyond basic logic and allows people to prove notions using the natural numbers. For instance, every natural number except 0 is the successor of some other natural number.

3.2 Transitive sets

A set A is defined to be **transitive** (not to be confused with our previous notion of transitivity) iff every member of a member of A is itself a member of A:

$$\exists a(x \in a \in A) \implies x \in A$$

For a transitive set a, $\bigcup(a^+) = a$. Every natural number is a transitive set. And every the set of natural numbers, ω, is a transitive set.

3.3 Recursion on ω

The recursion theorem (very involved proof) says that if we have a set A, a set $a \in A$, and a function $F : A \to A$, there exists a unique function $h : \omega \to A$ such that $h(0) = a$ and for every $n \in \omega$, $h(n^+) = F(h(n))$.

3.4 Arithmetic

A **binary operation** is a function from $A \times A$ to A. The recursion theorem gives us a set $A_m : \omega \to \omega$ such that $A_m(0) = m$ and $A_m(n^+) = A_m(n)^+$ for $n \in \omega$; this we define as adding m to the argument natural number n. Using subset, we can write the **addition function** as the set $+ = \{\langle\langle m, n\rangle, p\rangle | m \in \omega \wedge n \in \omega \wedge p = A_m(n)\}$. The construction of $+$ gives us additive identity, that $m + 0 = m$, and that $m + n^+ = (m + n)^+$. We can define a **multiplication function** similarly, starting with a set $M_m : \omega \to \omega$ for which $M_m(0) = 0$ and $M_m(n^+) = M_m(n) + m$. As expected, we have that $m \cdot 0 = 0$ and $m \cdot n^+ = m \cdot n + m$.

Associativity and commutativity of addition, the distributive law, and associativity and commutativity of multiplication can by proven by induction in set theory.

3.5 Ordering on ω

For $x, y \in \omega$, we say that $x < y$ if $x \in y$. This ordering relation is transitive because each natural number is a transitive set, so $m \in n \wedge n \in p \implies m \in p$. It is a linear ordering because it also satisfies trichotomy: for all m and n in ω, either $m \in n$, $m = n$, or $n \in m$, but not more than one of these. We define the **proper subset** $\subset$ as $A \subset B$ iff $A \subseteq B$ and $A \neq B$. For $m, n \in \omega$, $m \in n \iff m \subset n$, and $m \in n \vee m = n \iff m \subseteq n$. For any natural numbers $m, n, p \in \omega$,

$m \in n \iff m+p \in n+p$, and if $p \neq 0$, $m \in n \iff m \cdot p \in n \cdot p$. As a consequence, and by trichotomy, $m+p = n+p \implies m = n$, and $m \cdot p = n \cdot p \wedge p \neq 0 \implies m = n$.

Let A be a nonempty subset of ω. Then there is a "least" element m of A, in that $m \leq n$ for all $n \in A$. This is called the **well-ordering** principle. Consequently, by induction, there is no function $f : \omega \to \omega$ such that $f(n^+) \in f(n)$ for every natural number n. The **strong induction principle** states that if $A \subseteq \omega$, and for all $n \in \omega$, all numbers less than n being in A implies n is in A, then $A = \omega$. The well-ordering principle also provides an alternate approach to induction: consider not the set of natural numbers for which a statement holds, but the set C for which it does not; to show that $C = \emptyset$, show that it cannot have a least element.

4 Real numbers

4.1 Integers

To define the integers, we define an *equivalence* relation over $\omega \times \omega$ as follows: $\sim = \{\langle\langle m, n\rangle, \langle p, q\rangle\rangle \in (\omega \times \omega) \times (\omega \times \omega) | m + q = p + n\}$. Then, we define the set of integers, $\mathbb{Z}$, as $(\omega \times \omega)/\sim$, which exists by a previous theorem.

Before we define addition, we show that if $\langle m, n\rangle = \langle m', n'\rangle$ and $\langle p, q\rangle = \langle p', q'\rangle$, then $\langle m + p, n + q\rangle = \langle m' + p', n' + q'\rangle$. Armed with this lemma, we can now define the **addition of two integers** $a +_Z b$ by selecting one element from each's equivalence class, and regardless of which of these elements $\langle m, n\rangle$ and $\langle p, q\rangle$ we select, we will get a member of the same equivalence class by doing $\langle m + p, n + q\rangle$. This addition operation obeys the properties of commutativity and associativity which we have come to expect. 0 is an additive identity element, and for any integer a there is an additive inverse integer b. (As a side note, these properties show that the integers form an **Abelian group**.)

So we have a subtraction operation $-_Z$, and now we would like a multiplication operation. Guided by our previous intuitive grasp of multiplication, we define the **multiplication of two integers** $a \cdot_Z b$ by taking $\langle m, n\rangle \in a$, $\langle p, q\rangle \in b$, and spitting out the integer containing $\langle m \cdot p + n \cdot q, m \cdot q + p \cdot n\rangle$. With some work, we can show this multiplication operation is also commutative, associative, and even distributive over $+_Z$. The integer 1_Z, which is $\neq 0_Z$, serves as a multiplicative identity element for all integers, and we also can show that $a \cdot_Z b = 0$ iff either $a = 0_Z$ or $b = 0_Z$.

To obtain an ordering relation over the integers, we first observe that if $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then $m + q \in p + n \iff m' + q' \in p' + n'$. The

desired ordering relation $<_Z$ is defined as the subset of $\langle\langle m, n\rangle, \langle p, q\rangle\rangle \in \mathbb{Z} \times \mathbb{Z}$ for which $m + q \in p + n$. $<_Z$ is a linear ordering, in that it is transitive and obeys trichotomy. Additionally, addition of any integer and multiplication by a positive integer $c : 0 <_Z c$ preserves order. If we have that $a + c = b + c$, we can conclude $a = b$, and likewise if $a \cdot c = b \cdot c$ with $c \neq 0$.

Lastly, let us draw a comparison between the natural numbers and the integers. Define $E : \omega \to \mathbb{Z}$ so that $E(n) = \big[\langle n, 0\rangle\big]$. E maps ω one-to-one into $\mathbb{Z}$, and satisfies these properties for any natural numbers m and n:

(a) $E(m + n) = E(m) +_Z E(n)$

(b) $E(m \cdot n) = E(m) \cdot_Z E(n)$

(c) $m \in n$ iff $E(m) <_Z E(n)$

So although ω is not a subset of $\mathbb{Z}$, $\mathbb{Z}$ extends ω in a way that preserves beautifully the operations and properties of addition, multiplication, and ordering.

4.2 Rational numbers

The rationals extend from the integers much like the integers extend from the naturals. We start by defining a relation $\sim$ on $\mathbb{Z} \times \mathbb{Z}'$, with $\mathbb{Z}'$ the set of integers minus the set containing 0_Z. Using subset, let $\langle a, b\rangle \sim \langle c, d\rangle$ iff $a \cdot d = c \cdot b$. Now, we can construct the rationals $\mathbb{Q}$ as $(\mathbb{Z} \times \mathbb{Z}')/\sim$, the set of all equivalence classes of **fractions** (which are ordered pairs of integers, the second component of which is nonzero). As usual, $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$, obeying reflexivity, symmetry, and transitivity.

If we let out intuition guide us, an addition operation $+_Q$ can be defined so that $\big[\langle a, b\rangle\big] +_Q \big[\langle c, d\rangle\big] = \big[\langle ad + cb, bd\rangle\big]$. This leaves $0_Q = \big[\langle 0, 1\rangle\big]$ as an additive identity element. An Abelian group has again sprung up, as addition over $\mathbb{Q}$ is associative and commutative, 0_Q as an additive identity element, and for any r in $\mathbb{Q}$ there is an additive inverse element s.

We also define a multiplication operation $\cdot_Q$ so that $\big[\langle a, b\rangle\big] \cdot_Q \big[\langle c, d\rangle\big] = \big[\langle ac, bd\rangle\big]$. $1_Q = \big[\langle 1, 1\rangle\big]$ is a multiplicative identity element. Multiplication of rationals is associative, commutative, and distributive over addition. For any $r \in \mathbb{Q}$, there is a multiplicative inverse $q \in \mathbb{Q}$ such that $r \cdot_Q q = 1_Q$. If r and s are nonzero, then so is $r \cdot_Q s$.

To obtain an ordering relation, we again follow our intuition to arrive at $\big[\langle a, b\rangle\big] <_Q \big[\langle c, d\rangle\big]$ iff $ad <_Q cb$, but only when the denominators b and d are positive. Then

it does not matter which a, b, c, and d we use, as long as b and d are positive. $<_Q$ is a linear ordering on $\mathbb{Q}$. Now, $r <_Q s$ iff $r +_Q t <_Q s +_Q t$, and if $0 <_Q t$, then $r <_Q s$ iff $r \cdot_Q t <_Q s \cdot_Q t$. And again, if $r +_Q t = s +_Q t$, then $r = s$; if $r \cdot_Q t = s \cdot_Q t$ with $t \neq 0_Q$, then $r = s$.

Finally, like before, we can draw a comparison between the integers and the rational numbers. Define $E : \mathbb{Z} \to \mathbb{Q}$ so that $E(n) = \left[\langle n, 1\rangle\right]$. This one-to-one function obeys similar properties as the equivalent function for the integers:

(a) $E(a +_Z b) = E(a) +_Q E(b)$

(b) $E(a \cdot_Z b) = E(a) \cdot_Q E(b)$

(c) $E(0_Z) = 0_Q$ and $E(1_Z) = 1_Q$

(d) $a <_Z b$ iff $E(a) <_Q E(b)$

4.3 Real numbers

Long ago, mathematicians discovered that certain quantities simply could not be measured to complete precision with rational numbers. The real number system came along to circumvent this issue. The real numbers can extend from the rationals in several ways. One way is to define the real numbers as the set of all Dedekind cuts. A **Dedekind cut** is a subset $x \subseteq \mathbb{Q}$ such that

(a) $\emptyset \neq x \neq \mathbb{Q}$,

(b) x is "closed downward," i.e.

$$q \in x \wedge r < q \implies r \in x,$$

(c) and x has no largest member.

A linear ordering is obtained so that $x <_R y$ iff $x \subset y$. An **upper bound** on a set of real numbers A is a real number x such that for all $y \in A$, $y \leq x$. Any bounded, nonempty subset of $\mathbb{R}$ has a least upper bound in $\mathbb{R}$.

We define the addition operation so that for any $x, y \in \mathbb{R}$, $x +_R y = \{q + r | q \in x \wedge r \in y\}$. Addition is associative and commutative. The zero element is defined as the real number $0_R = \{r \in \mathbb{Q} | r < 0\}$. 0_R is real, and for any $x \in \mathbb{R}$, $x +_R 0_R = x$. For every $x \in \mathbb{R}$, there is an inverse element $-x \in \mathbb{R}$ such that $x +_R (-x) = 0_R$. So $\langle \mathbb{R}, +_R, 0_R \rangle$ is an Abelian group. The cancellation law holds: $x +_R z = y +_R z \implies x = y$. For any real numbers, $x <_R y \iff x +_R z <_R y +_R z$.

5 Cardinal numbers and the axiom of choice

5.1 Equinumerosity

In an effort to count sets which may be infinite, we say two sets A and B are **equinumerous** ($A \approx B$) iff there exists a one-to-one function from A onto B. Equinumerosity has the property of being reflexive, symmetric, and transitive for all sets A, B, and C:

(a) $A \approx A$.

(b) If $A \approx B$, then $B \approx A$.

(c) If $A \approx B$ and $B \approx C$, then $A \approx C$.

For example, ω is not equinumerous to $\mathbb{R}$ by a diagonalization argument; similarly, no set is equinumerous to its power set.

5.2 Finite sets

A set is called **finite** iff it is equinumerous to some natural number, n. Otherwise, it is called **infinite**. The **pigeonhole principle** states that no natural number is equinumerous to a proper subset of itself. By an extension of the same proof, no finite set is equinumerous to a proper subset of itself. Hence, any set equinumerous to a proper subset of itself is infinite; ω, for one, is infinite.

Any finite set A is equinumerous to a *unique* natural number, its **cardinal number**, $\operatorname{card} A$. While this defines $\operatorname{card} A$ when A is finite, we will define $\operatorname{card} A$ for infinite A in the next section, so that for any sets A and B, $\operatorname{card} A = \operatorname{card} B$ iff $A \approx B$. Now, without knowing its actual definition, we will now denote $\operatorname{card} \omega$ as $\aleph_0$. Note that the class of all sets of cardinality $\kappa > 0$ is not a set itself.

Lastly, any subset of a finite set is finite. This is accomplished through a lemma: if $C \subset n \in \omega$, then $C \approx m$ for some $m < n$.

5.3 Cardinal arithmetic

To extend addition, multiplication, and exponentiation to all sets, including infinite sets, we will establish notions of cardinal arithmetic. For cardinal numbers κ and λ, define these operations accordingly:

1. $\kappa + \lambda = \operatorname{card}(K \cup L)$, with K and L *disjoint* and of cardinalities κ and λ.

2. $\kappa \cdot \lambda = \text{card}(K \times L)$, with K and L of cardinalities κ and λ.

3. $\kappa^\lambda = \text{card}\, {}^L K$, with K and L of cardinalities κ and λ.

It can be shown that for each of these above operations, we'll get the same result for any suitable K and L.

Cardinal arithmetic follows similar properties as other forms of arithmetic. For any cardinal numbers κ, λ, and μ:

1. $\kappa + \lambda = \lambda + \kappa$ and $\kappa \cdot \lambda = \lambda \cdot \kappa$.

2. $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$ and $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$.

3. $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

4. $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$.

5. $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$.

6. $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$.

If m and n are finite cardinals, then addition, multiplication, and exponentiation produce the same result in cardinal arithmetic as in regular arithmetic:

$$m + n = m +_\omega n$$
$$m \cdot n = m \cdot_\omega n$$
$$m^n = m^n$$

If A and B are finite, then $A \cup B$, $A \times B$, and ${}^B A$ are finite.

5.4 Ordering cardinal numbers

We say that A is **dominated** by set B ($A \preccurlyeq B$) iff there is a one-to-one function from A into B, or equivalently, iff A is equinumerous with a subset of B (including B itself). We conveniently define that $\text{card}\, K \leq \text{card}\, L \iff K \preccurlyeq L$. Naturally, we likewise say that $\text{card}\, K < \text{card}\, L \iff K \prec L \iff K \preccurlyeq L \wedge K \not\approx L$.[2]

The following properties hold for all cardinal numbers κ, λ, and μ:

[2]Since we have not established the class of all cardinal numbers as a set, we technically have not rigorously defined this ordering as a relation. For now, we can consider it an extension of our notation, that using any one of the above statements implies them all.

1. $\kappa \leq \kappa$.

2. $\kappa \leq \lambda \leq \mu \implies \kappa \leq \mu$.

3. $\kappa \leq \lambda \wedge \lambda \leq \kappa \implies \kappa = \lambda$. This is one half of the **Schröder-Bernstein Theorem**, the other half being: if $A \preccurlyeq B$ and $B \preccurlyeq A$, then $A \approx B$.

4. Either $\kappa \leq \lambda$ or $\lambda \leq \kappa$. Proving this requires the axiom of choice.

These order-preserving properties also hold:

(a) $\kappa \leq \lambda \implies \kappa + \mu \leq \lambda + \mu$.

(b) $\kappa \leq \lambda \implies \kappa \cdot \mu \leq \lambda \cdot \mu$.

(c) $\kappa \leq \lambda \implies \kappa^{\mu} \leq \lambda^{\mu}$.

(d) $\kappa \leq \lambda \implies \mu^{\kappa} \leq \mu^{\lambda}$.

5.5 Axiom of choice

A couple times, we have already encountered the axiom of choice, which allows us to select members from nonempty sets. There are many equivalent formulations. Here are six different statements of the axiom:

1. For any relation R, there is a function $F \subseteq R$ with $\operatorname{dom} F = \operatorname{dom} R$.

2. The Cartesian product of nonempty sets is always nonempty. For a function H with $\operatorname{dom} H = I$, such that $(\forall i \in I) H(i) \neq \emptyset$, there is a function f with $\operatorname{dom} f = I$ such that $(\forall i \in I) f(i) \in H(i)$.

3. For any set A there is a "choice function" F such that dom is the set of nonempty subsets of A, and $F(B) \in B$ for every nonempty $B \subseteq A$.

4. Suppose each member of a set $\mathscr{A}$ is nonempty, and every two distinct members of $\mathscr{A}$ are disjoint. Then there exists a set C containing exactly one element from each member of $\mathscr{A}$.

5. For any two sets C and D, either $C \preccurlyeq D$ or $D \preccurlyeq C$. For any cardinal numbers κ and λ, either $\kappa \leq \lambda$ or $\lambda \leq \kappa$.

6. **Zorn's lemma**: Let $\mathscr{A}$ be a set such that for every chain $\mathscr{B} \subseteq \mathscr{A}$, $\bigcup \mathscr{B} \in \mathscr{A}$. ($\mathscr{B}$ is a **chain** iff for any $C, D \in \mathscr{B}$, either $C \subseteq D$ or $D \subseteq C$.) Then $\mathscr{A}$ contains an element M (a "maximal" element) such that M is not a subset of any other set in $\mathscr{A}$.

Note that this axiom has been fairly controversial, so mathematicians make explicit mention whenever they use it.

Using the axiom of choice (e.g. the third version), we can show that the natural numbers are the "smallest" infinite set, in that for any infinite set, $\omega \preccurlyeq A$. This is equivalently stated as $\aleph_0 \leq \kappa$ for any infinite cardinal κ. Furthermore, we can now strengthen a previous result by proving a set is infinite *iff* (not just if) it is equinumerous to a proper subset of itself.

5.6 Countable sets

A set is said to be **countable** iff $A \preccurlyeq \omega$, i.e. iff card $A \leq \aleph_0$. A set is countable iff it is finite or has cardinality $\aleph_0$. Now, if $A \preccurlyeq B$, then there exists a function from B *onto* A.

5.7 Arithmetic of infinite cardinals

By a lengthy proof, for any infinite cardinal number κ, $\kappa \cdot \kappa = \kappa$. The **absorption law** of cardinal arithmetic states that for κ and λ, the larger being infinite and the smaller at least nonzero, $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$.

5.8 Continuum hypothesis

The **continuum hypothesis** asserts that there is no set with cardinality κ such that $\aleph_0 < \kappa < 2^{\aleph_0}$. The continuum hypothesis is actually neither provable nor refutable, but undecidable under our axioms. The **generalized continuum hypothesis**, the assertion that for every infinite cardinal κ there is no cardinal number between κ and 2^κ, is likewise undecidable. Also, the axiom of choice is undecidable from our other axioms.

6 Orderings and ordinals

6.1 Partial orderings

A **partial ordering** is a relation R that is transitive ($xRy \wedge yRz \implies xRz$) and irreflexive (for no x is xRx). If $<$ is a partial ordering, then for any x, y, and z, at *most* one of $x < y$, $x = y$, and $y < x$ can hold; and $x \leq y \leq x \implies x = y$. R is a **linear ordering** on a specific set A if R is a binary relation on A that is a transitive relation and satisfies trichotomy on A, i.e. for any $x, y \in A$ exactly one of xRy, $x = y$, and yRx holds. (Any linear ordering is also a partial ordering.) A **structure** is a pair $\langle A, R\rangle$ consisting of a set A and a binary relation R on A.

A element m of D is **minimal** iff for D's partial ordering $<$, there is no $x \in D$ such that $x < m$. And m is **least** (or **smallest** or **minimum**) iff $m \leq x$ for all $x \in D$. A least element is also minimal; for a linear ordering, this conclusion goes both ways and the concepts coincide. If there is a least element, it is the one, unique minimal element, but otherwise there could be zero or many minimal elements. Analogous results hold for **maximal** (minimal) and **greatest/largest/maximum** (least) elements of sets.

If R is a partial ordering, then R^{-1} is a partial ordering. The minimal elements of R^{-1} are exactly the maximal elements with respect to R.

If $<$ is a partial ordering on A and $C \subseteq A$, then an **upper bound** of C is an element $b \in A$ such that $x \leq b$ for all $x \in C$. If $b \in C$, then b is C's greatest element. If b is the least element of the set of all upper bounds for C, then b is the **least upper bound** (**supremum**) of C. **Lower bound**, **greatest lower bound**, and **infimum** are defined analogously.

6.2 Well orderings

A **well ordering** on A is a linear ordering on A for which every nonempty subset of A has a least element. If $<$ is a linear ordering on A, then it is a well ordering iff there does not exist a function $f : \omega \to A$ with $f(n^+) < f(n)$ for all $n \in \omega$ (f is sometimes (ambiguously) called a **descending chain**).

If $<$ is any ordering on A and $t \in A$, then the set $\operatorname{seg} t = \{x | x < t\}$ is the **initial segment up to** t. Now, assume $<$ is a well ordering on A. Assume that B is a subset of A with the special property that for every $t \in A$, $\operatorname{seg} t \subseteq B \implies t \in B$ (B is a **$<$-inductive** subset of A). Then by the **transfinite induction principle**, B coincides with A. For the next theorem, let $<$ be a linear ordering on A, such that the only $<$-inductive subset of A is A itself. Then $<$ is a well ordering on A.

Next, we have a well ordering $<$ and would like to define a function F so that $F(t)$ is determined by all values in $\operatorname{seg} t$. We say that F is **G-constructed** if $F(t) = G(F \restriction \operatorname{seg} t)$ for all $t \in \operatorname{dom} F$. We also define ${}^{<A}B$ as the set of all functions in $\mathscr{P}(A \times B)$ (a subset axiom) which, for some $t \in A$, are from the initial segment $\operatorname{seg}_< t$ into B. Now, for the **transfinite recursion theorem**, one can show that if $<$ is a well ordering on A and $G : {}^{<A}B \to B$, then there is a unique function $F : A \to B$ such that for any $t \in A$, $F(t) = G(F \restriction \operatorname{seg} t)$. The more general **transfinite recursion theorem schema** (infinite package of theorems) states that for any formula $\gamma(x, y)$: If $<$ is a well ordering on a set A, and for any f there is a unique y such that $\gamma(f, y)$, then there exists a unique function F with domain A such that $\gamma(F \restriction \operatorname{seg} t, F(t))$ for all $t \in A$. ($\gamma(x, y)$ is "allowed to mention other fixed sets in addition to x and y.")

6.3 Replacement axioms

Unfortunately, we are unable to prove the transfinite recursion theorem schema, and a number of ideas about sets like inductive sets, without the help of another axiom.

Ax9. **Replacement axioms**: For any formula $\varphi(x, y)$ not containing the letter B, then the following is an axiom:

$$\forall A \Big[(\forall x \in A) \forall y_1 \forall y_2 \left(\varphi(x, y_1) \wedge \varphi(x, y_2) \implies y_1 = y_2 \right) \\ \implies \exists B \forall y \, (y \in B \iff (\exists x \in A) \varphi(x, y)) \Big]$$

Intuitively, $\varphi(x, y)$ can be read as "x nominates y"; the axiom supposes that each member of A nominates at most one object, and concludes that the collection of all nominees is a set, and furthermore a unique set.

6.4 Epsilon-images

Let $<$ be a well ordering on A and take $\gamma(x, y)$ to be the formula $y = \operatorname{ran} x$. By the transfinite recursion theorem, we can obtain a unique function E with domain A such that for any $t \in A$, $E(t) = \operatorname{ran}(E \restriction \operatorname{seg} t) = E[\operatorname{seg} t] = \{E(x) | x < t\}$. Let $\alpha = \operatorname{ran} E$ be the **$\in$-image** of the well-ordered structure $\langle A, < \rangle$. Then

(a) $E(t) \notin E(t)$ for all $t \in A$.

(b) E maps A one-to-one onto α.

(c) For any s and t in A, $s < t$ iff $E(s) \in E(t)$.

(d) α is a transitive set.

The binary relation (on α) $\in_\alpha = \{\langle x, y\rangle \in \alpha \times \alpha | x \in y\}$ is a well ordering on α, under these assumptions.

6.5 Isomorphisms

6.6 Ordinal numbers