# Foundational Mathematics

Abiyaz Chowdhury

May 6, 2019

## 1 Zermelo-Frenkel and Choice Set Theory (ZFC) Formulation

**Axiom 1.1** Extension: For every set $A$ and every set $B$, $A = B$ if and only if for every set $x$, $x \in A$ if and only if $x \in B$.

**Definition 1.1** Two sets $A$ and $B$ are disjoint from one another if no set is both an element of $A$ and an element of $B$.

**Axiom 1.2** Regularity: Every non-empty set $A$ contains an element $x$ such that $A$ and $x$ are disjoint sets.

**Axiom 1.3** Empty set: There exists a set $\varnothing$ such that for every set $x$, $x \notin \varnothing$. We call this set the empty set.

**Definition 1.2** A set that is not the empty set is called nonempty.

**Axiom 1.4** Specification: If $A$ is a set and $P(x)$ is a formula of first order logic, then there exists a set $B$ containing precisely each $x \in A$ such that $P(x)$ is true.

**Axiom 1.5** Pairing: If $A$ and $B$ are sets, then there exists a set containing precisely $A$ and $B$.

**Theorem 1.1** ■ No set is an element of itself.

**Theorem 1.2** ■ If $a$ and $b$ are sets such that $a \in b$, then it is not the case that $b \in a$.

**Axiom 1.6** Unions: Let $\mathcal{A}$ be a collection of sets. Then there exists a set $\bigcup_{A \in \mathcal{A}} A$ such that $x \in \bigcup_{A \in \mathcal{A}} A$ if and only if there exists an $A \in \mathcal{A}$ such that $x \in A$.

**Definition 1.3** The union of two sets, $A$ and $B$, is usually denoted by $A \cup B = \bigcup_{X \in \{A,B\}} X$.

**Definition 1.4** A set $A$ is said to be a subset of a set $B$ if for every set $x$, $x \in A$ implies $x \in B$. When this is the case, we write $A \subseteq B$. If $A \subseteq B$ and $A \neq B$, we write $A \subset B$, and say $A$ is a proper subset of $B$.

**Theorem 1.3** ■ $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

**Theorem 1.4** ■ If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

**Theorem 1.5** ■ For every set $A$, $A \subseteq A$.

**Theorem 1.6** ■ For every set $A$, $\varnothing \subseteq A$.

**Theorem 1.7** ■ $\varnothing$ has no proper subsets, and its only subset is $\varnothing$.

**Definition 1.5** Let $\mathcal{A}$ be a nonempty collection of sets. Let $X \in \mathcal{A}$. Then the intersection of $\mathcal{A}$ is the set set $\bigcap_{A \in \mathcal{A}} A = \{x \in X | x \in A \text{ for every } A \in \mathcal{A}\}$

**Theorem 1.8** ■ If $A$ and $B$ are sets, then $A$ and $B$ are disjoint if and only if their intersection is $\varnothing$.

**Definition 1.6** Let $A$ and $B$ be sets. The difference of $A$ and $B$ is the set $A \backslash B = \{x \in A | x \notin B\}$.

**Definition 1.7** Let $a$ and $b$ be sets. The ordered pair $(a, b)$ is the set $(\{\{a\}, \{a, b\}\}$.

**Theorem 1.9** ■ $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

**Axiom 1.7** Replacement: Let $A$ be a set and let $\phi(a, b)$ be a formula of first-order logic such that for each $a \in A$ there is a unique $b$ for which $\phi(a, b)$ is true. Then there exists a set $B$ consisting of all $b$ for which some $a \in A$ satisfies $\phi(a, b)$.

**Axiom 1.8** Infinity: There exists a set $X$ such that $\varnothing \in X$ and whenever $w \in X$, then $\{w \cup \{w\}\} \in X$.

**Axiom 1.9** Powers: For every set $X$, there exists a set $\mathcal{P}(X)$ such that $A \in \mathcal{P}(X)$ if and only if $A \subset X$.

Remarks: The above axioms form the ZF part of ZFC. The final axiom, or the axiom of choice, is deferred to the next section. The axiom of pairing follows from the axioms of replacement, powers, and infinity. The axiom of the empty set can be inferred from the axiom of specification when at least one set is known to exist. In the semantics of first-order logic, at least one set exists since the domain of discourse is nonempty. Hence some set must exist, and we can use this to construct the empty set. In a free logic, where the domain of discourse could be empty, the axiom of infinity can be modified to also imply the axiom of the empty set but we do not do this for simplicity and convenience. Nevertheless, the above axioms as a whole are not minimal, and are listed for the sake of completeness.

# 2 Functions

**Definition 2.1** Let $A$ and $B$ be given sets. The Cartesian product of $A$ and $B$ is $A \times B = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) | z = (a, b) \text{ for some } a \in A, b \in B\}$

**Definition 2.2** Let $A$ and $B$ be sets. A relation $R$ from $A$ to $B$ is a subset of $A \times B$. If $(a, b) \in R$, we write $aRb$. The domain of $R$ is the set $\text{dom}(R) = \{a \in A | \exists b \in B \text{ s.t. } aRb\}$. The range of $R$ is the set $\text{ran}(R) = \{b \in B | \exists a \in A \text{ s.t. } aRb\}$. If $R$ is a relation from $A$ to $A$, we say $R$ is a relation in $A$.

**Definition 2.3** A function (or mapping) $f$ from $A$ to $B$ is a relation from $A$ to $B$ with the following property: For every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$. Given $a \in A$, we write $f(a)$ for the unique element of $B$ such that $(a, f(a)) \in f$. If a function $f$ is from $A$ to $B$, we write $f : A \to B$. $A$ is said to be the domain of $A$ and $B$ the codomain. Typically, when a function $f$ is defined, its domain and codomain are implicitly assumed to be non-empty.

**Theorem 2.1** ■ Two functions $f : S \to T$ and $g : S \to T$ are equal if and only if $f(x) = g(x)$ $\forall x \in S$.

## 2.1 The axiom of choice

**Axiom 2.1** Choice: If $X$ is a collection of nonempty sets, then there exists a function $f : X \to \bigcup X$ satisfying $f(A) \in A$ for all $A \in X$.

## 2.2 Inverse mappings

**Definition 2.4** Let $f : A \to B$, and $A' \subset A$. The restriction of $f$ to $A'$ is the function $f|_{A'}$, which maps from $A'$ to $B$, and is defined on as $f|_{A'}(x) = f(x)$ for all $x \in A'$.

**Definition 2.5** A family of sets is a function $A$ with domain $I$. When $A$ is a family over the set $I$, we write $\{A_i\}_{i \in I}$, we write $A_i$ for $A(i)$.

**Definition 2.6** Let $S \neq \varnothing$ be a set. Then the function $f : S \to S$ defined as $f(x) = x$ for all $x \in S$ is called the identity function on $S$ and often denoted as $I_S$.

**Definition 2.7** Composition of two functions: Let $f : S \to T$ and $g : R \to S$ be functions such that the domain of $f$ is the same as the codomain of $g$. Then the composite of $f$ and $g$ is defined as $f \circ g = \{(x, z) \in R \times T : \exists y \in S : (x, y) \in g \wedge (y, z) \in f\}$

**Theorem 2.2** ■ The compositon of two functions $f : S \to T$ and $g : R \to S$ is a function from $R$ to $T$ and we have that for all $x \in R$, $f(g(x)) = (f \circ g)(x)$.

**Theorem 2.3** ■ Composition of functions is associative, i.e. if $f_1 : S_1 \to S_2$, $f_2 : S_2 \to S_3$ and $f_3 : S_3 \to S_4$, then $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$

**Definition 2.8** Let $S, T$ be sets where $S \neq \varnothing$, and let $f : S \to T$ be a function. If $g : T \to S$ is a function such that $g \circ f = I_S$, then $g : T \to S$ is called a left inverse of $f$.

**Definition 2.9** Let $S, T$ be sets where $S \neq \varnothing$, and let $f : S \to T$ be a function. If $g : T \to S$ is a function such that $f \circ g = I_T$, then $g : T \to S$ is called a right inverse of $f$.

**Definition 2.10** Let $S, T$ be sets where $S \neq \varnothing$, and let $f : S \to T$ be a function. If $g : T \to S$ is a function such that $g \circ f = I_S$, then $g : T \to S$ is called a left inverse of $f$.

**Definition 2.11** Let $f : S \to T$. $f$ is said to be injective if $f(x) = f(y)$ implies $x = y$ for all $x, y \in S$. $f$ is said to be surjective if for every $y \in T$, there exists at least one $x \in A$ such that $f(x) = y$. $f$ is said to be bijective (or invertible) if $f$ is both injective and surjective.

**Theorem 2.4** ■ For any nonempty set $S$, the identity function $I_S$ is both an injection and a surjection.

**Theorem 2.5** ■ Let $f, g$ be functions such that $g \circ f$ is an injection. Then $f$ is an injection.

**Theorem 2.6** ■ Let $f, g$ be functions such that $g \circ f$ is an surjection. Then $g$ is an surjection.

**Definition 2.12** If $f : S \to T$ is a function, then $f(S) = \{y \in T | f(x) = y \text{ for some } x \in S\}$ is called the range or image of $f$.

**Definition 2.13** If $f : S \to T$ is a function, then we define a left inverse of $f$ to be a function $g : T \to S$ such that $g \circ f = I_S$.

**Definition 2.14** If $f : S \to T$ is a function, then we define a right inverse of $f$ to be a function $g : T \to S$ such that $f \circ g = I_T$.

**Theorem 2.7** ■ The function $f : S \to T$ is an injection if and only if it has a left inverse.

**Theorem 2.8** ■ The function $f : S \to T$ is a surjection if and only if it has a right inverse.

**Theorem 2.9** ■ If $S$ and $T$ are nonempty sets, then there exists an injection from $S$ to $T$ if and only if there exists a surjection from $T$ to $S$.

**Theorem 2.10** ■ If $f : S \to T$ and $g : R \to S$ are injections, then the composition $f \circ g : R \to T$ is an injection.

**Theorem 2.11** ■ If $f : S \to T$ and $g : R \to S$ are surjections, then the composition $f \circ g : R \to T$ is a surjection.

**Theorem 2.12** ■ The function $f : S \to T$ is a surjection if and only if $T = f(S)$.

**Theorem 2.13** ■ Let $f$ be a function having a left inverse and a right inverse. Then $f$ is a bijection.

**Theorem 2.14** ■ Let $f : S \to T$ be a bijection. Then it has a unique left inverse, and a unique right inverse. Moreover, these two inverses are the same function, and are denoted by $f^{-1}$, which is called the inverse of $f$. The function $f^{-1}$ is thus the only left inverse and only right inverse of $f$.

**Theorem 2.15** ■ For any function $f$, its inverse $f^{-1}$ is also a bijection. Moreover, $(f^{-1})^{-1} = f$.

**Theorem 2.16** ■ If there exists a bijection from $S$ to $T$, then there exists a bijection from $T$ to $S$.

**Theorem 2.17** ■ If $f : S \to T$ and $g : R \to S$ are bijections, then the composition $f \circ g : R \to T$ is a bijection. In particular, $(f \circ g)^{-1} = (g^{-1} \circ f^{-1})$.

**Theorem 2.18** ■ Schröder-Bernstein: If there exists an injection from $S$ to $T$ and an injection from $T$ to $S$, then there exists a bijection between the sets.

# 3 The natural numbers $\mathbb{N}$

## 3.1 Inductive sets

**Theorem 3.1** ■ If $\mathcal{A}$ is a nonempty collection of sets, then the set $\left[\bigcap_{A\in\mathcal{A}} A\right] \subseteq A$ for all $A \in \mathcal{A}$.

**Theorem 3.2** ■ If $\mathcal{A}$ is a nonempty collection of sets, then the set $A \subseteq \left[\bigcup_{A\in\mathcal{A}} A\right]$ for all $A \in \mathcal{A}$.

**Definition 3.1** For any set $x$, we may define the set $x^+ = x \cup \{x\}$.

**Definition 3.2** A set $S$ is said to be inductive if and only if $\varnothing \in S$ and $x^+ \in S$ whenever $x \in S$. From the axiom of infinity, at least one inductive set exists.

**Theorem 3.3** ■ Let $S$ be any inductive set. Let $\mathbb{N}_S = \cap\{A \subseteq S | A \text{ is inductive }\}$. Then $\mathbb{N}_S$ is a set, since it is the intersection of elements in $\mathcal{P}(S)$. Moreover, $\mathbb{N}_S \subseteq S$.

**Theorem 3.4** ■ The intersection of any nonempty collection of inductive sets is inductive.

**Theorem 3.5** ■ If $S$ is inductive, then $\mathbb{N}_S$ is inductive.

**Theorem 3.6** ■ If $S$ and $T$ are any two inductive sets, then $\mathbb{N}_S = \mathbb{N}_T$. Therefore, we may define the unique set $\mathbb{N} = \mathbb{N}_S$ which is unique regardless of the choice of $S$. We call $\mathbb{N}$ the set of natural numbers, or the set of counting numbers.

**Theorem 3.7** ■ If $S$ is any inductive set, then $\mathbb{N} \subseteq S$.

**Theorem 3.8** ■ No proper subset of $\mathbb{N}$ is inductive.

**Theorem 3.9** ■ If $S$ is an inductive set such that no proper subset of $S$ is inductive, then $S = \mathbb{N}$.

**Theorem 3.10** ■ If $n \in \mathbb{N}$, and $m \in n$, then $m \subseteq n$.

**Theorem 3.11** ■ If $n \in \mathbb{N}$ and $m \in n$, then $n \not\subseteq m$.

## 3.2 Peano Axioms

**Theorem 3.12** Let $0 = \varnothing$ and let $s(x) = x^+$. Then $\mathbb{N}$ satisfies the following:

1. ■ $0 \in \mathbb{N}$
2. ■ If $n \in \mathbb{N}$, then $s(n) \in \mathbb{N}$.
3. ■ For all $n \in \mathbb{N}$, $s(n) \neq 0$.
4. ■ If $s(n) = s(m)$, then $n = m$.
5. ■ If $S \subseteq \mathbb{N}$ is such that $0 \in S$, and $s(n) \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

Remark: The Peano axioms are typically formulated as a definition of the natural numbers. However, as shown above, they can be derived from the axiom of infinity, and hence are stated here as theorems. We may sometimes write $s(x)$, the successor function, as $x+1$. In the decimal system, we may represent the naturals using Arabic numerals as follows: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, ...\}$.

## 3.3 Order

**Definition 3.3** Let $R$ be a relation in a set $S$. Then $R$ is a partial order if it satisfies the following properties:

1. Reflexivity: $(a, a) \in R \; \forall a \in S$.
2. Antisymmetry: If $(a, b) \in R$ and $(b, a) \in R$, then $a = b$.
3. Transitivity: If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

A set with a partial order is called a partially ordered set (or poset). We usually write $a \leq b$ to denote that $(a, b) \in R$. For elements $a, b$ of a poset $P$, if either $a \leq b$ or $b \leq a$, then the elements $a, b$ are said to be comparable to one another. In some cases, $(P, \leq)$ is used to denote the partially ordered set $P$ under the partial order $\leq$.

**Theorem 3.13** ■ If $\mathcal{X}$ is a collection of sets, then the relation $R$ defined for all $A, B \in \mathcal{X}$ by $(A, B) \in R$ if and only if $A \subseteq B$ is a partial order in $\mathcal{X}$.

**Definition 3.4** Given a partial order $R$ in a set $S$, we may define a relation $R'$ in $S$ as $(a, b) \in R'$ if and only if $(a, b) \in R$ and $a \neq b$. If $(a, b) \in R$ is denoted by $a \leq b$, then $(a, b) \in R'$ is usually denoted by $a < b$. The relation $R'$ thus induced from the partial order $R$ is called a strict (or irreflexive) order.

**Theorem 3.14** ■ The relation $R'$ in $S$, as defined above, is transitive. Moreover, it is anti-reflexive, meaning that for all $x \in S$, $(x, x) \notin R'$. If $(x, y) \in R'$ for some $x, y \in S$, then $(y, x) \notin R'$.

**Definition 3.5** If we write $a \leq b$ to denote $(a, b) \in R$, then we usually write $a \geq b$ to denote $(b, a) \in R$. Similarly, $a > b$ means that $a \geq b$ and $b \neq a$.

**Definition 3.6** A partial order under which every pair of elements is comparable is called a total order or linear order. A totally ordered set is also called a chain.

**Theorem 3.15** ■ Let $R$ be a total order in $S$ and let $x, y \in S$. Then $(x, y) \in R'$ if and only if $(y, x) \notin R$.

**Definition 3.7** Let $R$ be a partial order in $S$. $R$ is said to be dichotomous if for all $a, b \in S$, exactly one of the following is true:

1. $a \leq b$
2. $b < a$

**Definition 3.8** Let $R$ be a partial order in $S$. $R$ is said to be trichotomous if for all $a, b \in S$, exactly one of the following is true:

1. $a < b$
2. $b < a$
3. $a = b$

**Theorem 3.16** ■ A partial order is a total order if and only if it is dichotomous.

**Theorem 3.17** ■ A partial order is a total order if and only if it is trichotomous.

**Definition 3.9** A subset of a partial order in which no two elements are comparable to one another is called an antichain.

**Definition 3.10** If $X$ is a family of sets, then the relation $R$ in $X$ defined by $(x, y) \in R$ if and only if $x \subseteq y$ is a partial order in $X$.

**Definition 3.11** Define a relation $R$ in $\mathbb{N}$ as $(n, m) \in R$ if and only if $n \subseteq m$. We typically write $n \leq m$ to denote this relation.

**Theorem 3.18** ■ The relation $\leq$ is a partial order in $\mathbb{N}$.

**Theorem 3.19** ■ Given the above relation, $n < m$ in $\mathbb{N}$ if and only if $n \subset m$.

**Theorem 3.20** ■ Let $n \in \mathbb{N}$. Then either $n = 0$, or there exists $k \in \mathbb{N}$ such that $n = s(k)$.

**Theorem 3.21** ■ Let $k, n \in \mathbb{N}$. If $k \subset n$, then $s(k) \subseteq n$.

**Theorem 3.22** ■ The relation $\leq$ is a total order in $\mathbb{N}$.

**Theorem 3.23** ■ For all $n \in \mathbb{N}$, $n < s(n)$.

### 3.4 Mathematical induction

**Theorem 3.24** ■ If $n \in \mathbb{N}$, there is no $k \in \mathbb{N}$ for which $n < k < s(n)$.

**Theorem 3.25** ■ 0 is the smallest element in $\mathbb{N}$. That is, for all $a \in \mathbb{N}$, it is the case that $0 \leq a$. Moreover, there is no $k \in \mathbb{N}$ such that $k < 0$.

**Theorem 3.26** ■ If $A \subseteq \mathbb{N}$ and $0 \in A$, then 0 is the smallest element of $A$.

We now establish three major results, which are equivalent to one another, given what we have established so far.

**Theorem 3.27** ■ Well-ordering principle: If $A \subseteq \mathbb{N}$ and $A \neq \varnothing$, then $A$ has a smallest element, i.e. there is an element $x \in A$ such that $x \leq y$ for all $y \in A$.

**Theorem 3.28** ■ Finite induction: Let $S \subseteq \mathbb{N}$ such that $0 \in S$ and $n \in S \implies (n + 1) \in S$. Then $S = \mathbb{N}$.

**Theorem 3.29** Complete finite induction : Let $S \subseteq \mathbb{N}$ such that $0 \in S$ and $\{0, 1, 2, ..., n\} \subseteq S \implies (n + 1) \in S$. Then $S = \mathbb{N}$.

### 3.5 Bounds and minimal/maximal elements

**Definition 3.12** Let $(P, \leq)$ be a partial ordered set and let $S \subseteq P$ be nonempty. Then $m \in S$ is a maximal element of $S$ if for all $s \in S$, $m \leq s$ implies $m = s$.

**Definition 3.13** Let $(P, \leq)$ be a partial ordered set and let $S \subseteq P$ be nonempty. Then $m \in S$ is a minimal element of $S$ if for all $s \in S$, $m \geq s$ implies $m = s$.

**Theorem 3.30** $\mathbb{N}$ has no maximal element under the partial order $\subseteq$. More generally, no inductive set has a maximal element under the partial order $\subseteq$.

**Theorem 3.31** $\mathbb{N}$ has a unique minimal element under the partial order $\subseteq$, namely $\varnothing$. Every nonempty subset of $\mathbb{N}$ has a unique minimal element by the well-ordering principle.

## 4 Cardinality and Ordinality

**Definition 4.1** A set $A$ has cardinality less than or equal to that of set $B$ if there is an injection from $A$ to $B$. A set $A$ has cardinality greater than or equal to that of set $B$ if there is an injection from $A$ to $B$. We may write these two statements as $|A| \geq |B|$ and $|A| \leq B$ respectively. Two sets have equation cardinality, or are said to be equipollent, if $|A| \geq |B|$ and $|A| \leq B$.

**Theorem 4.1** The relation $R$ defined in a family of sets by $(A, B) \in R$ if and only if $|A| \leq B$ is a partial order.

## 4.1 Equivalence relations

**Definition 4.2** Let $R$ be a relation in a set $S$. Then $R$ is an equivalence relation if it satisfies the following properties:

1. Reflexivity: $(a, a) \in R \; \forall a \in S$.
2. Symmetry: If $(a, b) \in R$, then $(b, a) \in R$.
3. Transitivty: If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

We typically write $a \cong_R b$ or $a \equiv_R b$ to denote that $(a, b) \in R$

**Definition 4.3** If $R$ is an equivalence relation in a set $S$, we may define the equivalence classes of $S$ under $R$ to be the collection of sets

$$\big\{[a] \mid x \in [a] \iff (x, a) \in R\big\}$$

Each equivalence class $[a]$ contains precisely those elements $x$ of $S$ such that $(x, a) \in R$.

**Definition 4.4** A partition of a nonempty set $S$ is a collection $\mathcal{C}$ of nonempty subsets of $S$ such that:

1. $\bigcup_{X \in \mathcal{C}} X = S$
2. For any two distinct sets $X_1, X_2$ in $\mathcal{C}$, $X_1 \cap X_2 = \varnothing$

**Theorem 4.2** The equivalence classes of a set $S$ under an equivalence relation $R$ form a partition of $S$. Moreover, given a partition $\mathcal{P}$ of $S$, we may define an equivalence relation $R$ in $S$ as $(a, b) \in R$ if and only if $a \in X$ and $b \in X$ for some $X \in \mathcal{P}$.