Definitions and Theorems
Connor Baker, March 2017

Definition 1 (Statement)**.** Any sentence which can be evaluated as either true or false.

Definition 2 (Compound Statement)**.** A statement made up of one or more component statements connected by logical connectors.

Definition 3 (Equivalence of Logical Operators)**.** Two sets of logical operators are said to be equivalent if they produce the same output.

Definition 4 (Tautology)**.** A statement that's always true.

Definition 5 (Contradiction)**.** A statement that's always false.

Definition 6 (A Set)**.** Any collection of objects.

Definition 7 (Set Builder Notation)**.** {expression: rule}

Definition 8 (Universal Set)**.** The given or implied set that contains all other sets in the problem. This set fixes Russel's Paradox.

Definition 9 (Tautology)**.** A statement that's always true.

Definition 10 (Natural Numbers)**.** The set $\mathbb{N} : \{1, 2, 3, \dots\}$.

Definition 11 (Integers)**.** The set $\mathbb{Z} : \{\dots, -1, 0, 2, \dots\}$.

Definition 12 (Rational Numbers)**.** The set $\mathbb{Q} : \{\frac{a}{b} : a \in \mathbb{Z}$ and $b \in \mathbb{N}\}$.

Definition 13 (Real Numbers)**.** The set $\mathbb{R} : \{a_n a_{n-1} \dots a_1 a_0 a_{-1} a_{-2} \cdots : n \in \mathbb{N} \cup \{0\}$ and $a_i \in \{0, \dots, 9\}\}$.

Definition 14 (Complex Numbers)**.** The set $\mathbb{C} : \{a + bi : i^2 = -1$ and $a, b \in \mathbb{R}\}$.

Definition 15 (Subset)**.** Given two sets A and B, $A \subseteq B \iff \forall a \in A \implies a \in B$.

Definition 16 (Open Sentence (AKA Predicate))**.** A statement that contains a variable. The truth value depends on the variable.

Definition 17 (Truth Set)**.** The set of values that make the statement true.

Definition 18 (Quantifiers and Negations)**.** Logical Quantifiers and Negators:

1. Universal Quantifier: $\forall$ – Must be true for all x in the universal set such that $P(x)$ is true: $(\forall x)(P(x))$.
2. Existential Quantifier: $\exists$ – True if for at least one x in the universal set such that $P(x)$ is true: $(\exists x)(P(x))$.
3. Unique Quantifier: $\exists!$ – True if there exists only one x in the universal set such that $P(x)$ is true: $(\exists! x)(P(x))$.
4. Negation of the Universal Quantifier: $\sim (\forall x)(P(x))$ is $(\exists x)(\sim P(x))$.
5. Negation of the Existential Quantifier: $\sim (\exists x)(P(x))$ is $(\forall x)(\sim P(x))$.

Definition 19 (Direct Proof)**.** $P \implies Q$.

Definition 20 (Contrapositive Proof)**.** $(\sim Q) \implies (\sim P)$.

Definition 21 (Proof by Contradiction)**.** We start with $P \implies Q$. Assume that $\sim P \wedge Q$ is true. Then $\sim P \implies A_1 \implies A_2 \implies \cdots \implies R$. And, if $Q \implies B_1 \implies B_2 \implies \cdots \implies \sim R$. Then,$\sim R \wedge R$ must be true, which is a contradiction, so the original assumption is false, and $P \implies Q$.

Definition 22 (Axioms of the Natural Numbers)**.** The following are axioms for the set of the Natural Numbers, $\mathbb{N}$:

1. Successor property
   (a) One is a natural number
   (b) One is not the successor of any number
   (c) Every natural number has a unique successor
2. Closure under addition and multiplication
3. Associativity
4. Commutativity
5. Distribution of multiplication over addition
6. Cancellation
   (a) Real numbers have this property unless the number being cancelled is a zero
   (b) Matrix multiplication does not have this property

Definition 23 (Divisible)**.** Let $a, b \in \mathbb{N}$. Then $a|b$ if $\exists k \in \mathbb{N} : ak = b$.

Definition 24 (Prime)**.** A number p, where $p \in \mathbb{N}$, is prime if $p > 1$ and its only divisors are one and itself.

Definition 25 (Factor)**.** A number q, where $q \in \mathbb{N}$, is a factor of r if $q|r$.

Definition 26 (Prime Factor Decomposition)**.** Let $p_1, p_2, \ldots, p_k$ be all primes less than q. Then, the prime factor decomposition of q is $p_1^{n_1} p_2^{n_2}, \ldots, p_k^{n_k}$ where $n_i \in (\mathbb{N} \cup \{0\})$.

Theorem 27 (Fundamental Theorem of Arithmetic)**.** All natural numbers have a unique prime factorization up to commutativity.

Definition 28 (Union over $\mathcal{A}$)**.** Let $\mathcal{A}$ be a family of sets. The union over $\mathcal{A}$ is defined as:

$$\bigcup_{A \in \mathcal{A}} = \{x : (\exists A \in \mathcal{A})(x \in A)$$

which is equivalent to:

$$\bigcup_{A \in \mathcal{A}} = \{x : (\exists A)((A \in \mathcal{A}) \wedge (x \in A))$$

Definition 29 (Intersection over $\mathcal{A}$)**.** Let $\mathcal{A}$ be a family of sets. The intersection over $\mathcal{A}$ is defined as:

$$\bigcap_{A \in \mathcal{A}} = \{x : (\forall A \in \mathcal{A})(x \in A)$$

which is equivalent to:

$$\bigcap_{A \in \mathcal{A}} = \{x : (\forall A)((A \in \mathcal{A}) \implies (x \in A))$$

Theorem 30 (Relative Cardinality of Intersection and Union)**.** For every set $B \in \mathcal{A}$:

$$B \subseteq \bigcup_{A \in \mathcal{A}} A,$$

$$\bigcap_{A \in \mathcal{A}} A \subseteq B.$$

The intersection is no bigger than the smallest set, and the union is no smaller than the biggest set.
Assume that $\mathcal{A} \neq \emptyset$. Then:

$$\bigcap_{A \in \mathcal{A}} A \subseteq \bigcup_{A \in \mathcal{A}} A.$$

If $\mathcal{A} \neq \emptyset$, the union isn't a problem but the intersection would be the set of all sets, and as such is undefined.

Definition 31 (Indexed Family of Sets)**.** Let Δ be a nonempty set. Then, $\forall \alpha \in \Delta$, there is a corresponding set A_α. The family of sets $\mathcal{A} = \{A_\alpha : \alpha \in \Delta\}$.

Definition 32 (Union and Intersection over an Indexed Family of Sets $\mathcal{A}$)**.** Let $\mathcal{A}$ be a family of sets with indicies $\alpha \in \Delta$. Then, the union over A_α is defined as:

$$\bigcap_{\alpha \in \Delta} A_\alpha = \{x : (\exists \alpha \in \Delta)(x \in A_\alpha)$$

and the intersection is defined as:

$$\bigcup_{\alpha \in \Delta} A_\alpha = \{x : (\forall \alpha \in \Delta)(x \in A_\alpha)$$

Theorem 33 (Relative Cardinality of Intersection and Union over Indexed Family of Sets)**.** For every set $\beta \in \Delta$:

$$A_\beta \subseteq \bigcup_{\alpha \in \Delta} A_\alpha,$$

$$\bigcap_{\alpha \in \Delta} A_\alpha \subseteq A_\beta.$$

$$\overline{\bigcup_{\alpha \in \Delta} A_\alpha} = \bigcap_{\alpha \in \Delta} \overline{A_\alpha}$$

$$\overline{\bigcap_{\alpha \in \Delta} A_\alpha} = \bigcup_{\alpha \in \Delta} \overline{A_\alpha}$$

Definition 34 (Pairwise Disjoint)**.** Let $\mathcal{A} = \{A_\alpha : \alpha \in \Delta\}$. Then $\mathcal{A}$ is pairwise disjoint if $\forall \alpha, \beta \in \Delta$ with $A_\alpha \neq A_\beta$, $A_\alpha \cap A_\beta = \emptyset$.

Theorem 35 (Order Properties of the Natural Numbers)**.** Let $x, y, z \in \mathbb{N}$. Then, $\forall x, y, z$:

1. $x < y \iff \exists w \in \mathbb{N} : x + w = y$
2. $x \leq y \iff x = y or x < y$
3. if $x < y$ and $y < z$, then $x < z$ (transitivity)
4. if $x \leq y$ and $y \leq x$, then $x = y$
5. if $x < y$, then $x + z < y + z$ and $xz < yz$

Theorem 36 (Principle of Mathematical Induction (PMI))**.** If S is any subset of the natural numbers, with the properties that:

1. $1 \in S$
2. if $k \in S$, then $(k + 1) \in S$

then $S = \mathbb{N}$.
The general process of mathematical induction is as follows:

1. Define $S = \{n \in \mathbb{N} : \text{some statement is true}\}$
   (a) Prove that the basis case holds: that means that $1 \in S$
   (b) Assume $k \in S$. Then, based on this assumption, prove it to be the case that $(k + 1) \in S$.
   (c) Conclude that by the Principle of Mathematical Induction, $S = \mathbb{N}$.

Definition 37 (Inductive Set)**.** A set $S \subseteq \mathbb{N}$ is inductive if whenever $n \in S$, then $(n + 1) \in S$.

Definition 38 (Factorial)**.** If $n \in \mathbb{N}$, then $n! = n(n - 1)!$.

Definition 39 (Zero Factorial)**.** $0! = 1$.

Definition 40 (General Principle of Mathematical Induction)**.** $S \subseteq \mathbb{N}$ where $k \in S$ and if $j \in S$, then $(j+1) \in S$, and it is true for all $\{k, k+1, \dots\}$, then S is inductive.

Theorem 41 (Principle of Strong Mathematical Induction (PSMI))**.** If $S \subseteq \mathbb{N}$ with the property that $\forall m \in \mathbb{N}$, if $\{1, 2, \dots, m-1\} \subseteq S$, then $m \subseteq S$, then $S = \mathbb{N}$.
PSMI is different from PMI because with PMI we assume that we can start at a value and carrying forward from that value something holds. With PSMI, we assume that it holds over an interval.

Theorem 42 (Well Ordering Principle (WOP))**.** Every nonempty subset of $\mathbb{N}$ has a least element.

Theorem 43 (The Division Algorithm)**.** Let $a, b \in \mathbb{N}$, with $b \leq a$. Then we will prove that $\exists q \in \mathbb{N}$ and $r \in \mathbb{N} \cup \{0\} : a = bq + r$ where $0 \leq r < b$.
Consider all multiples of $b > a$. Let $S = \{s \in \mathbb{N} : sb > a\}$. By (WOP), S has a least element $q + 1$, so $q \notin S$. Therefore, $qb \leq a$.
Let $r = q - qb$. Since $qb \leq a$, $a - qb \geq 0$, so it must be the case that $r \geq 0$.
If $r \geq b$, then $r = q - qb \geq b \implies a - qb - b \geq 0 \implies q - b(q+1) \geq 0$. So, $a \geq b(q+1)$. But, for $(q+1) \in S$, it must be that $b(q+1) > a$. Then, $(q+1) \in S$. This is a contradiction. Therefore, $r < b$.
Furthermore, q and r are unique.
Assume $\exists q_1, r_1$ with $a = bq_1 + r_1$ where $0 \leq r_1 < b$. Then $a = bq + r$, $a = bq_1 + r_1$. This implies that $0 = b(q - q_1) + (r - r_1), b \neq 0$. If it is the case that $q - q_1 \neq 0$, then $|q - q_1| \in \mathbb{N}$. Then $r_1 > r$ and $|r_1 - r| = mb$ for some $m \in \mathbb{N}, m = |q - q_1|$. Thus, $r_1 \geq mb \implies r_1 \geq b$, which is a contradition such that $q - q_1$ would be zero and $r_1 - r = 0$.

Definition 44 (Greatest Common Divisor (GCD))**.** For $a, b \in \mathbb{N}$, the GCD of a and b can be written as the linear combination of a and b – that is, if:

$$d = \mathrm{GCD}(a, b), \exists x, y \in \mathbb{Z} : xa + yb = d$$

Definition 45 (Ordered Pair)**.** A set whose order matters. $(x, y) = \{x, \{x, y\}\}$. The reason the ordered pair translates to this is because x is the first coordinate, since it is an element at every level of the set.

Definition 46 (n-tuples)**.** A set of n-tuples $(x_1, x_2, \dots, x_n)$ can be re-written as a set like so:
$\{x_1, \{x_1, x_2\}, \{x_1, \{x_1, x_2\}, \{x_1, x_2, x_3\}\}, \dots, \{x_1, \{x_1, x_2\}, \dots, \{x_1, x_2, \dots, x_n\}\}\}$.

Definition 47 (Cartesian Product)**.** let A, B be sets. Then, the Cartesian product $A \times B$ is the set:

$$A \times B = \{(a, b) : (a \in A) \wedge (b \in B)\}$$

In general, $A \times B \neq B \times A$. While it might be tempting, note that (again, in general) $A \times B \times C \neq (A \times B) \times C \neq A \times (B \times C)$.

Theorem 48 (Properties of the Cartesian Product)**.** Let A, B, C, D be sets. Then:

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
3. $A \times \emptyset = \emptyset$
4. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
5. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$
6. $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$

Definition 49 (Relation)**.** A relation R from a set A to a set B is any subset of $A \times B$. If $a \in A$, and $b \in B$, then:

1. $aRb \iff (a, b) \in R$

2. $a \not R b \iff (a,b) \notin R$

Definition 50 (Domain)**.** The domain of a relation R from a set A to a set B ($R : A \to B$) is $\text{dom}(R) = \{x \in A : \exists y \in B : xRy\}$.

Definition 51 (Domain)**.** The range of a relation $R : A \to B$) is $\text{rang}(R) = \{y \in B : \exists x \in A : xRy\}$.

Definition 52 (Identity Relation)**.** Let A be any set. Then:

$$I_A = \{(x,x) : x \in A\}$$

Definition 53 (Inverse Relation)**.** Let $R : A \to B$. Then $R^{-1} = \{(y,x) : xRy\}$.

Theorem 54 (Range and Domain of Inverse Relation)**.** Let $R : A \to B$. Then:

1. $\text{dom}(R) = \text{rang}(R^{-1})$
2. $\text{dom}(R^{-1}) = \text{rang}(R)$

Definition 55 (Composition of Relations)**.** Let $R : A \to B$, and $S : B \to BC$. Then:

1. $S \circ R : A \to C$
2. $S \circ R = \{(x,z) : \exists y \in B : (xRy) \wedge (ySz)$

Theorem 56 (Properties of Relations)**.** Assuming that all compositions are well defined:

1. $(R^{-1})^{-1} = R$
2. $T \circ (S \circ R) = (T \circ S) \circ R$ (associativity)
3. $I_B \circ R = R \circ I_A = R$ (identity relation)
4. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Definition 57 (Unary Operator)**.** Requires only a single argument.

Definition 58 (Binary Operator)**.** Requires two arguments.

Definition 59 (Reflexive Relation)**.** A relation R on A is reflexive if, $\forall x \in A, xRx$.

Definition 60 (Symmetric Relation)**.** A relation R on A is symmetric if $xRy \implies xRx$.

Definition 61 (Transitive Relation)**.** A relation R on A is transitive if $((xRy) \wedge (yRz)) \implies xRz$.

Definition 62 (Equivalence Relation)**.** A relation R on A is an equivalence relation if R is reflexive, symmetric, and transitive.

Definition 63 (Equivalence Class)**.** Given R, a equivalence relation on A, for any $x \in A$, the equivalence class of x, denoted $[x]$, is the set $\{y \in A : xRy\}$.

Definition 64 (Cardinality of a Relation)**.** If the cardinality of a set $|A| = n$, then the cardinality of $|A \times A| = n^2$, by the multiplication principle.
If $\mathcal{P}(n)$ is the powerset on $A \times A$, then $|\mathcal{P}(n)| = 2^{n^2}$.