Principal of Mathematical Induction.
Let $P(n)$ denote a (mathematical) statemant that involves occurences of a positive integer n.
Assume that (i) $P(n_0)$ is true, where $n_0 \in \mathbb{N}$
(ii) $P(k)$ is true, where $k \in \mathbb{N} \Rightarrow P(k+1)$ is true.
Then $P(n)$ is true for all positive integer $n \geq n_0$.

Principal of Mathematical Induction (Strong Form.)
Let $P(n)$ denote a mathematical statemant involving a positive integer n.
Assume that

(i) $P(n_0)$ is true where $n_0 \in \mathbb{N}$, and

(ii) $\forall i \leq k, P(i)$ is true $\Rightarrow P(k+1)$ is true.

Then $P(n)$ is true for all positive integer $n \geq n_0$.

The Well - Ordering Principle.
Every nonempty set of nonnegative integers has a least element.

Division Algorithm.
For any $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ with

$$a = bq + r \quad \text{and} \quad 0 \leq r < b$$

.

The Pigeonhole Principle.
If m pigeons occupy n pigeonholes and $m > n$, then there is at least one hole with at least $\lceil \frac{m}{n} \rceil$ pigeons.

Archimedean Property.
For each real number x, there exists a positive integer n such that $x < n$.
For each positive real number x, there exists a positive integer n such that $\frac{1}{n} < x$.

The Density Theorem.
Between teo distinct rael numbers, there always exists a rational number.

Relations

Definition. Let A and B be the sets. The **cartesian product** of A and B, denoted by $A \times B$ is defined to be the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$. In symbols,

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Note that two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$.

A **binary relation** from A to B is a subset of $A \times B$. If R is a relation from A to B and $(a, b) \in R$, we will denote by aRb. The **domain** of R (denoted by $\mathrm{Dom}(R)$) and the **range** of R (denoted by $\mathrm{Range}(R)$) are defined as follow:

$$\mathrm{Dom}(R) = \{a \mid (a, b) \in R\}, \qquad \mathrm{Range}(R) = \{b \mid (a, b) \in R\}.$$

The range of R is sometimes called the **image** of R and denoted by $\mathrm{Im}(R)$.

Definition. Let R be a relation on set A (i.e. $R \subseteq A \times A$). Then we say
R is **reflexive** if $\forall a \in A, aRa$.
R is **symmetric** if $\forall a, b \in A, aRb \to bRa$.
R is **transitive** if $\forall a, b, c \in A, (aRb \wedge bRc) \to aRc$.
R is **irreflexive** if $\forall a \in A, \sim (aRa)$.
R is **antisymmetric** if $\forall a, b \in A$ and $a \neq b, aRb \to \sim (bRa)$.
(equivalently, $\forall a, b \in A, arb \wedge bra \to a = b$)
R is an **equivalence relation** if R is reflexive, symmetric and transitive.
R is a **partial order** if R is reflexive, antisymmetric and transitive.
R is **complete** if $\forall a, b \in A, a \neq b \to (aRb \vee bRa)$.
R is a **total order** (or linear order) if R is a partial order which is complete.

Definition. Let R be a relation from A to B. R **inverse**, denoted by R^{-1}, is the relation from B to A given by

$$R^{-1} = \{(x, y) \mid (y, x) \in R\}.$$

Definition. Let R be a relation from A to B and S a relation from B to C. Then R **composed with** S (denoted $S \circ R$) is the relation from A to C given by

$$S \circ R = \{(x, z) \in A \times C \mid \exists y \in B, (x, y) \in R \text{ and } (y, z) \in S\}.$$

Theorem 1. Let A, B, C be sets, R a relation from A to B and S a relation from B to C. Then

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

Theorem 2. Let A, B, C, D be sets with R, S and T relations from A to B, B to C and C to D, respectively. Then

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Theorem 3. Let R be a relation on A. Then R is transitive if and only if $R \circ R \subseteq R$.

Equivalence relations

Definition. Let A be a nonempty set. A **partition** Π of A is a collection of nonempty subsets of A such that every element of A is an element of exactly one of these sets.

Equivalently, $\Pi = \{A_\alpha | \ \emptyset \neq A_\alpha \subseteq A \text{ and } \alpha \in \Omega\}$ is a partition of A iff

(i) $\bigcup\limits_{\alpha \in \Omega} A_\alpha = A$, and

(ii) $A_\alpha \cap A_\beta = \emptyset$ or $A_\alpha = A_\beta$ for all $\alpha, \beta \in \Omega$.

Definition. Let R be an equivalence relation on a nonempty set A. Let $a \in A$. The **equivalence class** of a **modulo** R, denoted by $[a]_R$ or $[a]$ (if there is no abiguity) is defined by

$$[a]_R = \{x \in A \mid xRa\}.$$

Note that $a \in [a]_R$ for all $a \in A$. The set of all such equivalence classes is denoted by ${}^{A}\!/_{R}$ and called A modulo R. i.e.

$${}^{A}\!/_{R} = \{[a]_R \mid a \in A\}.$$

Theorem 4. Let E be an equivalence relation on a set $A \neq \emptyset$. Then

(i) $[a] \cap [b] \neq \emptyset \Leftrightarrow aEb$

(ii) $[a] \cap [b] \neq \emptyset \Leftrightarrow [a] = [b]$

(iii) ${}^{A}\!/_{E}$ is a partition of A

(iv) $\rho_{{}^{A}\!/_{E}} = E$.

Theorem 5. Let Π be a partition of a set $A \neq \emptyset$. Define ρ_{Π} on A by

$$x \rho_{\Pi} y \Leftrightarrow \exists C \in \Pi, x \in C \text{ and } y \in C.$$

Then (i) ρ_{Π} is an equivalence relation on A

(ii) ${}^{A}\!/_{\rho_{\Pi}} = \Pi$.

In this case, Π is called the **equivalence relations determined** by the partition Π.

Partial Orders

Definition. A nonempty set P together with a partial ordering $\preccurlyeq$ on P is called a **partially ordered set** or poset. For a poset $(P, \preccurlyeq)$, a relation $\prec$ is defined on P by

$$a \prec b \quad \text{iff} \quad a \preccurlyeq b \text{ and } a \neq b$$

a is then said to be **less than** b or b is **greater than** a.

Definition. Let $(P, \preccurlyeq)$ be a poset and $\emptyset \neq S \subseteq P$. Define

$$\preccurlyeq_S = \{(a, b) \in S \times S \mid a \preccurlyeq b\}.$$

Then $\preccurlyeq_S$ is a partial ordering on S and $(S, \preccurlyeq_S)$ is called a **subposet** of $(P, \preccurlyeq)$. We usually write S is a subposet of $(P, \preccurlyeq)$ and denoted $\preccurlyeq_S$ by $\preccurlyeq$.

Definition. Let $(A, \preccurlyeq)$ be a poset. The **lexicographic order** is defined on the set of words in A as follows :
For $a = a_1a_2 \dots a_m$ and $b = b_1b_2 \dots b_n$, $a \preccurlyeq b$ if
(i) a and b are identical, or
(ii) there is $\imath_0 \leq \min\{m, n\}$ such that $a_i = b_i$ for all $i \leq i_0$ and $a_{i_0} \preccurlyeq b_{i_0}$
(iii) $m < n$ and $a_i = b_i$ for all $i = 1, 2, \dots, m$.
Note that a **word** in A is means a string of elements in A.

Definition. Let S be a subposet of a poset $(P, \preccurlyeq)$.

$m \in S$ is said to be a **maximal element** of S if no element in S is greater than m. (equiv. $\forall s \in S, m \preccurlyeq s \Rightarrow m = s$)

$n \in S$ is said to be a **minimal element** of S if no element in S is less than n. (equiv. $\forall s \in S, s \preccurlyeq n \Rightarrow s = n$)

$u \in P$ is said to be an **upper bound** of S if $s \preccurlyeq u$ for all $s \in S$.

$\ell \in P$ is said to be a **lower bound** of S if $\ell \preccurlyeq s$ for all $s \in S$.

An upper bound u_0 of S is a **least upper bound** or **supremum** of S if no element less than u_0 is an upper bound of S. u_0 is denoted by $\sup S$. If $\sup S \in S$, then it is called a **maximum** of S.

A lower bound ℓ_0 of S is a **greatest lower bound** or **infimum** of S if no element greater than ℓ_0 is a lower bound of S. ℓ_0 is denoted by $\inf S$. If $\inf S \in S$, then it is called a **minimum** of S.

Definition. A poset in which every two elements have a infimum and a suppremum is called a **lattice**.

Theorem 6. Let S be a subposet of a poset $(P, \preccurlyeq)$. Then S has at most one supremum (infimum).

Definition. A poset P is said to be a **well-ordered set** if every subset of P contains a smallest element.

Definition. A subposet of a poset $(P, \preccurlyeq)$ is a **chain** if $(S, \preccurlyeq)$ is a total order.

Functions

Definition. A relation f from A to B is called a **function** if for $(x_1, y_1) \in f$ and $(x_2, y_2) \in f, x_1 = x_2$ implies $y_1 = y_2$.

Notation. 1) $f : A \to B, f$ is a function from A to B means f is a function whose domain is A and Range$f \subseteq B$.

2) If $f : A \to B$, for each $x \in A$, we write $y = f(x)$ and say that y is the value of f at x.

Definition. Let $f : A \to B$. Then we say that
f is **one-to-one** (or f is an injection) if $\forall x_1, x_2 \in B, f(x_1) = f(x_2)$ implies $x_1 = x_2$.
f is **onto** (or surjection) if Range$f = B$ (i.e. for each $y \in B \exists x \in A, f(x) = y$).
f is a **one-to-one correspondence** (or bijection) if f is both one-to-one and onto.

Theorem 7. Let $f : X \to Y$. Then
(i) f is an injection iff f^{-1} is a function
(ii) f is a bijection implies $f^{-1} : Y \to X$.

Theorem 8. If f and g are functions, then $g \circ f$ is a function whose domain is the set $\{x \in \text{ Dom} f \mid f(x) \in D_g\}$.

Theorem 9. Let $f : X \to Y$ and $g : Y \to Z$
(i) If f and g are injective, the $g \circ f$ is injective.
(ii) If f and g are surjective, then $g \circ f$ is surjective
(iii) If f and g are bijective, then $g \circ f$ is bijective.

Theorem 10. Let $f : X \to Y$ and $g : Y \to Z$
(i) If $g \circ f$ is injective, the f is injective.
(ii) If $g \circ f$ is surjective, then g is surjective
(iii) If $g \circ f$ is bijective, then f is injective and g is surjective.

Definition. A function f is said to be **invertible** if f^{-1} is a function.

Theorem 11. Let $f : A \to B$ and $Y =$ Range$f$. Then f is invertible if and only if $\exists g : Y \to A$ such that $g \circ f = \imath_A$ and $f \circ g = \imath_Y$.

Definition. A **binary operation** on a nonempty set S is a mapping $* : S \times S \to S$. $(S, *)$ is called an **algebraic system**. A binary operation $* : S \times S \to S$ is said to be
associative if $x * (y * z) = (x * y) * z$ for all $x, y, z \in S$
commutative if $x * y = y * x$ for all $x, y \in S$.

Definition. Let $(S, *)$ be an algebric system. $e \in S$ is called a **neutral element** or **identity element** if

$$e * x = x = x * e \quad \text{for all } x \in S.$$

Definition. Let $(S, *)$ be an algebric system with the neutral element e. $b \in S$ is said to be an **inverse** of $a \in S$ if $a * b = e = b * a$.

Image and inverse image of a set

Definition. Let $f : A \to B, C \subseteq A$ and $D \subseteq B$. We define

$$f[C] = \{b \in B \mid \exists a \in C, f(a) = b\}$$
$$f^{-1}[D] = \{a \in A \mid f(a) \in D\}.$$

$f[C]$ is called the **image** of C (under f) and $f^{-1}[D]$ is called the **inverse image** (preimage) of D.

Theorem 12. $f : A \to B$ and $A_1, A_2 \subseteq A$. Then
(i) $A_1 \subseteq A_2 \Rightarrow f[A_1] \subseteq f[A_2]$.
(ii) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$.
(iii) $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$. The equality holds if
(iv) $f[A_1] \setminus f[A_2] \subseteq f[A_1 \setminus A_2]$.

Theorem 13. $f : A \to B$ and $B_1, B_2 \subseteq B$. Then
(i) $B_1 \subseteq B_2 \Rightarrow f^{-1}[B_1] \subseteq f^{-1}[B_2]$.
(ii) $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$.
(iii) $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$.
(iv) $f^{-1}[B_1 \setminus B_2] \subseteq f^{-1}[B_1] \setminus f^{-1}[B_2]$.

Theorem 14. $f : A \to B$ and $X \subseteq A, Y \subseteq B$. Then
(i) $X \subseteq f^{-1}[f[X]]$. The equality holds if
(ii) $f[f^{-1}[Y]] \subseteq Y$. The equality holds if

Theorem 15. $f : A \to B$ and $g : B \to C$
(i) $g \circ f[X] \subseteq g[f[X]]$.
(ii) $(g \circ f)^{-1}[Y] \subseteq f^{-1}[g^{-1}[Y]]$.

Finite sets

Definition. A set A is said to be **finite** if $A = \emptyset$ or there is a bijection between A and $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. We shall show later that n is unique. We say that, in the fromer case, A has n elements and n is called the **cardinal** of A. In the later case, we say that A has 0 element and 0 is the cardinal of A. For a finite set A, the cardinal (number) of A is denoted card(A). If A is a finite set with cardinal $n \geq 1$, we may write $A = \{a_1, a_2, \ldots, a_n\}$.

Lemma 16. Let A be a set and $n \in \mathbb{N}$. Let $a_0 \in A$. Then there exists a bijection of the set A with the set $\{1, 2, \ldots, n+1\}$ if and only if there exists a bijection of the set $A \setminus \{a_0\}$ with $\{1, 2, \ldots, n\}$.

Theorem 17. If there is a bijection between A and $\{1, 2, \ldots, n\}$, where $n \geq 1$, then for any proper subset B of A, there is no bijection between B and $\{1, 2, \ldots, n\}$, but (provided $B \neq \emptyset$) there exists a bijection between B and $\{1, 2, \ldots, m\}$ for some $m < n$.

Corollary. (i) If A is finite, then there is no bijection between A and any proper subset of A.

(ii) Let A and B be sets with $B \subseteq A$. If A is finite, then B is finite.

(iii) The number of elements in a finite set A is uniquely determined by A.

(iv) $\mathbb{N}$ is not finite. (so $\mathbb{Z}$ is not finite)

Theorem 18. Let A be a nonempty set and $n \in \mathbb{N}$. Then TFAE

(i) There is a surjection from $\{1, 2, \ldots, n\}$ to A.

(ii) There is an injection from A to $\{1, 2, \ldots, n\}$.

(iii) A is finite and has at most n elements.

Theorem 19. If A and B are finite sets, then so are $A \cup B$ and $A \times B$. Moreover,

$$\begin{aligned}\text{card}(A \cup B) &= \text{card}(A) + \text{card}(B) - \text{card}(A \cap B),\\ \text{card}(A \times B) &= \text{card}(A) \cdot \text{card}(B).\end{aligned}$$

Theorem 20. (i) A finite union of finite sets is finite.

(ii) A finite product of finite sets is finite.

Infinite sets

Definition. A set A is said to be **infinite** if A is not finite.

Definition. Let A be a set. A is said to be **denumerable** or **countably infinite** if there is a bijection between A and $\mathbb{N}$. A is said to be **countable** if A is finnite or denumerable. A is said to be **uncountable** if A is not countable.

Theorem 21. An infinite set contains a countably infinite subset.

Theorem 22. Any subset of $\mathbb{N}$ is countable.

Theorem 23. A set A is infinite iff there exists a bijection between A and a proper subset of A.

Theorem 24. Any subset of a countable set is countable.

Theorem 25. $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Theorem 26. Let A be a nonempty set. Then TFAE
(i) There is a surjection from $\mathbb{N}$ to A.
(ii) There is an injection from A to $\mathbb{N}$.
(iii) A is countable.

Theorem 27.
(i) A countable union of countable sets is countable.
(ii) A finite product of countable sets is countable.

Theorem 28. $\mathbb{Q}$ is countably infinite.

Theorem 29. $(0, 1)$ is uncountable.

Corollary. (i) $\mathbb{R}$ is uncountable.
(ii) $\mathbb{Q}^c$ is uncountable.

Similarity and Dominance

Definition. Let A and B be sets. We say that A is **similar** to B and write $A \approx B$ if there is a bijection from A to B.

Definition. Let A and B be sets. We say that B **dominates** A and write $B \succcurlyeq A$ or $A \preccurlyeq B$ if there is an injection from A to B. We say that B **strongly dominates** A and write $B \succ A$ or $A \prec B$ if $B \succcurlyeq A$ and $A \not\approx B$.

Theorem 30. For any set $A, A \prec \wp(A)$.

Theorem 31. For any set $A, \wp(A) \approx 2^A$ where 2^A is the set of functions from A to a set of two elements ($\{0, 1\}$).

Theorem 32. **(Schröder-Berstein)** Let A and B be sets. If $A \preccurlyeq B$ and $B \succcurlyeq A$, then $A \approx B$.

Theorem 33. (i) $(0, 1) \approx 2^{\mathbb{N}}$.
(ii) $(0, 1) \times (0, 1) \approx (0, 1)$.

Corollary. $\mathbb{N} \prec \mathbb{R}$.

Theorem 34. If $A \approx C$ and $B \approx D$, then $A^B \approx C^D$.

Cardinal Numbers

Definition. $\text{card}(\emptyset) = 0$,
If $A \approx \{1, 2, \ldots, n\}$, then $\text{card}(A) = n$,
$\text{card}(\mathbb{N}) = \aleph_0$ (aleph null), $\text{card}(\mathbb{R}) = \aleph_1$,
$\text{card}(A) = \text{card}(B)$ iff $A \approx B$,
$\text{card}(A) \leq \text{card}(B)$ iff $A \preccurlyeq B$,
$\text{card}(A) < \text{card}(B)$ iff $A \prec B$.

Definition. Let u and v be cardinal numbers. Let A and B be disjoint sets such that $\text{card}(A) = u$ and $\text{card}(B) = v$. Then $u + v = \text{card}(A \cup B)$.

Definition. Let u and v be cardinal numbers. Let A and B be sets such that $\text{card}(A) = u$ and $\text{card}(B) = v$. Then

$$\begin{aligned} u \times v = & \ \text{card}(A \times B), \text{ and} \\ u^v = & \ \text{card}(A^B). \end{aligned}$$

Theorem 35. For any cardinal numbers u and v, the followings hold
(i) $u + v = v + u, uv = vu$.
(ii) $u + (v + w) = (u + v) + w,\ u(vw) = (uv)w$.
(iii) $u(v + w) = uv + uw$.
(iv) $u^v u^w = u^{v+w}$.
(v) $(uv)^w = u^w v^w$.
(vi) $(u^v)^w = u^{vw}$.

Theorem 36. For any cardinal numbers u, v and w,
(i) if $u \leq v$, then $u + w \leq v + w$,
(ii) if $u \leq v$, then $uw \leq vw$.