Propositional Equivalences

$p \wedge T \Leftrightarrow p$ $p \vee F \Leftrightarrow p$	Identity laws
$p \vee T \Leftrightarrow T$ $p \wedge F \Leftrightarrow F$	Domination laws
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Idempotent laws
$\neg(\neg p) \Leftrightarrow p$	Double negation law
$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Commutative laws
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	De Morgan's laws

Rules of Inference

$\frac{p}{p \vee q}$	Addition
$\frac{p \wedge q}{p}$	Simplification
$\frac{p, q}{p \wedge q}$	Conjunction
$\frac{p, p \to q}{q}$	Modus ponens
$\frac{\neg q, p \to q}{\neg p}$	Modus tollens
$\frac{p \to q, q \to r}{p \to r}$	Hypothetical syllogism
$\frac{p \vee q, \neg p}{q}$	Disjunctive syllogism
$\frac{\forall x P(x)}{P(c) \text{ if } c \in U}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c \in U}{\forall x P(x)}$	Universal generalization
$\frac{\exists x P(x)}{P(c) \text{ for some } c \in U}$	Existential instantiation
$\frac{P(c) \text{ for some } c \in U}{\exists x P(x)}$	Existential generalization

Sets

- $\mathcal{P}(S)$**:** The **power set** of S is the set of all subsets of the set S.
- $A \times B$**:** The **Cartesian product** of A and B is the set of all ordered pairs (a, b) where $a \epsilon A$ and $b \epsilon B$.
- $A_1 \times A_2 \times \ldots \times A_n$**:** The **Cartesian product** of the sets $A_1, A_2, \ldots, A_n$ is the set of ordered $n{-}tuples(a_1, a_2, \ldots, a_n)$, where a_i belongs to A_i for $i = 1, 2, \ldots, n$.

Functions

- $f : A \to B$**:** A **function** from A to B is an assignment of exactly one element of B to each element of A.
- A is the **domain** of f and B is the **codomain** of f.

- If $f(a) = b$, we say that b is the **image** of a and a is a **pre-image** of b. The **range** of f i the set of all images of elements of A.
- **Injection:** Function f is said to be **one-to-one**, if and only if $f(x) = f(y)$ implies that $x = y$ for all x and y in the domain of f.
- **Surjection:** Function f is said to be **onto / surjective**, if and only if for every element $b \epsilon B$ there is an element $a \epsilon A$ with $f(a) = b$.
- **Bijection:** Function f is a **one-to-one correspondence**, or **bijection**, if it is both one-to-one and onto.
- **Inverse function:** Let f be a one-to-one correspondence from A to B. The **inverse function of** f assigns to an element b in B the unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^-1. Hence, $f^-1(b) = a$ when $f(a) = b$.
- $f \circ g$**:** $g : A \to B$, $f : B \to C$. The **composition** of the functions f and g is defined by $(f \circ g)(a) = f(g(a))$

Integers

- Let a, b, and c be integers, $a \neq 0$.
- $a \mid b$: a **divides** b if there is an integer c such that $b = ac$. When a divides b we say that a is a **factor** of b and that b is a **multiple** of a.
- **Prime:** A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called **composite**.
- **Fundamental Theorem of Arithmetic:** Every positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.
- **Division algorithm:** Let a be an integer and d a poisitive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
- **gcd**(a, b)**:** Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** of a and b.
- The integers a and b are **relatively prime** if $\gcd(a, b) = 1$.
- $a \equiv b$ (**mod** m) If a and b are integers and m is a positive integer, then a **is congruent to** b **modulo** m if m divides $a - b$.
- **Theorem 1:** Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.
- **Theorem 2:** Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$) and $ac \equiv bd \pmod{m}$.
- **Lemma 1:** Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Counting Principles

- **Pascal's Identity:** Let n and k be positive integers with $n \geq k$. Then $C(n + 1, k) = C(n, k - 1) + C(n, k)$
- **Binomial Theorem:** Let x and y be variables, and let n be a positive integer. Then

$$(x + y)^n = \sum_{j=0}^{n} C(n, j) x^{n-j} y^j$$

Probability Theory

- Let S be the sample space of an experiment with a finite or countable number of outcomes. We assign **probability** $p(s)$ **to each outcome** s. The following two conditions have to be met:
  (i) $0 \leq p(s) \leq 1$ for each $s \epsilon S$
  (ii) $\sum_{s \epsilon S} p(s) = 1$
- The **probability of the event** E is the sum of the probabilities of the outcomes in E. That is, $p(E) = \sum_{s \epsilon E} p(s)$.

- Let E and F be events with $p(F) > 0$. The **conditional probability** of E given F is defined
$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}.$$
- The events E and F are said to be **independent** if
$$p(E \cap F) = p(E)P(F).$$
- **Bernoulli Trial**: Experiment with only two possible outcomes: success or failure.
- **Probability of k successes in n independent Bernoulli trials** with probability of success p and probability of failure $q = 1 - p$, is $C(n, k)p^k q^{n-k}$.
- A **random variable** is a function from the sample space of an experiment to the set of real numbers.
- The **expected value** (or expectation) of a random
$$E(X) = \sum_{s \epsilon S} p(s)X(s).$$
- **Theorem 3**: If X and Y are random variables on a space S, then $E(X + Y) = E(X) + E(Y)$.Furthermore, if $X_i, i = 1, 2, \ldots, n$, with n a positive integer, are random variables on S, and $X = X_1 + X_2 + \ldots + X_n$, then $E(X) = E(X_1) + E(X_2) + \ldots + E(X_n)$.
- The random variables X and Y on a sample space S are **independent** if for all real numbers r_1 and r_2 $p(X(s) = r_1 \text{ and } Y(s) = r_2) = p(X(s) = r_1)\dot{p}(Y(s) = r_2)$.
- **Theorem 4**: If X and Y are independent random variables on a space S, then $E(XY) = E(X)E(Y)$.
- Let X be random variables on a sample space S . The **variance** of X, denoted by $V(X)$, is
$$V(X) = \sum_{s \epsilon S} (X(s) - E(X))^2 p(s).$$
- **Theorem 5**: If X is a random variable on a space S, then $V(X) = E(X^2) - E(X)^2$.

Relations

- Let A and B be sets. A **binary relation from A to B** is a subset of $A \times B$. If $(a, b)\epsilon R$, we write aRb and say a **is related to** b **by** R.
- Let R be a relation from a set A to a set B and S be a relation from B to a set C. The **composite** of R and S is the relation consisting of ordered pairs (a, c), where $a\epsilon A$, $c\epsilon C$, and for which there exists an element $b\epsilon B$ such that $(a, b)\epsilon R$ and $(b, c)\epsilon S$. We denote the composite of R and S by $S \circ R$.
- Let R be a relation on the set A. The **powers** R^n, $n = 1, 2, 3, \ldots$, are defined inductively by $R^1 = R$ and $R^{n+1} = R^n \circ R$.
- Let P be a property of relations (e.g. transitivity, refexivity, symmetry). A relation S **is losure of** R **w.r.t.** P if and only if S has property P, S contains R, and S is a subset of every relation with property P containing R.
- There is a **path** from a to b in a relation R is there is a sequence of elements $a, x_1, x_2, \ldots x_{n-1}, b$ with $(a, x_1) \in R, (x_1, x_2) \in R, \ldots, (x_{n-1}, b) \in R$.
- **Theorem 6**: Let R be a relation on a set A. There is a path of length n from a to b if and only if $(a, b) \in R^n$.
- Let R be a relation on a set A. The **connectivity relation** R^* consists of pairs (a, b) such that there is a path between a and b in R.
- **Theorem 7**: The transitive closure of a relation R equals the connectivity relation R^*.
- A relation on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive. Two elements that are related by an equivalence relation are called equivalent.
- Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the **equivalence class** of a. $[a]_R$: equivalence class of a w.r.t. R.If $b \in [a]_R$ then b is **representative** of this equivalence class.

- **Theorem 8**: Let R be an equivalence relation on a set A. The following statements are equivalent:
  (1) aRb
  (2) $[a] = [b]$
  (3) $[a] \cap [b] \neq \emptyset$
- A **partition** of a set S is a collection of disjoint nonempty subsets $A_i, i \in I$ (where I is an index set) of S that have S as their union: $A_i \neq \emptyset$ for $i \in I A_i \cap A_j = \emptyset$, when $i \neq j \bigcup_{i \in I} A_i = S$
- **Theorem 9**: Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set S, there is an equivalence relation R that has the sets $A_i, i \in I$, as its equivalence classes.

Graphs

- The **degree** of a vertex in an undirected graph is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. The degree of the vertex v is denoted by deg(v).
- **The Handshaking Theorem**: Let $G = (V, E)$ be an undirected graph with e edges. Then $2e = \sum_{v \in V} \deg(v)$.
- **Theorem 10**: An undirected graph has an even number of vertices of odd degree.
- In a graph with directed edges the **in-degree** of a vertex v, denoted by $\deg^{-}(v)$, is the number of edges with v as their terminal vertex. The **out-degree** of v, denoted by $\deg^{+}(v)$, is the number of edges with v as their initial vertex.
- **Theorem 11**: Let $G = (V, E)$ be a graph with directed edges. Then $\sum_{v \in V} \deg^{-}(v) = \sum_{v \in V} \deg^{+}(v) = |E|$.
- A simple graph is G is called **bipartite** if its vertex V can be partitioned into two disjoint nonempty sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2.
- The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are **isomorphic** if there is a one-to-one and onto function f from V_1 to V_2 with the property that$a$ and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2, for all a and b in V_1. Such a function f is called an **isomorphism**.