Midterm Reference Sheet

This sheet contains helpful properties and definitions to be used throughout the exam. You do not need to cite any rules found here throughout your work. This is not comprehensive.

Logic

i. **Disjunctive Normal Form:** $(P \wedge Q) \vee (S \wedge R)$

- The disjunction (clauses ORed together) of conjunctions (literals ANDed together).

ii. **Conjunctive Normal Form:** $(P \vee Q) \wedge (S \vee R)$

- The conjunction (clauses ANDed together) of disjunctions (literals ORed together).

Logical Equivalences:

Identity Laws	**Double Negation Law**	**Idempotent Laws**	**Distributive Laws**
$p \wedge T \equiv p$ $p \vee F \equiv p$	$\neg(\neg p) \equiv p$	$p \wedge p \equiv p$ $p \vee p \equiv p$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

De Morgan's Laws	**Absorption Laws**	**Definition of Conditional**
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	$p \to q \equiv \neg p \vee q$

Set Identities

1. **Set Difference Law:** For all sets A and B, $A \setminus B = A \cap \overline{B}$
2. **Double Complement Law:** For all sets B, $\overline{\overline{B}} = B$
3. **Distributive Law:** For all sets A, B, and C
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

4. **Identity Law:** For all sets A,
   (a) $A \cup \emptyset = A$
   (b) $A \cap U = A$
5. **De Morgan's Law:** For all sets A and B,
   (a) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$
   (b) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

Relations and Functions

1. An **equivalence relation** is one that is reflexive, symmetric, and transitive.
2. A **bijective** function is one that is **injective** and **surjective**.
   (a) A function $f : A \to B$ is **injective** if for any arbitrary $a, b \in A$, $f(a) = f(b) \to a = b$.
   (b) A function $f : A \to B$ is **surjective** if, for all $b \in B$, there exists some $a \in A$ such that $f(a) = b$.

Number Theory

Definition 1: We say that a *divides* b, denoted $a \mid b$, when $b = ka$ for some $k \in \mathbb{Z}$.

Definition 2: We say that a is *congruent* to b mod m, denoted $a \equiv b \pmod{m}$, if $m \mid (b - a)$.

Properties of Congruence Relations:

For $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$,

1. $a + c \equiv b + c \pmod{m}$ for any $c \in \mathbb{Z}$
2. $ac \equiv bc \pmod{m}$ for any $c \in \mathbb{Z}$
3. $a^n \equiv b^n \pmod{m}$ for $n \in \mathbb{Z}^+$

If we also have $c \equiv d \pmod{m}$,

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$

Theorem 1: For any $a, b \in \mathbb{Z}$ there exists $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$.

Theorem 2: An integer is a linear combination of a and b if and only if it is a multiple of their gcd.