Sets

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} \quad \text{(natural numbers)} \tag{1}$$
$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \quad \text{(integers)} \tag{2}$$
$$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\} \quad \text{(rational numbers)} \tag{3}$$
$$\mathbb{R} = \text{real numbers} \tag{4}$$
$$\mathbb{C} = \text{complex numbers} \tag{5}$$

Logical Form and Logical Equivalences

Notation	Name	Read as
$\sim$ or $\neg$	Negation	not
$\wedge$	Conjunction	and
$\vee$	Disjunction	or
$\rightarrow$	Conditional	implies / if...then
$\leftrightarrow$	Biconditional	if and only if

p	q	$p \wedge q$	$p \vee q$	$\neg p$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	F	T	T
T	F	F	T	F	F	F
F	T	F	T	T	T	F
F	F	F	F	T	T	T

Statements: true or false but not both.
Tautology: always true (T).
Contradiction: always false (F).

$$\begin{aligned}
\text{Commutative:} \quad & p \wedge q \equiv q \wedge p, \quad p \vee q \equiv q \vee p \\
\text{Associative:} \quad & (p \wedge q) \wedge r \equiv p \wedge (q \wedge r), \\
& (p \vee q) \vee r \equiv p \vee (q \vee r) \\
\text{Distributive:} \quad & p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r), \\
& p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \\
\text{Identity:} \quad & p \wedge T \equiv p, \quad p \vee F \equiv p \\
\text{Negation:} \quad & p \vee \neg p \equiv T, \quad p \wedge \neg p \equiv F \\
\text{Double negation:} \quad & \neg(\neg p) \equiv p \\
\text{Idempotent:} \quad & p \wedge p \equiv p, \quad p \vee p \equiv p \\
\text{Universal bound:} \quad & p \vee T \equiv T, \quad p \wedge F \equiv F \\
\text{De Morgan:} \quad & \neg(p \vee q) \equiv \neg p \wedge \neg q, \\
& \neg(p \wedge q) \equiv \neg p \vee \neg q \\
\text{Absorption:} \quad & p \vee (p \wedge q) \equiv p, \quad p \wedge (p \vee q) \equiv p \\
\text{Negations of } T \text{ and } F\text{:} \quad & \neg T \equiv F, \quad \neg F \equiv T
\end{aligned}$$

Conditional Statements

$$\begin{aligned}
p \rightarrow q &\equiv \neg p \vee q \\
\neg(p \rightarrow q) &\equiv p \wedge \neg q \\
\text{Contrapositive: } p \rightarrow q &\equiv \neg q \rightarrow \neg p \\
\text{Converse:} \quad & q \rightarrow p \\
\text{Inverse:} \quad & \neg p \rightarrow \neg q
\end{aligned}$$

$$\begin{aligned}
\text{“}p \text{ only if } q\text{”} &\equiv p \rightarrow q \equiv \neg q \rightarrow \neg p \\
\text{“}p \text{ if } q\text{”} &\equiv q \rightarrow p \\
p \leftrightarrow q &\equiv (p \rightarrow q) \wedge (q \rightarrow p) \\
r \text{ sufficient for } s\text{:} \quad & r \rightarrow s \\
r \text{ necessary for } s\text{:} \quad & s \rightarrow r \equiv \neg r \rightarrow \neg s \\
r \text{ necessary and sufficient for } s\text{:} \quad & r \leftrightarrow s
\end{aligned}$$

Quantified Statements

Universal: $\forall x \in D, Q(x)$ — true if $Q(x)$ is true for every x in D.
Existential: $\exists x \in D$ such that $Q(x)$ — true if $Q(x)$ is true for at least one x in D. **Negations:**

$$\begin{aligned}
\neg(\forall x \in D, Q(x)) &\equiv \exists x \in D \text{ such that } \neg Q(x) \\
\neg(\exists x \in D \text{ such that } Q(x)) &\equiv \forall x \in D, \neg Q(x) \\
\neg(\forall x, P(x) \rightarrow Q(x)) &\equiv \exists x \text{ such that } P(x) \wedge \neg Q(x)
\end{aligned}$$

Methods of Proof

Direct Proof Techniques:

- **Direct proof**: Assume hypothesis, derive conclusion
- **Proof by exhaustion**: Check all possible cases
- **Proof by cases**: Divide into exhaustive, mutually exclusive cases
- **Element method**: For sets, take arbitrary element and show property holds

Indirect Proof Techniques:

- **Proof by contradiction**: Assume negation of conclusion, derive contradiction
- **Proof by contraposition**: To prove $p \rightarrow q$, prove $\neg q \rightarrow \neg p$
- **Counterexample**: Find one example where universal statement fails

Valid Inference Rules:

Rule	Form
Modus ponens	$p \rightarrow q, p \vdash q$
Modus tollens	$p \rightarrow q, \neg q \vdash \neg p$
Generalization	$p \vdash p \vee q$
Specialization	$p \wedge q \vdash p$
Conjunction	$p, q \vdash p \wedge q$
Disjunctive syllogism	$p \vee q, \neg q \vdash p$
Hypothetical syllogism	$p \rightarrow q, q \rightarrow r \vdash p \rightarrow r$
Proof by cases	$p \vee q, p \rightarrow r, q \rightarrow r \vdash r$

Fallacies: Converse error ($p \rightarrow q, q \nvdash p$), Inverse error ($p \rightarrow q, \neg p \nvdash \neg q$)

Mathematical Induction

Standard Induction: To prove $P(n)$ for all $n \geq a$:

1. Base case: Prove $P(a)$
2. Inductive step: Prove $\forall k \geq a$, $P(k) \Rightarrow P(k+1)$

Strong Induction: To prove $P(n)$ for all $n \geq a$:

1. Base cases: Prove $P(a), P(a+1), \ldots, P(b)$ for some $b \geq a$
2. Inductive step: If $P(i)$ holds for all $a \leq i \leq k$ (where $k \geq b$), then $P(k+1)$ holds

Elementary Number Theory

Basic Definitions:

- **Even**: $n = 2k$ for some integer k
- **Odd**: $n = 2k + 1$ for some integer k
- **Prime**: $n > 1$ and only positive divisors are 1 and n
- **Composite**: $n > 1$ and $n = ab$ with $1 < a, b < n$
- **Rational**: $r = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$

Parity Facts:

- Even $\pm$ even $=$ even; odd $\pm$ odd $=$ even; even $\pm$ odd $=$ odd
- Even $\times$ any $=$ even; odd $\times$ odd $=$ odd

Divisibility: $d \mid n \iff \exists k \in \mathbb{Z}$ such that $n = dk$ **Properties:**

- If $a \mid b$ and $b \mid c$, then $a \mid c$ (transitivity)
- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$

Division Algorithm & Special Functions

Quotient-Remainder Theorem: For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, $\exists$ unique $q, r \in \mathbb{Z}$:

$$n = dq + r \quad \text{and} \quad 0 \leq r < d$$

Notation: $q = n \text{ div } d$ (quotient), $r = n \bmod d$ (remainder)

Absolute Value: $|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$

Properties: $-|x| \leq x \leq |x|$, $|-x| = |x|$, $|x + y| \leq |x| + |y|$

Floor & Ceiling:

- **Floor:** $\lfloor x \rfloor = n$ where $n \leq x < n + 1$ (largest integer $\leq x$)
- **Ceiling:** $\lceil x \rceil = n$ where $n - 1 < x \leq n$ (smallest integer $\geq x$)

Important Theorems & Formulas

Binomial Theorem:

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \quad \text{where} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Factorization: $p^n - q^n = (p - q)(p^{n-1} + p^{n-2}q + \cdots + q^{n-1})$

Key Results:

- $\sqrt{2}$ is irrational
- There are infinitely many prime numbers
- Fundamental Theorem of Arithmetic: Every integer > 1 has unique prime factorization

Complex Numbers

Definition: $z = a + bi$ where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$. $a = \text{Re}(z)$ (real part), $b = \text{Im}(z)$ (imaginary part)

Basic Operations: For $z = a + bi$ and $w = c + di$:

$$\begin{aligned} z + w &= (a + c) + (b + d)i \\ z \cdot w &= (ac - bd) + (ad + bc)i \\ \bar{z} &= a - bi \quad \text{(complex conjugate)} \\ |z| &= \sqrt{a^2 + b^2} \quad \text{(modulus)} \\ z \cdot \bar{z} &= |z|^2 = a^2 + b^2 \end{aligned}$$

Polar Form: $z = r(\cos\theta + i \sin\theta) = re^{i\theta}$ where $r = |z|$ and $\theta = \arg(z)$

Key Formulas:

- **Euler's Formula:** $e^{i\theta} = \cos\theta + i \sin\theta$
- **De Moivre's Theorem:** $(re^{i\theta})^n = r^n e^{in\theta} = r^n(\cos(n\theta) + i \sin(n\theta))$
- **nth Roots:** $z^{1/n} = r^{1/n} e^{i(\theta + 2\pi k)/n}$ for $k = 0, 1, \ldots, n - 1$

Useful Properties:

- $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- $|z \cdot w| = |z| \cdot |w|$, $|z/w| = |z|/|w|$ (for $w \neq 0$)
- $z^{-1} = \frac{\bar{z}}{|z|^2}$ (for $z \neq 0$)

Set Theory

Operations (relative to universe U):

$$\begin{aligned} A \cup B &= \{x \in U \mid x \in A \text{ or } x \in B\} \\ A \cap B &= \{x \in U \mid x \in A \text{ and } x \in B\} \\ A - B &= \{x \in U \mid x \in A \text{ and } x \notin A\} = A \cap B^c \\ A^c &= \{x \in U \mid x \notin A\} \end{aligned}$$

Properties:

- $A \cap B \subseteq A \subseteq A \cup B$
- $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$ (transitivity)
- $A \subseteq B \iff A \cap B = A \iff A \cup B = B$
- $\emptyset \subseteq A$ for all sets A

Partition: Non-empty sets $\{A_1, \ldots, A_n\}$ partition A if: $A = A_1 \cup \cdots \cup A_n$ and $A_i \cap A_j = \emptyset$ for $i \neq j$. **Power set:** $\mathcal{P}(A) = \{S \mid S \subseteq A\}$, $|\mathcal{P}(A)| = 2^{|A|}$ **Cartesian product:** $A \times B = \{(a, b) \mid a \in A, b \in B\}$

Relations

A relation R from A to B is a subset of $A \times B$. Write $xRy \iff (x, y) \in R$. **Inverse:** $R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}$ **Composition:** If $R \subseteq A \times B$ and $S \subseteq B \times C$:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in R \text{ and } (b, c) \in S\}$$

Properties on set A:

- **Reflexive:** $\forall x \in A, (x, x) \in R$
- **Symmetric:** $\forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$
- **Transitive:** $\forall x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$

Equivalence relation: Reflexive, symmetric, and transitive. **Transitive closure** R^t of R:

- R^t is transitive
- $R \subseteq R^t$
- If S is transitive and $R \subseteq S$, then $R^t \subseteq S$ (minimality)