1. **Basic set definitions.** Given sets A and B, and a universe U that contains all sets in question, we define:

   (a) $A \cup B = \{x \in U : x \in A \text{ or } x \in B\}$.

   (b) $A \cap B = \{x \in U : x \in A \text{ and } x \in B\}$.

   (c) $A - B = \{x \in A : x \notin B\}$.

   (d) $A \Delta B = (A - B) \cup (B - A)$.

   (e) $A \times B = \{\text{ordered pairs } (x, y) : x \in A \text{ and } y \in B\}$.

   (f) $\overline{A} = U - A$.

   (g) $\mathscr{P}(A) = \{\text{all subsets of } A\}$.

   (h) $\left|P(A)\right| = 2^{|A|}$ for any set A.

   (i) The statement $A \subseteq B$ is equivalent to the statement $x \in A \Rightarrow x \in B$.

---

2. **Proof templates.**

   (a) $P \Rightarrow Q$, direct proof.

   Theorem. $P \Rightarrow Q$.
   Proof. Assume P. [Now do what you need to conclude:] Therefore, Q.
   So $P \Rightarrow Q$. □

   (b) $P \Rightarrow Q$, contrapositive proof.

   Theorem. $P \Rightarrow Q$.
   Proof. Assume $\sim Q$. [Now do what you need to conclude:] Therefore, $\sim P$.
   So $P \Rightarrow Q$. □

   (c) $P \Leftrightarrow Q$.

   Theorem. $P \Leftrightarrow Q$.
   Proof. Assume P. [Now do what you need to conclude:] Therefore, Q.
   So $P \Rightarrow Q$.
   Next, assume Q. [Now do what you need to conclude:] Therefore, P.
   So $Q \Rightarrow P$.
   Therefore, $P \Leftrightarrow Q$. □

(d) $A \subseteq B$.

Theorem. $A \subseteq B$.
Proof. Assume $x \in A$. [Now do what you need to conclude:] Therefore, $x \in B$.
So $A \subseteq B$. □

(e) $A = B$.

Theorem. $A = B$.
Proof. Assume $x \in A$. [Now do what you need to conclude:] Therefore, $x \in B$.
So $A \subseteq B$.
Now assume $x \in B$. [Now do what you need to conclude:] Therefore, $x \in A$.
So $B \subseteq A$.
Therefore, $A = B$. □

(f) Proof by counterexample. To prove that a statement is false, you need only find one instance where the statement fails.

(g) Proof by the principle of mathematical induction.

Theorem. $\forall n \in \mathbb{N},\ A(n)$.
Proof. Step 1: Is $A(1)$ true? [Now do what you need to conclude:] So $A(1)$ is true.
Step 2: Assume $A(k)$. [Now do what you need to conclude:] So $A(k+1)$ follows. So $A(k) \Rightarrow A(k+1)$.
Therefore, by the principle of mathematical induction, $A(n)$ is true $\forall n \in \mathbb{N}$.
□

---

3. Some special sets.

(a) $\mathbb{Z} = \{\text{integers}\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

(b) $\mathbb{N} = \{\text{natural numbers}\} = \{1, 2, 3, \ldots\}$.

(c) $\mathbb{R} = \{\text{real numbers}\} = (-\infty, \infty)$.

(d) $\mathbb{Q} = \{\text{rational numbers}\} = \{\text{fractions } m/n : m, n \in \mathbb{Z} \text{ and } n \neq 0\}$.

(e) Let $a, b \in \mathbb{Z}$. We write $a + b\mathbb{Z}$ for the set $\{a + bm : m \in \mathbb{Z}\}$.

---

4. Facts about integers.

(a) Let $a, b \in \mathbb{Z}$. We say a divides b, written $a|b$, if $b = na$ for some $n \in \mathbb{Z}$.

(b) Let $a, b \in \mathbb{Z}$. If $a|b$ then $a|nb$ for any $n \in \mathbb{Z}$.

(c) Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|(b + c)$.

(d) (Division algorithm.) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

---

5. Counting.

(a) Multiplication principle: if there are m ways of doing Thing 1 and, for each of these ways, there are n ways of doing Thing 2, then there are mn ways of doing Thing 1 and Thing 2 together.

Corollary: the number of length-k lists that can be made from n items is

- n^k if repetition is allowed;
- $n(n-1)(n-2)\cdots 2\cdot 1$ if not.

(b) Subtraction principle: the number of lists, or sets, with a property P equals the total number of possible lists, or sets, minus the number of lists, or sets, without property P.

(c) Addition principle: if there are m ways of doing Thing 1 and n ways of doing Thing 2, then there are $m+n$ ways of doing Thing 1 *or* Thing 2 (or both), provided you're not counting twice.

(d) Inclusion-exclusion principle: in general (that is, even if you are counting twice), if there are m ways of doing Thing 1 and n ways of doing Thing 2, then the number of ways of doing Thing 1 *or* Thing 2 (or both) is $m+n$ minus the number of ways of doing Thing 1 *and* Thing 2 together.

(e) The number of k-elements subsets of a set with n elements is

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

---

6. The Binomial Theorem. For $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j.$$

---

7. Probability.

(a) Some definitions:

- *Experiment*: a repeatable procedure.
- *Sample space*: the set of possible outcomes of an experiment.
- *Event*: a subset of the sample space.
- $P(A)$: the probability of the event A.
- *Random variable, or rv:* A way of assigning numbers to the outcomes of an experiment.
- *Probability mass function, or pmf,* for an rv X: The function $P(X = x)$, as x ranges over all possible values of X.

- *Expected value* $E(X)$ of an rv X:

$$E(X) = \sum_x x \cdot P(X = x),$$

where the sum is over all possible values x of X.

(b) Some axioms:

- Axiom 1: If all outcomes of an experiment are equally likely, then for any event A,

$$P(A) = \frac{|A|}{|S|},$$

where $|A|$ is the cardinality of the set A and $|S|$ is the cardinality of the sample space S (assuming these cardinalities are finite).
- Axiom 2: If A and B are independent events, and AB denotes $A \cap B$ (meaning the event where both A and B occur), then

$$P(AB) = P(A)P(B).$$

(c) Some facts about the binomial distribution:

- A *binomial experiment* is one with only two possible outcomes, called a *success* and a *failure*.
- In a binomial experiment with $P(\text{success}) = p$, let X be the number of successes (in a single trial of the experiment). Then $E(X) = p$.
- In a binomial experiment with $P(\text{success}) = p$, let X be the number of successes in n independent trials of the experiment. Then

$$P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

for $0 \le k \le n$.