Objectives for the First Midterm Exam, and in addition

STATE THE DEFINITIONS AND USE THEM IN PROOFS

• Numbers
  – Congruence of integers
  – Rational number, irrational number
  – Prime number
  – Binomial coefficients
• Ordered Sets
  – Upper (resp. lower) bound of a subset
  – Bounded subset
  – Least upper (resp. greatest lower) bound of a subset
  – Least upper bound property (completeness)
• Relations and Functions
  – Relation, Function
  – Domain, codomain and range of a function: equality of functions
  – Injective function, surjective function, bijective function
  – Composition of functions
  – Identity function on a set
  – Inverse of a relation
  – Image of a set in the domain of a function;
  – Preimage (inverse image) of a subset of a function’s codomain

STATE THE THEOREMS AND USE THEM IN PROOFS

• Integers
  – Division algorithm for integers
  – Arithmetical properties of congruence of integers
  – For integers \( a \) and \( b \) not both zero, the \( \gcd(a, b) \) is the smallest positive integral linear combination of \( a \) and \( b \).
  – Euclid’s Lemma: If \( a \) and \( b \) are integers and \( p \) is a prime such that \( p \mid ab \), then \( p \mid a \) or \( p \mid b \).
  – Properties of binomial coefficients:
    * Pascal triangle relation
    * Binomial coefficient \( \binom{n}{k} \) is the number of \( k \)-element subsets of an \( n \)-element set.
    * Factorial formula for binomial coefficients
  – Pigeonhole Principle
• Ordered Sets
  – Basic properties of ordered fields
  – If \( a \) and \( b \) are elements of an ordered field, then \( a = b \iff a \leq b \land b \leq a \).
• Arithmetic-geometric mean inequality: if \( x \) and \( y \) are nonnegative real numbers, then \( \sqrt{xy} \leq \frac{1}{2}(x+y) \).
• Bernoulli’s inequality: if \( n \in \mathbb{N} \) and \( x > -1 \), then \( 1 + nx \leq (1 + x)^n \).
• Sum of a finite geometric progression: if \( c \in \mathbb{R} \) and \( c \neq 1 \), then for all \( n \in \mathbb{N} \),
\[
1 + c + c^2 + \cdots + c^n = \frac{1 - c^{n+1}}{1 - c}.
\]
• The set of positive rational numbers \( x \) satisfying \( x^2 < 2 \) has no least upper bound in \( \mathbb{Q} \).
• Functions
  − Composition of functions is associative.
  − The composition of injective functions is injective.
  − The composition of surjective functions is surjective.
  − A function \( f \) is bijective if and only if the inverse relation \( f^{-1} \) is a function.
  − Inverse functions preserve all set operations.
  − Functions do not necessarily preserve set operations:
    If \( f : A \to B \) and \( W, X \subseteq A \) and \( Y \subseteq B \), then
    * \( f(W \cap X) \subseteq f(W) \cap f(X) \), but equality need not hold.
    * \( f(W \cup X) = f(W) \cup f(X) \).
    * \( X \subseteq f^{-1}(f(X)) \), but equality need not hold.
    * \( Y \subseteq f(f^{-1}(Y)) \), but equality need not hold.

**Use Proof Techniques**

• Use the contrapositive to prove statements of the form \( P \Rightarrow Q \).
• Construct proofs by contradiction.
• Prove biconditional statements.
• Prove existence and uniqueness statements.
• Prove set-membership statements.
• Prove that a set is a subset of, or is equal to, another set.
• To disprove a statement \( P \):
  − Prove \( \sim P \); or
  − Assume \( P \) and derive a contradiction.
• Use a counterexample to disprove a universal statement.
• Construct proofs by induction.
• Prove that a function is
  − Injective
  − Surjective
  − Bijective