1. Functions
   - A function \( f : X \to Y \) is injective/one-to-one if whenever \( x_1, x_2 \in X \) and \( f(x_1) = f(x_2) \) then \( x_1 = x_2 \).
   - A function \( f : X \to Y \) is surjective/onto if for all \( y \in Y \) there exists an \( x \in X \) such that \( f(x) = y \).

2. Polynomials
   - If \( f(x) \) and \( g(x) \) are polynomials with coefficients in a field \( F \), then there exists unique polynomials \( q(x) \) and \( r(x) \) with coefficients in \( F \) such that \( f(x) = q(x)g(x) + r(x) \) where the degree of \( r(x) \) is less than the degree of \( g(x) \). It is said that \( g(x) \) divides \( f(x) \) if and only if \( r(x) = 0 \).
   - If \( p(x) \) is a polynomial over a field \( F \) and \( a \in F \), then \( p(a) = 0 \) if and only if \( x - a \) divides \( p(x) \).
   - If \( p(x) \) and \( q(x) \) are polynomials of degree at most \( n \) with coefficients in a field \( F \) that agree at \( n + 1 \) distinct points in \( F \), then \( p = q \).
   - (Rational Root Theorem) If \( p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) where \( a_0, a_1, \ldots, a_n \in \mathbb{Z} \) and \( a_n \neq 0 \), then if a rational number \( r = \frac{b}{c} \) with \( \gcd(b, c) = 1 \) is a root of \( p(x) \), then \( b|a_0 \) and \( c|a_n \).
   - (Gauss’ Lemma) A polynomial \( p(x) \) with integer coefficients is a product of two non-constant polynomials with integer coefficients if and only if \( p(x) \) is a product of two non-constant polynomials with rational coefficients.
   - (Eisenstein Irreducibility Criterion) Let \( p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) where \( a_0, a_1, \ldots, a_n \in \mathbb{Z} \) and \( a_n \neq 0 \). If there exists a prime number \( q \) such that \( q \) does not divide \( a_n \), \( q^2 \) does not divide \( a_0 \), and \( q \) divides \( a_j \) for all \( j \in \{1, \ldots, n-1\} \), then \( p(x) \) is not divisible by any non-constant polynomial with rational coefficients.
   - (Fundamental Theorem of Algebra) Consider the complex polynomial \( p(z) = a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \) where \( a_0, a_1, \ldots, a_n \in \mathbb{C} \) and \( a_n \neq 0 \). Then \( p(z) = a_n(z-r_1)(z-r_2)\cdots(z-r_n) \) where \( r_1, \ldots, r_n \in \mathbb{C} \).

3. Algebra
   - (Binomial Theorem) For all natural numbers \( n \) and elements \( x, y \) such that \( xy = yx \), \((x + y)^n = \sum_{k=0}^{n} \binom{n}{k}x^ky^{n-k} \).
   - A group is a set \( G \) together with an operation \( \cdot : G \times G \to G \) such that:
     (i) for all \( a, b, c \in G \), \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \),
     (ii) there exists a (unique) element \( e \in G \) such that \( a \cdot e = a = e \cdot a \) for all \( a \in G \), and
     (iii) for each \( a \in G \) there exists a \( b \in G \) (denoted \( a^{-1} \)) such that \( a \cdot b = e = b \cdot a \).
   - Give a group \( G \), the order of an element \( g \in G \) is the smallest natural number \( n \) (possibly including 0) such that \( g^n = e \), provided such a number exists.
   - A finite group is a group with a finite number of elements. If \( n = |G| \) is the number of elements in a group \( G \), then \( g^n = e \) for all \( g \in G \).
   - A subgroup of a group \( G \) is a set \( H \subseteq G \) that is a group with the same operations as \( G \); that is, \( H \subseteq G \) and \( h_1 \cdot h_2 \in H \) for all \( h_1, h_2 \in H \), and \( h^{-1} \in H \) for all \( h \in H \).
   - If \( H \) is a subgroup of a group \( G \) with a finite number of elements, then \( |H| \) divides \( |G| \).
   - A group is said to be abelian if \( a \cdot b = b \cdot a \) for all \( a, b \in G \).
   - Every finite abelian group is of the form \((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_m\mathbb{Z})\) for some natural number \( m, n_1, \ldots, n_m \).