Elementary Mathematics

Contents

1 Introduction to Number Theory **2**
1.1 Natural Numbers . . . 2
1.2 Integer Division and Modular Arithmetic . . . 2
1.3 Prime Numbers . . . 3

2 Basic Algebra **3**
2.1 Algebraic Expressions . . . 3
2.2 Equations and Inequalities . . . 3
2.3 Functions . . . 4

3 Advanced Algebra **4**
3.1 Complex Numbers . . . 4
3.2 Vector Spaces . . . 4

4 Linear Algebra **5**
4.1 Matrices and Determinants . . . 5
4.2 Eigenvalues and Eigenvectors . . . 5

5 Geometry **6**
5.1 Euclidean Geometry . . . 6
5.2 Triangles . . . 6
5.3 Circles . . . 6

6 Trigonometry **7**
6.1 Trigonometric Functions . . . 7
6.2 Trigonometric Equations . . . 7

7 Calculus **7**
7.1 Limits . . . 7
7.2 Derivatives . . . 8
7.3 Integrals . . . 8

8 Set Theory **8**
8.1 Basic Set Operations . . . 8
8.2 Functions and Relations . . . 9

9 Probability Theory **9**
9.1 Basic Probability . . . 9
9.2 Conditional Probability . . . 9
9.3 Random Variables . . . 10

1 Introduction to Number Theory

1.1 Natural Numbers

The set of natural numbers, denoted by $\mathbb{N}$, is the foundation of elementary mathematics. It consists of the counting numbers:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

Definition 1.1 (Peano Axioms)**.** *The Peano Axioms are the fundamental axioms for the natural numbers:*

1. *0 is a natural number.*
2. *For every natural number n, there exists a unique natural number called the successor of n, denoted by $S(n)$.*
3. *0 is not the successor of any natural number.*
4. *If $S(m) = S(n)$, then $m = n$.*
5. *If a set K of natural numbers contains 0 and the successor of every number in K, then K is the entire set of natural numbers.*

1.2 Integer Division and Modular Arithmetic

For any two integers a and b ($b \neq 0$), there exist unique integers q (quotient) and r (remainder) such that:

$$a = bq + r, \quad 0 \leq r < |b|$$

This is known as the Division Algorithm.

Definition 1.2 (Congruence)**.** *Two integers a and b are said to be congruent modulo m if m divides their difference. We write:*

$$a \equiv b \pmod{m}$$

This means that a and b have the same remainder when divided by m.

Theorem 1.3 (Properties of Congruences)**.** *For any integers a, b, c, and d, and positive integer m:*

1. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:*
   - $a + c \equiv b + d \pmod{m}$
   - $a - c \equiv b - d \pmod{m}$
   - $ac \equiv bd \pmod{m}$
2. *If $a \equiv b \pmod{m}$, then for any integer k:*
   - $ka \equiv kb \pmod{m}$
   - $a^k \equiv b^k \pmod{m}$

1.3 Prime Numbers

A natural number $p > 1$ is called prime if its only positive divisors are 1 and itself.

Theorem 1.4 (Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than 1 can be represented uniquely as a product of prime powers:*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

where $p_1, p_2, \ldots, p_k$ are distinct primes and $a_1, a_2, \ldots, a_k$ are positive integers.

Theorem 1.5 (Infinitude of Primes)**.** *There are infinitely many prime numbers.*

Proof. Suppose, for the sake of contradiction, that there are only finitely many primes: $p_1, p_2, \ldots, p_k$. Consider the number:

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$$

N is not divisible by any of $p_1, p_2, \ldots, p_k$, as it leaves a remainder of 1 when divided by each of them. Therefore, either N is itself prime, or it has a prime factor larger than any in our supposed finite list. In either case, we have a prime not in our original list, contradicting our assumption. Thus, there must be infinitely many primes. □

Theorem 1.6 (Euler's Totient Function)**.** *For a positive integer n, Euler's totient function $\phi(n)$ counts the number of integers between 1 and n that are coprime to n. If $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, then:*

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

2 Basic Algebra

2.1 Algebraic Expressions

An algebraic expression is a combination of variables, numbers, and operations. For example:

$$3x^2 + 2y - 5$$

Definition 2.1 (Polynomial)**.** *A polynomial in x is an expression of the form:*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

where n is a non-negative integer and $a_0, a_1, \ldots, a_n$ are constants, with $a_n \neq 0$.

2.2 Equations and Inequalities

An equation is a statement that two expressions are equal. For example:

$$x^2 + 3x - 4 = 0$$

An inequality is a statement that one quantity is greater than or less than another. For example:

$$2x + 5 > 7$$

Theorem 2.2 (Quadratic Formula)**.** *For a quadratic equation in the form $ax^2 + bx + c = 0$, where $a \neq 0$, the solutions are given by:*

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

2.3 Functions

A function f from a set A to a set B is a rule that assigns to each element x in A exactly one element y in B. We write:

$$f : A \to B$$

Definition 2.3 (Injective, Surjective, and Bijective Functions)**.** *Let $f : A \to B$ be a function.*

- *f is injective (one-to-one) if $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in A$.*
- *f is surjective (onto) if for every $y \in B$, there exists an $x \in A$ such that $f(x) = y$.*
- *f is bijective if it is both injective and surjective.*

Theorem 2.4 (Composition of Functions)**.** *If $f : A \to B$ and $g : B \to C$ are functions, then their composition $g \circ f : A \to C$ is defined as:*

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$.

3 Advanced Algebra

3.1 Complex Numbers

Definition 3.1 (Complex Number)**.** *A complex number is a number of the form $a + bi$, where a and b are real numbers and i is the imaginary unit defined by $i^2 = -1$.*

The set of all complex numbers is denoted by $\mathbb{C}$. For a complex number $z = a + bi$:

- a is called the real part, denoted by $\mathrm{Re}(z)$
- b is called the imaginary part, denoted by $\mathrm{Im}(z)$

Theorem 3.2 (Fundamental Theorem of Algebra)**.** *Every non-constant polynomial with complex coefficients has at least one complex root.*

3.2 Vector Spaces

Definition 3.3 (Vector Space)**.** *A vector space over a field F is a set V together with two operations:*

- *Vector addition: $+ : V \times V \to V$*
- *Scalar multiplication: $\cdot : F \times V \to V$*

satisfying the following axioms for all $u, v, w \in V$ and $a, b \in F$:

1. *$u + v = v + u$ (commutativity)*
2. *$(u + v) + w = u + (v + w)$ (associativity)*
3. *There exists a zero vector $0 \in V$ such that $v + 0 = v$ for all $v \in V$*
4. *For each $v \in V$, there exists $-v \in V$ such that $v + (-v) = 0$*
5. *$a(u + v) = au + av$ (distributivity)*
6. *$(a + b)v = av + bv$ (distributivity)*

7. $(ab)v = a(bv)$ *(associativity of scalar multiplication)*

8. $1v = v$ *where* 1 *is the multiplicative identity in* F

Definition 3.4 (Linear Independence). *A set of vectors* $\{v_1, v_2, \ldots, v_n\}$ *in a vector space* V *is linearly independent if the equation:*

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0$$

has only the trivial solution $a_1 = a_2 = \ldots = a_n = 0$.

Definition 3.5 (Basis). *A basis for a vector space* V *is a linearly independent set of vectors that spans* V.

Theorem 3.6 (Dimension Theorem). *Any two bases of a finite-dimensional vector space have the same number of elements, called the dimension of the vector space.*

4 Linear Algebra

4.1 Matrices and Determinants

Definition 4.1 (Matrix). *A matrix is a rectangular array of numbers, symbols, or expressions arranged in rows and columns. An* $m \times n$ *matrix* A *has* m *rows and* n *columns:*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Definition 4.2 (Determinant). *The determinant of a square matrix* A *is a scalar value that provides information about the system of linear equations represented by* A. *For a* 2×2 *matrix:*

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

For larger matrices, the determinant is calculated recursively using cofactor expansion.

Theorem 4.3 (Properties of Determinants). *For square matrices* A *and* B *of the same size:*

1. $\det(AB) = \det(A)\det(B)$

2. $\det(A^T) = \det(A)$, *where* A^T *is the transpose of* A

3. $\det(A^{-1}) = \frac{1}{\det(A)}$, *if* A *is invertible*

4. $\det(kA) = k^n \det(A)$, *where* k *is a scalar and* n *is the size of* A

4.2 Eigenvalues and Eigenvectors

Definition 4.4 (Eigenvalue and Eigenvector). *For a square matrix* A, *a scalar* λ *is called an eigenvalue of* A *if there exists a non-zero vector* v *such that:*

$$Av = \lambda v$$

The vector v *is called an eigenvector of* A *corresponding to the eigenvalue* λ.

Theorem 4.5 (Characteristic Equation). *The eigenvalues of a square matrix* A *are the solutions to the characteristic equation:*

$$\det(A - \lambda I) = 0$$

where I *is the identity matrix of the same size as* A.

5 Geometry

5.1 Euclidean Geometry

Euclidean geometry is based on five postulates:

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one endpoint as center.
4. All right angles are congruent.
5. If two lines are drawn which intersect a third in such a way that the sum of the inner angles on one side is less than two right angles, then the two lines inevitably must intersect each other on that side if extended far enough.

5.2 Triangles

Theorem 5.1 (Angle Sum of a Triangle)**.** *The sum of the measures of the interior angles of a triangle is always 180°.*

Theorem 5.2 (Pythagorean Theorem)**.** *In a right-angled triangle, the square of the length of the hypotenuse is equal to the sum of squares of the other two sides.*

If a and b are the lengths of the legs and c is the length of the hypotenuse, then:

$$a^2 + b^2 = c^2$$

Theorem 5.3 (Law of Sines)**.** *For a triangle with sides a, b, and c, and opposite angles A, B, and C:*

$$\frac{\sin A}{a} = \frac{\sin B}{b} = \frac{\sin C}{c}$$

Theorem 5.4 (Law of Cosines)**.** *For a triangle with sides a, b, and c, and opposite angles A, B, and C:*

$$c^2 = a^2 + b^2 - 2ab\cos C$$

5.3 Circles

Definition 5.5 (Circle)**.** *A circle is the set of all points in a plane that are at a fixed distance (called the radius) from a central point.*

Theorem 5.6 (Area of a Circle)**.** *The area A of a circle with radius r is given by:*

$$A = \pi r^2$$

Theorem 5.7 (Circumference of a Circle)**.** *The circumference C of a circle with radius r is given by:*

$$C = 2\pi r$$

6 Trigonometry

6.1 Trigonometric Functions

The six basic trigonometric functions are:

- Sine: $\sin\theta = \frac{\text{opposite}}{\text{hypotenuse}}$
- Cosine: $\cos\theta = \frac{\text{adjacent}}{\text{hypotenuse}}$
- Tangent: $\tan\theta = \frac{\sin\theta}{\cos\theta} = \frac{\text{opposite}}{\text{adjacent}}$
- Cosecant: $\csc\theta = \frac{1}{\sin\theta}$
- Secant: $\sec\theta = \frac{1}{\cos\theta}$
- Cotangent: $\cot\theta = \frac{1}{\tan\theta}$

Theorem 6.1 (Fundamental Trigonometric Identity). *For any angle θ:*

$$\sin^2\theta + \cos^2\theta = 1$$

6.2 Trigonometric Equations

Theorem 6.2 (Addition Formulas). *For angles α and β:*

$$\begin{aligned}\sin(\alpha+\beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta \\ \cos(\alpha+\beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta\end{aligned}$$

Theorem 6.3 (Double Angle Formulas). *For any angle θ:*

$$\begin{aligned}\sin(2\theta) &= 2\sin\theta\cos\theta \\ \cos(2\theta) &= \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta\end{aligned}$$

7 Calculus

7.1 Limits

Definition 7.1 (Limit). *The limit of a function $f(x)$ as x approaches a is L, written as:*

$$\lim_{x\to a} f(x) = L$$

if for every $\epsilon > 0$, there exists a $\delta > 0$ such that:

$$0 < |x-a| < \delta \implies |f(x) - L| < \epsilon$$

Theorem 7.2 (Limit Laws). *For functions f and g and constant c:*

1. $\lim_{x\to a}[f(x) + g(x)] = \lim_{x\to a} f(x) + \lim_{x\to a} g(x)$
2. $\lim_{x\to a}[f(x) \cdot g(x)] = \lim_{x\to a} f(x) \cdot \lim_{x\to a} g(x)$
3. $\lim_{x\to a}[c \cdot f(x)] = c \cdot \lim_{x\to a} f(x)$
4. $\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{\lim_{x\to a} f(x)}{\lim_{x\to a} g(x)}$, *if* $\lim_{x\to a} g(x) \neq 0$

7.2 Derivatives

Definition 7.3 (Derivative). *The derivative of a function $f(x)$ at a point $x = a$ is defined as:*

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}$$

if this limit exists.

Theorem 7.4 (Differentiation Rules). *For functions f and g and constant c:*

1. $\frac{d}{dx}[c] = 0$
2. $\frac{d}{dx}[x^n] = nx^{n-1}$
3. $\frac{d}{dx}[cf(x)] = c\frac{d}{dx}[f(x)]$
4. $\frac{d}{dx}[f(x) + g(x)] = \frac{d}{dx}[f(x)] + \frac{d}{dx}[g(x)]$
5. $\frac{d}{dx}[f(x)g(x)] = f'(x)g(x) + f(x)g'(x)$ *(Product Rule)*
6. $\frac{d}{dx}\left[\frac{f(x)}{g(x)}\right] = \frac{f'(x)g(x) - f(x)g'(x)}{[g(x)]^2}$ *(Quotient Rule)*
7. $\frac{d}{dx}[f(g(x))] = f'(g(x)) \cdot g'(x)$ *(Chain Rule)*

7.3 Integrals

Definition 7.5 (Definite Integral). *The definite integral of a function $f(x)$ from a to b is defined as:*

$$\int_a^b f(x)dx = \lim_{n \to \infty} \sum_{i=1}^{n} f(x_i^*)\Delta x$$

where $\Delta x = \frac{b-a}{n}$ and x_i^* is any point in the i-th subinterval $[x_{i-1}, x_i]$.

Theorem 7.6 (Fundamental Theorem of Calculus). *If f is continuous on $[a, b]$ and F is an antiderivative of f on $[a, b]$, then:*

$$\int_a^b f(x)dx = F(b) - F(a)$$

Theorem 7.7 (Integration by Parts). *For functions u and v:*

$$\int u\frac{dv}{dx}dx = uv - \int v\frac{du}{dx}dx$$

8 Set Theory

8.1 Basic Set Operations

Definition 8.1 (Set Operations). *For sets A and B:*

- *Union:* $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- *Intersection:* $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- *Difference:* $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$
- *Complement:* $A^c = \{x : x \notin A\}$

- *Cartesian Product:* $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$

Theorem 8.2 (De Morgan's Laws)**.** *For sets* A *and* B*:*

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

8.2 Functions and Relations

Definition 8.3 (Function)**.** *A function* f *from set* A *to set* B *is a subset of* $A \times B$ *such that for each* $a \in A$*, there exists exactly one* $b \in B$ *with* $(a, b) \in f$*.*

Definition 8.4 (Relation)**.** *A relation* R *from set* A *to set* B *is any subset of* $A \times B$*.*

Theorem 8.5 (Composition of Functions)**.** *If* $f : A \to B$ *and* $g : B \to C$ *are functions, then their composition* $g \circ f : A \to C$ *is defined by:*

$$(g \circ f)(a) = g(f(a))$$

for all $a \in A$*.*

9 Probability Theory

9.1 Basic Probability

Definition 9.1 (Probability)**.** *For a sample space* Ω *and an event* $A \subseteq \Omega$*, the probability of* A *is a function* P *satisfying:*

1. $0 \leq P(A) \leq 1$
2. $P(\Omega) = 1$
3. *For mutually exclusive events* $A_1, A_2, \ldots$*:*

$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$$

Theorem 9.2 (Addition Rule)**.** *For events* A *and* B*:*

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

9.2 Conditional Probability

Definition 9.3 (Conditional Probability)**.** *The conditional probability of event* A *given event* B *is:*

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

where $P(B) > 0$*.*

Theorem 9.4 (Bayes' Theorem)**.** *For events* A *and* B*:*

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

9.3 Random Variables

Definition 9.5 (Random Variable)**.** *A random variable X is a function from a sample space Ω to the real numbers $\mathbb{R}$.*

Definition 9.6 (Expected Value)**.** *The expected value of a discrete random variable X with probability mass function $p(x)$ is:*

$$E[X] = \sum_{x} x \cdot p(x)$$

Definition 9.7 (Variance)**.** *The variance of a random variable X is:*

$$Var(X) = E[(X - E[X])^2] = E[X^2] - (E[X])^2$$

Theorem 9.8 (Chebyshev's Inequality)**.** *For a random variable X with finite expected value μ and finite non-zero variance σ^2:*

$$P(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2}$$

for any positive real number k.