Glossary of Useful Terms

A

Aleph numbers are used to refer to the cardinality of infinite sets. $\aleph_0$ is the cardinality of the natural numbers (countably infinite).

Algorithms are step by step procedures to follow for carrying out some operation, often requiring a repeated step.

Antisymmetric Relations are relations on sets in which if a is related to b and b is related to a, then $a = b$.

Associative Property refers to the properties

$$\begin{aligned} a + (b + c) &= (a + b) + c && \text{for addition} \\ a(bc) &= (ab)c && \text{for multiplication} \end{aligned}$$

for scalars a, b, c.

Asymmetric Relations are relations on sets in which if a is related to b then b cannot be related to a.

Axioms are statements made without proof, but are considered self evident and used as a foundation for a system of mathematics. Also called postulates.

B

Biconditional Statements are statements of the form "P if and only if Q," where P and Q are statements. Denoted $P \Leftrightarrow Q$. True when P and Q are both true or both false.

Bijective Correspondence refers to two sets that can be shown to have the same cardinality by finding a bijective function from one set to the other.

Bijective Functions are functions that are both injective and surjective. The inverse of a bijective function is also a bijection.

Binary Operations are operations on two elements of a set S that results in a third element. If the third element is also in the set S, the operation is called closed.

Binomials are polynomials with exactly two terms, such as $x + 1$ or $4x^5 - 2x^3$.

C

Cardinality refers to the number of elements in the set S, with repeated elements counted only once. The empty set has cardinality 0, and all other sets have a cardinality that is a natural number or infinite. Denoted $|S|$.

Cartesian Product is a binary operation on sets A and B, denoted $A \times B$ and defined by

$$A \times B = \{(a, b) \ : \ a \in A, b \in B\}$$

Note that $A \times B$ is a set itself, but not a subset of either A nor B. The Cartesian plane is the set $\mathbb{R} \times \mathbb{R}$.

Closed (see binary operation)

Codomain of a function $f : A \to B$ is the set B. The range of a function is a (possibly improper) subset of the codomain.

Commutative Property refers to the properties

$$\begin{aligned} a + b &= b + a && \text{for addition} \\ ab &= ba && \text{for multiplication} \end{aligned}$$

for scalars a, b.

Comparable Relations are relations on sets in which if a, b are elements of the set, either a is related to b or b is related to a.

Complex Numbers are numbers of the form $a + bi$, where a, b are real numbers and $i = \sqrt{-1}$. The set of complex numbers is denoted $\mathbb{C}$.

Composite Numbers are integers that are not prime; that is, integers with factors other than 1 and themselves.

Conditional Statements are statements of the form "If P then Q," where P and Q are statements. Denoted $P \Rightarrow Q$. True if P is false, or if both P and Q are true.

Congruent Modulo n refers to two numbers being considered equivalent if they leave the same remainder upon division by n.

Conjectures are statements that have not been proven.

Conjunction refers to joining two statements P and Q using the logical "and". Denoted $P \wedge Q$. True only if both P and Q are true.

Contradication may refer to a statement that is always false, or two statements that are logically inconsistent.

Contrapositive of a conditional statement $P \Rightarrow Q$ is the statement $\sim Q \Rightarrow \sim P$. Logically equivalent to the original conditional.

Converse of a conditional statement $P \Rightarrow Q$ is the statement $Q \Rightarrow P$. Not logically equivalent to the original conditional.

Corollaries are theorems that follow immediately from another theorem or its proof.

Countable refers to the cardinality of a set that can be put into bijective correspondence with a subset of the natural numbers. Countable sets may be finite or infinite. The rational numbers, integers, and natural numbers are infinite countable sets.

Counterexample is a specific example of a number, function, set, or other object that can be used to demonstrate that a particular statement is false. For instance, the number 3 serves as a counterexample to the false statement "All integers are even."

D

Direct Proof refers to a style of proof that uses only the given hypotheses, axioms, definitions, and previous theorems to build an argument towards the given conclusion.

Disjoint refers to two or more sets with no common elements; that is, the intersection of disjoint sets will be empty.

Disjunction refers to joining two statements P and Q using the logical "or". Denoted $P \vee Q$. True if either P is true or Q is true, or both.

Distributive Property refers to the properties

$$a(b+c) = ab + ac$$

$$(b+c)a = ba + ca$$

for scalars a, b, c.

Divides is used to express one integer is a divisor of another, such as "4 divides 12". If d is a divisor of x we write $d|x$.

Divisors of an integer x are the integers d such that x/d has no remainder. Also called factors.

Domain of a function $f : A \rightarrow B$ is the set A.

E

Elements are members of a set.

Empty Set is the set that contains no elements and has cardinality zero. Also called null set. Denoted $\varnothing$.

Even Number refers to an integer than has a factor of 2. Can be written in the form $2k$ for some integer k.

Equivalence Relations are relations that are symmetric, transitive, and reflexive.

F

Factor (see divisors)

Factorial of a natural number x is the product of all natural numbers less than or equal to x. Denoted $x!$

Fields are sets that allow for addition, subtraction, multiplication, and division. Common examples include the real numbers, rational numbers, and complex numbers. The integers and natural numbers do not form fields.

Finite Sets are sets with a finite cardinality; that is, a finite number of elements.

Fractions are ratios of integers.

Functions are relations between two sets A and B that can be expressed as ordered pairs (a, b) with $a \in A$ and $b \in B$ such that every $a \in A$ is assigned to exactly one element in B. Functions are relations that pass the vertical line test - a vertical line drawn anywhere through the graph of the function will intersect the graph at most once. A function called f from the set A to the set B is denoted $f : A \to B$.

G

Greatest Common Divisor of two integers a, b is the largest positive integer that is a factor of both a and b. Denoted $\gcd(a, b)$.

Groups are sets with a closed, associative binary operation that include a unique identity element and in which every element has an inverse under the operation. Vector spaces are groups under vector addition.

I

Identity Element is an element that has no effect on another element under a binary operation. For the real numbers and its subsets, 0 is the additive identity, and 1 is the multiplicative identity.

Indirect Proof refers to proof by contradiction or proof by contrapositive.

Intersection of two sets A and B is the set formed from all elements that appear in both A and B. Denoted $A \cap B$. A subset of both A and B.

Imaginary Numbers are numbers of the form bi, where b is a real number and $i = \sqrt{-1}$. A subset of the complex numbers.

Improper Subsets are subsets that are equal to the original set.

Injective Functions are functions $f : A \to B$ such that for each b in the range of the function, there is exactly one $a \in A$ with $f(a) = b$. Also called one-to-one.

Integers are real numbers that are whole numbers, both positive and negative, including 0. Denoted $\mathbb{Z}$.

Inverse Element of an element x under a binary operation $*$ is an element x^{-1} such that $xx^{-1} = x^{-1}x = 1$ where 1 is the identity element of the operation. The symbol $-x$ is used to denote the inverse element under addition.

Inverse of a Function $f : A \to B$ is a function $f^{-1} : B \to A$ such that

$$(f^{-1} \circ f)(a) = a \qquad (f \circ f^{-1})(b) = b$$

for all $a \in A$ and $b \in B$. The inverse of a function may not exist.

Irrational Numbers are real numbers that cannot be expressed as a ratio of integers. Equivalently, these are numbers whose decimal representation does not terminate nor repeat.

L

Lattice Points are points (x, y) on the Cartesian plane where both x and y are integers.

Least Common Multiple of two integers a, b is the smallest positive integer that is divisible by both a and b. Denoted $\text{lcm}(a, b)$.

Lemmas are theorems used to support the proof of a theorem.

Linear Operation is a map $T : V \to W$ from one vector space V to another W that preserves addition and scalar multiplication; that is, for all $v_1, v_2 \in V$ and any scalar a,

$$T(v_1 + v_2) = T(v_1) + T(v_2) \qquad T(av_1) = aT(v_1)$$

Linear Ordering (see total ordering)

M

Matrix is an array of scalars arranged into rows and columns. An $m \times n$ matrix has m rows and n columns.

Modulo (see congruent modulo n)

N

Natural Numbers are positive whole numbers. Generally does not include 0, but some authors will make that assumption. A subset of the integers, rational numbers, and real numbers. Denoted $\mathbb{N}$.

Negation of a statement is its logical opposite; true when the original statement is false, and false when the original statement is true.

Null Set (see empty set)

O

Odd Number refers to an integer than does not have a factor of 2. Can be written in the form $2k+1$ for some integer k.

One-to-one (see injective)

Onto (see surjective)

Open Statements are statements whose truth value depends on a variable, such as "$x < 7$" which is true for some values of x but not others.

P

Paradox refers to a statement that appears to contradict itself, leading to an impossible, senseless, or logically unacceptable conclusion.

Parity refers to the property of an integer, function, or permutation being even or odd.

Partial Ordering is a relation on a set that is antisymmetric, transitive, and reflexive. Every total ordering is a partial ordering, but a partial ordering may not be a total ordering. An example would be the "inclusion" relation on the elements of a power set.

Partition of a set is a disjoint collection of its subsets, whose union makes up the entire set. For example, the real numbers may be partitioned into the rational and irrational numbers, and the integers can be partitioned into the even integers and odd integers.

Perfect Square is an integer whose square roots are also integers, such as 4, 16, 25, 36, etc.

Permutation is an ordered arrangement of elements of a set. A set with cardinality n can be arranged in $n!$ permutations.

Polynomials in one variable are sums of multiples of powers of that variable, where all exponents on the variable are positive integers or zero.

Poset refers to a set together with a relation that is a partial ordering; a **p**artially **o**rdered **set**.

Postulates (see axioms)

Power Set of a set S is the set of all subsets of S, including S itself and the empty set. Denoted $\mathcal{P}(S)$. If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.

Prime Numbers are positive integers greater than 1 that are only divisible by 1 and themselves.

Principle refers to an important theorem that often serves as a fundamental fact in a mathematical system.

Proofs are logical, structured arguments that employ definitions, axioms, and theorems to show that a conjecture is true.

Proper Subsets are subsets that are not equal to the given set.

Proposition (see theorem)

Q

Quadratic Functions are polynomials with degree 2, often written in the form ax^2+bx+c for single variable polynomials.

Quotient refers to a ratio; the result of dividing one value by another. May refer to only the integer part of such a division, as in the quotient of 16 divided by 3 is 5.

R

Range of a function $f : A \to B$ is the set of all actual outputs in the codomain B. The range is a (possibly improper) subset of the codomain B.

Rational Numbers are real numbers that can be expressed as a ratio a/b of integers with $b \neq 0$ and where a and b have no common factors. May also be defined as the real numbers that can be expressed as terminating or repeating decimal. Includes the integers.

Real Numbers include all rational and irrational numbers. Represented as the points on an infinite number line. Denoted $\mathbb{R}$.

Reciprocal of a number $x \neq 0$ is a number x^{-1} such that $xx^{-1} = x^{-1}x = 1$.

Reflexive Relations are relations on sets in which every element is related to itself.

Relation between sets A and B is a well-defined association of elements from A to elements of B. Often realized as a set of ordered pairs (a, b) with $a \in A$ and $b \in B$. Functions are relations with the additional property that each element of A is associated to exactly one element of B.

Relatively Prime refers to two integers that have no common positive factors other than 1.

S

Scalars are elements of a field. Unless otherwise specified, typically refers to real numbers or complex numbers.

Sets are unordered, well-defined collections of unique objects.

Sequences are ordered lists of numbers that can often be described by a function or algorithm for finding each term.

Statements are phrases or expressions that can be determined to be definitely true or definitely false.

Subset are sets in which every element also belongs to another, given set. We write $T \subset S$ to indicate that T is a proper subset of S, and $T \subseteq S$ to indicate that T is a possibly equal to S (an improper subset).

Surjective Functions are functions $f : A \to B$ such that for each b in the codomain B, there is at least one $a \in A$ with $f(a) = b$. Also called onto.

Symbolic Logic refers to the use of symbols to denote propositions and operations on them to determine the truth value of compound statements.

Symmetric Relations are relations on sets in which if x is related to y, then y is also related to x.

T

Tautologies are statements that are always logically true, independent of the truth value of its variables.

Theorems are statements that are proven to be true using accepted definitions, axioms, and previously proven theorems. Theorems of lesser importance may be called propositions.

Total Ordering is a relation on a set that is antisymmetric, transitive, and comparable. Every total ordering is a partial ordering, but a partial ordering may not be a total ordering. An example would be the "less than or equal to" relation on the real numbers.

Transitive Relations are relations on sets in which if x is related to y and y is related to z, then x is also related to z.

U

Uncountable refers to an infinite set that does not allow a bijection with the natural numbers. Examples include the complex numbers, real numbers, and irrational numbers.

Union of two sets A and B is the set formed from all elements that appear in either A or B. Denoted $A \cup B$. A and B are both subsets of $A \cup B$.

Universal Set may refer to a larger set that includes all other sets being considered as subsets, or to the "set of all objects including itself" that leads to a paradox given certain set axioms.

V

Vectors are ordered tuples of numbers called scalars that can be realized as a physical quantity with magnitude and direction.

Vector Spaces are sets V of vectors that are closed under the binary operations of vector addition and scalar multiplication, and so that the following axioms are satisfied:

- Vector addition is associative: $v + (u + w) = (v + u) + w$ for all $v, u, w \in V$
- Vector addition is commutative: $v + u = u + v$ for all $u, v \in V$
- Additive identity: there exists $\mathbf{0} \in V$ such that $v + 0 = 0 + v = v$ for all $v \in V$
- Additive inverses: for each $v \in V$ there exists $-v \in V$ such that $v + (-v) = -v + v = \mathbf{0}$
- Compatibility of multiplication: $a(bv) = (ab)v$ for all $v \in V$ and scalars a, b
- Scalar identity: $1v = v1 = v$ for all $v \in V$
- Distribution over vector addition: $a(v + u) = av + au$ for $v, u \in V$ and scalar a
- Distribution over scalar addition: $(a + b)v = av + bv$ for $v \in V$ and scalars a, b

Important examples include the complex numbers, real numbers, and the $m \times n$ matrices.

Venn Diagrams are illustrations of sets, in which each set is depicted by a shape (often a circle), that can be used to represent intersections and unions of abstract sets.

W

Well Defined refers to a description of a set, relation, algorithm, or operation that leaves no ambiguity in its interpretation.

Well Ordered Sets are totally ordered sets with a least element. The natural numbers are well ordered.

Symbols Guide

$\mathbb{C}$	Complex numbers
$\mathbb{N}$	Natural numbers
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathbb{Z}$	Integers
$\mathbb{R} - \mathbb{Q}$	Irrational numbers
$\varnothing$	Empty set
$\lvert S \rvert$	Cardinality of set S
$x \in S$	x is an element of set S
$x \notin S$	x is not an element of set S
$T \subset S$	T is a proper subset of set S
$T \subseteq S$	T is a (possibly improper) subset of set S
$T \not\subset S$	T is not a subset of set S
$\mathcal{P}(S)$	Power set of set S
$T \cup S$	Union of sets T and S
$T \cap S$	Intersection of sets T and S
$T \times S$	Cartesian product of sets T and S
$T - S$	Set difference of sets T and S
$\overline{S}$, S^C	Complement of set S
$\sim P$	Negation, "Not P"
$P \wedge Q$	Conjunction, "P and Q"
$P \vee Q$	Disjunction, "P or Q"
$P \Rightarrow Q$	Conditional, "If P then Q"
$P \Leftrightarrow Q$	Biconditional, "P if and only if Q"
$\exists$	There exists
$\nexists$	There does not exist
$\forall$	For all
$\therefore$	Therefore
$\because$	Because, since
$\square$, $\blacksquare$, QED	End of proof
$a \mid b$	a divides b
$a \mod b$	Modulus, remainder of a upon division by b
$x!$	Factorial, $x! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot x$
xRy	x is related to y by relation R; $(x, y) \in R$
$f : A \to B$	f is a function with domain A and codomain B

α, A	Alpha
β, B	Beta
γ, Γ	Gamma
δ, Δ	Delta
ε, E	Epsilon
ζ, Z	Zeta
η, H	Eta
θ, Θ	Theta
ι, I	Iota
κ, K	Kappa
λ, Λ	Lambda
μ, M	Mu
ν, N	Nu
ξ, Ξ	Xi
o, O	Omicron
π, Π	Pi
ρ, P	Rho
σ, Σ	Sigma
τ, T	Tau
υ, Υ	Upsilon
ϕ, Φ	Phi
χ, X	Chi
ψ, Ψ	Psi
ω, Ω	Omega