Definition

Subset

Notation: $A \subseteq B$, informally $A \subset B$

if $x \in A$, then $x \in B$

Definition

Proper Subet

Notation: $A \subset B$

$A \subseteq B$ and $A \neq B$

Definition

Union

Notation: $A \cup B$

$\{x \mid x \in A \text{ or } x \in B\}$

Definition

Intersection

Notation: $A \cap B$

$\{x \mid x \in A \text{ and } x \in B\}$

Definition

Disjoint Sets

A and B are disjoint if $A \cap B = \emptyset$

Definition

Equal Sets

A and B are equivalent if $A \subset B$ and $B \subset A$

Definition

Complement

For any set $A \subset U$

$$A' = \{x \in U \mid x \notin A\}$$

Definition

Difference

$$A \backslash B = A \cap B'$$

Definition

Cartesian Product

$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$

Definition

Relation

A relation from A to B is a subset of $A \times B$

Definition

Function or Map

Notation: $f : A \to B$, where A is the *domain* and B is the *target*

A relation from A to B where $\forall a \in A, \exists!\ (a, b)$

$f(a) = b$ means $(a, b) \in f$

Definition

Image of Function

$f(A) = \{f(a) : a \in A\}$

Note: $f(A) \subset B$

Definition

Surjective

Also known as *onto*

A function $f : A \to B$ for which $f(A) = B$

Definition

Injective

Also known as *one-to-one*

A function $f : A \to B$ for which $f(a_1) = f(a_2)$ implies $a_1 = a_2$

Definition

Bijective

A function which is both injective and surjective.

Definition

Composition

For $f : A \to B$ and $g : B \to C$, the composition $g \circ f$ is defined as:

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

Notes: $g \circ f : A \to C$, and composition is associative

Definition

Composition Properties

- If g and f are surjective, $g \circ f$ is surjective
- If g and f are injective, $g \circ f$ is injective
- If g and f are bijective, $g \circ f$ is bijective

Definition

Identity Map

Notation: id_s

$id(x) = x, id : S \to S$

Note: $id_s = \{(x, x) : x \in S\}$

Definition

Inverse

Notation: f^{-1}

$g = f^{-1} \iff g \circ f = id_A$

f is invertible means it has an inverse.

f is invertible iff it's bijective.

Definition

Partition

Let X be a set. P is a partition of X means:

$P = \{p_i \subset X \mid P \neq \emptyset\}$, all p_i are disjoint, and the union of all p_i is P.

Definition

Equivalence Relation

Relation R of X with these properties:

- Reflexive: $\forall x \in X, (x,x) \in R$
- Symmetric: $(x,y) \in R \implies (y,x) \in R$
- Transitive: $(x,y),(y,z) \in R \implies (x,z) \in R$

$x \sim y$ means $(x,y) \in R$

Definition

Equivalence Class

$[x] = \{y \in X \mid y \sim x\}$

Two equivalence classes are either disjoint or equal.

Definition

Divisibility

Notation: $b \mid a$ (b divides a)

$a = bk$ for some $k \in \mathbb{Z}$

Definition

Congruence

Let $r, s \in \mathbb{Z}$ and $n \in \mathbb{N}$.

Notation: $r \equiv_n s$

$n \mid (r - s)$

Note: $\equiv_n$ is an equivalence relation of $\mathbb{Z}$

Definition

Properties of Congruence

- $a + b \equiv b + a \quad ab \equiv ba$
- $(a + b) + c \equiv a + (b + c) \quad (ab)c \equiv a(bc)$
- $a + 0 \equiv a \quad a1 \equiv a$
- Multiplication distributes over addition
- $\exists b \in \mathbb{Z} \mid a + b \equiv 0$
- Let $a \in \mathbb{Z}, a \neq 0$
  $gcd(a, n) = 1 \iff \exists b \in \mathbb{Z} \mid ab \equiv_n 1$

Definition

Mathematical Induction

Let $S(n)$ be a statement about $n \in \mathbb{N}$

If $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and $S(k) \implies S(k + 1)$, then $S(n)$ is true for all $n \geqslant n_0$

Definition

Strong Mathematical Induction

Let $S(n)$ be a statement about $n \in \mathbb{N}$

If $S(n_0)$ is true for some $n_0 \in \mathbb{N}$, and $S(n_0), S(n_0 + 1), S(n_0 + 2) \ldots S(k) \implies S(k + 1)$, then $S(n)$ is true for all $n \geqslant n_0$

Definition

Well-Ordered

A non-empty subset of $\mathbb{Z}$ which contains a least element.

Definition

Well-Ordering Principle

Every non-empty subset of $\mathbb{N}$ is well-ordered.

Definition

Division Algorithm

Let $a, b \in \mathbb{Z}$ and $b > 0$

$\exists!\ q, r \in \mathbb{Z} \mid a = qb + r$ and $0 \leqslant r < b$

Definition

Common Divisor

Let $a, b, d \in \mathbb{Z}$

d is a common divisor of a and b means that
$d \mid a$ and $d \mid b$

Definition

Greatest Common Divisor

Notation: $gcd(a, b)$ where $a, b \in \mathbb{Z}$

Note: If $a, b > 0,\ \exists r, s \in \mathbb{Z} \mid gcd(a, b) = ar + bs$

Definition

Relatively Prime

$gcd(a, b) = 1$

Definition

Prime

p is prime if only numbers that divide it are 1 and p

Otherwise, p is *composite*

Definition

Prime Number Properties

$p \mid ab \implies p \mid a$ or $p \mid b$

There exists an infinite number of primes.

Definition

Fundamental Theorem of Arithmetic

Let $n \in \mathbb{N}, n > 1$

$n = p_1 p_2 p_3 \dots p_k$ where p_i are prime

This factorization is unique.

Definition

Binary Operation

A function $f : S \times S \to S$ on a set S

$f(a,b)$ is denoted by $a \circ b$ or ab

Definition

Group

Notation: $(S, \circ)$ for operation $\circ$ on set S

Properties:

- Associative: $(ab)c = a(bc)$
- Identity Exists: $\exists e \in S \mid ai = a = ia, \forall a \in S$
- Inverses Exist: $\forall a \in S, \exists b \in S \mid ab = e = be$

Definition

Group Properties

The inverses are unique for each element.

$$(ab)^{-1} = a^{-1}b^{-1}$$

Definition

Commutative/Abelian Group

A group for which $ab = ba \ \forall a, b \in S$

Definition

Finite Group

$(G, \circ)$ is a finite group if G is a finite set.

Otherwise, it's an infinite group.

Definition

Group Order

The order of finite group $(G, \circ)$ is $\mid G \mid$.

The order of an infinite group is ∞.

Definition

Quaternion Group

$(Q_8, \circ)$ where $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ and:

- $i^2 = j^2 = k^2 = -1$
- 1 is identity
- -1 commutes everything
- $ij = k, jk = i, ki = j$
- $ik = -j, kj = -i, ji = -k$

Definition

Matrix Group

$\mathbb{M}_2(\mathbb{R})$ is multiplicative group for all 2x2 real number matrices.

Non-abelian group.

Definition

General Linear Group

$GL_2(\mathbb{R})$ is subset of $\mathbb{M}_2(\mathbb{R})$ where every matrix is invertible.

Non-abelian group.

Definition

Multiplicative Group Exponents

- $g^n = g \circ g \circ g \circ g \cdots \mid n \geqslant 1$
- $g^0 = e$
- $g^{-1} = g^{-1} \circ g^{-1} \circ g^{-1} \cdots \mid n < 0$
- $g^m g^n = g^{m+n}$, $(g^m)^n = g^{mn}$
- $(gh)^n = (h^{-1}g^{-1})^{-n}$
  If group is abelian, then $(gh)^n = g^n h^n$

Definition

Additive Group Exponents

- $ng = g + g + g \cdots \mid n \geqslant 0$
- $-ng = -g + -g + -g \cdots \mid n < 0$

If group is abelian, then $m(g + h) = mg + mh$

Definition

Group Cancellation Laws

If G is a group, and $a, b, c \in G$, then:

$ba = bc \implies a = c$ (left cancellation)

$ab = cb \implies a = c$ (right cancellation)

Definition

Subgroup

A group $(H, \circ)$ is a subgroup of $(G, \circ)$ if $H \subseteq G$ and if H also forms a group under the operation $\circ$. This is true iff:

- Identity $e \in G$ is in H
- $h_1, h_2 \in H \implies h_1 \circ h_2 \in H$
- $h_1 \in H \implies {h_1}^{-1} \in H$

Definition

Subgroup Alternative Criteria

Let $H \subseteq G$. H is a subgroup of G iff:

- $H \neq \emptyset$
- $a, b \in H \implies a \circ b^{-1} \in H$

Definition

Trivial Subgroup

$\{e\}$

Definition

Proper Subgroup

H is a proper subgroup of G if H is a subgroup, and $H \subset G$

DEFINITION

Cyclic Subgroup

$<g>$ is the cyclic subgroup of G generated by $g \in G$

$<g>= \{g^n \mid n \in \mathbb{Z}\}$

g is the generator of $<g>$

$<g>$ is the smallest subgroup of G containing g

DEFINITION

Order of Generator

Order $\mid g \mid$ is the smallest $n \in \mathbb{N} \mid g^n = e$

If none exist, $\mid g \mid = \infty$

DEFINITION

Cyclic Group

G is a cyclic group if $\exists\, g \in G \mid G = <g>$

DEFINITION

Cyclic Group Properties

Every cyclic group is abelian.

Let $G = <x>, \quad x^k = e \iff n \mid k$

Every subgroup of a cyclic group is cyclic.

For cyclic group G of order n, and a generating $<a>, \quad b = a^k \implies \mid b \mid = \frac{n}{gcd(k,n)}$

Definition

Finite Cyclic Group in $\mathbb{Z}$

Let $Z_n = \{0, 1, 2, 3, 4, \ldots, n-1\}$

$(Z_n, +)$ is an abelian group such that:

$a + b = c$ where $a + b \equiv_n c$

Definition

Group of Units

$U_n = \{m \mid 1 \leqslant m < n,\ gcd(m, n) = 1\}$

Definition

Permutation

A permutation of a set X is a bijective map
$f : X \to X$

Notation:

$\binom{A\ B\ C}{B\ A\ C}$

Definition

Symmetric Group

All permutations of a set X.

S_n (or S_X) for set X or order n.

Binary operation is function composition.

Note: $\mid S_n \mid = n!$

Definition

Permutation Group

Subgroup of a symmetric group.

Not usually abelian.

Definition

Cycle

A permutation $p \in S_X$ such that $\exists a_1 a_2 a_3 \dots a_n \in X$ and:

$$p(a_1) = a_2$$
$$p(a_2) = a_3$$
$$\dots$$
$$p(a_n) = a_1$$

Notation: $(a_1 a_2 a_3 \dots a_n)$ for an n-cycle

Definition

Disjoint Cycles

Two cycles $(a_1 a_2 a_3 \dots a_n)$ and $(b_1 b_2 b_3 \dots b_m)$ are disjoint if $a_j \neq b_k$ for all $j \in [1, n]$ and $k \in [1, m]$.

Definition

Transposition

A cycle of length 2

Definition

Cycles Properties

Every permutation in S_n can be written as a product of disjoint cycles.

The product of disjoint cycles cannot be simplified to smaller disjoint cycles.

Disjoint cycles are commutative.

Every cycle can be written as the product of transpositions.

Definition

Alternating Groups

A_n is alternating group on n letters.

Subgroup of S_n with all even permutations.

Order $|S_n|/2$

Definition

Dihedral Group

$D_n = \{r_0, r_1, r_2, \ldots, r_{n-1}, s_1, s_2, \ldots, s_n\}$

The n^{th} dihedral group. Rigid motions of n-gon. Subgroup of S_n.

$s^2 = 1,\ r^n = 1,\ srs = r^{-1}$

Definition

Motion Group of Cube

24 elements

Made up of all rotations around midpoint diagonals.

Isomorphic to S_4

Definition *Complex Numbers*	$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$
Definition *Complex Conjugate*	$\overline{z} = a - bi$
Definition *Absolute Value of Complex Number*	$\lvert z\rvert = \sqrt{a^2 + b^2}$
Definition *Inverse of Complex Number*	$z^{-1} = \frac{z\overline{z}}{\lvert z\rvert^2}$

Definition

Complex Number Polar Coordinates

$a + bi = rcis(\theta)$

Definition

cis

$cis(\theta) = cos(\theta) + isin(\theta)$

Definition

Polar Complex Number Multiplication

Let $z = rcis(\theta) \quad w = scis(\phi) \quad z, w \neq 0$

$wz = rscis(\theta + \phi)$

Definition

De Moivre Theorem

Let $z = rcis(\theta) \quad z \neq 0$

$(rcis(\theta))^n = r^n cis(n\theta)$ where $n \in \mathbb{N}$

Definition

Circle Group

$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$

$\mathbb{T}$ is a subgroup of $\mathbb{C}^*$

$|T|$ is infinite

Definition

Roots of Unity

Elements of $\mathbb{T}$ satisfying $z^n = 1$ are the n^{th} roots of unity.

$z = cis(\frac{2k\pi}{n}) \mid k \in \{0, 1, 2, \ldots, n-1\}$

Cyclic subgroup of $\mathbb{T}$ of order n. A generator is a primitive n^{th} root of unity.

Definition

Coset

Let H be a subgroup of G.

$gH = \{gh \mid h \in H\}$ (left coset)
$Hg = \{hg \mid h \in H\}$ (right coset)

If gH = Hg, they're cosets.

g is a representative of the coset.

Definition

Coset Properties

The number of left and right cosets of H in G are equal.

The left/right cosets of H in G form a partition of G.

Definition

Coset Equivalences

For $g_1, g_2 \in G$, the following are equivalent:

- $g_1 H = g_2 H$
- $H {g_1}^{-1} = H {g_2}^{-1}$
- $g_1 H \subset g_2 H$
- $g_2 \in g_1 H$
- ${g_1}^{-1} g_2 \in H$

Definition

Index

$[G : H]$ is index of H in G

Number of left/right cosets of H in G.

Definition

Well-Defined

A function whos value is independent of the choice of representation of the input.