MA2202

Misc

- To prove uniqueness, suppose not unique and try to show equality.
- To prove equality of two sets, show that each is a subset of the other.
- To show multiple, use Euclidean algorithm, then show $r = 0$.

Basic Set Theory

A set is a collection of objects called elements.

Examples of sets

- $\mathbb{N}$ is the set of positive integers.
- $\mathbb{Z}^\times$ is the set of integers excluding 0.
- $\mathbb{Q}^\times$ is the set of rational numbers excluding 0.

Set operations

Let A, B be sets.

1. If B is a subset of A, write $B \subseteq A$.
2. $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
3. $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
4. $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.
5. $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

Functions

Let A, B be sets, and let $f : A \to B$ be a function.

- For $a \in A$, denote $f(a) = b \in B$.
- The set A is called the domain, and the set B is called the co-domain.
- The range/image of f is
$$\{b \in B : b = f(a) \text{ for some } a \in A\}$$
- Let $B' \subseteq B$. Define
$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$
- If $g : C \to D$ is another function, then we say $f = g \iff A = C, B = D$ and $f(a) = g(a)\ \forall a \in A$
- If $S \subseteq A$, then $f|_S$ denotes the same function except that the domain A is replaced by S. This function $f|_S$ is called the restriction of f to S.
- If $h : B \to C$, then the composite of h and f is a function $h \circ f : A \to C$ given by
$$(h \circ f)(a) = h(f(a)) \quad \forall a \in A$$

Notable examples

- The identity function on A is $f : A \to A$ defined by
$$f(x) = x \quad \forall x \in A$$
We also denote the identity function on A by id_A.
- The inclusion function on Y for some $Y \subset X$ is the function $h : Y \to X$ defined by $h(y) = y\ \forall y \in Y$.

Injection/Surjection/Bijection Let $f : A \to B$ be a function.

1. f is an injection if $f(a) = f(a') \implies a = a'$.
2. f is a surjection if $\forall b \in B, \exists a \in A$ such that $f(a) = b$.
3. f is a bijection if it is both an injection and a surjection.
4. If f is a bijection, we can define the inverse function $f^{-1} : B \to A$ in the following way:
For every $b \in B$, we have a unique $a \in A$ such that $f(a) = b$. Then $f^{-1}(b) = a$.
5. A function is a bijection $\iff$ its inverse function exists.

Integers

Divisbility

Given $a, b \in \mathbb{Z}$ where $a \neq 0$.

- We say a divides b if $b = ma$ for some $m \in \mathbb{Z}$. The integer b is called a multiple of a, and we write $a|b$.
- An integer n is called a unit if it divides 1. Hence $n = 1$ or -1.
- Transitivity holds, i.e. $a|b$ and $b|c \implies a|c$

Prime

A nonzero $p \in \mathbb{Z}$ is called a prime integer if:

1. p is not a unit (i.e $p \neq \pm 1$), and
2. if p divides ab for some $a, b \in \mathbb{Z}$, then $p|a$ or $p|b$.

A positive prime integer is called a prime number.

Irreducible

A nonzero $p \in \mathbb{Z}$ is called a irreducible integer if:

1. p is not a unit (i.e $p \neq \pm 1$), and
2. if p divides xy for some $x, y \in \mathbb{Z}$, then either x or y is a unit, i.e. x or y is ± 1.

Prime vs irreducible

Let p be an integer. It is an irreducible integer $\iff$ it is a prime integer.

The Euclidean algorithm

Let $x, y \in \mathbb{Z}$ with $y \neq 0$. Then there exist unique integers q and r such that
$$x = qy + r \text{ and } 0 \leq r < |y|$$
This is also known as the division algorithm.

Common divisor

Given two integers x and y where $y \neq 0$.

- A nonzero integer m is called a common divisor if $m|x$ and $m|y$.
- 1 is always a common divisor.
- If m is a common divisor, $-m$ is also a common divisor.
- Every common divisor lies bewtween $-|y|$ and $|y|$.
- There are only finitely many common divisors.

Greatest common divisor

There is a largest number d among the common divisors of x and y, which we call the GCD of x and y. Denote it by $d = \gcd(x, y)$.

- Since 1 is always a common factor, $d \geq 1$
- $\gcd(0, y) = |y|$
- $\gcd(x, y) = \gcd(y, x) = \gcd(x, |y|) = \gcd(|x|, y) = \gcd(|x|, |y|)$
- $\gcd(cx, cy) = |c| \gcd(x, y)$
- $\gcd(x, y) = \gcd(x + y, y) = \gcd(x - y, y)$

Connection with Euclidean algorithm Let x, y be integers where $y \neq 0$. Let $x = qy + r$ where $0 \leq r < |y|$. Then
$$\gcd(x, y) = \gcd(y, r)$$

Computing GCD

Given $x_1, x_2 \in \mathbb{Z}$.

- If $x_2 = 0$, then $\gcd(x_1, x_2) = |x_1|$.
- Else, $x_2 \neq 0$.

Assume $x_2 \neq 0$. Since $\gcd(x_1, x_2) = \gcd(x_1, |x_2|)$, suppose $x_2 > 0$. By the division algorithm,
$$x_1 = qx_2 + x_3 \quad \text{for some } 0 \leq x_3 < x_2$$
By the lemma above,
$$\gcd(x_1, x_2) = \gcd(x_2, x_3)$$
Doing this repeatedly, we get
$$\gcd(x_1, x_2) = \gcd(x_2, x_3) = \cdots = \gcd(x_m, 0) = x_m$$
where $|x_2| > x_3 > x_4 > \cdots \geq 0$.

Example $\gcd(6804, -930) = \gcd(6804, 930)$.
$$\begin{aligned} 6804 &= 7(930) + 294 \\ 930 &= 3(294) + 48 \\ 294 &= 6(48) + 6 \\ 48 &= 8(6) + 0 \end{aligned}$$
Hence,
$$\begin{aligned} \gcd(6804, -930) &= \gcd(6804, 930) = \gcd(930, 294) \\ &= \gcd(294, 48) = \gcd(48, 6) = \gcd(6, 0) = 6 \end{aligned}$$
Then, by reverse engineering,
$$\begin{aligned} 6 &= 294 - 6(48) \\ &= 294 - 6(930 - 3(294)) \\ &= -6(930) + (19)(294) \\ &= -6(930) + (19)(6804 - 7(930)) \\ &= 19(6804) - 139(930) \\ &= (19)(6804) + 139(-930) \end{aligned}$$
Hence, $6 = a(6804) + b(-930)$ for some $a, b \in \mathbb{Z}$.

Proposition Let $d = \gcd(x, y)$ where $y \neq 0$. Then

1. We have $d = ax + by$ for some $a, b \in \mathbb{Z}$
2. Let $I = \{mx + ny \in \mathbb{Z} : m, b \in \mathbb{Z}\}$. Then $I = d\mathbb{Z}$ is the set of all the multiples of d.
3. If an integer c divides both x and y, then c divides d.

GCD of 3 or more integers

Let $x, y, z \in \mathbb{Z}$, and not all are 0. We say c is a common divisor of x, y, z if c divides x, y, z. The GCD of x, y, z is denoted by $d = \gcd(x, y, z)$.

1. If c divides x, y, z then c divides $\gcd(x, y)$ and z.
2. $\gcd(x, y, z) = \gcd(\gcd(x, y), z)$
3. $d = mx + ny + pz$ for some $m, n, p \in \mathbb{Z}$
4. $I = \{mx + ny + pz : m, n, p \in \mathbb{Z}\} = d\mathbb{Z}$

Tut 1 Q2 (GCD given prime factorization)

Suppose

$$x = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, y = p_1^{f_1} p_2^{f_2} \cdots p_s^{f_s}, d = p_1^{g_1} p_2^{g_2} \cdots p_s^{g_s}$$

are prime factorizations of x and y, with p_i being distinct positive prime integers, and $e_i, f_i \geq 0$. Then

- The integer d divides $x \iff g_i \leq e_i$ for all i.
- If $d|x$ and $d|y$, then $g_i \leq \min\{e_i, f_i\}$ for all i.
- GCD is
$$gcd(x, y) = p_1^{\min\{e_1,f_1\}} p_2^{\min\{e_2,f_2\}} \cdots p_s^{\min\{e_s,f_s\}}$$
- If $d|x$ and $d|y$, then $d|\gcd(x, y)$

The fundamental theorem of arithmetic

Let $n > 1$ be a positive integer. Then there exists a factorization

$$n = p_1 p_2 \cdots p_s$$

where p_i is a (positive) prime number for all i, and $p_1 \leq p_2 \leq \cdots \leq p_s$. This factorization is unique.

Mathematical induction

Mathematical induction

Let $P(1)$ be a property that depends on $n \in \mathbb{N}$. If

1. $P(1)$ holds and
2. if $P(k)$ holds, then $P(k+1)$ holds

then $P(n)$ holds $\forall n \in \mathbb{N}$.

Strong MI

Let $P(1)$ be a property that depends on $n \in \mathbb{N}$. If

1. $P(1)$ holds and
2. if $P(i)$ holds for $1 \leq i \leq k$, then $P(k+1)$ holds

then $P(n)$ holds $\forall n \in \mathbb{N}$.

Binomial theorem

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \quad \forall n \in \mathbb{N}$$

Fermat's little theorem

Let p be a prime number. Then

$$p|(n^p - n) \quad \forall n \in \mathbb{Z}$$

i.e.

$$n^p \equiv n \pmod{p}$$

Equivalence relations

Relation

Let A be a set. A subset R of $A \times A$ is a relation on A. For $a, b \in A$, $a \sim b \iff (a, b) \in R$. We may write it as $a \sim_R b$.

Equivalence relation

Let A be a set. A relation R on A (i.e. $R \subseteq A \times A$) is an equivalence relation on A if for all a, b, c,

- (E1) $a \sim a$ (reflexive)
- (E2) $a \sim b \implies b \sim a$ (symmetric)
- (E3) $a \sim b \wedge b \sim c \implies a \sim c$ (transitive)

Equivalence class

Let R be an equivalence relation on a set A. Let $a \in A$. The equivalence class of $a \in A$ is the subset

$$\{x \in A : a \sim x\}$$

and we denote it by $Cl(a)$.

Partition

Let A be a set and let $\{A_i : i \in I, A_i \subseteq A\}$ be a collection of subsets of A. We say that the collection $\{A_i : i \in I\}$ forms a partition of A if

- (P1) $A = \bigcup_{i \in I} A_i$, and
- (P2) $A_i \cap A_j = \emptyset$ for all $i, j \in I$ and $i \neq j$

Alternatively, P2 can be stated as: If $A_i \cap A_j$ is a nonempty subset, then $A_i = A_j$.

Collection of all equivalence classes

Let R be an equivalence relation on a set A. The set of equivalence classes $\{Cl(a) : a \in A\}$ is denoted by A/R, $A/_{\sim_R}$, or simply $A/\sim$.

- The collection of all equivalence classes forms a partition of A.
- The map $p : A \to A/R$ given by $p(a) = Cl(a)$ is called the quotient map.

Linear Congruences

Congruent modulo m

Let m be a positive integer. Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{m}$ if $m|(a-b)$.

Simultaneous congruence equations

Solution to congruence equation

Suppose $\gcd(a, m) = 1$. For $b \in \mathbb{Z}$, the congruence equation

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

has a solution $x \in \mathbb{Z}$, that is unique modulo m, i.e. $x' \in \mathbb{Z}$ is another solution iff

$$x \equiv x' \pmod{m}$$

Chinese Remainder Theorem

Suppose $\gcd(m, m') = 1$. Then the congruence equations

$$x \equiv b \pmod{m}$$
$$x \equiv b' \pmod{m'}$$

have a common solution $x \in \mathbb{Z}$, that is unique modulo mm', i.e. if $x' \in \mathbb{Z}$ is another solution, then

$$x \equiv x' \pmod{mm'}$$

Solving simultaneous congruence equations

Solve the simultaneous congruence equations

$$x \equiv 3 \pmod{13}$$
$$x \equiv 5 \pmod{11}$$

By the division algorithm, we have $13 = 11 + 2$ and $11 = 5(2) + 1$. Hence,

$$\begin{aligned} \gcd(13, 11) = 1 &= 11 - 5(2) \\ &= 11 - 5(13 - 11) = -5(13) + 6(11) \end{aligned}$$

This implies

$$6(11) \equiv 1 \pmod{13}$$
$$-5(13) \equiv 1 \pmod{11}$$

Consider $x = 5(-5)(13) + 3(6)(11) = -127$. We can show that this is a solution, and then by the Chinese Remainder Theorem, all solutions are of the form $x = -127 + k(13)(11)$.

Binary operations

Definition

Let G be a set. A binary op $*$ on G is a function

$$*: G \times G \to G$$

- For $(x, y) \in G$, we denote $*(x, y)$ by $x * y$.
- Associative if $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- Commutative/abelian if $\forall a, b \in G$, $a * b = b * a$.

Multiplication table

Let $G = \{a, b, c\}$. We can represent a binary operation $*$ with a multiplication table:

$x * y$	$y = a$	b	c
$x = a$	a	a	b
b	a	c	c
c	b	a	c

For $*$ to be abelian, the multiplication table should be symmetric along the diagonal.

Identity

Let $(G, *)$ be a set with a binary op. Let $e \in G$.

- e is a left identity element if $\forall a \in G$, $e * a = a$.
- e is a right identity element if $\forall a \in G$, $a * e = a$.
- e is an identity element if $\forall a \in G$, $e * a = a * e = a$.

Groups

Group axioms

A group $(G, *)$ consists of a set G and a binary operation $*$ on G which satisfies four axioms:

- (G1) (Closure) For all $a, b \in G$, $a * b \in G$.
- (G2) (Associativity) For all $a, b, c \in G$,
$$(a * b) * c = a * (b * c)$$
- (G3) (Existence of identity element) $\exists e \in G$ such that for all $a \in G$,
$$e * a = a * e = a$$
Note that the identity element is unique.
- (G4) (Existence of inverse element) For each $a \in G$, $\exists b \in G$ such that
$$a * b = b * a = e$$
where e is the identity element in (G3). Note that the inverse of an element is unique.

Order

The number of elements in G is called the order of G. We denote it by $|G|$. If $|G|$ is finite, then we call G a finite group. Otherwise it is an infinite group.

Abelian group

A group $(G, *)$ is called an abelian group if $a * b = b * a$ for all $a, b \in G$.

Some theorems

Let $(G, *)$ be a group. Let $a, b, c \in G$. Then

- $(a^{-1})^{-1} - a$
- $(a * b)^{-1} = b^{-1} * a^{-1}$
- $a^{-1} * \cdots * a^{-1} = (a * \cdots * a)^{-1}$ where there are n copies of a^{-1} and a on both sides.
- (Cancellation Law) If $a * c = b * c$, then $a = b$. If $c * a = c * b$, then $a = b$.
- Given $a, b \in G$, the equation $a * x = b$ (and respectively $x * a = b$) has a unique solution $x \in G$.
- $a^n * a^m = a^{n+m}$ for $n, m \in \mathbb{Z}$.

Weakened axioms

For (G3) and (G4), if we show either

- just right identity + right inverse,
- or just left identity + left inverse,

and if (G1) and (G2) are already proven, then we have a group.

Examples of groups

nth roots of unity

Given a positive integer n. Let

$$\mu_n = \left\{ e^{\frac{2k\pi i}{n}} : k = 0, \cdots, n-1 \right\}$$

Then $(\mu_n, \times)$ forms a finite abelian group of order n, where $\times$ is the usual complex number multiplication.

- Identity is 1.
- Inverse of $e^{\frac{2k\pi i}{n}}$ is $e^{\frac{2(n-k)\pi i}{n}}$.

If we set $a = e^{\frac{2\pi i}{n}}$, then G could be written as

$$\mu_n = \left\{ 1 = a^n, a, a^2, \cdots, a^{n-1} \right\}$$

and we call μ_n a cyclic group of order n.

Integers modulo n

Let $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$. The binary operation $*$ is given by

$$x * y = \begin{cases} x + y & \text{if } x + y < n \\ x + y - n & \text{if } x + y \geq n \end{cases}$$

$(\mathbb{Z}/n\mathbb{Z})$ forms a group and is also a cyclic group of order n.

- Identity is 0.
- Inverse element is 0 for 0, $n - x$ for positive x.

Set of bijections

Let Y be a set (could be **infinite**) and let

$$S_Y = \{f : Y \to Y : f \text{ is a bijection.}\}$$

The binary operation $\circ$ is the composite of functions. Then $(S_Y, \circ)$ is a group.

- Identity is the identity function on Y.
- Inverse of a function f is its inverse function.

Symmetric group on n letters

Consider S_Y where $Y = \{1, 2, \cdots, n\}$. Then S_Y is a finite group of order $n!$.

Product group

Let $(G, *)$ and $(H, \star)$ be two groups. Consider the Cartesian product $G \times H = \{(g, h) : g \in G, h \in H\}$. Define binary operation $\cdot$ on $G \times H$ by

$$(g, h) \cdot (g', h') = (g * g', h \star h')$$

for all $(g, h), (g', h') \in G \times H$. Then $(G \times H, \cdot)$ forms a group, called the product group of $(G, *)$ and $(H, \star)$.

- Identity element is (e_G, e_H) where e_G and e_H are the identity elements of G and H respectively.
- Inverse element of (g, h) is (g^{-1}, h^{-1}).

General linear group

Let G be the set of invertible n by n matrices with entries in a field F. The binary operation $\times$ is the usual matrix multiplication. Then $(G, \times)$ is a group called the general linear group of rank n and we denote G by $\mathrm{GL}(n, F)$.

- Identity is the n by n identity matrix.
- Inverse of a matrix A is the usual inverse A^{-1}.

Special linear group

$\mathrm{SL}(n, F)$ is defined in the same way as in "General linear group", except we only have matrices with determinant 1.

Orthogonal group

$\mathrm{O}(n)$ is defined in the same way as in "General linear group", except we only have orthogonal matrices.

Group isomorphisms

Definition

Let $(G, *)$ and $(H, \star)$ be two groups. We say that these two groups are isomorphic if there exists a bijection $\phi : G \to H$ such that

$$\phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2)$$

for all $g_1, g_2 \in G$.

- The bijection ϕ is called a group isomorphism.
- We denote $(G, *) \simeq (H, \star)$ and $\phi : (G, *) \xrightarrow{\sim} (H, \star)$.
- If $(G, *)$ and $(H, \star)$ are isomorphic finite groups, then they have the same order.
- If $(G, *)$ is an abelian group, then $(H, \star)$ is an abelian group.
- $\phi : G \to G$ given by $\phi(g) = g^{-1}$ is a group isomorphism $\iff$ G is an abelian group.

Two isomorphisms

Suppose $\phi : (G, *) \to (H, \star)$ and $\psi : (H, \star) \to (K, \cdot)$ are two isomorphisms of groups. Then

- the inverse function $\phi^{-1} : (H, \star) \to (G, *)$ and
- the composite function $\psi \circ \phi : (G, *) \to (K, \cdot)$

are group isomorphisms.

Group homomorphism

Let $(G, *)$ and $(H, \star)$ be two groups. A function $\phi : G \to H$ is called a group homomorphism if

$$\phi(x * y) = \phi(x) \star \phi(y)$$

for all $x, y \in G$.

There is no requirement on ϕ to be injective or surjective. But if ϕ is a bijection, then we have a group isomorphism instead.

Subgroups

Definition

Let $(G, *)$ be a group. Let $H \subseteq G$ be a nonempty subset. Suppose $(H, *)$ forms a group, i.e. it satisfies the four group axioms. Then $(H, *)$ is called a subgroup of $(G, *)$. Note that the binary operation is the same for G and H.

Integer multiple

Suppose $(I, +)$ is a subgroup of $(\mathbb{Z}, +)$. Then $I = d\mathbb{Z}$ for some non-negative integer d.

Roots of unity

$(\mu_m, \times)$ is a subgroup of $(\mu_n, \times)$ if $m|n$.

Properties of subgroups

Proposition 30

Let $(G, *)$ be a group and let $H \subseteq G$ be a nonempty subset. Then $(H, *)$ is a subgroup iff:

- (S1) For all $a, b \in H$, we have $a * b \in H$.
- (S2) For all $a \in H$, we have $a^{-1} \in H$.

Proposition 31

Let $(G, *)$ be a group and let $H \subseteq G$ be a nonempty subset. Then $(H, *)$ is a subgroup iff:

- (S) For all $a, b \in H$, we have $a * b^{-1} \in H$.

Cyclic group

Let $(G, *)$ be a group and let $x \in G$. We call $H = \{x^n \in G : n\mathbb{Z}\}$ the cyclic subgroup of G generated by x, and we denote H by $\langle x \rangle$.

A group $(G, *)$ is called a cyclic group if $G = \langle x \rangle$ for some $x \in G$, i.e.

$$G = \langle x \rangle = \{x^n \in G : n \in \mathbb{Z}\}$$

Proposition 32

Let $(G, *)$ be a group and let $H \subseteq G$ be a nonempty finite subset. Then $(H, *)$ is a subgroup iff

- (S1) For all $a, b \in H$, we have $a * b \in H$.

Intersection of subgroups

If $\{(H_i, *) : i \in I\}$ is a collection of subgroups of $(G, *)$, then

$$\left(\bigcap_{i \in I} H_i, * \right)$$

is a non-empty subgroup of $(G, *)$.

Proposition 34

Let $(H, *)$ and $(K, *)$ be subgroups of $(G, *)$. If $(H \cup K, *)$ is a subgroup, then either $H \subseteq K$ or $K \subseteq H$.