MATH3121 Notes

SmokingPuddle58

December 23, 2023

The note is made by me during lecture time, with a software called GNU TeXmacs.

In this winter, I decided to remake it with LaTeX to improve readability. (Also to train my LaTeX skill)

If you found any error, please contact SmokingPuddle58. Many thanks.

🟧 Theorems, Corollary, Lemma, Proposition

🟦 Definitions

🟩 Examples

🟥 Warnings

Some special symbols, notations and functions that will appear in this note:

$\mathbb{C}$	Set of complex numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Set of rational numbers

$\mathbb{S}^*$	The set of $\mathbb{S}$ excluding 0 (Identity element for addition)
$\text{ord}(a)$	The order of the element a in a group
$\|A\|$	Cardinality of set A

0 Sets and Relations

To define a finite set, one may choose to list out every element in the set.
However, with infinite set, we may choose to characterize the set.
For example, we may write the set of all odd numbers as:

$$A = \{a \in \mathbb{R} | a = 2n + 1, n \in \mathbb{Z}\}$$

and some sets like:

$$B = \{a \in \mathbb{R} | \sin(a) + \cos(a) + 1 = 0\}$$

$$C = \{a \in \mathbb{R} | a^{10} + 100a^2 - 10a - 10000 = 0\}$$

Note that C has finitely many (≤ 10) elements (Result from root of unity)

Definition 0.1 (Subsets)
Given A, B are sets, if A is a part of B, then we call A to be a subset of B, writing in symbols, $A \subset B$.

For example, we have

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Definition 0.2 (Union, intersection)
If A, B are sets, then:

The union of A and B, denoted by $A \cup B$, are defined as $\{x | x \in A \text{ or } x \in B\}$.

The intersection of A and B, denoted by $A \cap B$, are defined as $\{x | x \in A \text{ and } x \in B\}$.

With union and intersection of sets, we have the following theorem:

Theorem 0.1 (Laws of operation of sets)
The following laws holds for any set A, B, C

1. Distributive law:

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$
$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

2. De Morgan's law:

$$(A \cap B)' = A' \cup B'$$
$$(A \cup B)' = A' \cap B'$$

Where $A' = U \backslash A$ is the compliment of A.

Proof.
We only prove 0.1.1 (Distributive law)
$\boxed{(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)}$
Pick arbitrary element x from the left hand side. Then we have

$$x \in (A \cup B) \text{ and } x \in C$$

If $x \in A, x \in C$, then we have $x \in A \cap C$ and thus $x \in (A \cap C) \cup (B \cap C)$
If $x \in B, x \in C$, then we have $x \in B \cap C$ and thus $x \in (A \cap C) \cup (B \cap C)$
$\boxed{(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C}$
Same as before, pick arbitrary element x from left hand side. We have

$$x \in (A \cap C) \text{ or } x \in (B \cap C)$$

If $x \in (A \cap C)$, then we have $x \in A$ and $x \in C$, and thus $x \in (A \cup B) \cap C$
If $x \in (B \cap C)$, then we have $x \in B$ and $x \in C$, and thus $x \in (A \cup B) \cap C$
As $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$ and $(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$ and hence

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

2. can be proved with similar methods as above.

Proof of 0.1.2 (De Morgan's law) is left as exercise.

Definition 0.3 (Cartesian product of sets)
If A, B are two sets, define Cartesian product $A \times B$ as

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

One of the common example we use would be

$$\mathbb{R}^n = \{(a, b, c, ..., n) | a, b, ..., n \in \mathbb{R}\}$$

Definition 0.4 (Map)
If A, B are sets, then a map $f : A \to B$ assigns each $a \in A$ to element $f(n) \in B$

For example, if $f(x) = x^2 - 1$, then f is a map, where $f : \mathbb{R} \to \mathbb{R}$.

Example 0.1
Let $A = 1, 2, 3, B = 4, 5$, how many maps from A to B are there?

There are two ways to choose $f(1)$, two ways to choose $f(2)$, and 2 ways to choose $f(3)$.
Therefore there are $2^3 = 8$ functions from A to B.

We extend the concept to other sets which contains different numbers of element. Say A has m element, while Y has n element, then we have the following proposition:

Proposition 0.1
Define two sets A and B with m and n elements respectively. The number of mapping from $A \to B$ is given by n^m.

Definition 0.5 (One-to-one, Onto)
For a map $f : A \to B$:

The map is one-to-one (injection), if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.
The map is onto (surjection), if for every element $b \in B$, there is $a \in A$ with $f(a) = b$.
The map is one-to-one correspondence (bijection), if f is both one-to-one and onto.

Example 0.2 (One-to-one)
$f : \mathbb{R} \to \mathbb{R}, f(x) = 3x - 1$ is one-to-one.
$h : \mathbb{R} \to \mathbb{R}, h(x) = 3x^2 - 1$ is NOT one-to-one.

Example 0.3 (Onto)
$f : \mathbb{R} \to \mathbb{R}, f(x) = 3x - 1$ is onto.
$h : \mathbb{R} \to \mathbb{R}, g(x) = e^x$ is NOT onto since negative numbers are not in image of g.

Example 0.4 (One-to-one correspondence)
$f : \mathbb{R} \to \mathbb{R}, f(x) = 3x - 1$ is bijection.
$h : \mathbb{R} \to \mathbb{R}, h(x) = 3x^2 - 1$ is NOT bijection because it is not onto.

Definition 0.6 (Cardinality of sets)
Given two sets A, B.

A, B have the same cardinality, if and only if there is a bijection $f : A \to B$.
If there is a injection $g : A \to B$, then A has a smaller cardinality than B. Also, $|A| \neq |B|$.
If there is a surjection $h : A \to B$, then A has a larger cardinality than B. Also, $|A| \neq |B|$.

Two finite sets A, B have the same cardinality if and only if they have same number of elements in the set.

Example 0.5
Let $A = 1, 2, 3, 4, 5, B = 4, 5, 6, 7$. Find the number of map such that the map is one-to-one.

Since $|A| > |B|$, it is impossible to find a one-to-one map.

However when we consider the following:

$$A = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \text{ and } B = \mathbb{R}$$

Note that set A and B have the same cardinality, although intuitively we may think set B is “larger” than set A in terms of cardinality.

Theorem 0.2
Any two intervals in $\mathbb{R}$ have the same cardinality.

Proof.
Let $I_1 = [s, t], I_2 = [u, v]$. Consider the map $f : \mathbb{R} \to \mathbb{R}$,

$$f(x) = \frac{v-u}{t-s}(x-s) + u$$

It is not hard to prove f is a bijection since:

$$f^{-1}(x) = \frac{t-s}{v-u}(y-u) + s$$

Example 0.6
Prove that $(-\frac{\pi}{2}, \frac{\pi}{2}) = |(-1, 1)$

Since $f : (-\frac{\pi}{2}, \frac{\pi}{2}) \to (-1, 1), f(x) = \frac{2}{\pi}x$ is bijective, thus both sets have equal cardinality.

Definition 0.7 (Partition)
Let A be a set. Partition is the decomposition of A:

$$A = A_1 \sqcup A_2 \sqcup A_3 \sqcup ... \sqcup A_n$$

such that none of $A_i, A_j \in A$ have intersection, i.e. $A_i \cap A_j = \emptyset$.

Example 0.7
If $f : A \to B$ is a surjective map, and $b \in B$, then $f^{-1}(b) = \{a \in A | f(a) = b\}$ forms a partition.

Definition 0.8 (Equivalence relation)
Let A be a set, a equivalence relation $\sim$ is defined if it satisfies the following properties:

1. $a \sim a$
2. $a \sim b \implies b \sim a$
3. $a \sim b$ and $b \sim c \implies a \sim c$

Definition 0.9 (Relation on partition)
If $A = A_1 \sqcup A_2 \ldots \sqcup A_n$ is a partition of A, then we define a relation $\sim$ on A as follow.

$$a \sim b, \text{ if and only if a and b are of the same part.}$$

Partition always satisfies the equivalence relation.

Example 0.8
Define an relationship $\sim$ if and only if $f(a_1, b_1) = f(a_2, b_2)$, where $f(a, b) = a^2 + b^2$.
The relation $\sim$ is equivalence relationship.

Theorem 0.3
Given an equivalence relation $\sim$ on A, for $a \in A$, define $\widetilde{a} = \{x \in A | x \sim a\}$. Then $\widetilde{a}$ is a subset of A. For any $a_1, a_2 \in A$, we have either $\widetilde{a_1} = \widetilde{a_2}$, or $\widetilde{a_1} \cap \widetilde{a_2} = \emptyset$

Definition 0.10 (Partial order)
Let A be a set. A relation $\leq$ on A is called partial order on A if for any $a, b, c \in A$,

1. $a \leq a$
2. $a \leq a$ and $b \leq a$ implies $a = b$
3. $a \leq b$ and $b \leq c$ implies $a \leq c$

If $A = \mathbb{R}$, then the relation is the inequality sign we commonly used.

1 Complex Numbers

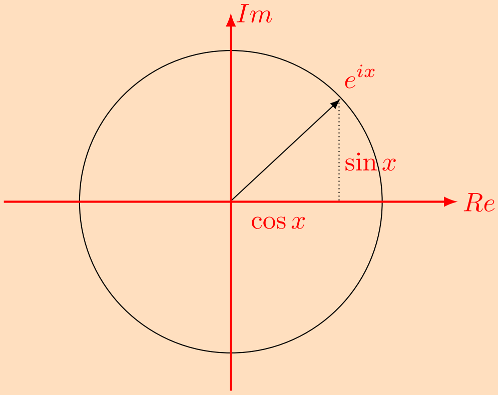
Definition 1.1 (Complex number $\mathbb{C}$)
Define $\mathbb{C}$ to be a set $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ with two operations $+, \cdot$, such that:

1. Addition: $(a + bi) + (c + di) = (a + c) + (b + d)i$
2. Multiplication:
   (a) $\cdot$ is distributive with respect to $+$
   (b) $i \cdot i = -1$

This is the definition that we commonly used in secondary school. However, we may also define complex number as the following:

Theorem 1.1 (Euler's Formula)
For any $x \in \mathbb{R}$, we have:

$$e^{ix} = \cos(x) + i\sin(x) = \text{cis}(x)$$



Theorem 1.2 (Polar form of complex number)
For any $a, b \in \mathbb{R}$, we have:

$$z = a + bi \iff z = re^{ix}$$

where $r = \sqrt{(a^2 + b^2)}, x = \tan^{-1}(\frac{b}{a})$.

Proof.

$$\begin{aligned} z &= re^{i\theta} \\ &= r(\cos\theta + i\sin\theta) \\ &= r\cos\theta + ir\sin\theta \end{aligned}$$

Theorem 1.3 (*Roots of unity)
The solution for $z^n = 1, z \in \mathbb{C}$ is given by $U_n = \{e^{\frac{2\pi i}{n}k}, k = 1, 2, ..., n-1\}$.

Proof.

$$\begin{aligned}
\left(e^{\frac{2\pi i}{n}k}\right)^n &= e^{2\pi k i} \\
&= \cos(2\pi k) + i\sin(2\pi k) \\
&= \cos 0 + i \sin 0 \\
&= 1
\end{aligned}$$

Theorem 1.4 (Fundamental Theorem of Algebra)
Every non-constant polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$.

4 Groups

Before we define groups, it is necessarily for us to define binary operation.

Definition 4.1 (Binary operation)
A binary operation $*$ on a set S is a map, where $* : S \times S \to S$ and $* : (a, b) \mapsto a * b$

For example, the addition operation $+$ is a binary operation, where

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$$

Proposition 4.1
If $|S| = n$, then there are $n^{(n^2)}$ binary operations on S.

We define a group as the following:

Definition 4.2 (Group)
A group is a set G with a binary operation $*$ on G such that the following axioms are satisfied:

1. There is $e \in G$, s.t. $\forall a \in G, e * a = a * e * a$ (Existance of identity element)
2. For every $a \in G, \exists a' \in G$, s.t. $a' * a = a * a' = e$ (Existance of inverse element)
3. For any $a, b, c \in G, (a * b) * c = a * (b * c)$ (Associativity)

Example 4.1
Prove that $(\mathbb{R}, +)$ is a group.

1. There is $0 \in \mathbb{R}, 0 + a = a + 0 = a, \forall a \in \mathbb{R}$
2. There is $-a \in \mathbb{R}, -a + a = a + (-a) = 0, \forall a \in \mathbb{R}$
3. Addition is associative in $\mathbb{R}$

Therefore $(\mathbb{R}, +)$ is a group by definition.

Note that $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ are groups under the binary operation $+$.

However, $\mathbb{N}$ is not a group under $+$ since there is no $a' \in \mathbb{N}$, s.t. $a + a' = 0$.

Example 4.2
Is $\mathbb{R}$ a group under $\cdot$?

Since for $0 \in \mathbb{R}$, there is no $0'$, s.t. $0' \cdot 0 = 1$, therefore $\mathbb{R}$ is not a group under $\cdot$.

To solve the issue, from now on, we define $\mathbb{R}^*$, where 0 is being removed from $\mathbb{R}$. i.e.

$$\mathbb{R}^* = \mathbb{R} - 0$$

We will apply this notation for other sets also, such as $\mathbb{Z}, \mathbb{C}, \mathbb{Q}, \ldots$

Example 4.3
Is $\mathbb{C}^*$ a group under multiplication?

We start to check the three axioms:

1. There is $1 \in \mathbb{C}^*$, s.t. $a \cdot 1 = 1 \cdot a = a$
2. The inverse element exists, since:
$$\frac{1}{a+bi} = \frac{1}{a+bi}\left(\frac{a-bi}{a+bi}\right) = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$
and $(a+bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) = 1$
3. The operation is associative for sure.

Hence $\mathbb{C}^*$ a group under multiplication by definition.

Definition 4.3 (Abelian groups)
If $(G, *)$ is a group, and if $*$ is commutative $(a * b = b * a), \forall a, b \in G$, then G is called abelian group.

Example 4.4
Let $M_n(\mathbb{R})$ be a set of $n \times n$ matrice, with all real number entries.

If $n \geq 2$, then the multiplication is not commutative and therefore not abelian.

However, is $M_n(\mathbb{R})$ a group under matrix multiplication?

Let $A \in M_n(\mathbb{R})$. Note that there is matrix with $|A| = 0$, for such matrix, There is no A', s.t. $AA' = A'A = I$

Thus $M_n(\mathbb{R})$ is not a group under matrix multiplication.

Similarly, we can create a new set, where $|A| \neq 0, \forall A \in M_n(\mathbb{R})$. Such set is called $\mathrm{GL}(n, \mathbb{R})$.

Example 4.6
Is $\mathrm{GL}(n, \mathbb{R})$ a group under matrix multiplication?

We first prove that the operation is binary. We need to prove that $A \times B \in \mathrm{GL}(n, \mathbb{R})$

Note that $|A \cdot B| = |A||B| \neq 0$. Thus the operation is closed.

We now prove that $\mathrm{GL}(n, \mathbb{R})$ is a group under matrix multiplication.

1. There is I_n, such that $I_n A = A I_n = A$

2. As $|A| \neq 0, \forall A \in \mathrm{GL}(n, \mathbb{R})$, thus there is A^{-1}, s.t. $AA^{-1} = A^{-1}A = I$

3. It is obvious that the multiplication of matrix is associative.

Thus $\mathrm{GL}(n, \mathbb{R})$ is a group under matrix multiplication.

Note that when $n \geq 2$, the group is not Abelian.

Definition 4.4 (Finite groups)
For a group $(G, *)$,

- The group is called finite group, if G is a finite set.
- The group is called infinite group, if G is a infinite set.

Example 4.7
Let $U_n = \{z \in \mathbb{C} | z^n = 1\}$. Consider the multiplication operation in U_n.

We first prove the set is closed under multiplication.

Pick any 2 arbitrary element from U_n, z_1 and z_2.

Note that $(z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1 \cdot 1 = 1 \in U_n$ (As $1^n = 1, \forall n \in \mathbb{N}$), hence $z_1 \cdot z_2 \in U_n$. U_n is closed under $\cdot$. $\cdot$ is a binary operator.

Now we prove that $(U_n, \cdot)$ is a group.

- There is an identity element $1 \in U_n$, such that $z^n \cdot 1 = 1 \cdot z^n = z^n$
- If $z \in U_n$, then $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = \frac{1}{1} = 1 \in U_n$, thus $\forall z \in U_n, \exists \frac{1}{z^n}$, s.t. $z^n \left(\frac{1}{z^n}\right) = 1$
- Complex number are associative under multiplication.

Thus $(U_n, \cdot)$ is a group.

Note that we may express $U_n = \left\{ e^{\frac{2\pi i}{n} k} | k = 0, 1, \ldots, n-1 \right\}$, hence $|U_n| = n$

At the first glance, we observe that

$$\begin{aligned} z_1 \cdot z_2 &= e^{\frac{2\pi i}{n} k_1} \cdot e^{\frac{2\pi i}{n} k_2} \\ &= e^{\frac{2\pi i}{n} (k_1 + k_2)} \end{aligned}$$

It is possible that $k_1 + k_2 > n - 1$, however, under modulo operation,

$$\exists k, 0 \leq n - 1, k \equiv (k_1 + k_2) \bmod n$$

Now consider a mod 3 modulo group. We can partition $\mathbb{Z}$ into 3 groups, namely

$$\mathbb{Z} = 3\mathbb{Z} \sqcup 3\mathbb{Z} + 1 \sqcup 3\mathbb{Z} + 2$$

Where

$$\begin{aligned} 3\mathbb{Z} &= \{3n | n \in \mathbb{Z}\} \\ 3\mathbb{Z} + 1 &= \{3n + 1 | n \in \mathbb{Z}\} \\ 3\mathbb{Z} + 2 &= \{3n + 2 | n \in \mathbb{Z}\} \end{aligned}$$

If we let the operation $+$ to be the same as $+$ in $\mathbb{Z}$, we can make a modular 3 addition table as:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Partition $\mathbb{Z}$ as

$$\mathbb{Z} = n\mathbb{Z} \sqcup (n\mathbb{Z}+1) \sqcup \cdots \sqcup (n\mathbb{Z}+n-1)$$

for any integers, we have $n\mathbb{Z}+k = \{mn+k | m \in \mathbb{Z}\}$. We have the following proposition:

Proposition 4.2
$\mathbb{Z}_n$ is a finite, abelian group under modulo n addition, and $|\mathbb{Z}_n| = n$

The following theorem is very important throughtout the entire course!

Theorem 4.1 (Left and right cancellation law)
If $(G, *)$ is a group, then the left cancellation and right cancellation law holds in group.

- Left cancellation law: $a * b = a * c \implies b = c$
- Right cancellation law: $a * b = c * b \implies a = c$

Proof.
Only left cancellation law is proved since right cancellation law can be proved similarly.

$$\begin{aligned} a * b &= a * c \\ a^{-1}(a * b) &= a^{-1}(a * c) \\ (a^{-1}a) * b &= (a^{-1}a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

Warning 4.1
Note that $a * c = b * a \not\Longrightarrow c = b$

Proof.
Pick two element from $\mathrm{GL}(\mathbb{Z}, 2)$, where $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$.

(Remark: Lower triangle matrix and Upper triangle matrix do not commute)

Define $C = ABA^{-1} \implies CA = AB$ (By multiplying A on both side)

Find the inverse of A: (Trick)

$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, thus inverse $A^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

As a result, we have $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$

Thus $CA = AB$ does not implies that $C = B$, thus $a * c = b * a \not\Longrightarrow c = b$.

Corollary 4.1.1 (Uniqueness of identity and inverse element)
If $(G, *)$ is a group, then for any $a \in G$, the inverse element a' s.t. $aa' = e$ is **unique**.
The identity element e for each group is also unique.

Proof.
Assume that there are two inverse element a' and a'' in G, for $a \in G$. We then have:

$$\begin{cases} a * a' = e \\ a * a'' = e \end{cases}$$

By left cancellation law, $a' = a''$

Similarly, assume there are two identity element e' and e'' in G. We then have:

$$\begin{cases} e' * e'' = e' \\ e' * e'' = e'' \end{cases}$$

By left cancellation law, $e' = e''$

Example 4.8 (2023 Homework 1, Problem 3, Modified)
If $(G, *)$ is a group, $a, b, c \in G$, prove that $abc = e$ implies that $bca = e$.

Proof. (1)
Since $a, b, c \in G$, by associative property of groups, we have:

$$abc = a(bc) = e$$

By the property of inverse element of groups, we also have:

$$a(bc) = (bc)a = e$$

Therefore, if $abc = e$, then $abc = (bc)a = bca = e$.

Proof. (2)
Consider the element $g = a^{-1}abca$. For the associativity, we have $g = a^{-1}(abc)a = a^{-1}ea$.

On the other hand, we have $g = (a^{-1}a)bca = bca$.

Above all, we proved that $bca = e$.

5 Subgroups

Before we define subgroup, we shall define the “closeness” of operation.

Definition 5.1 (Closeness of operation)
Let T be a set, $*$ be a binary operation on T. If $S \subset T$ is a subset, then S is closed under $*$ if

$$\forall a, b \in S, a * b \in S$$

If S is closed under $*$ on T, we can view $*$ as binary operation on S. We call such binary operation the induced operation from $*$ on T.

Under such defintion, if we let $T = \mathbb{R}$, then $\mathbb{Z}, \mathbb{Q}, \mathbb{R}_{>0}, \mathbb{R}_{<0}$ are closed under $+$.

However, $2\mathbb{Z} + 1$ is not closed since, $1, 3 \in 2\mathbb{Z} + 1$, but $1 + 3 = 4 \notin 2\mathbb{Z} + 1$.

Definition 5.2 (Subgroup)
If T is a set, $*$ is a binary operation on T.
A subset S in T is closed under $*$ if for any $a, b \in S$,

Example 5.1
$\mathbb{Z}, \mathbb{Q}$ are subgroup of $(\mathbb{R}, +)$.

Example 5.2
Let $S = \{n | n \notin \mathbb{Q}$ and $n \in \mathbb{R}\}$ to be the set of real irrational numbers, then S is not closed under the addition. One counterexample will be $\pi + (-\pi) = 0 \notin S$.

Example 5.3
$\mathbb{R}_{>0}$ is not a subgroup of $(\mathbb{R}, +)$. It is because it does not satisfy the group definition, as the identity element and inverse element does not exist.

Example 5.4
Let $(\mathbb{C}^*, \cdot)$ be a group. Determine whether the following are subgroups.

1. $U_2 = \{1, -1\}$	2. $\{1, 2, 2^2, 2^3, \ldots\}$	3. $\left\{1, 2, \frac{1}{2}, 2^2, \ldots\right\}$	4.$\mathbb{R}_{>0}$

Only 2 is not a subgroup, since inverse element does not exist for most of the elements.
(e.g. $2^{-1} = \frac{1}{2} \notin \{1, 2, 2^2, 2^3, ...\}$)

Example 5.5
Let $(\mathbb{C}^*, \cdot)$ be a group. Is $U = \{z \in \mathbb{C}^* : |z| = 1\}$ a subgroup? where $|z| = \sqrt{a^2 + b^2}$.

We first check whether the operation is closed or not.

Note that $\forall z, w \in \mathbb{C}, |zw| = |z||w|$. If $z, w \in U$, $|zw| = |z||w| = 1 \times 1 = 1$ and obviously, $1 \in U$.

Thus we know that U is closed under $\cdot$.

Then we check whether the inverse element exists.

$$\begin{aligned} |z \cdot z'| &= |1| \\ |z||z'| &= 1 \\ |z'| &= 1 \in U \end{aligned}$$

Thus the inverse element exist.

Finally, the multiplication of $\mathbb{C}^*$ is associative.

Thus $U = \{z \in \mathbb{C}^* : |z| = 1\}$ is a subgroup.

Example 5.6
Let $\mathrm{GL}(3,\mathbb{R})$ be a group of 3×3 real matrix under $\cdot$, where $|M|\neq 0, \forall M\in \mathrm{GL}(3,\mathbb{R})$.

Are the following sets a subgroup under matrix multiplication?

1. $A =$All 3×3 diagonal real matrix, with positive integer entry.

2. $B =$All 3×3 diagonal real matrix, with $|M| = 1$

3. $C =$All 3×3 upper triangular real matrix, $|M|\neq 0$, non-negative entry

Before we do the question, it will be good to know some of properties.
1. Matrix multiplication of diagonal matrix

$$\begin{bmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{bmatrix} \times \begin{bmatrix} b_1 & & \\ & b_2 & \\ & & b_3 \end{bmatrix} = \begin{bmatrix} a_1b_1 & & \\ & a_2b_2 & \\ & & a_3b_3 \end{bmatrix}$$

2. Inverse of diagonal matrix

$$\begin{bmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{bmatrix}^{-1} = \begin{bmatrix} a_1^{-1} & & \\ & a_2^{-1} & \\ & & a_3^{-1} \end{bmatrix}$$

Given the above properties, it will be easy for us to solve the question.

1. The operation is closed. However, most of the inverse does not exist. For example:

$$\begin{bmatrix} 2 & & \\ & 3 & \\ & & 5 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{2} & & \\ & \frac{1}{3} & \\ & & \frac{1}{5} \end{bmatrix} \notin A$$

2. Yes, note that the group is also abelian.

3. The operation is closed. However, most of the inverse does not exist. For example:

$$\begin{bmatrix} 1 & 2 & \\ & 1 & \\ & & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -2 & \\ & 1 & \\ & & 1 \end{bmatrix} \notin C$$

Let G be a group under $*$. Then we will be using the following set of notation throughtout the course:

$$\begin{aligned} a*b &= ab \\ \underbrace{a*a*...*a}_{n} &= a^n \\ a' &= a^{-1} \\ \underbrace{a'*a'*...*a'}_{n} &= a^{-n} \\ a^0 &= e \end{aligned}$$

Theorem 5.1 (*Subgroup)
A subset H of group G is a subgroup if and only if

1. H is closed under binary operation of G
2. The identity element in $G : e \in H$
3. For any $a \in H$, $a^{-1} \in H$

Proof.
$(\implies)$

If H is a subgroup, by the definition of subgroup, H is closed under binary operation of G.

H is a group under reduced operation, thus there is e', which is the identity element of H.

We now prove that $e' = e$, where e is the identity element of G.

$$\begin{cases} e'e' = e' \\ e'e = e' \end{cases} \implies e'e' = e'e \implies e' = e$$

by the left cancellation law.

Finally it is obvious that the associativity holds.

$(\impliedby)$

If the three rules holds, then we have:

- H is closed
- Identity element e exists in H
- For every $a \in H, \exists a^{-1} \in H$
- Associativity holds

6 Cyclic Groups

Proposition 6.1
Let G be a group and let $a \in G$. The set $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Moreover, $\langle a \rangle$ is the smallest subgroup. i.e. if H is a subgroup, $a \in H$, then $\langle a \rangle \subset H$.

Proof.
Since that $a^m a^n = a^{m+n} \in H$, the operation is therefore closed.

The identity element e exists in $\langle a \rangle$ because if we pick $n = 0$, then $a^0 = e$.

The inverse element $a' = a^{-n}$ also exists in $\langle a \rangle$.

Thus $\langle a \rangle$ is the smallest subgroup.

Warning 6.1
Be reminded that a^n implies n copies of **binary operation, not power**.

Example 6.1
For the group $(\mathbb{C}^*, *)$, we have

$$\begin{aligned} \langle 2 \rangle &= \{2^n : n \in \mathbb{Z}\} = \left\{1, 2, \frac{1}{2}, 4, \frac{1}{4}, \dots\right\} \\ \langle -1 \rangle &= \{(-1)^n\} = \{-1, 1\} \\ \langle i \rangle &= \{(i)^n\} = \{i, 1, -i, -1\} \end{aligned}$$

Note that $\langle n \rangle$ is infinite for any $n \in \mathbb{Z}$ except 0 since $\langle 0 \rangle = \{0\}$.

Definition 6.1 (Cyclic group)
A group G is called a cyclic group if there is a special element $a \in G$, s.t. $\langle a \rangle = G$.

We call a as the generator of G.

Example 6.2
$(\mathbb{Z}, +)$ is a cyclic group since $1, -1$ can generate $\mathbb{Z}$.

Example 6.3
$(\mathbb{Z}_n, +)$ is a cyclic group since 1 can generate $\mathbb{Z}_n$.

Example 6.4

$(U_n, \cdot) = \left\{e^{\frac{2\pi i}{n}k} : k = 0, 1, 2, \dots,\right\}$ is a cyclic group as $e^{\frac{2\pi i}{n}}$ can generate U_n.

Example 6.5
$(\mathbb{Q}^*, +)$ is not cyclic.

Proof.
Suppose the group is cyclic, then there is $a \in \mathbb{Q}$, s.t. $\langle a \rangle = \{na : n \in \mathbb{Z}\} = \mathbb{Q}$.

Since a is rational, therefore $a = \dfrac{p}{q}, (p, q) \in \mathbb{Z} \times \{\mathbb{Z} \backslash \{0, 1\}\}$.

Then we may write $\dfrac{1}{q^2} = na = n\dfrac{p}{q} \Rightarrow \dfrac{1}{q} = np \in \mathbb{Z}$, but $\dfrac{1}{q} \notin \mathbb{Z}$, contradiction!

Example 6.6
$(\mathbb{Q}^*, *)$ is not cyclic.

Proof.
If $\langle a \rangle = \mathbb{Q}^*$, then $a = \dfrac{p}{q} = p_1^{k_1} \ldots . p_n^{k_n}$ or $- p_1^{k_1} \ldots . p_n^{k_n}$, where $p_1, \ldots, p_n$ are distinct primes.

For example, we can express $\dfrac{10}{77} = 2 \times 5 \times 7^{-1} \times 11^{-1}$.

Let $p \notin \{p_1, \ldots, p_n\}$,then $p \notin \langle a \rangle$, however $p \in \mathbb{Z} \in \mathbb{Q}^*$, contradiction!

Example 6.7
$(\mathbb{R}, +)$ is not cyclic.

Proof.
For any $a \neq 0$, $\dfrac{1}{2}a \notin \langle a \rangle$, contradiction!

Example 6.8

Let $S = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z}_{\geqslant 1} \right\}$. Then $G = (S, \times)$ is cyclic.

Proof.

Let $a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Observe that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

Theorem 6.1
Any cyclic group G is abelian.

Proof.
If G is cyclic, then $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Pick any element $x, y \in G$, where $x = a^m, y = a^n$. We have:

$$\begin{aligned} xy &= a^m a^n \\ &= a^{m+n} \\ &= a^n a^m \\ &= yx \end{aligned}$$

Theorem 6.2
If $\langle a \rangle$ is infinite, then for any $n \in \mathbb{N}, a^n \neq e$.

Proof.
Assume that $a^n = e$ for some n, and assume that n is the smallest such exponential.
Then $\{e, a, a^2, ..., a^n\}$ already forms a subgroup. This contradicts the fact that $\langle a \rangle$ is infinite.

Definition 6.2 (Order)
If $a^n \neq e$ for any $n \in \mathbb{N}$, we call a has infinite order, or has order ∞.
If $a^n = e$ for some positive integer n, then the smallest positive integer n is called the order of a.

Example 6.9
Let $G = (\mathbb{R}, +)$. Then any $a \in \mathbb{R} - 0$ has order ∞.

Proof.
If $a = 0$, then then $a^n = \underbrace{a + a + a + \cdots + a}_{n} = na \neq 0$.

If $a = 0$, then a is already the identity element and the order is thus 1.

In fact, for any group G, if $e \in G$ is the identity element, we always have $\text{ord}(e) = 1$.

Example 6.10
Let $G = C^*$, then:

$$\begin{aligned} \text{ord}(2) &= \infty \\ \text{ord}(-1) &= 2 \\ \text{ord}(i) &= 4 \\ \text{ord}(1) &= 1 \end{aligned}$$

Example 6.11
Let $G = (\mathbb{Z}_12, +)$. We have:

$$\begin{aligned} \langle 3\rangle = \{3, 6, 9, 12 \to 0\} \implies \text{ord}(3) &= 4 \\ \langle 5\rangle = \{5, ..., 60 \to 0\} \implies \text{ord}(5) &= 12 \\ \langle 8\rangle = \{3, 6, 9, 12 \to 0\} \implies \text{ord}(3) &= 4 \end{aligned}$$

To help us to prove further results about groups, we shall introduce the division algorithm for $\mathbb{Z}$.

Intuitively, consider $n \div m, n \in \mathbb{Z}, m \in \mathbb{Z}_{>0}$, we always get quotient and remainder $0 \leqslant r < m$. We then have the following theorem:

Theorem 6.3 (Division algorithm for $\mathbb{Z}$)
If $m \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}$, then there exist unique integers q, r, s.t.

$$n = mq + r \text{ and } 0 \leq r < m$$

With the above theorem, we can prove the following theorem:

Theorem 6.4
If G is a cyclic subgroup, then every subgroup of G is also cyclic.

Proof.
Let $G = \langle a\rangle$. Let $H \subset G$ be a nonempty subgroup.

If $H = \{e\}$, then $\langle e\rangle = \{e\}$, which proves that H is cyclic.

If $H \neq \{e\}$, then there is $b \in H$, such that $\begin{cases} b &= a^k \\ b^{-1} &= a^{-k} \end{cases}, b, b^{-1} \in H$.

As one of the $k, -k$ must be greater than 0, therefore there exist $n \in \mathbb{Z}_{>0}$, s.t. $a^n \in H$.

Let $S = \{n \in \mathbb{Z}_{>0} : a^n \in H\}$, then S is not empty.

Let m be the smallest element in S. We claim $H = \langle a^{nm}\rangle$.

As $a^m \in H$, $\langle a^m\rangle \subset H$.

For $b \in H$, since $b \in G = \langle a\rangle$, therefore $b = a^n$ for some $n \in \mathbb{Z}$.

Consider $n \div m$. By division algorithm

$$\begin{aligned} n &= mq + r \\ r &= n - mq \end{aligned}$$

$$a^r = a^{n-mq} = a^n a^{-mq} = a^n (a^m)^{-q} \in H$$

Note that $a^r \in H$, and m was the smallest positive integer s.t. $a^m \in H$, hence $r = 0$.

Thus $b = a^n = (a^m)^q \in \langle a^n\rangle$, $H \subset \langle a^m\rangle$, thus $H = \langle a^m\rangle$

Corollary 6.4.1
Every subgroup of $\mathbb{Z}$ is $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Proof.
As $\mathbb{Z}$ is cyclic, thus $H = \langle n \rangle = n\mathbb{Z}$.

For $s, r \in \mathbb{Z}$ and $s, r \neq 0$, define $H = \{ms + nr : m, n \in \mathbb{Z}\}$.

Then H is closed. ($\because (m_1 s + n_1 r) + (m_2 s + n_2 r) = (m_1 + m_2)s + (n_1 + n_2)r \in H$)

Note that the identity element 0 also exists as $0s + 0r = 0 \in H$.

If $(ms + nr) \in H, \text{ then } -(ms + nr) \in H$. Now H is a subgroup of $\mathbb{Z}$, thus $H = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.

Consider the properties of d:

- d is a positive integer.
- $s \in H \subset d\mathbb{Z}$ implies d is a divisor of s and d is a divisor of r. Hence d is a common divisor of s and r.
- Let d' to be another common divisor of s and r. d' is also a divisor of every elements in H. In particular, d' is a divisor of d.

From above property, we conclude $d = \gcd(r, s) = ms + nr$ for some $n, m \in \mathbb{Z}$.

Theorem 6.5 (*Conditions for relatively prime)
Two integers r, s are relatively prime, i.e. $\gcd(r, s) = 1$, if and only if there exists integer m, n, such that:

$$mr + ns = 1$$

Theorem 6.6 (Estimation of growth of $\boldsymbol{\Pi(n)}$ (Not in syllabus))
Let $\Pi(n)$ to be the number of prime numbers, which are less or equal to n.

We have

$$\lim_{n \to \infty} \frac{\Pi(n)}{\frac{n}{\ln n}} = 1$$

i.e. $\Pi(n) \sim \dfrac{n}{\ln n}$.

Theorem 6.7
If H_1, H_2 are subgroups of G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof.
Since every subgroup has an identity element e, thus $e \in H_1 \cap H_2$.
For any element g, h in G, we have:

$$\begin{aligned} g, h \in H_1 \cap H_2 &\implies g, h \in H_1 \text{ and } g, h \in H_2 \\ &\implies gh^{-1} \in H_1 \text{ and } gh^{-1} \in H_2 \\ &\implies gh^{-1} \in H_1 \cap H_2 \end{aligned}$$

Corollary 6.7.1
Let m, n be non-zero integers. Then $m\mathbb{Z} \cap n\mathbb{Z} = N\mathbb{Z}$ for some positive integer N.

Moreover, N is a common multiple of m, n.

Theorem 6.8
The order of a is the number of elements in $\langle a \rangle$.

Proof.
If order of a is finite, then there exists $n \in \mathbb{Z}_{>0}$, $a^n = e, a^j \neq e$, $1 \leq j < n$.

Then $\langle a \rangle = \{e, a, a^2, a^3, \ldots, a^{n-1}, a^n = e, \ldots, \}$

Therefore $\langle a \rangle$ has n elements.

Suppose there are non-distinct elements in the set, then $a^j = a^i \implies e = a^{j-i}$ which leads to contradiction as we have for any $j < n, a^j \neq e$.

If the order of a is infinite, then
$$\langle a \rangle = \{e, a, a^2, \ldots\}$$
Suppose that there are non-distinct elements in the set, then $a^j = a^i \Rightarrow e = a^{j-i}$ which leads to contradiction as we have for any $j < n, a^j \neq e$.

Example 6.12
Consider a group $\mathrm{GL}(2, \mathbb{R})$, compute the order of the following element.

$$a = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, c = \begin{bmatrix} \cos\left(\frac{\pi}{101}\right) & -\sin\left(\frac{\pi}{101}\right) \\ \sin\left(\frac{\pi}{101}\right) & \cos\left(\frac{\pi}{101}\right) \end{bmatrix}$$

Note that $a^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, we deduce that $(a^2)^2 = a^4 = I$, but still we need to check a^3. $a^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. The order of a is 4.

For b, note that $b^2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}, b^3 = \begin{bmatrix} 1 & 0 \\ 6 & 1 \end{bmatrix}$, by observation, we have $b^n = \begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix} \neq I$. The order of b is therefore ∞.

For c, since for any rotational matrix, we have
$$A_\theta^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$
As a result, we have
$$c^{202} = I$$
Thus the order of c is 202.

Example 6.13
Let G be a group. $a \in G$ has order n. Suppose $a^m = e, m \in \mathbb{Z}$, prove that $m = nk, k \in \mathbb{Z}$.

Proof.
We write $m = nq + r$ for some $0 \leq r < n$, then $r = m - nq$. Therefore,

$$\begin{aligned} a^r &= a^{m-nq} \\ &= a^m a^{-nq} \\ &= a^m (a^n)^{-q} \\ &= ee^{-q} \\ &= e \end{aligned}$$

Therefore r must be equals to 0. Thus $m = nq$.

Example 6.14
Let G be a group, $a, b \in G$. Prove that ab and ba have the same order.

Proof.
Suppose n is a natural number. $(ab)^n = e$ implies $\underbrace{(ab)(ab)...(ab)}_{n} = e$.

$$\begin{aligned} (ab)(ab)...(ab) &= e \\ b(ab)(ab)...(ab) &= be \\ (ba)(ba)...(ba)b &= eb \\ (ba)(ba)...(ba) &= e \end{aligned}$$

Similarly, we can prove $(ba)^n = e$ implies $(ab)^n = e$.

Example 6.15
Suppose G is finite. $a \in G$, prove that $\exists n \in \mathbb{Z}_{>0}$, $a^n = e$.

Proof.
Assume that $|G| = N$, then $\{a, a^2, a^3, \dots, a^N, a^{N+1}\}$ have $N + 1$ element . Then there exists 2 element which are not unique from the piegonhole principle. Let a^i and a^j be such element, where $i < j$. Then by cancellation law we have $a^{j-i} = e$.

Now we state a lemma which will be useful for the proofs after (And also in exams and homework).

Lemma 6.9
Suppose G is finite group, $|G| = n$, $G = \{a_1, a_2, \dots, a_n\}$. For $a \in G$, $\{aa_1, aa_2, \dots, aa_n\}$ is a distinct list.

Proof.
Assume that two terms in the list are equal. By cancellation law:

$$aa_i = aa_j \implies a_i = a_j$$

Then $\{aa_1, aa_2, \dots, aa_n\}$ is simply a permutation of G.

Example 6.16
If G is abelian, $|G| = n$, prove that for any $a \in G$, we have $a^n = e$.

Proof.
We list out the element $G = \{a_1, ..., a_n\}$. Then $aa_1, aa_2, ..., aa_n$ is a permutation of the list. As G is abelian, therefore:

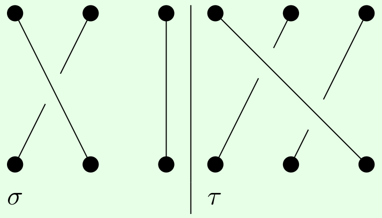
$$\begin{aligned} a_1, ..., a_n &= aa_{,}aa_2, ..., aa_n \\ a^n a_1, ..., a^n a_n &= a_1, ..., a_n \\ a^n &= e \end{aligned}$$

Example 6.17
Let $G = e, a, b$ be a group. We can write a table on binary operation:

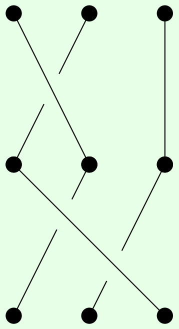
$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Note that the table is of permutation, and only hold for 2 and 3 element group.

Example 6.18 (Braid Groups)
Let B_3 be a braid group with 3 strings. Define σ and τ to be the following.

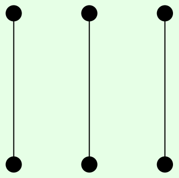


One may define the multiplication, $\sigma * \tau$, by joining the graph together with σ's bottom and τ's top. For example, $\sigma * \tau$ will be:



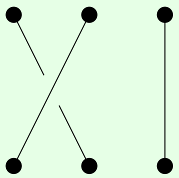
$\sigma * \tau$

The identity element e is defined as:



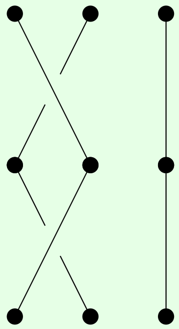
e

The inverse of σ is given by:



σ^{-1}

To see the reason, consider $\sigma * \sigma^{-1}$:



$\sigma * \sigma^{-1}$

and then when you try to move the two strings, they will become the identity element.

In fact every braid can be represented with 4 types of elements only, and each element has inverse, thus in general every braid has inverse under such "Multiplication".

8 Groups of Permutations

Definition 8.1 (Permutation)
Let A be a nonempty set. A map $\phi : A \to A$ is called a permutation of A, if it is one to one and onto.