# MATH3121 Notes

SmokingPuddle58

December 25, 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

Proofs, Answers

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 |
| $\lvert A\rvert$ | Cardinality of set $A$ |

# Contents

# 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 ($\leq 10$) 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

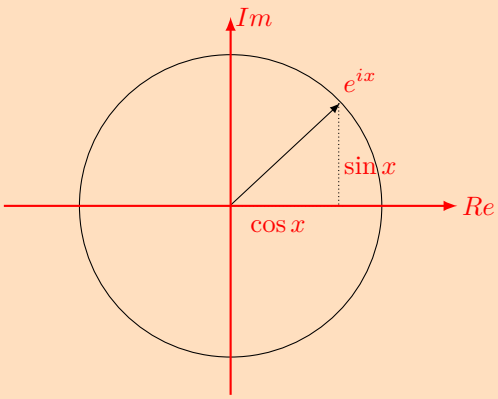
**Definition 1.1 (Complex number $\mathbb{C}$)**
Define $\mathbb{C}$ to be a set $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ with two operations $+, \cdot$, such that:

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.

Since:

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 $\mathbb{Z}, \mathbb{C}, \mathbb{Q}, ...$

**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 4.5**
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 $a * c = b * a \not\implies c = b$

**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 $a * c = b * a \not\implies c = b$.

**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)**
Let $(G, *)$ be a group, a nonempty subset $(H, *)$ is called subgroup of $G$, if:

- H is closed under $*$
- $H$ is a group under $*$

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

**Example 5.2**
Let $S = \{n | n \notin \mathbb{Q} \text{ and } n \in \mathbb{R}\}$ 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 $3\times 3$ 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 $3\times 3$ diagonal real matrix, with positive integer entry.
2. $B$ =All $3\times 3$ diagonal real matrix, with $|M|=1$
3. $C$ =All $3\times 3$ 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:

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

**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 $a = \frac{p}{q}, (p, q) \in \mathbb{Z} \times \{\mathbb{Z} \backslash \{0, 1\}\}$.

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

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

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

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

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 $a \neq 0$, $\frac{1}{2}a \notin \langle a \rangle$, 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 $\infty$.

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 $\infty$.

**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 $G = (\mathbb{Z}_1 2, +)$. 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 $(ms + nr) \in H$, 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 $\Pi(n)$ (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 $\infty$.

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 $\{a, a^2, a^3, \ldots, a^N, a^{N+1}\}$ 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, $|G| = n$, $G = \{a_1, a_2, \ldots, a_n\}$. For $a \in G$, $\{aa_1, aa_2, \ldots, aa_n\}$ 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 $\{aa_1, aa_2, \ldots, aa_n\}$ 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:

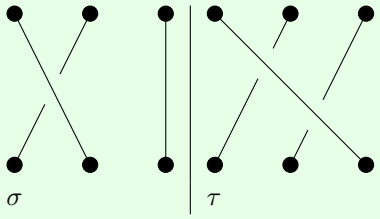
$$\begin{aligned} a_1, ..., a_n &= aa_1, aa_2, ..., aa_n \\ a^n a_1, ..., a^n a_n &= a_1, ..., a_n \\ a^n &= e \end{aligned}$$

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

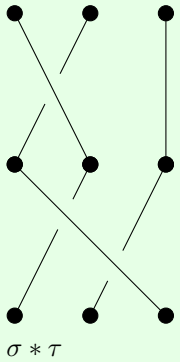
| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

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

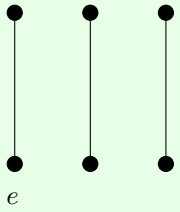
**Example 6.18 (Braid Groups)**
Let $B_3$ be a braid group with 3 strings. Define $\sigma$ and $\tau$ to be the following.



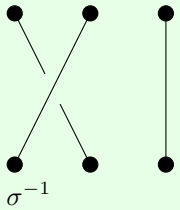

One may define the multiplication, $\sigma * \tau$, by joining the graph together with $\sigma$'s bottom and $\tau$'s top. For example, $\sigma * \tau$ will be:




The identity element $e$ is defined as:

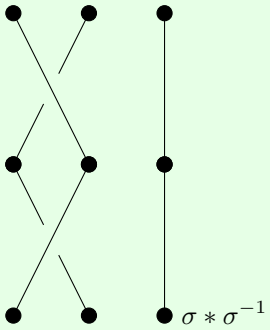


The inverse of $\sigma$ is given by:



$\sigma^{-1}$

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.

**Example 8.1**
Let $f : \mathbb{R} \to \mathbb{R}$. Then $f \mapsto 3x + 1$ is a permutation.

**Example 8.2**
Let $g : \mathbb{R} \to \mathbb{R}$. Then $f \mapsto e^x$ is **not** a permutation since it is not onto.

**Example 8.3**
Let $\iota : A \to A$. Then $\iota(a) = a$ is a permutation.

**Example 8.4**
Let $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$. The map:

$$\begin{cases} \sigma(1) = 2 \\ \sigma(2) = 3 \\ \sigma(3) = 1 \end{cases}$$

is a permutation.

**Theorem 8.1**
If $\sigma : A \to A$ and $\tau : A \to A$ is a permutation, then $\sigma \circ \tau$ is also a permutation.

**Lemma 8.2**
Let $\sigma, \tau, \phi$ be three maps: $A \to A$. Then $(\sigma \circ \tau) \circ \phi = \sigma \circ (\tau \circ \phi)$

**Proof.**
Pick any $a \in A$, then $(\sigma \circ \tau) \circ \phi(a) = (\sigma \circ \tau) \circ (\phi(a)) = \sigma(\tau(\phi(a)))$.

And $\sigma \circ (\tau \circ \phi)(a) = \sigma((\tau \circ \phi)(a)) = \sigma(\tau(\phi(a))) = (\sigma \circ \tau) \circ \phi(a)$.

**Theorem 8.3**
Let $S_A$ be the set of all permutation of $A$, then $\circ$ is a binary operation of $A$.

Furthermore, $S_A$ is a group under composition $\circ$ map. $S_A$ is called the permutation group of set $A$.

If $|A| = \infty$, then $S_A$ is a huge group.

**Proof.**
Since $(\sigma \circ \iota) = \sigma(\iota(a)) = \sigma(a)$, this proves $\sigma \circ \iota = \sigma$.

Also, $(\iota \circ \sigma) = i(\sigma(a)) = \sigma(a)$, this proves that $\iota \circ \sigma = \sigma$.

Hence, $\iota$ is an identity element under $S_A$ under $\circ$.

By lemma above, we have the associativity holds.

Finally, as $\sigma$ is bijective, thus there is **unique** $a \in A$, s.t. $\sigma(a) = b$. Define $\sigma^{-1}(b) = a$.

Note that $\sigma \circ \sigma^{-1} = \iota$ and $\sigma^{-1}\sigma = \iota$, thus the inverse element exists.

If $A$ is an infinite set with extra structure, we consider the permutation that can preserve the structure, we get a subgroup of $S_A$.

**Example 8.5**
Let $A = \mathbb{R}^2$, let $g$ be the set of all linear isomorphism from $\mathbb{R}^2 \to \mathbb{R}^2$. Then $g = \mathrm{GL}(2, \mathbb{R})$. This is a symmetry group of $\mathbb{R}^2$ vector space.

**Definition 8.2 (Symmetric groups)**
Let $A = 1, 2, ..., n$. $S_A = S_n$ is called the symmetric group on $n$ letters.

We use a two-row matrix to represent $\sigma = S_n$. i.e.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

**Example 8.6**
Let $\sigma \in S_3$, where:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Then $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2$.

The identity element is given by:

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

However, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 3 & 4 \end{pmatrix}$ is not a member of $S_5$ since there are repeated elements in the second row.

**Theorem 8.4**
The number of element in symmtric group $|S_n| = n!$

**Proof.**
Choose the entries in the second row in the order $i_1, i_2, \ldots, i_n$: $i_1$ has $n$ options; after $i_1$ is chosen, $i_2$ has $(n-1)$ options; after $i_1, i_2$ are chosen, $i_3$ has $(n-2)$ options. Repeating the procedure, we have $i_n$ has only 1 option left. Thus there are totally $n(n-1)(n-2)\ldots(2)(1) = n!$ permutations in $S_n$.

**Example 8.7**

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Note that the order of $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 3$ because $1 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 1$.

**Example 8.8**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$. Find $\sigma^{-1}$. Also find the order of $\sigma$.

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 6 & 1 & 3 & 7 & 2 \end{pmatrix}$$

Note that $1 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 1$, then $\sigma^7(1) = \sigma^6(4) = \sigma^5(2) = \sigma^4(7) = \cdots = \sigma(5) = 1$

Thus the order is 7.

**Example 8.9**

Let $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$, then $1 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 1$, pick arbitrary element 5, since:

$$5 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 7$$

Thus the order of $\tau = 3 \times 4 = 12$.

# 9 Orbits, Cycles, Alternating Groups

**Theorem 9.1**
Given $\tau \in S_n$. define relation $\sim$ on the set $A = \{1, 2, \ldots, n\}$ as follow:

$$i \sim j \text{ if } \tau^k(i) = j \text{ for some } k \in \mathbb{Z}$$

Then $\sim$ is an equivalence relation on $A$.

**Proof.**
Reflexivity: Take $k = 0$. Then $\tau^0 = e$.

Symmetry: If $a \sim b$, then $b = \tau^k(a)$ for some $k \in \mathbb{Z}$. then $\tau^{-k}(b) = \tau^{-k} \circ \tau^k(a) = a$, thus $b \sim a$.

Transitivity: If $a \sim b$ and $b \sim c$, then $c = \tau^m(b)$, and $b = \tau^n(a)$, then $c = \tau^m(b) = \tau^m \circ \tau^n(a) = \tau^{m+n}(a)$.

This implies $A$ can be written as disjoint union of equivalence classes.

**Example 9.1**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 4 & 7 & 1 & 3 & 6 \end{pmatrix} \in S_7$. Find the partition of $\sigma$.

Pick arbitrary element, say 1. Then $1 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 1$. Thus we may define $\{1, 5\}$ as an equivalence class.

Pick 2: Then $2 \xrightarrow{\sigma} 2$, thus $\{2\}$ is an equivalence class.

Pick 3, then $3 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 3$, thus $\{3, 4, 6, 7\}$ is an equivalence class.

Thus $\sigma$ induces the following partition.

$$\{1, 2, \ldots, 7\} = \{1, 5\} \sqcup \{2\} \sqcup \{3, 4, 6, 7\}$$

We name each partition as orbit. thus $\sigma$ has 3 orbits.

**Example 9.2**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 7 & 1 & 2 & 3 & 6 \end{pmatrix}$. We first pick arbitrary element, say 1: $1 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 1$, thus one of the orbit will be $\{1, 4\}$.

Then we pick arbitrary element that is not picked from above, say 2: $2 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 2$, then another orbit will be $\{2, 5\}$.

Continuing, we have $3 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 3$, giving orbit $\{3, 6, 7\}$.

Finally, we have the $\sigma = \{1, 4\} \sqcup \{2, 5\} \sqcup \{3, 6, 7\}$.

**Theorem 9.2**
Identity element $\sigma = e$ has the most orbits.

**Definition 9.1 (Cycle)**
$\sigma \in S_n$ is called a cycle if $\sigma = e$ or $\sigma$ has only one unique orbit containing more than 1 element.

The length of the cycle is the number of elements in its largest orbit.

That is, $\sigma$ can only have one orbit with more than 1 element, all other orbits must have 1 element only.

**Example 9.3**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 4 & 7 & 1 & 3 & 6 \end{pmatrix}$. Note that the orbits of $\sigma = \{1,5\}, \{2\}, \{3,4,7,6\}$ and there are 2 orbits with more than 1 element. Hence $\sigma$ does not form a cycle.

**Example 9.4**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$, note that $\sigma$ has 4 orbits, namely $\{1,4,5,7\}, \{2\}, \{3\}, \{6\}$. Thus $\sigma$ forms a cycle.

Also $\sigma$ has a length of 4, because $|\{1,4,5,7\}| = 4$

From now on, we can use one row notation to denote a cycle with length not equal to $e$.

For example, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$ can be written as $\sigma = (1,4,5,7)$.

**Example 9.5**

Let $\sigma \in S_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 4 & 5 & 3 & 1 & 8 & 9 & 7 \end{pmatrix}$. The orbits of $\sigma$ are $\{1,6\}, \{2\}, \{3,4,5\}, \{7,8,9\}$.

Note that $(1,6), (3,4,5), (7,8,9)$ forms 3 cycles, and $\sigma = (1,6)(3,4,5)(7,8,9)$.

**Proof.**
Take $i = 3$, by product of permutation, $(7,8,9) \times 3$=3.

$(1,6), (3,4,5), (7,8,9) \times 3 = (1,6), (3,4,5) \times 3 = (1,6) \times 4 = 4 = \sigma(3)$.

Repeat the steps for $i = 1, \ldots, 9$. We have $(1,6) \times (3,4,5) \times (7,8,9)i = \sigma(i)$.

**Definition 9.2 (Disjoint cycles)**
If $\sigma, \tau \in S_n$ are cycles, both are not $e$, we call $\sigma, \tau$ to be disjoint cycles, if their largest orbits have empty intersections.

**Example 9.6**
Let $\sigma = (7,1,3,4,5), \tau = (2,6,8) \in S_8$. Then $\sigma, \tau$ are disjoint.

**Theorem 9.3**
If $\sigma, \tau$ are disjoint cycles in $S_n$, then $\sigma \circ \tau = \tau \circ \sigma$

**Proof.**
Let $\sigma = (i_1, \ldots, i_s)$ with length $s$, let $\tau = (j_1, \ldots, j_t)$ with length $\tau$. where $s, t > 1$. Then $(i_1, \ldots, i_s) \cap (j_1, \ldots, j_t) = \emptyset$.

We want to prove that $(i_1, \ldots, i_s) \circ (j_1, \ldots, j_t)k = (j_1, \ldots, j_t) \circ (i_1, \ldots, i_s)k$.

Case 1: $k \in (i_1, \ldots, i_s)$. Then LHS $= (i_1, \ldots, i_s)i$, RHS $= (i_1, \ldots, i_s)k =$ LHS.

Case 2: $k \in (j_1, \ldots, j_t)$: Similar proof as Case 1.

Case 3: $k \notin (j_1, \ldots, j_t) \notin (i_1, \ldots, i_s)$: Then LHS $=$ RHS $= k$.

**Theorem 9.4**
Every permutation is a product of disjoint cycles.

**Example 9.7**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 3 & 5 & 4 & 6 & 8 & 9 & 1 \end{pmatrix}$. Decompose $\sigma$ as a product of disjoint cycles.

We have $1 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 9$, $2 \xrightarrow{\sigma} 2$, $3 \xrightarrow{\sigma} 3$, $4 \xrightarrow{\sigma} 5$, $6 \xrightarrow{\sigma} 6$, thus $\sigma = (1, 7, 8, 9)(4, 5)$

**Theorem 9.5**
If $\sigma = \tau 1 \tau 2 ... \tau k$ are disjoint cycles of length $l_1, .., l_k$, then $\sigma$ has order of $\text{lcm}(l_1, ..., l_k)$

**Definition 9.3 (Transposition)**
Transposition is a cycle of length 2 $(i, j)$ that interchanes $i$ with $j$, and have all other elements fixed.

**Theorem 9.6**
If $n \geq 2$, then there are $\begin{pmatrix} n \\ 2 \end{pmatrix} = \dfrac{n(n-1)}{2}$ transpositions in $S_n$.

**Theorem 9.7**
Every cycle of length $k \geq 3$ can be written as a product of $(k-1)$ transpositions.

**Proof.**
Let $\sigma = (a_1, \ldots, a_k)$. Write $\sigma = (a_1, a_k), (a_1, a_{k-1}), \ldots, (a_1, a_2)$, then $|(a_1, a_k), (a_1, a_{k-1}), \ldots, (a_1, a_2)| = k-1$. Now we want prove that $(a_1, \ldots, a_k)i = (a_1, a_k), (a_1, a_{k-1}), \ldots, (a_1, a_2)i$.

If $i \notin \{a_1, \ldots, a_k\}$, then LHS = RHS = $i$.

Otherwise, pick $i = a_1$. We have:

$$\begin{aligned} \text{LHS} &= (a_1, \ldots, a_k)a_1 \\ &= a_2 \\ \text{RHS} &= (a_1, a_k), (a_1, a_{k-1}), \ldots, (a_1, a_2)a_1 \\ &= (a_1, a_k), (a_1, a_{k-1}), \ldots, (a_1, a_3)a_2 \\ &= a_2 \\ &= \text{LHS} \end{aligned}$$

Perform this for any $i \in \{a_1, \ldots, a_k\}$, then LHS = RHS = $i$.

**Example 9.8**
$\sigma = (2, 7, 1, 9) = (2, 9)(2, 1)(2, 7)$

**Proof.**
We aim to prove $(2, 7, 1, 9)i = (2, 9)(2, 1)(2, 7)i$.

Case 1: If $i \notin \{2, 7, 1, 9\}$. Then LHS$= i =$RHS.

Case 2: If $i \in \{2, 7, 1, 9\}$, we pick any element, say, $i = 9$. Then we have:

$$\begin{aligned} \text{LHS} &= (2, 7, 1, 9)i \\ &= 2 \\ \text{RHS} &= (2, 9)(2, 1)(2, 7)i \\ &= (2, 9)(2, 1)9 \\ &= (2, 9)9 \\ &= 2 \end{aligned}$$

**Corollary 9.7.1**
Any permutation in $S_n$ is a product of transpositions. For example, $e = (1, 2)(1, 2)$.

**Example 9.9**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 6 & 2 & 8 & 4 & 5 & 7 \end{pmatrix} \in S_8$. Decompose $\sigma$ as a product of transpositions.

We first find the orbits. Since the orbit of $\sigma = (1, 3, 6, 4, 2)(5, 8, 7)$. The decomposition can be written as

$$\sigma = (1, 2)(1, 4)(1, 6)(1, 3)(5, 7), (5, 8) = (1, 2)(1, 4)(1, 6)(1, 3)(4, 6)(5, 7)(5, 8)(4, 6)$$

**Theorem 9.8**
No permutation in $S_n$ can be expressed both as a product of an even number of transpositions, and as a product of an odd number of transposition.

**Proof.**
Choose $n \times n$ matrix $A$ ,s.t. $|A| \neq 0$. Write $A = (a_1, \ldots, a_n)$ in column form, with $a_k$ to be the $k$-th column.

For $\sigma \in S_n$, $\sigma$ permute the columns of $A$ to obtain a new matrix, $\sigma A$.

$\sigma$ moves 1st column of $A$ to $\sigma(1) -$ th column, moves 2nd column of A to $\sigma(2) -$ th column. etc.

Note that every transposition will interchange two colums, and by linear algebra, by interchanging two columns, determinant is multiplied by $-1$.

If we write $\sigma = r_1 r_2 \ldots r_s$ as a product of $s$ transposition, then we have:

$$A \xrightarrow{r_s} r_s A \xrightarrow{r_{s-1}} r_s r_{s-1} A \to \cdots \to \sigma A$$

Thus $\det(\sigma A) = (-1)^s \det(A)$.

We may also write $\sigma = \tau_1 \ldots \tau_m$ as a product of $m$ transposition. Then $\det(\sigma A) = (-1)^m \det(A)$.

Then we have:

$$\begin{aligned} (-1)^s \det(A) &= (-1)^m \det(A) \\ (-1)^s &= (-1)^m \end{aligned}$$

Thus $s$ and $m$ must be both even, or both odd.

**Definition 9.4 (Odd Permutation, Even Permutation)**
If $\sigma \in S_n$ can be written as a product of an even number of transpositions, we call $\sigma$ an even permutation.

If $\sigma$ can be written as a product of an odd number of transpositions, we call $\sigma$ an odd permutation.

Every permutation is either odd or even (can't be both).

**Theorem 9.9**
Suppose $\sigma$ is a cycle with length $k$, if $k$ is odd, then $\sigma$ is even. if $k$ is even, then $\sigma$ is odd.

**Proof.**
If the length is even, then for some $k \in \mathbb{N}$, we have :

$$(a_1, a_2, \ldots, a_{2k}) = (a_1, a_{2k}), (a_2, a_{2k-1}), \ldots, (a_1, a_2)$$

Note that there are $2k - 1$ transposition. Thus $\sigma$ is odd.

The case where the length is odd can be proved similarly.

**Theorem 9.10**
The product of two even or two odd permutations is even.

The product of odd and even permutations is odd.

Moreover, the set of the even permutation is closed.

**Proof.**
Given that $\sigma, \tau$ are even, then we write $\sigma = s_1 \dots s_{2m}, \tau = t_1 \dots t_{2n}$ in their transposition form.

Then $\sigma \circ \tau = s_1 \dots s_{2m} t_1 \dots t_{2n}$ must be even as they have $2m + 2n$ transpositions.

**Theorem 9.11**
In any group $G$, if $g_1, \dots, g_n \in G$, then $(g_1 \dots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \dots g_2^{-1} g_1^{-1}$

**Proof.**
The proof is simple. as $(g_1 \dots g_n)(g_1 \dots g_n)^{-1} = g_1 \dots g_n g_n^{-1} g_1^{-1} = g_1 \dots e \dots g_1^{-1} = e$

**Theorem 9.12**
Let $\sigma$ be a permutation. Then $\sigma$ and $\sigma^{-1}$ have the same parity (oddness/evenness).

**Proof.**
Let $\sigma$ be even. Then

$$\begin{aligned} \sigma &= (a_1, b_1)(a_2, b_2) \dots (a_{2m}, b_{2m}) \\ \sigma^{-1} &= (a_{2m}, b_{2m})^{-1} \dots (a_2, b_2)^{-1} (a_1, b_1)^{-1} \\ &= (a_{2m}, b_{2m}) \dots (a_2, b_2)(a_1, b_1) \end{aligned}$$

By similar proof, if $\sigma$ is odd, we can also prove that $\sigma^{-1}$ is also odd.

**Theorem 9.13**
If $n \geq 2$, then the set of all even permutations of $\{1, 2, ..., n\}$ forms a subgroup of order of $\frac{1}{2}n!$ of symmetric group $S_n$. Such group is called the alternating group $A_n$ on $n$ letters.

**Proof.**
1. The identity element $e \in A_n$
2. $A_n$ is closed under $\cdot$.
3. If $\sigma \in A_n$, then $\sigma^{-1} \in A_n$ also.

This proves that $A_n$ is a subgroup of $S_n$.

**Example 9.10**
Let $S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$, then $A_3 = \{e, (1,2,3), (1,3,2)\}$.

**Theorem 9.14**
For $n \geq 2$, we have $|A_n| = \frac{1}{2}n!$

**Proof.**
Let $B_n$ =set of odd permutation of $S_n$. Then $S_n = A_n \sqcup B_n$. It is enough to prove that $|A_n| = |B_n|$.

Define a map $f : A_n \to B_n$, where $f(\sigma) = (1,2)\sigma$. Then the multiplication is odd, as $(1,2)$ is odd.

By cancellation law, $f$ is one-to-one. Since:

$$\begin{aligned} f(\sigma_1) &= f(\sigma_2) \\ (1,2)\sigma_1 &= (1,2)\sigma_2 \\ \sigma_1 &= \sigma_2 \end{aligned}$$

Now we prove that $f$ is also onto. We need to find $\sigma \in S_n$, s.t. $f(\sigma) = \tau$. If we let $\sigma = (1,2)\tau$, then

$$\begin{aligned} f((1,2)\tau) &= (1,2)(1,2)\tau \\ &= \tau \end{aligned}$$

This proves that $f$ is both onto and one-to-one. Hence $f$ is a bijection. This implies that $|A_n| = |B_n|$.

Thus half of permutations in $S_n$ are even, half are odd. $A_n = \frac{1}{2}S_n$.

**Example 9.11**

$|A_4| = \frac{1}{2}|S_4| = \frac{1}{2}4! = 12$

How to find the elements in $A_4$?

Consider regular tetrahedron. Note that tetrahedron have $120^\circ, 240^\circ$ of rotational symmetry.

Thus totally there are 8 elements related to this symmetry. And there are 3 more elements, that are obtained by rotating with $180^\circ$. And there is one identity element $e$. This gives all 12 elements in $A_4$.

Rotational symmetry: By watching at the 4 vertex of the tetrahedron, and rotate (read) clockwisely, we have 4 elements to be $(2,3,4), (1,4,3), (4,1,2), (3,2,1)$. Rotating anti-clockwisely, we have other 4 elements to be $(4,3,2), (3,4,1), (2,1,4), (1,2,3)$.

Also the other 3 elements are $(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$, they are formed by joining the midpoints of each line segments.

# 10 Cosets and the Theorem of Lagrange

**Definition 10.1 (Coset)**
The left coset of $H$ containing $a, a \in G$ is

$$aH = \{ah : h \in H\}$$

The right coset of $H$ containing $a$ is

$$Ha = \{ha : h \in H\}$$

.

**Example 10.1**
Let $H = \{h_1, \ldots, h_k\}$, then $aH = \{ah_1, \ldots, ah_k\}$.

**Example 10.2**
Let $H = \{e, (1,2)\}$. $G = S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. Then we have:

$$\begin{aligned}
eH &= \{ee, e(1,2)\} = \{e, (1,2)\} \\
(1,2)H &= \{(1,2)e, (1,2)(1,2)\} = \{(1,2), e\} = (1,2)H \\
(1,3)H &= \{(1,3)e, (1,3)(1,2)\} = \{(1,3), (1,2,3)\} \\
(2,3)H &= \{(2,3)e, (2,3)(1,2)\} = \{(2,3), (1,3,2)\} \\
(1,2,3)H &= \{(1,2,3)e, (1,2,3)(1,2)\} = \{(1,2,3), (1,3)\} \\
(1,3,2)H &= \{(1,3,2)e, (1,3,2)(1,2)\} = \{(1,3,2), (2,3)\}
\end{aligned}$$

**Example 10.3**
Let $G = (\mathbb{Z}, +)$, and $H = 3\mathbb{Z}$. Then the coset of $H$ containing 1:

$$\begin{aligned}
1 + 3\mathbb{Z} &= \{1 + 3n : n \in \mathbb{Z}\} \\
2 + 3\mathbb{Z} &= \{2 + 3n : n \in \mathbb{Z}\} \\
4 + 3\mathbb{Z} &= \{4 + 3n : n \in \mathbb{Z}\} = \{1 + 3n : n \in \mathbb{Z}\} = 1 + 3\mathbb{Z}
\end{aligned}$$

Different cosets such as $1 + 3\mathbb{Z}$ and $2 + 3\mathbb{Z}$ have empty intersection.

**Example 10.4**
Let $A_n$ be a alternating group on $n$ symbols $S_n$, and $A_n \subset S_n$. Then $A_n$ is the set of even permutations in $S_n$. For example, $A_3 = \{e, (1,2,3), (1,3,2)\}$. Then $(1,2)A_n$ is the set of all odd permutations.

**Theorem 10.1**
Let $H = \{h_1, \ldots, h_n\}$, and $|H| = n$. Then $|aH| = |\{ah_1, \ldots, ah_n\}| = n$. For any $a, b \in G$, given $aH, bH$, we have only two possible relations:

$$\begin{cases} aH & = & bH \\ aH \cap bH & = & \emptyset \end{cases}$$

**Proof.**
Suppose $aH \cap bH \neq \emptyset$, then exists $c \in aH \cap bH$.

Then $c \in aH = ah_1, h_1 \in H$, and $c \in bH = bh_2, h_2 \in H$.

$(aH \subset bH)$

For arbitrary $ah \in aH$, $h \in H$. As $ah_1 = bh_2 \Rightarrow a = bh_2h_1^{-1}$. Thus $ah = bh_2h_1^{-1}h = b(h_2h_1^{-1}h) \in bH$.

The opposite direction can be proven similarly.

**Theorem 10.2 (Lagrange theorem)**
If $H$ is a subgroup of a finite group $G$, then $|G|$ is a multiple of $|H|$.

**Proof.**
Let $a_1H, \ldots, a_nH$ be a array of all left cosets. Let $G = a_1H \sqcup \ldots \sqcup a_nH$.

Then $|G| = |a_1H| + \cdots + |a_nH| = |H| + \cdots + |H| = n|H|$

**Example 10.5**
Take the vector space of $\mathbb{R}^2$, where $\dim(\mathbb{R}^2) = 2$. Let $H = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R} \right\}$. Then $H$ is the set of $x-$axis. Moreover, $\begin{pmatrix} 0 \\ 1 \end{pmatrix} + H = \left\{ \begin{pmatrix} x \\ 1 \end{pmatrix} : x \in \mathbb{R} \right\}$. $H$ is now a horizontal line. Thus $\mathbb{R}^2$ is a disjoint union of horizontal lines.

Note: Everything proven for left coset also holds for right cosets.

**Corollary 10.2.1**
If $|G| = p$ is prime, then $G$ is cyclic group.

**Proof.**
Choose arbitrary element $a \in G, a \neq e$. Consider $\langle a \rangle$ = cyclic subgroup generated by a. Then such group must contain at least 2 element, namely $\{a, e\}$. Then $|\langle a \rangle| \geq 2$. By Lagrange theorem, $|\langle a \rangle|$ is a divisor of $|G| = p$. As $p$ is prime ,then $|\langle a \rangle| = p \neq 1$. Thus $\langle a \rangle = G$.

**Theorem 10.3 (*)**
The order of an element of a finite group is a divisor of the order of the group.

**Example 10.6**
If $H_1, H_2$ are subgroup of the finite group $G$, and $|H_1|$ and $|H_2|$ are relatively prime, prove that $H_1 \cap H_2 = \{e\}$.

**Proof.**
Let $|H_1 \cap H_2| = p$. Since $H_1 \cap H_2$ is a subgroup of both $H_1$ and $H_2$, by Lagrange theorem, we have

$$\begin{aligned} |H_1| &= ap \\ |H_2| &= bp \end{aligned}$$

Since $|H_1|, |H_2|$ are relatively prime, therefore $\gcd(ap, bp) = 1$. Assume that $p \geq 2$.

Then if $a = b$, then $\gcd(ap, bp) = ap = bp \geq 2$, which contradicts the fact that $|H_1|, |H_2|$ are relatively prime.

Since $a \neq b$, then we must have $p = 1$, otherwise $\gcd(ap, bp) \geq 2$.

The group $|H_1 \cap H_2| = p$ is thus trivial. i.e. $H_1 \cap H_2 = \{e\}$

**Theorem 10.4**
If $V_1, V_2$ are subspace in vector space $V$, then $V_1 \cap V_2$ is a subspace of $V$. However, $V_1 \cup V_2$ might not be a subgroup of $V$.

In general, if $H_1, H_2$ are subgroup of $G$, then $H_1 \cup H_2$ is not a subrgroup of $H$.

**Example 10.7**
Let $U_n = \{z \in \mathbb{C} : z^n = 1\} = \left\{ e^{\frac{2\pi i}{n} k} : k = 1, 2, \ldots, k-1 \right\}$. Then $|U_n| = n$. Take a special example $U_{10}$.

Then $U_2, U_5$ are also subgroups of $U_{10}$ as $|U_2| = 2, |U_5| = 5$. Moreover, $|U_2|$ and $|U_5|$ are relatively prime, thus $U_2 \cap U_5 = \{e\}$ .

# 11 Direct Products and Finitely Generated Abelian Groups

**Definition 11.1 (Direct set)**
If $S_1, S_2$ are sets, then direct set $S_1 \times S_2 = \{(x, y) : x \in S_1, y \in S_2\}$.
Moreover if $S_1 \dots S_n$ are sets, then their direct product set is

$$S_1 \times \cdots \times S_n = \{(a_1, a_2, \dots, a_n) : a_1 \in S_1, \dots, a_n \in S_n\}$$

The cardinality, $|S_1 \times \cdots \times S_n| = |S_1| * \dots * |S_n|$.

**Example 11.1**
Let $S_1 = \{a, b\}, S_2 = \{1, 2, 3\}$, then $S_1 \times S_2 = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

$\mathbb{R}^2 \times \mathbb{R}^3 = \{(a, b) : a \in \mathbb{R}^2, b \in \mathbb{R}^3\} = \{(a_1, a_2, b_1, b_2, b_3) : (a_1, a_2) \in \mathbb{R}^2, (b_1, b_2, b_3) \in \mathbb{R}^3\}$,
and $\dim(\mathbb{R}^2 \times \mathbb{R}^3) = 5$.

**Theorem 11.1**
Suppose $G_1, \dots, G_n$ are groups, then $G_1 \times \cdots \times G_n$ has the binary operation

$$(a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$$

The directed product set is a group under such operation.

**Proof.**
Identity: If $e_1 \in G_1, \dots, e^m$ are the identity elemens,s then identity element is $(e_1, \dots, e_n)$.
Associativity: We proof that $(a_1, \dots, a_n)(b_1, \dots, b_n)(c_1, \dots, c_n) \in G_1 \times \cdots \times G_n$

$$\begin{aligned}
\text{LHS} &= ((a_1, \dots, a_n)(b_1, \dots, b_n))(c_1, \dots, c_n) \\
&= (a_1 b_1, \dots, a_n b_n)(c_1, \dots, c_n) \\
&= (a_1 b_1 c_1, \dots, a_n b_n c_n) \\
\text{RHS} &= (a_1, \dots, a_n)((b_1, \dots, b_n)(c_1, \dots, c_n)) \\
&= (a_1, \dots, a_n)(b_1 c_1, \dots, b_n c_n) \\
&= (a_1 (b_1 c_1), \dots, (a_n (b_n c_n)))
\end{aligned}$$

Thus each of $G_1, \dots, G_n$ has associativity, so associativity holds for any $G_1 \times \cdots \times G_n$.
Inverse: The inverse for $(a_1, \dots, a_n)$ is $(a_1^{-1}, \dots, a_n^{-1})$. To prove that, consider

$$\begin{aligned}
(a_1, \dots, a_n)(a_1^{-1}, \dots, a_n^{-1}) &= (a_1 a_1^{-1}, \dots, a_n a_n^{-1}) = (e_1, \dots, e_n) \\
(a_1^{-1}, \dots, a_n^{-1})(a_1, \dots, a_n) &= (a_1^{-1} a_1, \dots, a_n^{-1} a_n) = (e_1, \dots, e_n)
\end{aligned}$$

This proves that the directed product set is a group under multiplication.

**Theorem 11.2**
If $G_1, \dots, G_n$ are Abelian group, then $G_1 \times \cdots \times G_n$ is also Abelian group.

**Example 11.2**
Give a finite Abelian group that is not cyclic. Consider the following finite group we've discussed so far:

$$S_n, A_n, \mathbb{Z}_n, V_n$$

Note that $S_n, A_n$ are not Abelian, for $n \geq 3$ and $n \geq 4$. While $\mathbb{Z}_n$ is Abelian and cyclic. $V_n$ is cyclic.

Consider the group (Hint of HW)

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \{1, -1\} \right\}$$

$G$ is Abelian as the diagonal matrix commutes.

$G$ is not cyclic, as $G$ is going to generate 2 element subgroup. How about if we want to generate more such example?

Consider $S_1 = \{1, -1\}$ to be a subgroup under $\cdot$. Let $S_2 = \{1, -1\}$. By consider direct product, we have:

Consider $\mathbb{Z}_5 \times \mathbb{Z}_5$, note that $|\mathbb{Z}_5 \times \mathbb{Z}_5| = 25$. The group is Abelian, but the group is not cyclic, as if we take any $(a, b) \in \mathbb{Z}_5 \times \mathbb{Z}_5$, then $(a, b) + \cdots + (a, b) = (5a, 5b) = (0, 0)$. Thus $(a, b)$ will generate a group of 5 elements, but not 25 elements. Thus $\mathbb{Z}_5 \times \mathbb{Z}_5$ is never cyclic.

Consider $\mathbb{Z}_3 \times \mathbb{Z}_5$, is $\mathbb{Z}_3 \times \mathbb{Z}_5$ cyclic?

If $|G| = n$, then $G$ is cyclic, if and only if $G$ has an element where its order is $n$.

Consider $\underbrace{(1,1) + ... + (1,1)}_{n} = (n, n) = (0, 0)$if and only $n$ is a multiple of 3 and multiple of 5. As $3, 5$ are relatively prime, thus this means $n$ need to be a multiple of 15. The order of $(1, 1)$ therefore is 15.

Thus the group is cyclic.

In general, $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, if and only if $m, n$ are relatively prime, moreover $(1, 1)$ is a generator.

**Theorem 11.3**
If $G$ is a cyclic group of order $m$, $G'$ is a cyclic group of order $n$, if $m, n$ are relatively prime, then $G \times G'$ is cyclic.

**Proof.**
Let $G = \langle a \rangle$, $G' = \langle b \rangle$, so a has order m and b has order n. Consider $(a, b) \in G \times G'$, it has order mn, which is $|G \times G'|$, so $G \times G'$ is cyclic.

**Definition 11.2**
If $G$ is a group, $S$ is a subset, then we say $S$ generates $G$, if every element $g \in G$ can be expressed as $g = a_1^{k_1} \dots a_m^{k_m}$, for some $a_1, \dots, a_m \in S$, and $k_1, \dots, k_n \in \mathbb{Z}$.

**Example 11.3**
Consider $S_n$. Let $S$ be a set of all transpositions, then $S$ generates $S_n$. (As every permutation can be written as transpositions).

**Example 11.4**
Let $S' = \{(1,2), \ldots, (n-1,n)\}$. This interchange two integers. Then $S'$ can generate $S_n$. (Not required)

**Example 11.5**
Consider $\mathrm{GL}(3,\mathbb{R})$, the $3 \times 3$ invertible real matrices.
We Consider the following method to find the inverse. (Commonly used in linear algebra course)

$$(A|I) \xrightarrow{\text{series of row operation}} (I|B)$$

Then when you perform row operations, you are actually multiplying an elementary matrix $E_i$. Hence we have:

$$\begin{aligned}
(A|I) &\xrightarrow{1^{\text{st}} \text{ row operation}} (E_1A_1|E_1I_3) \\
&\xrightarrow{2^{\text{nd}} \text{ row operation}} (E_2E_1A_1|E_2E_1I_3) \\
&\vdots \\
&\xrightarrow{m^{\text{th}} \text{ row operation}} (E_mE_{m-1}\ldots E_2E_1A_1|E_mE_{m-1}\ldots E_2E_1I_3)
\end{aligned}$$

$$\begin{aligned}
(E_mE_{m-1}\ldots E_2E_1)A &= I \\
A^{-1} &= (E_mE_{m-1}\ldots E_2E_1)
\end{aligned}$$

Thus if we let $S =$ all $3 \times 3$ elementary matrices, then $S$ generates $\mathrm{GL}(3,\mathbb{R})$.

**Example 11.6**
Let $E$ be the set of $n \times n$ matrices. $n \times n$ matrix $A$ is called an elementary matrix $A$, if $A$ is obtained from $I_n$ by performing a single elementary row operation, including:

- Multiplying a row by a non-zero scalar.
- Interchanging two rows.
- Adding multiple of a row to another row.

Take $n = 2$, we have:

$$E = \left\{ \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \right\}, c \in \mathbb{R}\backslash\{0\}$$

We say that $E$ generates $\mathrm{GL}(n,\mathbb{R})$

**Example 11.7**
Consider $\mathbb{Z} \times \mathbb{Z} = \{(m,n) : m,n \in \mathbb{R}\} \subset \mathbb{R}^2$. Then $S = \{(0,1),(1,0)\}$ generates $\mathbb{Z} \times \mathbb{Z}$.

In general, $(m,n) = m(1,0) + n(0,1)$.

Also consider $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, then $T = \{(0,0,1),(0,1,0),(0,0,1)\}$ generates $\mathbb{Z}^3$.

Consider $\mathbb{Z}_9 \times \mathbb{Z}_8$, then as 1 generates $\mathbb{Z}_9$ and $\mathbb{Z}_8$ (As both of them are cyclic), thus $S = \{(0,1),(1,0)\}$ generates $\mathbb{Z}_9 \times \mathbb{Z}_8$.

**Definition 11.3 (Finitely generated group)**
A group $G$ is called a finitely generated group, if there is finite subset $S$ that generates $G$.

**Example 11.8**
A finite group is finitely generated.

$\mathbb{Z}, \mathbb{Z} \times \mathbb{Z}, \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \ldots$ are finitely generated.

$\mathbb{Z}_{k_1} \times \cdots \times Z_{k_n} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{m}$ is finitely generated.

**Definition 11.4 (Isomorphic (Brief introduction))**
$G$ and $G'$ is isomorphic, if there is $\phi : G \to G'$, where $\phi$ is bijective, and $\phi$ preserves group structure, i.e. $\phi(ab) = \phi(a)\phi(b)$.

**Theorem 11.4 (* Fundamental Theorem of finitely generated Abelian Groups *)**
Every finitely generated Abelian group is **isomorphic** to a direct product of cyclic groups in the form

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \cdots \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{m}$$

where $p_1, \ldots, p_n$ are primes, $r_1, \ldots, r_n$ are positive integers. $m > 0$.

**Definition 11.5 (Vector Space)**
A vector space is a set with two operation: addition, $+ : V \times V \to V$, and scalar multiplication, $\cdot : \mathbb{R} \times V \to V$, following the 8 axioms below:

1. $+$ is commutative: $a + b = b + a$
2. $+$ is associative: $(a + b) + c = a + (b + c)$
3. There is $0 \in V$, s.t. $0 + a = a + 0 = a$
4. $\forall a \in V, \exists! a \in V, a + (-a) = 0$
5. $\exists 1 \in V$, s.t. $1 \cdot a = a \cdot 1 = a$
6. $\forall k_1, k_2 \in \mathbb{R}, k_1(k_2 \cdot a) = (k_1 k_2)a$
7. $(k_1 + k_2)a = k_1 a + k_2 a$
8. $k(a + b) = ka + kb$

**Example 11.9**
The following groups are isomorphic.

$$\mathbb{R}^3 \text{ and } V = \{ax^2 + bx + c : a, b, c \in \mathbb{R}\}$$

The following groups are **NOT** isomorphic.

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in (1, -1) \right\} \text{ and } G' = \mathbb{Z}_4$$

# 13 Homomorphisms

**Definition 13.1 (Homomorphism)**
A map $\phi : G \to G'$ is homomorphism (of groups) if $\phi(a * b) = \phi(a) \star \phi(b)$, where $*$ is the operation on $G$, while $\star$ is the operation on $G'$.

**Definition 13.2 (Isomorphism)**
$\phi : G \to G'$ is an isomorphism of groups, if and only if:

- $\phi$ is a bijection.
- $\phi$ is a homomorphism.

Two groups $G_1$ and $G_2$ are isomorphic, if there exists an isomorphism $\phi : G_1 \to G_2$

**Example 13.1**
Let $\mathbb{R}$ is a group under $+$, and $\mathbb{R}_{>0}$ is a group under multiplication. Find an isomorphism $\phi : \mathbb{R} \to \mathbb{R}_{>0}$.

Take $\phi : \mathbb{R} \to \mathbb{R}_{>0} = e^x$. Then $\phi(x)$ is actually a bijection. And also $e^{a+b} = e^a e^b$. This imples that actually
$\mathbb{R}$ and $\mathbb{R}_{>0}$ are isomorphic, even under the different operations.

**Example 13.2**
Consider $\phi : \mathbb{R} \to \mathbb{R}, \phi(x) = 2x$. Then $\phi$ is a isomorphism.

**Example 13.3**
Consider the regular tetrahedron again, there are totally 12 symmtries, let $G$ be the symmetry group, then $|G| = 12$. Note that every symmetry is a permutation of $\{1, 2, 3, 4\}$, thus $G \subset S_4$ and $G = A_4$.

**Example 13.4**
Consider a square, Then $|G| = 8$, including 4 rotations and 4 reflections.

**Example 13.5**
Consider a regular triangle. There are rotational symmetry, which are $\{120°, 240°, 360° = 0°\}$, and also there are 3 reflections. Thus $|G| = 6$. Thus such group is isomorphic to $S_3$.

**Example 13.6**
Let $\phi : \mathbb{R} \to \mathbb{R}^*$, where $\phi \mapsto e^x$. Then $\phi$ is a homomorphism. Note that $\mathbb{R}$ has binary operation $+$, while $\mathbb{R}^*$ has binary operation $*$.

**Proof.**
Since $e^{x+y} = e^x e^y$ Therefore $\phi(x + y) = \phi(x) \cdot \phi(y)$.

Note that $\phi$ is not a isomorphism, because $\phi$ is not surjective. However, if $\phi : \mathbb{R} \to \mathbb{R}^*_{>0}$, then $\phi$ is a isomorphism.

**Definition 13.3 (Isomorphic groups)**
Two groups $G_1, G_2$ are isomorphic, if there exists an isomorphism $\phi : G_1 \to G_2$.

**Example 13.7**
Prove that $S_3$ and $\mathbb{Z}_6$ are not isomorphic.

**Proof.**
Suppose $S_3$ and $\mathbb{Z}_6$ are isomorphism. Then we have an isomorphism $\phi : S_3 \to \mathbb{Z}_6$.

We start with the fact that $(1,2)(1,3) \neq (1,3)(1,2)$.

$$\begin{aligned} \text{LHS} &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \text{RHS} &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \text{LHS} \end{aligned}$$

Note that by homomorphism property,

$$\begin{aligned} \phi((1,2)(1,3)) &= \phi(1,2) + \phi(1,3) \\ \phi((1,3)(1,2)) &= \phi(1,3) + \phi(1,2) \\ &= \phi(1,2) + \phi(1,3) \\ &= \phi((1,2)(1,3)) \end{aligned}$$

By the property of homomorphism,

$$\begin{aligned} \phi((1,3)(1,2)) &= \phi((1,2)(1,3)) \\ (1,3)(1,2) &= (1,2)(1,3) \end{aligned}$$

Contradiction!

There are another theorem that can be used to prove the example, but before that we need to introduce several theorems.

**Theorem 13.1**
If $\phi : G \to G'$ is an homomorphism, $e \in G$ is the identity element of $G$, while $e' \in G'$ is the identity element of $G'$, then $\phi(e) = e'$

**Proof.**
Note that

$$\begin{aligned} \phi(a * e) &= \phi(a) \\ &= \phi(a)\phi(e) \\ &= \phi(a) * e' \end{aligned}$$

By cancellation law, we have

$$\begin{aligned} \phi(a) * e' &= \phi(a)\phi(e) \\ \phi(e) &= e' \end{aligned}$$

**Theorem 13.2**
If $\phi : G \to G'$ is an isomorphism, $a \in G$, then for any positive integer $n$,

$$a^n = e \quad \text{if and only if} \quad \phi(a)^n = e'$$

and moreover, $a$ and $\phi(a)$ have the same order.

**Proof.**
$(\implies)$
If $a^n = e$, apply $\phi$ on both sides, we have

$$\begin{aligned} \phi(a^n) &= \phi(e) = e' \\ \phi(a * a \ldots * a) &= \phi(a) \ldots \phi(a) = \phi(a)^n \\ \phi(a)^n &= e' \end{aligned}$$

$(\impliedby)$

$$\begin{aligned} \phi(a)^n &= \phi(a * a \ldots * a) = \phi(a^n) \text{ (property of homomorphism)} \\ \phi(a^n) &= \phi(e) \\ a^n &= e \end{aligned}$$

**Theorem 13.3**
Any two cyclic groups of equal order are isomorphic.

**Proof.**
Suppose $G$ and $G'$ are cyclic, and $|G| = |G'|$, then consider following cases:

[Case 0: $|G| = |G'| = n \in \mathbb{Z}_{>0}$]

$$\begin{aligned} G &= \{e, a, a^2, \ldots, a^{n-1}\}, \text{ and } a^n = e \\ G' &= \{e, b, b^2, \ldots, b^{n-1}\}, \text{ and } b^n = e \end{aligned}$$

Let $\phi : G \to G'$. Then $\phi(a^k) = b^k$ is a isomorphism.

[Case 1: $|G| = |G'| = \infty$]

$$\begin{aligned} G &= \{a^n : n \in \mathbb{Z}\} \\ G' &= \{b^n : n \in \mathbb{Z}\} \end{aligned}$$

Then $\phi : G \to G'$, $\phi(a^n) = b^n$ is a isomorphism.

**Theorem 13.4**
Let $\phi : G \to G', \phi(x) = x$ is always isomorphic.

Moreover, $\Phi : G \to G', \Phi(x) = e'$ is always homomorphic, but not isomorphic.

**Example 13.8**
Let $\phi : \mathbb{C}^* \to \mathbb{C}^*$, where $\phi(z) = \phi(x + yi) = \sqrt{x^2 + y^2}$, then $\phi$ is homomorphism.

**Example 13.9**
Let $\phi : \mathbb{C}^* \to \mathbb{C}^*$, where $\phi(z) = z^n, n \in \mathbb{Z}$, then $\phi$ is homomorphism.

**Example 13.10**
Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$, where $\phi(x) = |x|$, then $\phi$ is homomorphism.

**Example 13.11**
Let$\phi : \det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*, \phi(A) = \det(A)$ forms an homomorphism.

**Theorem 13.5**
If $G$ is an Abelian group, where $n \in \mathbb{Z}$, then $\phi : G \to G$, $\phi(a) = a^n$ is a homomorphism.

**Example 13.12**
Let $\phi : \mathbb{R}_{>0} \to \mathbb{R}, \phi(x) = \log_a(x)$ is a group homomorphism.

Note that $\phi$ is one-to-one and onto, thus $\phi$ is also an isomorphism.

**Proof.**
We need to prove that the map $\phi$ is bijective.

[one-to-one]

Note that:

$$\begin{aligned} \log_a x &= \frac{\ln x}{\ln a} \\ (\log_a x)' &= \frac{1}{x \ln a} > 0 (\because a > 1) \end{aligned}$$

Thus $\phi$ is strictly increasing, $\phi$ is one-to-one.

[Onto]

As:

$$\begin{aligned} \lim_{x \to 0} \log_a x &= -\infty \\ \lim_{x \to \infty} \log_a x &= \infty \end{aligned}$$

And $\phi$ is continuous, thus $\phi$ is onto.

**Example 13.13**
If $\phi_1 : G_1 \to G_2$ is a homomorphism, $\phi_2 : G_2 \to G_3$ is a homomorphism, then $\phi_1 \circ \phi_2 : G_1 \to G_3$ is also a homomorphism.

**Proof.**
Take $x, y \in G_1$. We want to prove that $(\phi_1 \circ \phi_2)(xy) = (\phi_1 \circ \phi_2)(x) * (\phi_1 \circ \phi_2)(y)$.
Note that:

$$\begin{aligned} \text{LHS} &= \phi_2(\phi_1(xy)) = \phi_2(\phi_1(x) * \phi_1(y)) = \phi_2(\phi_1(x)) * \phi_2(\phi_1(y)) \\ \text{RHS} &= (\phi_1 \circ \phi_2)(x) * (\phi_1 \circ \phi_2)(y) = \phi_2(\phi_1(x)) * \phi_2(\phi_1(y)) \\ &= \text{LHS} \end{aligned}$$

**Example 13.14**
Find a homomorphism

$$f : \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}$$

such that $f(2I) = 3$.

Consider:

$$\mathrm{GL}(2, \mathbb{R}) \xrightarrow{\det} \mathbb{R}^* \xrightarrow{\text{abs}} \mathbb{R}_{>0} \xrightarrow{\log_a} \mathbb{R} \left( \xrightarrow{c} \mathbb{R} \right)$$

Then $f(A) = \log_a |\det(A)|$ for some $a$. Note that

$$\begin{aligned} \log_a |\det(2I)| &= 3 \\ \log_a 4 &= 3 \\ 4 &= a^3 \\ a &= \sqrt[3]{4} \end{aligned}$$

Thus the homomorphism required is $\phi = \log_{\sqrt[3]{4}} |\det(A)|$.

**Example 13.15**
Let $C[0, 2]$ be the space of continuous function on $[0, 2]$. The integration map $\sigma : C[0, 2] \to \mathbb{R}$

$$\sigma(f) = \int_0^2 f(x)dx$$

is a linear map, so it is a homomorphism.

**Theorem 13.6**
Let $\phi : G \to G'$ be a homomorphism of groups. Then we have:

- $\phi(e) = e'$ where $e$ is the identity for $G$, while $e'$ is the identity for $G'$.
- $\phi(a^{-1}) = \phi(a)^{-1}$.
- If $H \subset G$ is a subgroup, then $\phi(H) = \{\phi(h) : h \in H\}$ is a subgroup of $G'$.
- If $H' \subset G'$ is a subgroup, $\phi^{-1}(H') = \{h \in G : \phi(h) \in H'\}$ is a subgroup of $G$.

**Proof.**
(1)

$$\begin{aligned} \because \quad ea &= a \\ \phi(ea) = \phi(e)\phi(a) = \phi(a) &= e'\phi(a) \\ \phi(e)\phi(a) &= e'\phi(a) \\ \phi(e) &= e' \end{aligned}$$

(2)

$$\begin{aligned} \because aa^{-1} &= e \\ \phi(aa^{-1}) = \phi(e) &\overset{(1)}{=} e' \\ \phi(a)\phi(a^{-1}) &= e' \\ \phi(a^{-1}) &= \phi^{-1}(a) \end{aligned}$$

(3)
If $\phi(h_1), \phi(h_2) \in \phi(H), h_1, h_2 \in H$,

$$\phi(h_1)\phi(h_2) = \phi(h_1h_2) \quad \in \quad \phi(H)$$

This proves that $\phi(H)$ is closed.

As $e \in H$, thus $e' = \phi(e) \in \phi(H)$. If $\phi(h) \in \phi(H), h \in H$, then $\phi(h)^{-1} \overset{(2)}{=} \phi(h^{-1}) \in \phi(H)$.

These properties proves that $\phi(H)$ is a subgroup.

(4)

If $h_1, h_2 \in \phi^{-1}(H')$, then $\phi(h_1), \phi(h_2) \in H'$. As $H'$ is a subgroup, thus:

$$\begin{aligned} \phi(h_1)\phi(h_2) &\in H' \\ \phi(h_1h_2) &\in H' \\ h_1h_2 &\in \phi^{-1}(H') \end{aligned}$$

This proves that $\phi^{-1}(H')$ is closed.

Note that $\phi(e) = e' \in H$, thus $e \in \phi^{-1}(H')$.

If $h \in \phi^{-1}(H')$, then $\phi(h) \in H'$. As $H'$ is a subgroup, thus $\phi(h)^{-1} \in H'$.

As $\phi(h^{-1}) = \phi(h)^{-1} \in H'$, thus $h^{-1} \in H$.

These properties proves that $\phi^{-1}(H')$ is a subgroup.

**Definition 13.4 (Kernel for linear map)**
If $T : V \to V'$ is a linear map, then $\ker(T) = T^{-1}(0)$

**Example 13.16**
Consider:

$$(*)\begin{cases} 2x_1 + 3x_2 - x_3 = 0 \\ x_1 + 4x_2 + 5x_3 = 0 \end{cases}$$

Then $T : \mathbb{R}^3 \to \mathbb{R}^2$, where

$$T\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & -1 \\ 1 & 4 & 5 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Solving $(*)$ is equivalent of finding the kernel of $T$.

**Definition 13.5**
Let $\phi^{-1}(e') = \{a \in G : \phi(a) = e'\}$ be a subgroup of $G$. Such group is called the kernel of $\phi$. Written as $\ker(\phi)$.

**Example 13.17**
Let $A : m \times n$ be a matrix, Then $A$ defines a linear map $T_A : \mathbb{R}^n \to \mathbb{R}^m$, where $T_A(v) = Av$.
Then

$$\begin{aligned} \ker(T_A) &= \{x \in \mathbb{R}^n : T_A(x) = 0\} \\ &= \{x \in \mathbb{R}^n : Ax = 0\} \\ &= \text{solution set of homogenous system } Ax = 0 \end{aligned}$$

**Theorem 13.7**
Let $\phi : G \to G'$ be a homomorphism of groups, $\ker(\phi) = H$.

Let $b \in G'$, $\phi^{-1}(b) = \{a \in G : \phi(a) = b\}$ has two cases:

- Case 0: $\phi^{-1}(b) = \emptyset$.
- Case 1: $\phi^{-1}(b) \neq \emptyset$, then let $a \in \phi^{-1}(b)$, then $\phi^{-1}(b) = aH$

**Proof.**
If case 1 does not happen, then $\phi^{-1}(b) \neq \emptyset$. Then we can find $a \in G$ such that $\phi(a) = b$.

We want to prove $\phi^{-1}(b) = aH$.

$\boxed{\phi^{-1}(b) \subseteq aH}$

For arbitrary $ah \in aH, b \in H$, then

$$\begin{aligned} \phi(ah) &= \phi(a)\phi(h) \\ &= be' \\ &= b \end{aligned}$$

this proves that $ah \in \phi^{-1}(b)$ and $\phi^{-1}(b) \subseteq aH$.

$\boxed{\phi^{-1}(b) \subseteq aH}$

For arbritary $c \in \phi^{-1}(b)$, note that

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

Thus $a^{-1} \in \ker(\phi) = H$, thus $\phi^{-1} \subset aH$.

This proves such theorem.

**Corollary 13.7.1**
A group of homomorphism $\phi : G \to G'$ is a one to one map if and only if $\ker(\phi) = \{e\}$.

**Proof.**
If $\phi$ is one to one, then $\phi(e) = e'$, this implies that $\ker(\phi) = \phi^{-1}(e') = e$.

Conversely if $\ker(\phi) = \{e\}$, then for $b \in G$, we have $\phi^{-1}(b) = \emptyset$ or equal to $a\ker(\phi) = \{a\}$.

**Corollary 13.7.2**
If $G, G'$ are finite groups, $\phi : G \to G'$ is a homomorphism, and $\phi$ is onto, then $|G'|$ is a divisor of $|G|$.

**Proof.**
Note that $\phi$ is onto, thus $\forall b \in G'$, $\phi^{-1}(b) = \emptyset$, then $\phi^{-1}(b) = aH$ for some $a \in G$, $H = \ker(\phi)$.

**Example 13.18**
Let $G = \mathbb{C}^*, G' = \mathbb{R}^*$. Then let $\phi : \mathbb{C}^* \to \mathbb{R}^*$, where $\phi(z) = |z|$. Note that $|zw| = |z||w|$, thus $\phi$ is a group homomorphism.

Then $H = \ker(\phi) = \{z \in \mathbb{C}^* : |z| = 1\} = \{z \in \mathbb{C}^* : z\bar{z} = 1\}$.

Let $\phi^{-1}(b) = \{z \in \mathbb{C}^* : |z| = b\}$, then if:

- $b < 0, \phi^{-1}(b) = \emptyset$
- $b > 0, \phi^{-1}(b) = bH$

**Theorem 13.8**
If $A : m \times n$ is a matrix, we consider the system of linear equations:

$$Ax = b \qquad (*)$$

Where $x, b$ are column vector, where $x : n \times 1, b : m \times 1$, then there are two cases:

- $(*)$ has no solution.
- If $x = a \in \mathbb{R}^m$ is a solution, then every other solution can be written as :

$$a + h_1 : h \text{ is a solution of } Ax = 0$$

**Proof.**
Since $A$ defines a linear map $T_A : \mathbb{R}^n \to \mathbb{R}^m$, $T_A(x) = Ax$. Then $T_A$ is a group homomorphism.

Then $\ker(T_A) = \{x \in \mathbb{R}^n : T_A(x) = 0\}$ = solution set of $Ax = 0$.

Solving $Ax = b$ is equivalent of finding $T_A^{-1}(b)$.

**Definition 13.6 (Normal subgroup)**
A subgroup $H$ of a group $G$ is a normal subgroup if $\forall g \in G$, $gH = Hg$

**Example 13.19**
If $G$ is abelian, then every subgroup is normal.

Consider $S_3$, let $\{e\} \in S_3$, then such group is normal. Actually for any group $G$, $\{e\}$ and $G$ are normal.

Let $H = \{e, (1,2)\} \subset S_3$, then:

$$\begin{aligned} (1,3)H &= \{(1,3),(1,2,3)\} \\ H(1,3) &= \{(1,3),(1,3,2)\} \end{aligned}$$

$H$ is thus not a normal subgroup.

**Lemma 13.9**
A subgroup $H \subset G$ is normal if and only if $\forall g \in G, b \in H$, then

$$gbg^{-1} = H$$

**Proof.**
$\boxed{\Rightarrow}$

Suppose $H$ is normal, then $gH = Hg$, then $gh \in gH = Hg$, then $gh = h'g$ for some $h' \in H$. Then:

$ghg^{-1} = h' \in H$, hence $\forall g \in G, b \in H$, $gbg^{-1} = H$.

$\boxed{\Leftarrow}$

Suppose that $ghg^{-1} \in H, \forall g \in G, b \in H$, we want to prove $H$ is normal, i.e. $gH = Hg$ for all $g \in G$.

$\boxed{gH \subset Hg}$

$\forall gh \in gH, h \in H$, we have $gh = ghg^{-1}g$, as $ghg^{-1} \in H$, thus $gh = (ghg^{-1})g \in Hg$.

Thus $gH \subset Hg$.

$\boxed{Hg \subset gH}$

$\forall hg \in Hg, h \in H$, we have $hg = gg^{-1}hg \in gH$, thus $Hg \subset gH$.

Thus $gH = Hg$. This proves that $H$ is normal.

**Example 13.20**
Prove that $A_n$ is a normal subgroup of $S_n$.

**Proof.**
Let $h \in A_n, g \in S_n$. Then consider:

- Case 0: if $g$ is even, then $g \in A_n$, then $ghg^{-1} \in A_n$.
- Case 1: if $g$ is odd, then $g^{-1}$ is also odd. Then $gh$ is odd. Thus $ghg^{-1}$ is even.

**Theorem 13.10**
If $\pi : G \to G'$ is a homomorphism, then $\ker(\pi)$ is a normal subgroup of $G$.

**Proof.**
If $h \in \ker(\pi)$, $g \in G$, then $\pi(ghg^{-1}) = \pi(g)\pi(h)\pi(g^{-1}) = \pi(g)\pi(g^{-1}) = \pi(gg^{-1}) = \pi(e) = e'$. Thus $ghg^{-1} \in \ker(\pi)$.

**Example 13.21**
Define special linear group as:

$$\mathrm{SL}(n, \mathbb{R}) = \{A \in \mathrm{GL}(n, \mathbb{R}) : \det A = 1\}$$

then $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$.

# 14 Factor Groups

**Theorem 14.1**
If $H$ is normal subgroup of $G$, let $G/H$ be the set of all left/right cosets of $H$, then:

1. Binary operation on $G/H$ defined by:

$$(aH) \cdot (bH) = (ab)H$$

   is well defined.

2. $G/H$ is a group under the binary operation in (1).

Then $G/H$ is called factor group of $G$ by $H$.

**Proof.**
(1)

If $aH = a'H, bH = b'H$, then we want to verify $(ab)H = (a'b')H$.

Because $a' \in a'H = aH$, thus $a' \in aH$. Thus $a' = ah_1$ for some $h_1 \in H$.

Similarly, $bH = b'H$ implies that $b' = bh_2$ for some $h_2 \in H$.

Thus $a'b' = abb^{-1}h_1bh_2$. Note that $H$ is normal, thus $b^{-1}h_1b \in H$, hence $b^{-1}h_1bh_2 \in H$, then $a'b' \in abH$.

$a'b' \in a'b'H \cap abH$. Therefore the intersection is non-empty, this implies that $a'b'H = abH$.

(2)

Associativity

$$\begin{aligned} ((aH)(bH))(cH) &= (abH)(cH) = (abc)H \\ (aH)((bH)(cH)) &= (aH)(bcH) = (abc)H \end{aligned}$$

Thus the associativity holds in $G/H$.

Identity

The $H$ itself is the identity element, and $H$ must exist, thus the identity element must also exist.

Inverse

The inverse is the $a^{-1}H$.

Thus $G/H$ is a group.

**Example 14.1**
Let $G = \mathbb{Z}$, and $H = 3\mathbb{Z}$. Then $ah = a + 3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ is $\{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$.

Moreover, $(a + 3\mathbb{Z}) + (b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z}$. Note that $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$.

In general, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

**Theorem 14.2**

- If $G$ is finite, then $|G/H|$ = number of cosets of $H = \dfrac{|G|}{|H|}$.
- Let $H$ be a normal subgroup of $G$, $G/H$ be the factor group of $G$ by $H$. Then the map:

  $\gamma : G \to G/H, \gamma(a) = aH$ is a homomorphism and $\ker(\gamma) = H$.
- If $\phi : G \to G'$ is a group homomorphism, then $\ker(\phi) = \{x \in G : \phi(x) = e'\}$ is a normal subgroup of $G$.

**Proof.**

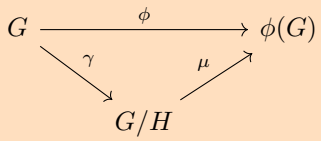
$$\begin{aligned} \gamma(ab) &= abH \\ \gamma(a)\gamma(b) &= (aH)(bH) = abH \\ \gamma(ab) &= \gamma(a)\gamma(b) \end{aligned}$$

Thus $\gamma$ must be a homomorphism.

$$\begin{aligned} \ker(\gamma) &= \{a \in G : \gamma(a) = eH\} \\ &= \{a \in G : aH = eH\} \\ &= \{a \in G : a \in H\} \\ &= H \end{aligned}$$

**Theorem 14.3 (The Fundamental Homomorphism Theorem for Groups)**
Suppose that $\phi : G \to G'$ is a group homomorphism, with $\ker(\phi) = H$, then:

- $\phi(G)$ is a subgroup of $G'$.
- $\mu : G/H \to \phi(G)$ given by $\mu(aH) = \phi(a)$ is well defined, and is isomorphism.
- $\phi = \mu \circ \gamma$. The relationship can be represented by the following diagram.



**Proof.**
We only prove the second property.

Well-defineness

If $aH = a'H$, then we want to prove $\phi(a) = \phi(a')$.

As $a' \in a'H = aH$, $a' \in aH$, $a' = ah$ for some $h \in H$.

$$\phi(a') = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)\,(h \in H = \ker(\phi))$$

This proves the well-defineness.

$\mu$ is homomorphism

Note that

$$\begin{aligned} \mu((aH)(bH)) &= \mu(abH) = \phi(ab) \\ \mu(aH)\mu(bH) &= \phi(a)\phi(b) = \phi(ab) \end{aligned}$$

Thus $\mu(aH)\mu(bH) = \mu((aH)(bH))$, thus $\mu$ is homomorphism.

$\mu$ is one-to-one

Note that $\mu$ is clearly onto.

To prove that $\mu$ is one-to-one, we prove that $\ker(\mu) = \{eH\}$.

$$\begin{aligned} aH \in \ker(\mu) \qquad & \mu(aH) = e' \\ \phi(a) = e' \qquad & a \in \ker(\phi) = H \\ aH &= H \end{aligned}$$

Thus $\ker(\mu) = \{H\}$.

**Example 14.2**
Identify the factor group of $\mathbb{C}^*/U_n$, moreover, is there any group homomorphism $\phi : \mathbb{C}^* \to G'$ where $U_n = \ker(\phi)$.

Let $\phi : \mathbb{C}^* \to \mathbb{C}^*$ be the homomorphism given by $\phi(z) = z^n$.

Note that $\ker(\phi) = \{z \in \mathbb{C}^* : \phi(z) = 1\} = \{z \in \mathbb{C}^* : z^n = 1\} = U_n$.

We claim that $\phi(\mathbb{C}^*) = \mathbb{C}^*$ (i.e. $\phi$ is onto).

For arbitrary $b \in \mathbb{C}^*$, the equation $z^n = b$ is always solvable (Fundamental theorem of algebra).

**Proof.**
Write $b = re^{i\theta}$, then $z = r^{\frac{1}{n}} e^{\frac{i\theta}{n}}$ satisfies $z^n = b$

**Theorem 14.4**
If $S \subset V$ is a subspace of vector space $V$, recall that every vector space $V$ is abelian group under the addition, and $S$ is a subgroup of $(V, +)$.

Then $V/S$ is the set of left costs of $S$, which is $\{a + s : a \in V\}$. This is the factor group of $V$ by $S$.

For every $k \in \mathbb{R}$, we can define the scalar multiplcation on $V/S$: $k(a + S) = ka + S$ is well-defined.

**Theorem 14.5 (The linear algebra version of 1st fundamental theorem for linear maps)**
If $\phi : V \to V'$ is a linear map, $S = \ker(\phi) = \{x \in V : \phi(x) = 0\}$, then $\mu : V/S \Rightarrow \phi(V')$ given by $\mu(a + V) = \phi(a)$ is well-defined, moreover, it is linear isomorphism.

**Proof.**
Note that $\dim(V/S) = \dim V - \dim S$.

If $e_1, \ldots, e_n$ is a basis for $S$, we can extend the set $\{e_1, \ldots, e_n\}$ to a basis $\{e_1, \ldots, e_n, \ldots, e_N\}$ to get a basis for $V_1$. where $\dim(V) = N$. Then $e_{n+1} + S, \ldots, e_n + S$ is a basis for $V/S$.

# 16 Group action on a set

Intuition

Consider a group $S_5$, let $X = \{1, \ldots, 5\}$ to be as set. For $\sigma \in S_5, i \in X$, applying $\sigma$ to $i$, we get $\sigma(i)$.

We then can create a map, where $(\sigma, i) \mapsto \sigma(i)$, with the following properties.

- $\sigma\tau(i) = \sigma(\tau(i))$
- $e(i) = i$

This is considered as a group action. Formal definition is given below:

**Definition 16.1 (Group Action)**
Let $G$ be a group, $X$ be a set. An group action of $G$ on $X$ is a map:

$$G \times X \to X$$

we will write the image of $(g, x)$ as $g \times x$ or $gx$, such that:

1. $ex = x, \forall x$
2. $g_1 g_2(x) = g_1(g_2(x)), \forall g_1, g_2 \in G, x \in X$

**Example 16.1**
Let $\sigma \in S_n$, and let $x \in X = \{1, \ldots, n\}$.

Then $\sigma x$ is the image of $x$ under permutation $\sigma$.

Note that $ex = x, \forall x \in X$, and $(\sigma_1\sigma_2)x = \sigma_1(\sigma_2(x))$, thus this is a action of $S_n$ on set $S$, or we say $S_n$ acts on $X$.

**Example 16.2**
If $A$ is a $2 \times 2$ matrix, then $A$ introduces a linear map from $\mathbb{R}^2 \to \mathbb{R}^2$ for $v \in \mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\}$

**Example 16.3**
Let $G = \mathrm{GL}(2, \mathbb{R})$. For any $g \in \mathrm{GL}(2, \mathbb{R})$, and $v \in \mathbb{R}^2$, $(g, v) = gv$. This is an action of $\mathrm{GL}(2, \mathbb{R})$ on $\mathbb{R}^2$.

**Proof.**
The identity element is given by $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $I_2 v = v$
Moreover, $(AB)v = A(Bv)$ as matrix multiplcation is associative.

In general, $\mathrm{GL}(n, \mathbb{R})$ acts on $\mathbb{R}^n$ with $(A, v) \mapsto Av$ by the properties of matrix multiplication.

**Example 16.4**
Let $G$ be a symmetry group of a square. Then $|G| = 8$.

Let $R_a$ be the rotation along the centre anticlockwisely by $a^\circ$.

Then when $a = 90, 180, 270$, they form symmetry, and they can form a subgroup.

Let $L_M$ be the reflexion along the axis $M$.

Then $G = \{R_0, R_{90}, R_{180}, R_{270}, L_A, L_B, L_C, L_D\}$.

$G$ acts on $V = \{1, 2, 3, 4\}$, which is the sets of vertices.

Moreover, $G$ can also acts on $E =$ set of edges.

**Theorem 16.1**
Let $G$ act on $X$. For each $x \in X$, we introduce following:

$$G_x = \{g \in G : gx = x\}$$

$G_x$ is always a subgroup of $G$. Such group $G_x$ is called the isotropy subgroup or stabilizer of $x$.

**Proof.**
Closeness

If $g_1g_2 \in G_x$, then $(g_1g_2)x = g_1(g_2x) = g_1(x) = x$, thus $g_1g_2 \in G_x$, thus $G_x$ is closed in operation.

Identity

As $ex = x$, thus $e \in G_x$, thus identity element is in the set $G_x$.

Inverse

If $g \in G_x$, then we want to prove $g^{-1}x = x$. Note that:

$$\begin{aligned} gx &= x \\ g^{-1}gx &= g^{-1}x \\ (g^{-1}g)x &= g^{-1}x \\ ex &= g^{-1}x \\ g^{-1}x &= x \end{aligned}$$

Thus $g^{-1} \in G_x$.

Thus $G_x$ is the subgroup.

**Example 16.5**
Let $G = S_5$ acts on $X = \{1, 2, 3, 4, 5\}$.

Then $G_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & a & b & c & d \end{pmatrix} : a, b, c, d \text{ is a permutation of } 2, 3, 4, 5 \right\}$. The group is isomorphic to $S_4$. Thus $|G_1| = 4! = 24$.

**Definition 16.2 (Orbit)**
Let $G$ act on $X$, $x \in X$, then define:

$$Gx = \{gx : g \in G\} \subset X$$

This is called the orbit of $x$.

Intuition

Consider an orbit system. Let $t \in \mathbb{R}$ acts on the space $\mathbb{R}^3$, and $v \in \mathbb{R}^3$.

Then $t \cdot v$ is the position of $v$ after time $t$. This forms a group action.

**Example 16.6**
Let $\mathrm{GL}(2, \mathbb{R})$ acts on $\mathbb{R}^2$, then the orbit of $\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \left\{ g \begin{pmatrix} 0 \\ 0 \end{pmatrix} : g \in \mathrm{GL}(2, \mathbb{R}) \right\} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$.

The orbit of $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} : ad - bc \neq 0 \right\} = \left\{ \begin{pmatrix} a \\ c \end{pmatrix} : ad - bc \neq 0 \right\} = \mathbb{R}^2 - \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

**Example 16.7**
Consider $G = S_5$ acts on $X = \{1, \ldots, 5\}$. Then $G1 = \{\sigma(1) : \sigma \in S_5\} = X$.
In fact, $G1 = G2 = G3 = G4 = G5 = X$.

**Theorem 16.2**
Let $G$ be a finite group, which $G$ acts on a set $X$. Then for every $x \in X$,

$$|Gx| \cdot |G_x| = |G|$$

**Proof.**
Let $G/G_x$ be the set of all left cosets of $G_x$.

Define a map $\varphi : G/G_x \to Gx$ by

$$\varphi(gG_x) = gx$$

Note that $\varphi$ is well defined, i.e.

$$g_1G_x = g_2G_x \Rightarrow g_1x = g_2x$$

Onto

$$\begin{aligned} g_1G_x = g_2G_x &\Rightarrow g_1 = g_2h, h \in G_x \\ g_1x &= (g_2h)x \\ &= g_2(hx) \\ &= g_2x (\because b \in G_x) \end{aligned}$$

Obviously $\varphi$ is a onto map.

One-to-one

Suppose:

$$\begin{aligned} \varphi(g_1G_x) &= \varphi(g_2G_x) \\ g_1x &= g_2x \\ g_2^{-1}g_1x &= g_2^{-1}g_2x = x \\ h = g_2^{-1}g_1 &\in G_x \\ g_2h = g_1 &\text{ so } g_1G_x = g_2G_x \end{aligned}$$

Hence $\varphi$ is one-to-one.

This imples $\varphi$ is a bijection.

Thus

$$\frac{|G|}{|G_x|} = |G/G_x| = |Gx| \Rightarrow |G| = |G_x||Gx|$$

**Example 16.8**
Consider a cube, where $X$ is the set of 6 faces, $G$ is the symmetry group of the cube. $G$ acts on $X$, and $X = \{1, 2, 3, 4, 5, 6\}$.
Then $G1 = X$, and as $|G_1| = 4$ (The rotation symmetry is 4), thus $|G| = 4 \times 6 = 24$.

**Example 16.9**
Consider a regular tetrahedron, let $G$ be a symmetry group, and $G$ acts on $V = \{1, 2, 3, 4\}$. Then $G1 = V$, and also $|G_1| = 3$, thus $|G| = |G_1| \times |G1| = 3 \times 4 = 12$, moreover, the group is a subgroup of $S_4$. Actually the group is exactly $A_4$.

**Example 16.10**
Consider a cube. And let $G$ be the symmetry group of the cube.

Let $F$ be the set of faces, then $|F| = 6$ and $G$ acts on $F$.

Also $G1 = F$ and $G_1 =$ set of symmetries that preserves face 1, and $|G_1| = 4$.

Then $|G| = 4 \times 6 = 24$.

Now, consider the set of vertices $V$, then $|V| = 8$ and $G$ also acts on $V$.

Then $G1 = V$. By the theorem, we have $|G| = |G_1||G1| \Rightarrow 24 = 8|G_1| \Rightarrow |G_1| = 3$.

Finally, let $E$ be the set of all edges, then $|E| = 12$ and $G$ also acts on $|E|$.

Then $G1 = E$. As $|G| = |G_1||G_1| \Rightarrow |G_1| = 2$.

**Proposition 16.1**
If $G$ acts on $X$, then:

- If $x_1, x_2 \in X$, then $Gx_1 = Gx_2$ or $Gx_1 \cap Gx_2 = \emptyset$.
- $X$ is a disjoint union of orbits.

**Example 16.11**
Let GL(2.$\mathbb{R}$) acts on $\mathbb{R}^2$. Then $\{0\}$ is an orbit, and $\mathbb{R}^2 \backslash \{0\}$ is also an orbit. Then

$$\mathbb{R}^2 = \{0\} \sqcup \mathbb{R}^2 \backslash \{0\}$$

Let $U = \{z \in \mathbb{C} : |z| = 1\}$, then $U$ acts on $\mathbb{C}$ by

$$za : z \in U_1, a \in \mathbb{C}$$

Then convert $U$ as polar form, we have $U = \{e^{i\theta} : \theta \in [0, 2\pi)\}$.

Note that $|za| = |z||a| = |a|$. Thus the orbit $Ua$ is a circle centered at origin, with radius of $|a|$.

# 18 Ring and Fields

**Definition 18.1 (Ring)**
A ring is a set $R$ with an addition and a multiplcation following the axioms below:

1. $(R, +)$ is an abelian **group**.
2. $\times$ is associative. i.e. $(a \times b) \times c = a \times (b \times c), \forall a, b, c \in R$.
3. Distributive law holds. i.e.

$$\begin{aligned}(a+b) \times c &= a \times c + b \times c \\ c \times (a+b) &= c \times a + c \times b\end{aligned}$$

$\forall a, b, c \in R$

**Example 18.1**
For a positive integer $n$, let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Define $+$ as the modulo $n$ addition, and $\times$ as the modulo $n$ multiplcation.

Then $(\mathbb{Z}_n, +, \times)$ is a ring, and it is finite.

Consider $\mathbb{Z}_9 = \{0, \ldots, 8\}$. Then $7 \times 8 = 56 = 2$.

**Definition 18.2 (Commutative ring)**
A ring $R$ is a commutative ring, if the multiplcation is commutative. i.e.

$$ab = ba$$

$\forall a, b \in \mathbb{R}$.

**Example 18.2**
For each $n \geq 2$, let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices. On $M_n(\mathbb{R})$ we have matrix addition and matrix multiplcation.

Then $M_n(\mathbb{R})$ is a ring under $+$ and $\times$.

However, such ring is not a commutative ring.

**Example 18.3**
Consider $C(\mathbb{R})$ be the space of all continuous functions on $\mathbb{R}$.

Define $+$ to be function addition, and $\times$ to be function multiplcation.

Then $C(\mathbb{R})$ is a ring.

Let $C^\infty(\mathbb{R})$ be the function on $\mathbb{R}$ that has derivative of all order, then it is also a ring.

Moreover, $C^\infty(\mathbb{R}) \subset C(\mathbb{R})$. For example, take $f = |x|$, then $f \in C(\mathbb{R})$, but $f \notin C^\infty(\mathbb{R})$.

**Example 18.4**
If $R_1, \ldots, R_n$ are rings, then the product set $R_1 \times \cdots \times R_n$ is a ring under $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$, and $(a_1, \ldots, a_n) \times (b_1, \ldots, b_n) = (a_1 \times b_1, \ldots, a_n \times b_n)$.

**Theorem 18.1**
If $R$ is a ring, with additive identity 0, and for $a \in R$, we denote its inverse in additive group by $-a$. Then:

- $(0a) = (a0) = 0$
- $a(-b) = (-a)b = -(ab)$
- $(-a)(-b) = ab$

**Proof.**

1. Note that:

$$\begin{aligned} 0a &= (0+0)a \\ &= 0a + 0a \\ 0a &= 0 \end{aligned}$$

   The case $a0 = 0$ can be proved similarly.

2. Note that:

$$\begin{aligned} a(-b) + ab &= a(-b+b) \\ &= a0 \\ &= 0 \\ a(-b) &= -ab \end{aligned}$$

   The case $-a(b) = a(-b)$ can be proved similarly.

3.

$$\begin{aligned} (-a)(-b) + a(-b) &= (-a+a)(-b) \\ &= 0(-b) \\ &= 0 \\ (-a)(-b) - ab &= 0 \\ (-a)(-b) &= ab \end{aligned}$$

**Definition 18.3 (Ring homomorphism)**
Let $R, R'$ be two rings, Define $\phi : R \to R'$ is called a ring homomorphism if:

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \end{aligned}$$

**Example 18.5**
The map $\phi : \mathbb{Z} \to \mathbb{Z}_3$, $\phi(n) = \begin{cases} 0 & \text{, if } n \text{ is a multiple of 3} \\ 1 & \text{, if } n \text{ has remainder 1 divided by 3} \\ 2 & \text{, if } n \text{ has remainder 2 divided by 3} \end{cases}$ gives a homomorphism.

**Example 18.6**
For arbitrary positive integer $n$, $\phi : \mathbb{Z} \to \mathbb{Z}, \phi(a) = a \bmod n$ is a ring homomorphism.

**Example 18.7**
Let $\phi : \mathbb{R} \to M_2(\mathbb{R}), \phi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2$ gives a ring homomorphism, where $I_2$ is the identity for $2 \times 2$ matrix.

**Proof.**

$$\begin{aligned} \phi(a+b) &= \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \\ &= \phi(a) + \phi(b) \\ \phi(ab) &= \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \\ &= \phi(a)\phi(b) \end{aligned}$$

Thus $\phi$ gives a ring homomorphism.

**Example 18.8**
Let $\phi : \mathbb{C} \to M_2(\mathbb{R})$. Imagine $\mathbb{C}$ to be a $2-$dim vector space over $\mathbb{R}$.

Then we can represent $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. Then it has a basis of $1, i$ over $\mathbb{R}$.

Consider a map: $\mathbb{C} \to \mathbb{C}, z \mapsto (a+bi)z$ is a linear map.

Define $T_{a+bi}(z) = (a+bi)z$. Then $T$ is a linear transformation.

Note that

$$\begin{aligned} T_{a+bi}(1) &= a + bi \\ T_{a+bi}(i) &= -b + ai \end{aligned}$$

Then the matrix for $T_{a+bi} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Then $\phi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ is a ring homomorphism.

**Proof.**
Trivial (Actually I don't want to type but it should be trivial for our reader right 😝)

**Definition 18.4 (Ring isomorphism)**
An isomorphism $\phi : R \to R'$ from ring $R$ to ring $R'$ is a homomorphism that is bijective.

**Example 18.9**
Let $\phi : \mathbb{C} \to A$, where $A = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a ring, and $\phi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ gives a ring **isomorphism**.

**Definition 18.5 (Ring with unity and Unit)**
A ring $R$ with multiplcative identity element (unity) is a ring with unity. It is usually denoted by 1, which satisfies $1 \times a = a \times 1 = a, \forall a \in R$.

Let $R$ be a ring with unity 1, suppose that $1 \neq 0$, an element $u$ is called a unit (Invertible element) if there is $u' \in R$ such that $uu' = u'u = 1$.

Why $1 \neq 0$?

In a ring $R$ with unity 1, and $1 = 0$, then $0a = 0 = 1a = a$. This imples $R$ is trivial, i.e. $R = \{0\}$.

**Example 18.10**
$\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, M_n(\mathbb{R}), \mathbb{Z}_n$ all are ring with unity. However, $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ is a ring, without unity.

**Example 18.11**
Consider the ring $\mathbb{Z}$, only $1, -1$ are units.

**Example 18.12**
For $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, all nonzero elements are units.

**Example 18.13**
For $M_n(\mathbb{R})$, all invertible matrices are units.

**Example 18.14**
For $C[0,1]$, $f$ is a unit if and only if $f(a) \neq 0, \forall a \in [0,1]$.

**Definition 18.6 (Division Ring and Field)**
Let $R$ be a ring with unity 1, we call $R$ a division ring if every nonzero element $a \in R$ is a unit.

A commutative division ring is called a field.

Also, a field can be defined as following, with $R$ being a ring:

- $R$ is commutative.
- $R$ has a unity 1.
- For all $a \in R, a \neq 0, a^{-1}$ exists.

**Example 18.15**
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. However, $\mathbb{Z}$ is not a field since only $\{1, -1\}$ are units. For most of the element, the inverse does not exist.

# 19 Integral Domains

Intuition

In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, if $a \neq 0, b \neq 0$, then $ab \neq 0$. However, consider the following example:

**Example 19.1**
In $\mathbb{Z}_{10}, 4 \neq 0, 5 \neq 0$. However, $4 \times 5 = 20 = 0$.

**Definition 19.1 (Zero divisor)**
Let $R$ be a commutative ring. $a \in R$ is called a zero divisor if $a \neq 0$, and there is $b \neq 0, ab = 0$.

**Example 19.2**
In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, there are no zero divisors.

**Example 19.3**
Consider $\mathbb{Z}_{10} = \{0, \ldots, 9\}$. The zero divisors are $2, 4, 5, 6, 8$.

**Theorem 19.1**
If $R$ is a commutative ring with unity $1, 1 \neq 0$, suppose $u \in R$ is a unit, then $u$ is not a zero divisor.

**Proof.**
Assume that $u$ is a zero divisor. Then $\exists b \in R, b \neq 0, ub = 0$. Then:

$$\begin{aligned} u^{-1}ub &= u^{-1}0 \\ b &= 0 \end{aligned}$$

Given that $b \neq 0$, this leads to a contradiction.

**Example 19.4**
Consider $C[0,1]$, let:

$$f(x) = \begin{cases} 0 & , x \in \left[0, \frac{1}{2}\right] \\ x - \frac{1}{2} & , x \in \left[\frac{1}{2}, 1\right] \end{cases} \quad \text{and} \quad g(x) = \begin{cases} \frac{1}{2} - x & , x \in \left[0, \frac{1}{2}\right] \\ 0 & , x \in \left[\frac{1}{2}, 1\right] \end{cases}$$

Then $f(x)g(x) = 0$. i.e. $f, g$ are zero divisor of $C[0,1]$.

**Definition 19.2 (Integral domain)**
A ring $D$ is a integral domain, if it satisfies:

1. $D$ is a commutative ring.
2. $D$ has a nonzero unity 1.
3. $D$ has no zero divisors.

**Example 19.5**
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are integral domains.

**Example 19.6**
$C[0,1]$ is not integral domain.

**Example 19.7**
$\mathbb{Z}_{10}$ is not a integral domain.

**Theorem 19.2**
if $n$ is not prime number, then $\mathbb{Z}_n$ is not a integral domain.

**Proof.**
If $n$ is not prime number, then $\mathbb{Z}_n$ is not a integral domain.

If $n$ is not a prime number, then $n = ab$ where $a \in (0, n), b \in (0, n)$.

Then $a \neq 0, b \neq 0, ab = n = 0$, thus $a, b$ are zero divisors.

If $p$ is a prime number, then $\mathbb{Z}_p$ is a integral domain.

Let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, if $a, b \in \mathbb{Z}_p, a \neq 0, b \neq 0, ab = 0$, then the usual product $ab$ is a multiple of $p$.

This imples that one of $a, b$ is a multiple of $p$. This contradicts to $a \neq 0$ and $b \neq 0$ in $\mathbb{Z}_p$.

**Theorem 19.3**
Every field is an integral domain.

**Proof.**
Suppose $F$ is a field, If $F$ has zero divisor, then for some $a \neq 0, b \neq 0, ab = 0$.

As $a \neq 0$, and $F$ is a ring, thus $a^{-1}$ exists. Hence

$$\begin{aligned} ab &= 0 \\ a^{-1}ab &= 0 \\ b &= 0 \end{aligned}$$

Which leads to contradiction.

This implies that $F$ has no zero-divisors. So $F$ is a integral domain.

From this we can see the following relation:

$$\text{rings} \supset \text{commutative rings} \supset \text{integral domains} \supset \text{fields}$$

**Theorem 19.4**
If $R$ is a commutative ring, $a \neq 0$, $a$ is not a zero-divisor, then we have

$$ab = ac \implies b = c$$

**Proof.**

$$\begin{aligned} ab = ac &\Rightarrow ab - ac = 0 \\ &\Rightarrow a(b-c) = 0 \\ &\Rightarrow (b-c) = 0 \\ &\Rightarrow b = c \end{aligned}$$

as $a$ is not a zero-divisor.

**Theorem 19.5**
Every **finite** integral domain $D$ is a field.

**Proof.**
Assume that, for $a \in D$, we need to prove $a^{-1}$ exists for any $a \neq 0$.

We list all element in $D$ :

$$D = \{0, 1, a_2, \ldots, a_n\}$$

where $|D| = n + 1$.

Consider the following list

$$\{a0, a1, aa_2, \ldots, aa_n\}$$

As $ab = ac \Rightarrow b = c$ thus the list is distinct. Therefore there is $a_i$, where $i \in [1, n]$, s.t. $aa_i = 1$.

**Corollary 19.5.1**
If $p$ is prime, then $\mathbb{Z}_p$ is a field.

# 20 Fermat's and Euler's Theorem

**Theorem 20.1 (Fermat's theorem)**
If $p$ is prime, $a \in \mathbb{Z}$, then $a^p - a$ is a multiple of $p$.

**Proof.**
If $a = 0$, then $a^p - a = 0$ is a multiple of $p$.

If $a$ is a negative number, then $n$ is positive. We then have:

$$\begin{aligned} a^p - a &= (-n)^p - (-n) \\ &= -n^p + n \\ &= -(n^p - n) \end{aligned}$$

So we can reduce the case where $a$ is negative to $a$ is positive.

Now we prove by induction.

Let $a = 1$, then

$$a^p - a = 0$$

The result holds.

Now suppose for $a = n$, the result holds. Then for $a = n + 1$, we have:

$$\begin{aligned} a^p - a &= (n+1)^p - (n+1) \\ &= \sum_{j=0}^{p} \binom{p}{j} n^j - (n+1) \\ &= \sum_{j=1}^{p-1} \binom{p}{j} n^j + \binom{p}{0} n^0 + \binom{p}{p} n^p - (n+1) \\ &= \sum_{j=1}^{p-1} \binom{p}{j} n^j + n^p - n \end{aligned} \tag{1}$$

By induction assumption, we have $n^p - n$ is a multiple of $p$.

For $j \in [1, p-1]$, we have $\binom{p}{j} = \dfrac{p!}{j!(p-j)!}$.

Note that $p$ is prime, therefore $p$ is not a divisor of $j!(p-j)! = (1 \times 2 \times \cdots \times j)(1 \times 2 \times \cdots \times (p-j))$.

Thus $\binom{p}{j}$ is a multiple of $p$. So (1) is a multiple of $p$.

The results holds for $a = n + 1$.

**Example 20.1**
Let $a = 3, p = 5$, then $3^5 - 3 = 240$ and it is multiple of 5.

**Theorem 20.2 (Equivalent Formulation of Fermat's Theorem)**
If $p$ is a prime, $a$ is **NOT** a multiple of $p$, then $a^{p-1}-1$ is a multiple of $p$.

**Proof.**
Note that

$$a^p - a = a(a^{p-1}-1)$$

As $a$ is not a multiple of $p$, therefore $a^{p-1}-1$ must be a multiple of $p$.

Conversely, we have:

$$a(a^{p-1}-1) = a^p - a$$

As $a^{p-1}-1$ is a multiple of $p$, it follows that $a^p - a$ must be a multiple of $p$.

**Definition 20.1 (Euler's phi function)**
Define $\varphi(n)$ for some positive integer $n$, where it satisfies:

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(mn) &= \varphi(m)\varphi(n) \\ \varphi(p^k) &= p^k - p^{k-1} \end{aligned}$$

For some relatively prime $m, n$, and prime power $p^k (p \in \mathbb{P}, k \geq 1)$

**Example 20.2**

$$\begin{aligned} \varphi(300) &= \varphi(3)\varphi(2^2)\varphi(5^2) \\ &= (3-1)(2^2-2)(5^2-5) \\ &= 80 \end{aligned}$$

**Theorem 20.3 (Euler's Theorem)**
For $n \in \mathbb{Z}_{>0}$, if $a$ is relatively prime to $n$, then $a^{\varphi(n)-1}$ is a multiple of $n$.

Moreover, if $n = p$ is a prime, then $\varphi(p) = p-1$, hence $a^{p-1}-1$ is a multiple of $p$.

**Proof.**
We consider $a$ as an element in $Z_n$, since $a$ is relatively prime to $n$, $a \in G_n$. By the corollary of Lagrangian Theorem, $a^{|G_n|} = 1$ in $G_n$, so $a^{\phi(n)-1}$ is a multiple of $n$.

# 21 The Field of Quotients of an Integral Domain

We first recall some previous knowledges.

**Definition 21.1 (Integral domain)**
A ring $D$ is a integral domain, if it satisfies:

1. $D$ is a commutative ring.
2. $D$ has a nonzero unity 1.
3. $D$ has no zero divisors.

**Theorem 21.1**
If $F$ is a field, then $F$ is a integral domain. However the converse may not be correct.

But if $R$ is integral domain, and $R$ is finite, then $R$ is a field.

**Example 21.1**
We want to produce more example where a ring is an integral domain.

Consider $A = \mathbb{Z} \times \mathbb{Z}$.

$A$ is commutative. It contains an unit of $(1,1) \neq (0,0)$. Consider $(1,0) \times (0,1) = (0,0)$. Therefore there is zero divisors.

By the definition, $\mathbb{Z} \times \mathbb{Z}$ is not a integral domain. 😮

**Theorem 21.2**
Let $F$ be a field, $R \subset F$ is a subring. If $1 \in R$, then $R$ is an integral domain.

**Proof.**
(1) $R$ is commutative obviously.

(2) $R$ contains an unity, by definition.

(3) If $a, b \in R$, $a \neq 0, b \neq 0, ab = 0$, because $F$ is a field, therefore $a^{-1}$ exists. Multiplying $a^{-1}$ on both side, we have:

$$\begin{aligned} a^{-1}ab &= a^{-1}0 \\ b &= 0 \end{aligned}$$

Contradiction!

**Example 21.1 (Continued)**
Let's consider the following with the help of above theorem.

Let $F = \mathbb{C}$ be a field.

Then $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are subrings of $F$.

Define $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}$. It is called the ring of Gaussian integers. Then we have:

$$\begin{aligned}(m + ni) + (m' + n'i) &= (m + m') + (n + n')i \\ (m + ni)(m' + n'i) &= (mm' - nn') + (mn' + nm')i\end{aligned}$$

Therefore the operation is closed, and moreover, we have $-(m + ni) = (-m) + (-n)i$ is the addition inverse in $\mathbb{Z}[i]$.

Finally, we have $1 + 0i = 1 \in \mathbb{Z}[i]$. Therefore there is unity in $\mathbb{Z}[i]$.

Therefoe $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ containing 1. Therefore it is an integral domain.

Note that:

$$5 = (2 + i)(2 - i)$$

Therefore 5 is not a prime in $\mathbb{Z}[i]$. However, 7 and 3 are prime in $\mathbb{Z}[i]$.

**Example 21.2**
For arbitrary positive integer $d$, define

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{m + n\sqrt{d} : m, n \in \mathbb{Z}\right\}$$

is a subring of $\mathbb{R}$.

Note that:

$$\begin{aligned}\left(m + n\sqrt{d}\right)\left(m' + n'\sqrt{d}\right) &= mm' + mn'\sqrt{d} + nm'\sqrt{d} + nm'\sqrt{d}^2 \\ &= (mm' + dnm') + (mn' + nm')\sqrt{d}\end{aligned}$$

and $1 \in \mathbb{Z}\left[\sqrt{d}\right]$, therefore $\mathbb{Z}\left[\sqrt{d}\right]$ is a subring of $\mathbb{R}$. $\mathbb{Z}\left[\sqrt{d}\right]$ is a integral domain.

**Example 21.3**

Define $A = \left\{ m + nd^{\frac{1}{3}} : m, n \in \mathbb{Z} \right\}$.

Note it is closed under $+$.

And

$$\left(m + nd^{\frac{1}{3}}\right)\left(m' + n'd^{\frac{1}{3}}\right) = \left(mm' + nm'd^{\frac{2}{3}}\right)(mn' + nm')d^{\frac{1}{3}}$$

Note that $d^{\frac{2}{3}}$ is not in $A$. Therefore $A$ is not a subring.

However, if we modify the condition s.t.

$$A = \left\{ m + nd^{\frac{1}{3}} + pd^{\frac{2}{3}} : m, n, p \in \mathbb{Z} \right\}$$

then $A$ is a subring.

**Example 21.4**

Define $A = \left\{ \frac{b}{3^m} : b \in \mathbb{Z}, m \geq 0 \right\}$. We have

$$\begin{aligned} \frac{b_1}{3^{m_1}} + \frac{b_2}{3^{m_2}} &= \frac{b_1 3^{m_2} + b_2 3^{m_1}}{3^{m_1+m_2}} \\ \frac{b_1}{3^{m_1}} \times \frac{b_2}{3^{m_2}} &= \frac{b_1 b_2}{3^{m_1+m_2}} \end{aligned}$$

Therefore the operation is closed under $+, \times$.

Note that $\mathbb{Z} \subsetneq A \subsetneq \mathbb{Q}$. For example, $\frac{1}{2} \notin A$.

Given an integral domain $D$, we want to prove a field $F$ such that

1. $D \subset F$
2. $F$ is as small as possible

We can do the following:

Consider $D = \mathbb{Z}$, $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z}^* \right\}$.

Let $\hat{F} = \{(a, b) : a \in D, b \in D^*\}$. Think of $(a, b)$ as $\frac{a}{b}$. We define $+, \times$ on $\hat{F}$, where

$$\begin{aligned} (a_1, b_1) + (a_2, b_2) &= (a_1 b_2 + a_2 b_1, b_1 b_2) \\ (a_1, b_1)(a_2, b_2) &= (a_1 a_2, b_1 b_2)\,(b_1 b_2 \neq 0, \forall b_1, b_2 \neq 0 \text{ as integral domain}) \end{aligned}$$

Then $+, \times$ are both commutative and associative.

We have $(0, 1)$ be the additive identity element, while $(1, 1)$ is the multiplicative identity element.

However, we notice that

$$\begin{aligned}[(a_1,b_1)+(a_2,b_2)](c,d) &= ((a_1b_2+a_2b_1)c, b_1b_2d)\\ (a_1,b_1)(c,d)+(a_2,b_2)(c,d) &= (a_1cb_2d+b_1da_2c, b_1b_2dd)\\ [(a_1,b_1)+(a_2,b_2)](c,d) &\neq (a_1,b_1)(c,d)+(a_2,b_2)(c,d)\end{aligned}$$

Our assumption fails. We need to modify our addition and multiplication.

We define an equivalence relation on $\hat{F}$,

$$(a,b)\sim(a',b') \text{ if and only if } ab'=ba'$$

We want to prove $\sim$ is an equivalence relation.

**Lemma 21.3**
$\sim$ is an equivalence relation on $\hat{F}$.

**Proof.**

- Reflexive: $(a,b)\sim(a,b)$ since $ab=ba$ as the multiplication in $D$ is commutative.
- Symmetric: If $(a,b)\sim(c,d)$, then $ad=bc$. Since multiplcation in $D$ is commutative, therefore $cb=da$, consequently $(c,d)\sim(a,b)$.
- Transitive: If $(a,b)\sim(c,d)$ and $(c,d)\sim(r,s)$, then $ad=bc$ and $cs=dr$. Using these relations and the fact that multiplcation in $D$ is commutative, we have:

  $$asd=sad=sbc=bcs=bdr=brd$$

  Now $d=0$ and $D$ is an integral domain, therefore cancellation law holds. From $asd=brd$, we have $as=br$. Thus $(a,b)\sim(r,s)$.

Followed by that, we want to define additions and multiplications for $F$, where $F$ is the set of equivalence classes of $\hat{F}$.

**Lemma 21.4**
Define the addition and multiplcation on $\hat{F}$ as:

$$\begin{aligned}(a,b)+(c,d) &= (ad+bc,bd)\\ (a,b)*(c,d) &= (ac,bd)\end{aligned}$$

the equation above give well-defined operations of addition and multiplication on $\hat{F}$.

After checking two lemmas above, $+,\times$ on $\hat{F}$ decends to $+,\times$ on $F$.

**Lemma 21.5**
$(F,+,\times)$ is a field.

**Lemma 21.6**
$F$ can be regarded as containing $D$.

With such lemma above, we have the following theorem.

**Theorem 21.7 (Field of quotients)**
Any integral domain $D$ can be enlarged to (or embedded in) a field $F$ such that every element of $F$ can be expressed as a quotient of two elements of $D$. (Such a field $F$ is a field of quotients of $D$.)

For a more detailed proof of this section, please refer to the textbook P.190.

# 26 Homomorphism and Factor Rings

**Definition 26.1 (Ring Homomorphism)**
Let $R$ and $R'$ be rings. A map $\phi : R \to R'$ is called ring homomorphism if

$$\begin{aligned} \phi(a+b) &= \phi(a)+\phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \end{aligned}$$

for any $a, b \in R$.

**Example 26.1**
Let $\phi : \mathbb{C} \to \mathbb{C}$, $\phi \mapsto \bar{z}$ gives an homomorphism.

**Theorem 26.1**
If $\phi : \mathbb{Q} \to \mathbb{Q}$ is a ring homomorphism, then either $\phi(x) = x$ or $\phi(x) = 0$ for all $x \in \mathbb{Q}$.

**Proof.**

$$\begin{aligned} 1 \times 1 &= 1 \\ \phi(1 \times 1) &= \phi(1) \\ \phi(1)^2 &= \phi(1) \\ \phi(1) = 0 \quad &\text{or} \quad \phi(1) = 1 \end{aligned}$$

If $\phi(1) = 0$, then

$$\begin{aligned} \phi(x) &= \phi(1 \times x) \\ &= \phi(1)\phi(x) \\ &= 0 \end{aligned}$$

If $\phi(1) = 1$, then

$$\begin{aligned} \phi(2) &= \phi(1+1) \\ &= 2 \end{aligned}$$

For any positive integer $n$, we have $n = 1 + \cdots + 1 \Rightarrow \phi(n) = \phi(1 + \cdots + 1) = n\phi(1) = n$.

If $n$ is negative, we have $\phi(-n) = -\phi(n) = -n$.

**Example 26.2**
If $R_1, \ldots, R_n$ are rings, then $R_1 \times \cdots \times R_n$ is the product ring.
For each $i \in [1, n]$, consider projection map $\pi_i : R_1 \times \cdots \times R_n \to R_i$, $\pi_i(a_1, \ldots, a_n) = a_i$ is a ring homomorphism.

**Example 26.3**
$\pi : \mathbb{Z} \to \mathbb{Z}_n$, where $\pi(a) = a \mathrm{mod} n$ is a ring homomorphism.

**Example 26.4**
Consider $\phi : C[0,7] \to \mathbb{R}$, $\phi(f) = f(3)$ is a ring homomorphism. In general, $\phi(f) = f(l)$ for any $l \in [0,7]$ is a ring homomorphism.

**Example 26.5**
$\phi : \mathbb{R} \to M_2(R)$, where $\phi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ is a ring homomorphism.

**Proof.**

$$\begin{aligned} \phi(a+b) &= \begin{bmatrix} a+b & 0 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \\ &= \phi(a) + \phi(b) \\ \phi(ab) &= \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \\ &= \phi(a)\phi(b) \end{aligned}$$

**Theorem 26.2**
If $\phi : R \to R', \varphi : R' \to R''$ are ring homomorphism, then their composition:

$$\phi \circ \varphi : R \to R''$$

is also a ring homomorphism.

**Example 26.6**
If $R$ is a ring with unity 1, $a \in R$ is an multiplcative invertible element.

Define a map $\phi : R \to R, \phi(x) = axa^{-1}$ is a ring homomorphism.

**Definition 26.2 (Subring)**
If $R$ is a ring, a nonempty subset $S \subset R$ is called a subring if $S$ is closed under addition and multiplication, and $S$ is a ring under $+$ and $\times$.

**Example 26.7**
$\mathbb{Z}$ is a subring of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

**Proof.**
If a set $S$ is closed under addition and multiplication, to check $S$ is a subring, it is enough to check 0 is in $S$ and $a \in S \Rightarrow -a \in S$, since associativity holds if $R$ is a ring. Distributive law also holds, given that $R$ is a ring.

**Theorem 26.3**
Let $\phi : R \to R'$ is a ring homomorphism, then:

1. $\phi(0) = 0'$
2. $\phi(-a) = -\phi(a), \forall a \in R$
3. If $S \subset R$ is a subring, then $\phi(S)$ is a subring of $R'$.
4. If $S' \subset R'$ is a subring, then $\phi^{-1}(S')$ is a subring of $R$.
5. Do note that $\phi(a^{-1}) \neq \phi(a)^{-1}$

**Proof.**
Because $\phi(a+b) = \phi(a) + \phi(b)$ implies that $\phi : R \to R'$ is an group homomorphism of additive group, therefore (1),(2) are true.

(3),(4) are left as exercise.

**Definition 26.3 (Kernel)**
Let $\phi : R \to R'$ be a ring homomorphism. Then

$$\phi^{-1}(0') = \{a \in R : \phi(a) = 0'\}$$

is called the kernel of $\phi$. It is written as $\ker(\phi)$.

**Theorem 26.4**
$\ker(\phi)$ is a subring of $R$.

**Example 26.8**
Consider $\phi : C[0,7] \to \mathbb{R}$, $\phi(f) = f(3)$ is a ring homomorphism. Moreover, the kernel is given by:

$$\ker(\phi) = \{f \in C[0,7] : f(3) = 0\}$$

**Definition 26.4 (Ideal)**
Let $R$ be a ring, a subset $I \subset R$ is called an ideal, if:

1. $I$ is a subgroup of $(R, +)$
2. For all $a \in R, b \in I$, then $ab \in I, ba \in I$

Note that an ideal is a subring, however the converse might be false.

**Example 26.9**
For any integer $n$, we have $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

**Proof.**
1. $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.

2. If $a \in \mathbb{Z}, b \in n\mathbb{Z}, b = nc, c \in \mathbb{Z}$, then $ab = a(nc) = n(ac) \in \mathbb{Z}$.

**Lemma 26.5**
If $\phi : R \to R'$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of $R$.

**Proof.**
Since $\phi$ is an additive group homomorphism from $R \to R'$, thus $\ker(\phi)$ is an additive subgroup of $R$.

If $a \in R, b \in \ker\phi$, we want to prove that $ab \in \ker(\phi)$ and $ba \in \ker(\phi)$.

Check:

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \\ &= \phi(a)0' \\ &= 0' \\ \phi(ba) &= \phi(b)\phi(a) \\ &= 0'\phi(a) \\ &= 0' \end{aligned}$$

$\ker(\phi)$ is therefore an ideal of $R$.

**Theorem 26.6**
Let $I$ be an ideal of $R$, let $R/I$ be the set of coset $a + I$. Define $+$ and $\times$ on $R/I$ as follow:

$$\begin{aligned} (a+I)+(b+I) &= (a+b)+I \\ (a+I)(b+I) &= ab+I \end{aligned}$$

(Proof of multiplication is well-defined)

**Proof.**
For $a + I = a' + I, b + I = b' + I$, then we have $ab + I = a'b' + I$. To prove $ab + I = a'b' + I$, we may prove $ab - a'b' \in I$.

Note that:

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= (a - a')b + a'(b - b') \end{aligned}$$

as $a - a', b - b' \in I$, therefore, $(a - a')b \in I$ and $a'(b - b') \in I$, and as addition is closed in $I$, the proof is complete.

**Theorem 26.7**
Let $I$ be an ideal of the ring $R$, then $R/I$ is a ring under addition and multiplication defined as above.

The ring $R/I$ is called the factor ring of $R$ by $I$.

**Example 26.10**
Let $10\mathbb{Z}$ be an ideal of $\mathbb{Z}$.

Then $\mathbb{Z}/10\mathbb{Z} = \{0 + 10\mathbb{Z}, \ldots, 9 + 10\mathbb{Z}\} = \{0, 1, \ldots, 9\} = \mathbb{Z}_{10}$

**Theorem 26.8 (Fundamental homomorphism theorem for Rings)**
If $\phi : R \to R'$ is a ring homomorphism with $\ker(\phi) = N$, then the map given by $\mu : R/N \to \phi(R')$

$$\mu(a + N) = \phi(a)$$

is well defined and is isomorphism of rings.

The following topics are extra topics that **WILL NOT** appear in final exam.

In the following, we will talk about:

- Jordan Canonical form of square matrices over $\mathbb{C}$
- Polynomial Rings
- Famous impossibility theorems

# 27 Add. Topic 1. Jordan Canonical Forms of Square Matrices

**Definition 27.1 (Similar matrices)**
Two $n \times n$ matrices $A$ and $B$ are said to be similar, if there is $n \times n$ invertible matrices $T$, s.t

$$B = TAT^{-1}$$

**Example 27.1**
$\mathrm{GL}(n, \mathbb{R})$ acts on $M_n(\mathbb{R})$ by $g * A = gAg^{-1}$.
Thus we can claim that $A, B$ are similar, if $A, B$ are in the same orbit.

**Theorem 27.1**
If $A, B$ are similar, then $|A| = |B|$

**Proof.**

$$\begin{aligned} \det(B) &= \det(TAT^{-1}) \\ &= \det(T)\det(A)\det(T^{-1}) \\ &= \det(TT^{-1})\det(A) \\ &= \det(A) \end{aligned}$$

However, the converse may not be true. For example, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$ are not similar.

**Proof.**

$T \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} T^{-1} = TT^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, therefore $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is only similar to itself.

**Theorem 27.2**
If $A$ and $B$ are similar, then their characteristic polynomial are equal.

Note that characteristic polynomial is defined by $|xI_n - A|$ for any $n \times n$ matrix $A$.

**Proof.**
,

$$\begin{aligned} \mathrm{char}(B) &= \det(xI_n - B) \\ &= \det(xI_n - TAT^{-1}) \\ &= \det(T(xI_n - A)T^{-1}) \\ &= \det(xI_n - A) \\ &= \mathrm{char}(A) \end{aligned}$$

**Theorem 27.3**
If $|xI_n - A| = |xI_n - B|$, then $A$ may not be necessarily similar to $B$.

**Proof.**
Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, B = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$, then $|A| = |B| = 4$. However,

$$\begin{aligned} |A - xI| &= \begin{vmatrix} 2-x & 0 \\ 0 & 2-x \end{vmatrix} = (2-x)^2 \\ |B - xI| &= \begin{vmatrix} 2-x & 1 \\ 0 & 2-x \end{vmatrix} = (2-x)^2 \end{aligned}$$

If $A, B$ are similar, then

$$\begin{aligned} B &= TAT^{-1} \\ &= T(2I)T^{-1} \\ &= 2I \\ &= A \end{aligned}$$

Therefore $A$ is only similar to itself. Contradition!

**Theorem 27.4**
If $F$ is a field, then we can define $m \times n$ matrix over $F$, with entries are in $F$.

**Example 27.2**
For example, we can have complex matrices like $\begin{bmatrix} 1+i & 0 \\ 2 & i \end{bmatrix}$.

If $A, B$ are complex matrices, $A, B$ are said to be similar if there is $n \times n$ invertible complex matrices $T$, s.t.

$$TAT^{-1} = B$$

**Example 27.3**
The matrix

$$A = \begin{pmatrix} \cos 30^\circ & -\sin 30^\circ \\ \sin 30^\circ & \cos 30^\circ \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

is **not** diagonalizable over $\mathbb{R}$. However, it is diagonalizable over $\mathbb{C}$.

**Example 27.4**
The matrix

$$B = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$$

is **not** diagnoalizable even over $\mathbb{C}$.

**Proof.**
Suppose it is diagonalizable. Then

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = T \begin{bmatrix} \lambda_1 & \\ & \lambda_2 \end{bmatrix} T^{-1}$$

Note that the matrix has eigenvalue with multiplicity 2, and $\begin{bmatrix} \lambda_1 & \\ & \lambda_2 \end{bmatrix}$ has eigenvalues of $\lambda_1, \lambda_2$.
Therefore $\lambda_1 = \lambda_2 = 2$. Thus:

$$\begin{aligned} \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} &= T \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} T^{-1} \\ &= T(2I)T^{-1} \\ &= 2I \\ &= \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \end{aligned}$$

Contradiction!

**Definition 27.2 (Jordan block)**
A $n \times n$ Jordan block is a $n \times n$ upper triangular matrix s.t. all diagonal entries are equal, and the entries that are are $(i+1)$ are 1, remaining entries are all 0. where $i \in [1, n-1]$.

**Example 27.5**
Any $1 \times 1$ matrix is a Jordan block.

**Example 27.6**
The general format for Jordan block for $2 \times 2$ matrix is given by $\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$

**Example 27.7**
The general format for Jordan block for $3 \times 3$ matrix is given by $\begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$

**Example 27.8**
The general format for Jordan block for $4 \times 4$ matrix is given by $\begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix}$

**Definition 27.3 (Jordan Canonical Form)**
A $n \times n$ matrix $A$ is called a Jordan Canonical form, if $A$ can be written as a blockwise diagonal matrix, s.t. for each diagonal block is a Jordan block.

**Example 27.9**
Consider a $5 \times 5$ matrix,

$$A = \begin{bmatrix} 1 & 2 & & & \\ 4 & 5 & & & \\ & & 1 & 5 & \\ & & 0 & 4 & \\ & & & & 3 \end{bmatrix}$$

This is called blockwise diagonal matrix. However the matrix is not in Jordan block.

**Example 27.10**
The matrix

$$B = \begin{bmatrix} 2 & 1 & & & \\ & 2 & & & \\ & & 3 & 1 & \\ & & & 3 & \\ & & & & 4 \end{bmatrix}$$

is also blockwise diagonal matrix but not in Jordan block.

In general, there are different types of block matrix. For example, the one we mentioned above is $(2, 2, 1)$.

**Theorem 27.5**
For every $n \times n$ matrix $A$ over $\mathbb{C}$, there is an $n \times n$ invertible matrix $T$ over $\mathbb{C}$, s.t. $TAT^{-1}$ is of Jordan Canonical form. The Jordan blocks in $TAT^{-1}$ are unique up to conjugation.

**Proof.**
Note for every nonconstant polynomial, $f(z)$ over $\mathbb{C}$ has a root in $\mathbb{Z}$. (Fundamental theorem in Algebra).

Recall back that:

**Theorem 27.6 (Fundamental Theorem of finitely generated Abelian Groups)**
Every finitely generated Abelian group is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \cdots \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{m}$$

where $p_1, \ldots, p_n$ are primes, $r_1, \ldots, r_n$ are positive integers. $m > 0$.

in higher algebra. The two theorems can be considered as a special case of a single theorem.

# 28 Add. Topic 2. Polynomial Rings

**Definition 28.1 (Polynomials)**
A polynomial over $\mathbb{R}$ is an expression

$$a_n x^n + \cdots + a_1 x + a_0$$

where $a_n, \ldots, a_1 \in \mathbb{R}$.

We use $\mathbb{R}[x]$ to denote all polynomial in variable $x$ with coeff in $\mathbb{R}$.

As we can add and multiply polynomials, therefore $\mathbb{R}[x]$ is a commutative ring with unity 1. Note $\mathbb{R}$ is a subring of $\mathbb{R}[x]$.

Now we wish to check if $\mathbb{R}[x]$ is a integral domain.

Suppose $f \mapsto a_n x_n + \cdots + a_1 x + a_0$. Suppose $g \mapsto b_m x_m + \cdots + b_1 x + b_0$.

Then

$$\begin{aligned} fg &= a_n b_m + \cdots + a_0 b_0 \\ c_k &= \sum_{i=0}^{k} a_i b_{k-i} \end{aligned}$$

Since $a_i \neq 0, b_i \neq 0, a_i b_{k-i} \neq 0$.

Therefore $fg \neq 0$. $\mathbb{R}[x]$ is therefore an integral domain.

We therefore have the following theorem:

**Theorem 28.1**
If $f \in \mathbb{R}[x]$, $f$ is nonzero. Then we have for $f = a_n x^n + \cdots + a_0$, $\deg(f) = n$. Moreover, $\deg(fg) = f + g$

**Definition 28.2 (Polynomial over $R$)**
Let $R$ be a commutative ring with unity 1, then a polynomial over $R$ is an expression of

$$a_n x_n + \cdots + a_0$$

where all coeff are element in the ring $R$.

**Theorem 28.2**
Let $R[x]$ be the set of polynomial in variable $x$ with coeff in $R$.
Then this is a commutative ring with unity 1. Moreover, $R$ is a subring of $R[x]$.

**Example 28.1**
Let $f, g \in R[x]$ are nonzero, is it true that $\deg(fg) = \deg(f) + \deg(g)$?

False! Consider $R = \mathbb{Z}_6$. Let $f \mapsto 3x^2 + 1, g \mapsto 2x + 1$. Then $fg = 6x^3 + 3x^2 + 2x + 1 = 3x^2 + 2x + 1$. Then the degree for $fg = 2$ while $\deg(f) + \deg(g) = 3$!

**Proposition 28.1**
If $R$ is an integral domain, $f, g \in R[x]$, $f \neq 0, g \neq 0$, then $fg \neq 0$, therefore $R[x]$ is a integral domain. Moreover, $\deg(f) + \deg(g) = \deg(fg)$.

**Definition 28.3 (Derivative in $R$)**
If $f \mapsto a_n x^n + \cdots + a_1 x + a_0$, we define $f' \mapsto n a_n x^{n-1} + \cdots + a_1$. (Just like the usual formula for derivative.)

The usual definition (First principle) for derivative on $\mathbb{R}$ does not hold. However, we have the formula in $\mathbb{R}$ holds in $R$ also.

If $f$ is a constant, $f = a_0$, then $f' = 0$. However, the converse is not always true.

**Proposition 28.2**
If $F$ is a field, $f \in F[x]$, then we say $c \in F$ is a root of $f$ if $f(c) = 0$.

For example, can we find all the roots of $x^5 - x + 1 \in \mathbb{Z}_5[x]$.

Yes, we can plug in $x = 1, \ldots, 5$. We then have $f$ have no roots in $\mathbb{Z}_5$.

Are there any simplier ways? Also yes! By Fermat Little theorem, $x^5 - x = 1$, therefore $x^5 - x + 1 \neq 0$.

**Proposition 28.3**
If $f \in F[x]$, $\deg(f) = n > 0$, then we have:

- $c \in F$ is a root of $f$ iff $f(x) = (x - c)g(x)$ for some $g \in F[x]$, and $\deg(g) = n - 1$.
- $f$ has at most $n$ roots in $F$.

**Proof.**

$$\begin{aligned} f(x) &= (x-c)g(x) \\ f(c) &= (c-c)g(x) \\ &= 0g(x) = 0 \end{aligned}$$

Conversely, if $c$ is a root of $f$, i.e. $f(c) = 0$, then

$$a_n c^n + \cdots + a_0 = 0$$

We then have

$$\begin{aligned} f(x) &= f(x) - f(c) \\ &= (a_n x^n + \cdots + a_1 x + a_0) - (a_n c^n + \cdots + a_1 c + a_0) \\ &= (a_n)(x^n - c^n) + \cdots + a_1(x - c) \end{aligned}$$

Note that $x^n - c^n = (x - c)(x^{n-1} + \cdots + c^{n-1})$, hence $f = (x - c)g(x)$ for some $g(x)$.

# 29 Add. Topic 3. Introduction to field theory

**Definition 29.1 (Field)**
A field is a ring, $F$ satisfying three properties:

1. $F$ is commutative.

2. $F$ has 1 as unity, where $1 \neq 0$.

3. Every nonzero element $a \in F$ has a multiplicative inverse $a^{-1} \in F$.

For arbitrary number $\alpha \in \mathbb{C}$, $\alpha$ generates a field $\mathbb{Q}(\alpha)$ in $\mathbb{C}$.

$$\mathbb{Q}(\alpha) = \left\{ \frac{a_n\alpha^n + \cdots + a_1\alpha + a_0}{b_m\alpha^n + \cdots + b_1\alpha + b_0} \,\middle|\, a_0, \ldots, a_n, b_1, \ldots, b_m \in \mathbb{Q}, m, n \in \mathbb{Z}_{\geq 0}, b_m\alpha^n + \cdots + b_1\alpha + b_0 \neq 0 \right\}$$

We pick $\alpha = 0$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(0) = \left\{ \frac{a_0}{b_0} \,\middle|\, a_0, b_0 \in \mathbb{Q}, b_0 \neq 0 \right\} = \mathbb{Q}$

Pick $\alpha = 1$, then $\mathbb{Q}(\alpha) = \mathbb{Q}$. For any rational number $\alpha$, we have $\mathbb{Q}(\alpha) = \mathbb{Q}$ also.

Pick any $\alpha \notin \mathbb{Q}$, but $\alpha \in \mathbb{Q}(a)$, for example, we can pick $\alpha = \dfrac{\alpha + 0}{0\alpha + 1} \in \alpha$.

**Theorem 29.1**
If we pick $\alpha = i$, we then have $\mathbb{Q}(i) = \{ ai + b \mid a, b \in \mathbb{Q} \}$

**Proof.**
Since

$$\begin{aligned} a_n i^n + a_{n-1} i^{n-1} + \cdots + a_1 i + a_0 &= ci + d, (c, d) \in \mathbb{Q}^2 \\ b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0 &= vi + s, (v, s) \in \mathbb{Q}^2 \end{aligned}$$

And therefore,

$$\begin{aligned} \mathbb{Q}(i) &= \left\{ \frac{ci + d}{vi + s} \,\middle|\, c, d, v, s \in \mathbb{Q}, r, s \text{ not both zero} \right\} \\ &= \{ ai + b \mid a, b \in \mathbb{Q} \} \end{aligned}$$

Note that $\mathbb{Q}(\pi)$ is a very large set, however, $\mathbb{Q}(\pi) \subsetneq \mathbb{R}$, since $\mathbb{Q}(\pi)$ is countably finite, however $\mathbb{R}$ itself is not countable.

**Definition 29.2 (Fiel extension)**
If $F$ is a field, an extension of $F$ is a field $E$ with $F \subset E$. We say $F$ is a subfield of $E$, and $E$ is a extension of $F$.

**Example 29.1**
$\mathbb{Q}$ is the smallest subfield in $\mathbb{C}$.

**Proof.**
If $F$ is a subfield in $\mathbb{C}$, then $1+1+\cdots+1 = n \in F$. We have $-n \in F$, and $n^{-1} \in F$, and $\dfrac{m}{n} = mn^{-1} \in F$. Hence $\mathbb{Q} \subset F$.

**Definition 29.3 (Vector space over a field)**
If $F$ is a field, a vector space over $F$ is a set $V$ with addition and scalar multiplication s.t.

1. $(V, +)$ is a abelian group. (This imples 0 exists, $a^{-1}$ exists, and operation is associative)
2. $(k_1k_2)v = k_1(k_2v), \forall k_1, k_2 \in F, v \in V$. Also $1 \times v = v$
3. $(k_1 + k_2)v = k_1v + k_2v, k(v_1 + v_2) = kv_1 + kv_2$

Almost all results and concepts in linear algebra course can be generalized to a linear algebra over F. For example, linearly independence, basis, ...

**Example 29.2**

Consider $F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$. Define $+$ and scalar multiplication as same in $\mathbb{R}^2$.
Then $F^2$ has a basis of $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

**Definition 29.4 (Dimension of a vector space)**
A vector space $V$ over $F$ has a dimension $n$, $n \in \mathbb{Z}_{\geqslant 0}$, written as $\dim_F V = n$, if $V$ has a basis consisting of $n$ vector spaces. If $V$ has no finite basis , then $\dim_F V = \infty$.

**Example 29.3**
$\mathbb{R}^\infty = \{(a_1, \ldots, a_n) : a_1, \ldots, \in \mathbb{R}\}$ is a vector space with infinitely dimension.

**Theorem 29.2**
If $F \subset E$, $E$ is a field extension of field $F$, then $E$ is automatically a vector space over $F$.

**Definition 29.5 (Degree of extension)**
The degree of the extension $F \subset E$ is $[E : F] = \dim_F E$.

**Example 29.4**
$[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2$.

Consider the example we mentioned earlier:

**Example 29.5**
For arbitrary number $\alpha \in \mathbb{C}$, $\alpha$ generates a field $\mathbb{Q}(\alpha)$ in $\mathbb{C}$.

$$\mathbb{Q}(\alpha) = \left\{ \frac{a_n\alpha^n + \cdots + a_1\alpha + a_0}{b_m\alpha^n + \cdots + b_1\alpha + b_0} \,\middle|\, a_0, \ldots, a_n, b_1, \ldots, b_m \in \mathbb{Q}, m, n \in \mathbb{Z}_{\geq 0}, b_m\alpha^n + \cdots + b_1\alpha + b_0 \neq 0 \right\}$$

then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \begin{cases} 1 & , \quad a \in \mathbb{Q} \\ 2 & , \quad a = i \\ \vdots \end{cases}$

**Definition 29.6 (Algebraic and Transcendal Number)**
$\alpha$ is called an algebraic number if there is $f(x) \in \mathbb{Q}(x)$, s.t. $f(a) = 0$. We say $\alpha$ is transcendal if $\alpha$ is not algebraic.

**Example 29.6**
$e, \pi$ are transcendal number.

**Example 29.7**
Let $\bar{\mathbb{Q}}$ be the set of all algebraic number, then $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

$\mathbb{C} - \bar{\mathbb{Q}}$ is the set of transcendal number, moreover, this set is uncountable.

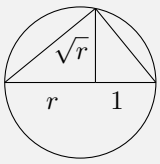
**Definition 29.7 (Constructible number)**
A real number $\alpha \in \mathbb{R}$ is called a constructible number if we can constructible a line segment with length $|\alpha|$ in a finitely number of steps from the given segment of length 1 by using a straight edge and a compass.

**Theorem 29.3**
$\mathbb{R}$ can be classifield into two types: Construstible number and non-constructible number.

**Example 29.8**
All integers are constructable. All rational numbers are constructable.

**Example 29.9**
If $\gamma$ is constructable, then $\gamma^{\frac{1}{2}}$ is constructable as well.

**Proof.**
Consider:




**Theorem 29.4**
Let $C$ be the set of constructible. Then:

1. C is a subfield of $\mathbb{R}$.
2. Any element in $C$ is algebraic.
3. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k, k \in \mathbb{Z}_{\geq 0}$, for any $\alpha \in C$.

**Example 29.10**

$2^{\frac{1}{3}}$ is not constructible.

**Proof.**

$$\left[\mathbb{Q}\left(2^{\frac{1}{3}}\right):\mathbb{Q}\right]=3\notin 2^k$$

In general, given $a\in\mathbb{Z}_{>0}$, if $a\notin\mathbb{Z}$, then $a^{\frac{1}{3}}$ is never constructible.

**Theorem 29.5**
It is not possible to trisect a given angle using straight edge and compass.

**Proof.**
If such statement is true, then one may construct $20^\circ$ from $60^\circ$. But

$$[\mathbb{Q}(\cos 20^\circ):\mathbb{Q}] \quad = \quad 3$$

Then $\cos 20^\circ$ is not constructible.