MATH3121 Notes

SmokingPuddle58

December 24, 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
$\|A\|$	Cardinality of set A

Contents

0 Sets and Relations **4**

1 Complex Numbers **9**

4 Groups **11**

5 Subgroups **17**

6 Cyclic Groups **21**

8 Groups of Permutations **30**

9 Orbits, Cycles, Alternating Groups **33**

10 Cosets and the Theorem of Lagrange **40**

11 Direct Products and Finitely Generated Abelian Groups **43**

13 Homomorphisms **48**

0 Sets and Relations

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

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

and some sets like:

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

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

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

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

For example, we have

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

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

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

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

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

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

1. Distributive law:

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

2. De Morgan's law:

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

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

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

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

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

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

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

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

2. can be proved with similar methods as above.

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

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

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

One of the common example we use would be

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

However when we consider the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Partition always satisfies the equivalence relation.

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

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

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

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

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

1 Complex Numbers

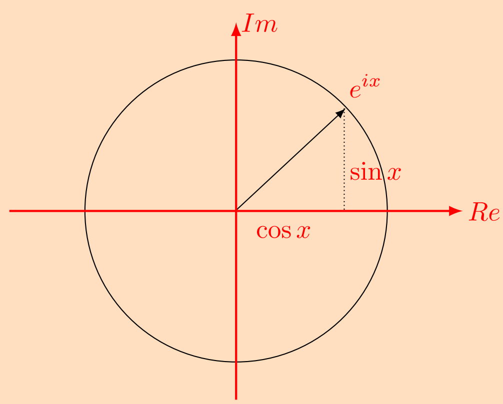
Definition 1.1 (Complex number $\mathbb{C}$)
Define $\mathbb{C}$ to be a set $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ with two operations $+, \cdot$, such that:

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

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

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

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



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

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

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

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

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

We start to check the three axioms:

1. There is $1 \in \mathbb{C}^*$, s.t. $a \cdot 1 = 1 \cdot a = a$
2. The inverse element exists, since:

$$\frac{1}{a+bi} = \frac{1}{a+bi}\left(\frac{a-bi}{a+bi}\right) = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

   and $(a+bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) = 1$
3. The operation is associative for sure.

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

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

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

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

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

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

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

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

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

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

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

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

1. There is I_n, such that $I_n A = A I_n = A$
2. As $|A| \neq 0, \forall A \in \mathrm{GL}(n, \mathbb{R})$, thus there is A^{-1}, s.t. $AA^{-1} = A^{-1}A = I$
3. It is obvious that the multiplication of matrix is associative.

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

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

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

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

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

We first prove the set is closed under multiplication.

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

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

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

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

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

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

At the first glance, we observe that

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

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

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

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

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

Where

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

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

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

Partition $\mathbb{Z}$ as

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

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

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

The following theorem is very important throughtout the entire course!

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

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

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

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

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

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

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

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

Find the inverse of A: (Trick)

$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, thus inverse $A^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$
As a result, we have $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 Subgroups

Before we define subgroup, we shall define the "closeness" of operation.

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

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

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

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

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

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

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

Example 5.2
Let $S = \{n | n \notin \mathbb{Q} \text{ and } n \in \mathbb{R}\}$ 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. $2^{-1} = \frac{1}{2} \notin \{1, 2, 2^2, 2^3, \ldots\}$)

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

We first check whether the operation is closed or not.

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

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

Then we check whether the inverse element exists.

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

Thus the inverse element exist.

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

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

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

Are the following sets a subgroup under matrix multiplication?

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

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

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

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

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

2. Inverse of diagonal matrix

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Example 6.8

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

Proof.

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

Theorem 6.1
Any cyclic group G is abelian.

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

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

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

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

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

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

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

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

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

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

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

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

Example 6.11
Let $G = (\mathbb{Z}_1 2, +)$. We have:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Consider $n \div m$. By division algorithm

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

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

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

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

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

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

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

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

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

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

Consider the properties of d:

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

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

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

$$mr + ns = 1$$

Theorem 6.6 (Estimation of growth of $\Pi(n)$ (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:

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

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

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

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

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

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

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

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

If the order of a is infinite, then

$$\langle a \rangle = \{e, a, a^2, \ldots\}$$

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

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

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

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

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

For c, since for any rotational matrix, we have

$$A_\theta^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

As a result, we have

$$c^{202} = I$$

Thus the order of c is 202.

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

Proof.
We write $m = nq + r$ for some $0 \le r < n$, 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:

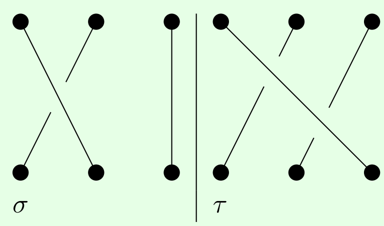
$$\begin{aligned} a_1, ..., a_n &= aa_{,}aa_2, ..., aa_n \\ a^n a_1, ..., a^n a_n &= a_1, ..., a_n \\ a^n &= e \end{aligned}$$

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

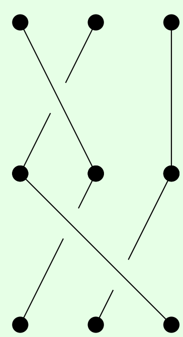
$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

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

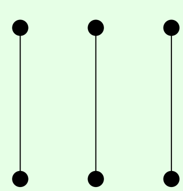
Example 6.18 (Braid Groups)
Let B_3 be a braid group with 3 strings. Define σ and τ to be the following.



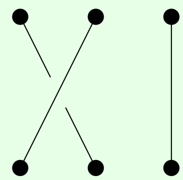
One may define the multiplication, $\sigma * \tau$, by joining the graph together with σ's bottom and τ's top. For example, $\sigma * \tau$ will be:


$\sigma * \tau$

The identity element e is defined as:

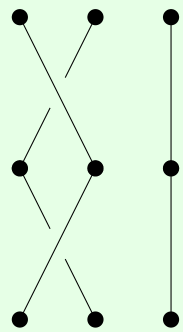

e

The inverse of σ is given by:



σ^{-1}

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



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

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

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

8 Groups of Permutations

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

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 σ, τ, ϕ 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, ι is an identity element under S_A under $\circ$.

By lemma above, we have the associativity holds.

Finally, as σ 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 σ^{-1}. Also find the order of σ.

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

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 σ.

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 σ induces the following partition.

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

We name each partition as orbit. thus σ 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 σ 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, σ 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 σ 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 σ has 4 orbits, namely $\{1,4,5,7\},\{2\},\{3\},\{6\}$. Thus σ forms a cycle.

Also σ 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 σ 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 σ, τ 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 σ, τ are disjoint.

Theorem 9.3
If σ, τ 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 τ. 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 σ 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 σ 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 $\begin{pmatrix} n \\ 2 \end{pmatrix} = \frac{n(n-1)}{2}$ 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 σ 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 $\sigma \in S_n$, σ permute the columns of A to obtain a new matrix, σA.

σ 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 σ an even permutation.

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

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

Theorem 9.9
Suppose σ is a cycle with length k, if k is odd, then σ is even. if k is even, then σ is odd.

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

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

Note that there are $2k - 1$ transposition. Thus σ 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 σ, τ 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 σ be a permutation. Then σ and σ^{-1} have the same parity (oddness/evenness).

Proof.
Let σ 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 σ is odd, we can also prove that σ^{-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 $|A_n| = \dfrac{1}{2}n!$

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. $A_n = \dfrac{1}{2}S_n$.

Example 9.11

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

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°. 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:

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

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

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

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 3×3 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:

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

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

Thus if we let $S =$ all 3×3 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 ϕ is bijective, and ϕ 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:

- ϕ is a bijection
- ϕ 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 ϕ 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 ϕ 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 ϕ is not a isomorphism, because ϕ is not surjective. However, if $\phi : \mathbb{R} \to \mathbb{R}^*_{>0}$, then ϕ 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 $(1,2)(1,3) \neq (1,3)(1,2)$.

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

Note that by homomorphism property,

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

By the property of homomorphism,

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

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

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

By cancellation law, we have

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

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

$$a^n = e \quad \text{iff} \quad \phi(a)^n = e'$$

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

Proof.
$(\implies)$
If $a^n = e$, apply ϕ 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 ϕ is homomorphism.

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

Example 13.10
Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$, where $\phi(x) = |x|$, then ϕ 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 ϕ is one-to-one and onto, thus ϕ is also an isomorphism.

Proof.
We need to prove that the map ϕ 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 ϕ is strictly increasing, ϕ 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 ϕ is continuous, thus ϕ is onto.