MATH3121 Note | Last edited on **09 Oct 2023** by SmokingPuddle58

Some special symbols, notations and functions used in this note

$\mathbb{R}^*$	The set of real number, excluding 0	ord()	The order of the element in a group
card()	The cardinality of the set	$\|A\|$	Cardinality of A

Sections with square brackets are mostly proofs.

Brief Introduction (Idk why this part exists but professor introduced it I will keep this)

Definition. *A group G is a set with binary operation*

For example, $(\mathbb{R},+)$ is an example of group.

Theorem. *Every n-D shape have a symmetry group* $(G,\circ)$.

Let's say, we define G to be the circle. Then symmetry group for G is infinite as, simply speaking, no matter how many rotations you made, the circle is still symmtrical (In both rotational and reflexional means).

It is impossible for us to visulize the group with dimension ≥ 4, but we can represent with equation. For example.

$$\left\{(x_1,x_2,x_3,x_4,\ldots,x_n)\colon \sum_{i=1}^{n} x_n^2=1\right\}$$

Definition. *A ring is a set R with two operation,* $+$ *and* $\cdot$*, with satisfying certain axioms.*

Variable set of functions are rings.

Let $C[0,2]$ to be the set of all continuous function in $[0,2]$. This satisfies the rings condition if we include two operator, $(+,\cdot)$. Thus $(C[0,2],+,\cdot)$ is a ring.

---

1 Sets and relations

To define a finite set, one may choose to list out every element in the set.

However, with infinite set, one may characterize the set.

For example, the set of all odd numbers, and like

$$B=\{a\in\mathbb{R}\,|\sin a+\cos a+1=0\}\ \text{ and }\ C=\{a\in\mathbb{R}|a^{10}+100a^2-10a-10000=0\}$$

Note that C has finitely many (≤ 10) element (From root of unity)

Definition. ***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. ***Union and 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 $\{x | x \in A \text{ and } x \in B\}$.

Theorem. *Laws of operation*

1. Distributive law

$$1.(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$
$$2.(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Proof. *We only prove 1.*

$\boxed{(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)}$

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. □

Theorem. ***Cartesian Product***

Suppose that A, B are two sets, then define Cartesian product $A \times B$ to be

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

A very common example,

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

Definition. ***Map(Function)***

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

For example, let $f(x) = x^2 - 1$, we can call f to be a map, where $f: \mathbb{R} \to \mathbb{R}$.

Example. Define $A=\{1,2,3\}, B=\{4,5\}$, how many maps from A to B are there?

Solution. There are two ways to choose $f(1)$, two ways to choose $f(2)$, two ways to choose $f(3)$. Thus the number of functions is

$$2^3=8$$

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. *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. ***One-to-one, Onto, Bijective function***

For a map $f: A\to B$

The map is called to be one-to-one (injection), if $a_1\neq a_2\Rightarrow f(a_1)\neq f(a_2)$

The map is called to be onto (surjection), if for every element $b\in B$, we have $a\in A$ with $f(a)=b$.

The map is called to be bijective, if f is both injective and surjective.

Theorem. ***Cardinality of sets***

Given two sets A, B.

*A, B have the same cardinality, `if and only if` a **bijection** $f: A\to B$ exists.*

*If there is a **injection** $g: A\to B$, then we say A has a smaller cardinality than B, and $|A|\neq|B|$.*

*If there is a **surjection** $h: A\to B$, then we say A has a larger cardinality than B, and $|A|\neq|B|$.*

For two finite sets, we say two sets A, B have equal cardinality iff they have the same number of elements in the set.

Example. 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

Solution. It is impoosible to find a map which is one to one because the cardinality $|A|>|B|$

———————————[END OF 2023-09-05]———————————

However some strange phenomenen exists. For example,

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

Note that set A and B have the same cardinality, although intuitively set B is greater than set A in terms of cardinality.

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

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

Solution 1. Take $f(x)=\frac{2}{\pi}x$, $f:\left(-\frac{\pi}{2},\frac{\pi}{2}\right)\to(-1,1)$ is bijective. Thus both have equal cardinality.

Definition. ***Partition***

Let A be a set. Define a partition of A as a decomposition of A:

$$A=A_1\sqcup A_2\sqcup\ldots\sqcup A_n$$

such that any two set A_i and A_j have empty intersection. i.e. $A_i \cap A_j = \varnothing$

Example.

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

Definition. *Let A be a set, a equivalence relation $\sim$ is defined if it satisfies the following properties:*

1. $a \sim a$
2. $a \sim b \Rightarrow b \sim a$
3. $a \sim b \wedge b \sim c \Rightarrow a \sim c$

Definition.

Given $A = A_1 \sqcup A_2 \ldots \sqcup A_n$ is a partition of A, we define relation $\sim$ on A as follow.

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

Partition always satisfies the equivalence relation.

Example. 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.

Example. Given an equivalence relation $\sim$ on A, for $a \in A$, define $\tilde{a} = \{x \in A | x \sim a\}$. Then $\tilde{a}$ is a subset of A.

Then for $a_1, a_2 \in A$, either $\tilde{a_1} = \tilde{a_2}$, or $\tilde{a_1} \cap \tilde{a_2} = \varnothing$

Theorem.

Concept of partition of A implies the concept of equivalent relations of A, where the part containing $a \in A$ is the subset $\{x \sim A | x \sim a\}$

Definition. ***Partial Order***

Let A be a set. a relation $\leq$ on A is called the partial order on A if

1. $a \leq a$
2. $a \leq b$ *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 $\leq$ will be the inequality sign we commonly used.

Proposition. ***Power Set***

Given S to be arbitrary sets. Power sets $P(S)$ is defined as all the subsets of S.

Suppose that S is a set. The subset relation $\subseteq$ is a partial order on $P(S)$

2 Complex Number

Definition. ***Complex Numbers***

Define $\mathbb{C}$ *to be a set:* $\mathbb{C}=\{a+bi|a,b\in\mathbb{R}\}$, *with two operations* $+,\cdot$

1. *Addition* $\boxed{+}$, *where* $(a+bi)+(c+di)=(a+c)+(b+d)i$
2. *Multiplication* $\boxed{\cdot}$, *where*
    1. $\cdot$ *is distributive w.r.t* $+$
    2. $i\cdot i=-1$

Thus we have

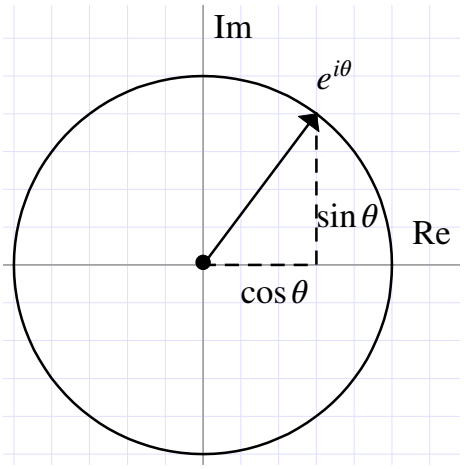
$$\begin{aligned}(a+bi)\cdot(c+di) &= ac+adi+bci+bd(i\cdot i)\\ &= (ac-bd)+(ad+bc)i\end{aligned}$$

Moreover, the two operators are both ***communicative and associative****.*

By definition, one may also define complex number in the form of:

$$e^{i\theta}=\cos\theta+i\sin\theta=\operatorname{cis}\theta$$

This is called Euler's Formula.



We may also express the complex number in polar form:

$$z=a+bi\Leftrightarrow z=re^{i\theta}$$

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

Proof:

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

It is thus in the form of $z=a+bi$, where $a=r\cos\theta, b=r\sin\theta$

Theorem.

Every non-constant polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$.

Example. The solution set of the equation $z^n = 1$,

$$U_n = \{z \in \mathbb{C} | z^n = 1\} = \left\{e^{\frac{2\pi i}{n}k}\right\}, k = \{1, 2, 3, \ldots, n-1\}$$

Proof.

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

□

Definition. *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 $\boxed{+}$ we used is an example of binary operation, where

$$+: \mathbb{C} * \mathbb{C} \longrightarrow \mathbb{R}$$

Proposition.

Given that $|S| = n$, then there are $n^{(n^2)}$ binary operation on S

———————————————[END OF 2023-09-07]———————————————

3 Groups

Definition. ***Group***

Group is a set $(G, *)$ following the follow 3 axioms.

(1) There is $e \in G$, s.t. $e * a = a * e = a$, $a \in G$ (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 all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$ (Asoociativity)

Example. Is $(\mathbb{R}, +)$ a group

$+$ on $\mathbb{R}$ is a binary operation as for $a, b \in \mathbb{R}$, we have $a + b \in \mathbb{R}$.

Now, we check that $(\mathbb{R}, +)$ is a group.

- There is an element 0, such that $0 + a = a + 0 = a$
- There is $(-a)$, s.t. $(a) + (-a) = (-a) + a = 0$
- The addition satisfies $(a + b) + c = a + (b + c)$

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

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

However, do note that $\mathbb{N}$ does not satisfy the definition of groups under binary operation $+$ as there is no element a' such that $a + a' = 0$

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

We check the 3 axioms:

- There is element 1, s.t. $a \cdot 1 = 1 \cdot a = a$
- For $a \neq 0$, $a' = \frac{1}{a}$, however there is no $0'$, s.t. $0 \cdot 0' = 1$

The set does not follow the axiom with such binary operator, thus $\mathbb{R}$ is not group under $\boxed{\cdot}$.

However, we can create another set $\mathbb{R}^*$, where 0 is removed from $\mathbb{R}$. i.e. $\mathbb{R}^* = \mathbb{R} - \{0\}$.

Example. Let $\mathbb{C}^* = \mathbb{C} - \{0\}$. Is this a group under multiplication?

We check the axioms again.

- There is an element 1, such that $a \cdot 1 = 1 \cdot a = a$
- There is an inverse element,

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

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

- The multiplication is for sure associative

Thus $(\mathbb{C}, \cdot)$ is a group by definition.

Example. Let A be a set of all integer excluding 0. Is A a group under multiplication?

First, we know that $\cdot$ is a binary operation on A.

We then check the 3 axioms.

- There is element 1, s.t. $\forall a \in A$, $a \cdot 1 = 1 \cdot a = a$

- The multiplication is associative
- However, if we pick 2 as an example, $2' = \frac{1}{2} \notin A$

Thus not every element has an inverse element in A. A is not a group under multiplication.

Definition. ***Abelian Group***

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

Example.

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.

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

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

Note that $|A \cdot B| = |A||B| \neq 0$

Thus the set is closed.

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

- There is I_n, such that $I_n A = A I_n = A$
- As $|A| \neq 0, \forall A \in \mathrm{GL}(n, \mathbb{R})$, thus there is A^{-1}, s.t. $AA^{-1} = A^{-1}A = I$
- 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. *Finite, infinite group.*

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.

Consider a set $S=\{-1,1\}$.

Note that $\cdot$ is a binary operation on the set.

- There is a identity element 1.
- There is an inverse element, which is itself.
- The multiplication is associative

Thus $(S,\cdot)$ is a finite group.

Example.

Let $U_n=\{z\in\mathbb{C}|z^n=1\}$, this is the set of $n-$th root of unity. 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 may 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,

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

Modulo groups

Consider a mod 3 modulo group, we can make partition on $\mathbb{Z}$ as

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

Where $3\mathbb{Z}=\{3n|n\in\mathbb{Z}\},3\mathbb{Z}+1=\{3n+1|n\in\mathbb{Z}\},3\mathbb{Z}+2\{3n+2|n\in\mathbb{Z}\}$.

Define $\mathbb{Z}_3$ to be the parts of above partition, where $\mathbb{Z}_3 = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\} = \{0,1,2\}$, which is finite.

Furthermore, we can define an operator $+$, which is the same as $\mathbb{Z}$. For example,

$$\begin{aligned} 2+2 &= 1 \,(4 \bmod 3 = 1) \\ 1+2 &= 0 \,(3 \bmod 3 = 0) \end{aligned}$$

Base on the calculation, we can made a modular 3 addition table,

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

Note that $\mathbb{Z}_3$ is a finite, Abelian group under modulo n addition, as

- Identity element 0 exists, s.t. $0+a=a+0=a$
- Each element has an unique inverse, where

$$1^{-1}=2, 2^{-1}=1, 0^{-1}=0$$

- Addition is associative

In general, for any $n \in \mathbb{N}$, we have the following partition of $\mathbb{Z}$:

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

and for any integer, $n\mathbb{Z}+k = \{mn+k | m \in \mathbb{Z}\}$

Note that $\mathbb{Z}_n$ is a finite, Abelian group under modulo n addition, and $|\mathbb{Z}_n| = n$

Theorem. ***Left and Right cancellation***

If $(G, *)$ is a group, then the left cancellation and right cancellation law holds in group, where

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

However, $a*c = b*a \not\Rightarrow c = b$.

Proof for L-R cancellation:

Left cancellation:

$$\begin{aligned} a*b &= a*c \\ a^{-1}(a*b) &= a^{-1}(a*c) \\ (a^{-1}a)*b &= (a^{-1}a)*c && \text{(Associative)} \\ e*b &= e*c && \text{(Definition of identity element)} \\ b &= c && \text{(Definition of identity element)} \end{aligned}$$

Right cancellation can be proved by similar method.

Proof of $a*c=b*a \not\Rightarrow c=b$

Pick two element from 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 $C=ABA^{-1} \Rightarrow CA=AB$ (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 $a*c=b*a \not\Rightarrow c=b$.

——————————[END OF 2023-09-12]——————————

4 Subgroups

Theorem. ***Uniqueness of identity and inverse element***

If $(G,*)$ is a group, then for any $a\in G$, there exists ***unique*** *$a'\in G$, s.t. $aa'=e$.*

Moreover, the identity element for each group is unique.

Proof:

Assume there are two inverse element for $a\in G$, namely a' and a''. Then we have

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

By the left cancellation rule, we have $a''=a'$.

By similar technique, assume that there are two identity element e' and e''. Then

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

By the left cancellation rule, we have $e''=e'$.

Definition. ***Closeness of operation***

If T is a set, $*$ is 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 as if we consider an example, $1,3\in 2\mathbb{Z}+1$, but $1+3=4\notin 2\mathbb{Z}+1$.

Definition. ***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 $*$*

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

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

Also, $\mathbb{R}_{>0}$ 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. Let $(\mathbb{C}^*,\cdot)$ be a group. Determine whether the following are subgroups.

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

Answer:

1,3,4 are subgroups.

2 is not a subgroup, because most of the inverse element does not belongs to the group.

(e.g. $2^{-1}=\frac{1}{2}\notin\{1,2,2^2,2^3,\dots\}$)

Example. 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 $\cdot$.

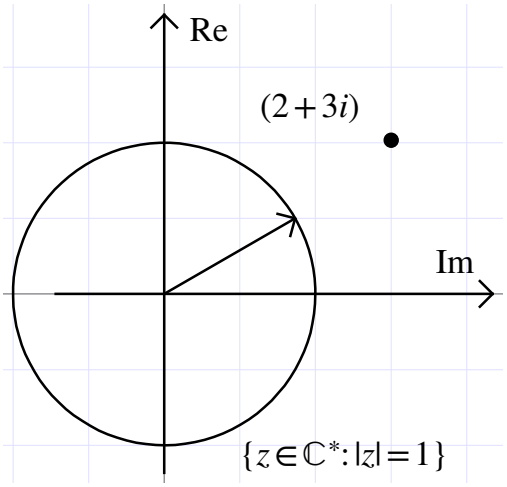
Then we check whether the inverse element exists.

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

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.

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

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

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 (1) and (2).

(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:

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

Notation

If G is a group under $*$, we will simply write

$$a*b: ab$$

$$\underbrace{a*a*a*\cdots*a}_{n}=a^n$$

$$a'=a^{-1}$$

$$a'a'a'\ldots a'=a^{-n}$$

$$a^0=e$$

Theorem. ***Subgroup***

A subset H of a group G is a subgroup of G iff

- *H is closed under binary operation of G*
- *Identity element* $G\in H$
- $\forall a\in H, a^{-1}\in H$

Proof

($\Rightarrow$)

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.

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

By the left cancellation rule.

Finally it is obvious that the associativity holds.

($\Leftarrow$)

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 automatically holds

Definition. ***Vector Space and Subspace***

Given that V is a vector space, a subset $S\subset V$ *is a subspace, iff*

- *S is nonempty*

- *S is closed under linear combination operation*

  i.e. $\forall v_n \in S, \sum_{\substack{v_n \in S \\ a_n \in \mathbb{R}}} a_n v_n \in S$

There should be some notes here but I did not copy them because I was too sleepy that day. Sorry :(

——————————[END OF 2023-09-15]——————————

5 Cyclic Groups

Theorem.

Let G be a group and let $a \in G$.

The set $<a> \{a^n : n \in \mathbb{Z}\}$ *to be a subgroup of G.*

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

Moreover, $<a>$ *is the smallest subgroup.*

i.e. if H is a subgroup, $a \in H$, *then* $<a> \subset H$.

Proof.

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

The identity element e exists in $<a>$ *because if we pick* $n = 0$, *then* $a^0 = e$.

The inverse element $a' = a^{-n}$ *also exists in* $<a>$.

Thus $<a>$ *is the smallest subgroup.* □

Example.

Consider the group $(\mathbb{C}^*, *)$, we have

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

Consider the group $(\mathbb{C}^*, +)$, we have

$$\begin{aligned} <2> &= \{2n : n \in \mathbb{Z}\} = \{0, 2, -2, 4, -4, \dots, \} \\ <n> &= \{na : n \in \mathbb{Z}\} \end{aligned}$$

One should note that $<n>$ is infinite for any $n \in \mathbb{Z}$, except 0, where $<0> = \{0\}$

Consider the group $(\mathbb{Z}_6, +)$, we have

$$\begin{aligned} <3> &= \{0, 3, 3+3=6=0, \dots, \} = \{0, 3\} \\ <5> &= <5> = \{0, 5, 5+5=10=4, 5+5+5=15=3, 5+5+5+5=20=2, \dots, \} = \{0, 1, 2, 3, 4, 5\} \end{aligned}$$

Observation:

1. The number of elements are divisible by 6
2. The element can be the same as $\mathbb{Z}_6$.

This theorem will be explained later.

Definition. ***Cyclic Group***

A group G is called a cyclic group if there exist a special element, $a \in G$, s.t. $<a>=G$.

In such case we call a as generator of G

Example.

$(\mathbb{Z},+)$ is cyclic group because 1,-1 can generate $\mathbb{Z}$

$(\mathbb{Z}_n,+)$ is in general cyclic as 1 can genrate $\mathbb{Z}_n$.

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

Example.

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

Proof. Suppose that the group is cyclic, then $\exists a \in \mathbb{Q}$, s.t. $<a>=\{na: n\in\mathbb{Z}\}=\mathbb{Q}$

Note that a is rational number, hence we can write $a=\frac{p}{q}, (p,q)\in\mathbb{Z}\times\mathbb{Z}^*\backslash\{1\}$.

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! □

Moreover, $(\mathbb{Q},*)$ is also not cyclic.

Proof. If $<a>=\mathbb{Q}^*$, 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 $\frac{10}{77}=2\times5\times7^{-1}\times11^{-1}$.

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

Also, $(\mathbb{R},+)$ is not cyclic

Proof. If $a\neq0$, then $\frac{1}{2}a\notin<a>$, contradiction! □

Example. (Extra)

Let $S=\left\{\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}: n\in\mathbb{Z}_{\geqslant1}\right\}$. 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.

A cyclic group is abelian group.

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

Pick arbitrary $x,y\in G$, then

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

□

For arbitrary group G, $a\in G$, sometimes $<a>$ is infinite, sometimes it is finite.

Example. Let $G=\mathbb{C}^*$, then we have $\text{card}(<2>)=\infty$, while $\text{card}(<i>)=4$

Theorem.

If $<a>$ is infinite, then for every $n\in\mathbb{Z}^+$, we have $a^n\notin e$.

Proof. *Assume that $a^n=e$ for some n, and assume that n is the smallest such exponential.*

Then $\{e,a,a^2,\ldots,a^n\}$ could already form a subgroup, which contradicts the fact that $<a>$ is infinite. □

Definition. ***Order***

If $a^n\neq e$, for all positive integer 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 order of a.

Example. Let $G=(\mathbb{R},+)$. then all $a\in\mathbb{R}$ has order ∞ other than 0.

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

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

In fact, for any group G, we always have $e=1$.

Example. Let $G=\mathbb{C}^*$, then

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

Example. Let $G=(\mathbb{Z}_{12},+)$, then

$<3>=\{3,3+3=6,3+3+3=9,3+3+3+3=12=0\}$, thus the order of 3=4

$<5>=\{5,10,15,20,25,30,35,40,45,50,55,60\to 0\}$, thus the order of $5=12$

$<8>=\{8,16,24\to 0\}$ thus order of $8=3$

Consider $n \div m, n \in \mathbb{Z}, m \in \mathbb{Z}_{>0}$, we always get quotient and remainder $0 \leqslant r < m$. Thus we have following lemma.

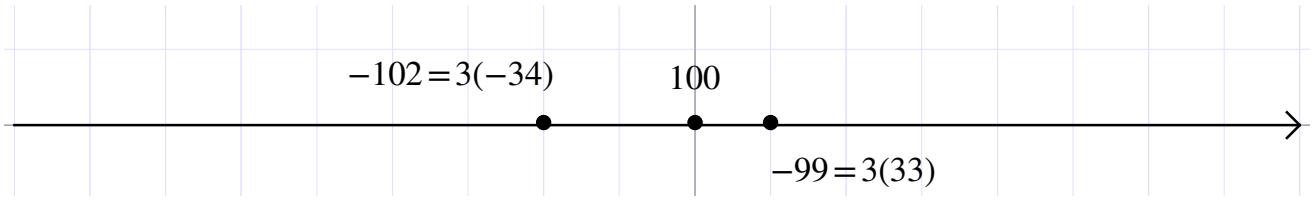
Lemma. ***Division algorithm for $\mathbb{Z}$***

If $m \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}$, then there exists unique integers q, r, s.t.

$$n = mq + r, r \in [0, m-1]$$

and n lies in exactly 1 of the interval $[nq, n(q+1))$

Example. Let $n = -100, m = 3$, then



Thus we have $-100 = 3 \times (-34) + 2$

With the above lemma, we can now prove the following theorem.

Theorem. *If G is cyclic subgroup, then every subgroup of G is cyclic.*

Proof. *Let $G = <a>$. Let $H \subset G$ be a nonempty subgroup.*

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

If $H \neq \{e\}$, then $\exists b \in H$, where $b \neq e$, s.t. $\begin{cases} b = a^k \\ b^{-1} = a^{-k} \end{cases}, b, b^{-1} \in H.$

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

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

Let m be the smallest element in S. We claim $H = <a^{nm}>$

As $a^m \in H$, $<a^m> \subset H$

For $b \in H, \because b \in G = <a>$, $b = a^n$ 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 we must have $r = 0$.

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

□

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

Proof. *As $\mathbb{Z}$ is cyclic, thus $H = <n> = n\mathbb{Z}$.*

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

then H is closed. $\boxed{\because (m_1 s + n_1 r) + (m_2 s + n_2 r) = (m_1 + m_2)s + (n_1 + n_2)r \in H.}$

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 may conclude $d = \mathrm{GCD}(r, s) = ms + nr$ for some $n, m \in \mathbb{Z}$. □

Theorem. ***Estimation of growth of*** **$\Pi(n)$**

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. $\Pi(n) \sim \frac{n}{\ln n}$.

———————————[END OF 2023-09-19]———————————

DISCLAIMER: I actually have no idea what I typed in the later part. :(

Recall:

Definition.

A group G is called cyclic, if there is $a \in G$, s.t. $G = <a>$.

Theorem. *Every subgroup of a cyclic group is cyclic*

Corollary. *The subgroup of $(\mathbb{Z}, +)$ are $n\mathbb{Z} = \{nj : j \in \mathbb{Z}\}$*

Theorem. ***Estimation of growth of*** **$\Pi(n)$**

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. $\Pi(n) \sim \frac{n}{\ln n}$.

Theorem. *If H_1 and H_2 are subgroup of G, then $H_1 \bigcap H_2$ is also a subgroup of G.*

Proof.

Note that every subgroup has an identity element e, thus $e \in H_1 \bigcap H_2$.

For any element g, h in G,

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

□

Example.

Let $m, n \in \mathbb{Z}$, where $m, n \neq 0$. Then $m\mathbb{Z} \bigcap n\mathbb{Z} = N\mathbb{Z}, N \in \mathbb{Z}$.

In this case, we can assume $N > 0$, as $N\mathbb{Z} = (-N)\mathbb{Z}$, and $N \neq 0$.

Example.

If k is another common multiple of m and n, $k \in m\mathbb{Z} \cap n\mathbb{Z} = N\mathbb{Z}$, then n is a multiple of N.

Definition. ***Order***

Let $a \in G$, the smallest positive integer n with $a^n = e$ is the order of a.

If $a^m \neq e$ for any positive integer m, then we say that the order of a is infinite.

Theorem.

The order of a is the number of elements in $<a>$.

Proof.

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

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

Thus we have $<a>$ has n elements.

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 $j < n, a^j \neq e$.

If the order of a is infinite, then

$$<a> = \{e, a, a^2, \ldots\}$$

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.

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 we have $(a^2)^2=a^4=I$, but still we need to check a^3. $a^3=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\begin{bmatrix}0&1\\-1&0\end{bmatrix}=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$

For b, note that $b^2=\begin{bmatrix}1&0\\2&1\end{bmatrix}\begin{bmatrix}1&0\\2&1\end{bmatrix}=\begin{bmatrix}1&0\\4&1\end{bmatrix}, b^3=\begin{bmatrix}1&0\\6&1\end{bmatrix}$, thus by observation, we have $b^n=\begin{bmatrix}1&0\\2n&1\end{bmatrix}\neq I$

For c, note that it is a rotational matrix. 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. Let G to be a group. $a\in G$ has order of n. Suppose $a^m=e$, for $m\in\mathbb{Z}$, prove that $m=nk$, $k\in\mathbb{Z}$.

Proof.

We write $m=nq+r$ for some $0\leqslant r<n$. $r=m-nq$. $a^r=a^{m-nq}=a^ma^{-nq}=a^m(a^n)^{-q}=e\times e^{-q}=e$

Then we force $r=0$. □

Example. Let G be a group, let $a,b\in G$, prove that ab and ba have the equal order.

Proof.

Suppose $n\in\mathbb{Z}^+$, $(ab)^n=e$ implies $(ab)(ab)(ab)\ldots(ab)=e$

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

To conclude, for any $n\in\mathbb{Z}_{>0}$, we have $(ab)^n$ if and only if $(ba)^n=e$.

Thus we have (ab) and (ba) have equal order. □

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

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 $e=a^{j-i}$, which is the result we desired.

Now we state a lemma which will be useful for the proofs after.

Lemma. *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,*

$$aa_i=aa_j\Rightarrow a_i=a_j$$

then $\{aa_1,aa_2,\ldots,aa_n\}$ is just a permutation of G. □

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

Proof. We list out the element, $G = \{a_1, \ldots, a_n\}$, then $aa_1, aa_2, \ldots, aa_n$ is a permutation of the list.

As G is abelian, we have $a_1, \ldots, a_n = aa_1, aa_2, \ldots, aa_n$, $a^n a_1 \ldots a_n = a_1 \ldots a_n \Rightarrow a^n = e$ □

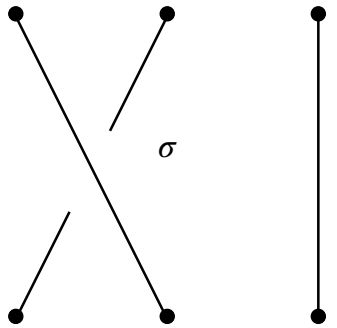
Example. Let G be a group, where $G = \{e, a, b\}$. We can write a table on binary operation.

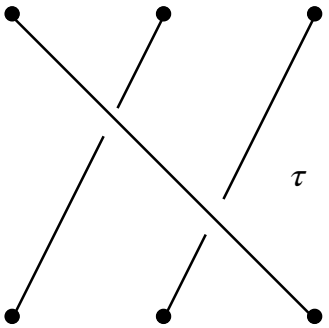
$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

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

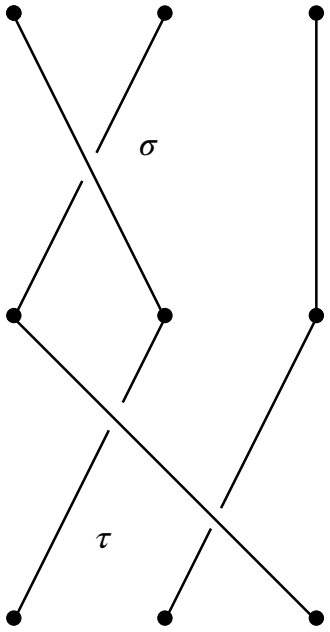
Example.

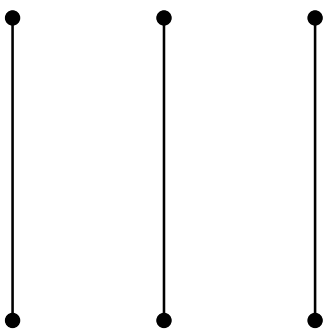
Let B_3 be a braid group with 3 strings. Define σ and τ to be the following.





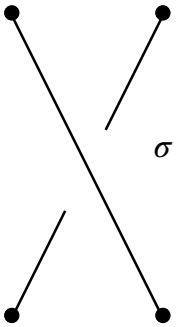
One may define the multiplication, $\sigma * \tau$, by joining the graph together with σ's bottom and τ's top. For example, $\sigma * \tau$ will be

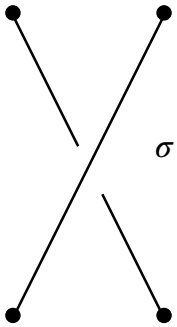


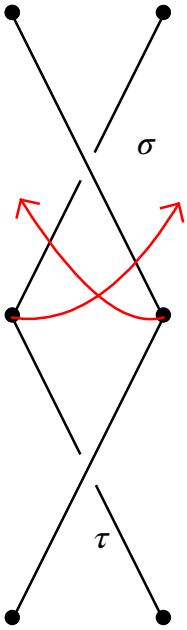
The identity element e can be defined as  , as no matter how you multiply the output still be the same.

Is $*$ associative? For sure yes! (Very intuitive)

Under the operation is there any inverse? Yes!

Let $\sigma =$ 


, then the inverse of $\sigma = \sigma' =$ 

Why? Consider $\sigma * \sigma'$: 


, and then 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"

[END OF 2023-09-21]

6 Groups of Permutation

Definition. *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.

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

Let $g: \mathbb{R} \to \mathbb{R}$, $g \mapsto e^x$ is not a permutation because it is one-to-one only.

Let $i: A \to A$, $\imath(a) = a$ is a permutation.

Consider $\sigma = \{1,2,3\} \to \{1,2,3\}$. The map

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

Is a permutation.

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

Lemma. *Define 3 maps, σ, τ, ϕ are map from $A \to A$.*

Then $(\sigma \circ \tau) \circ \phi = \sigma \circ (\tau \circ \phi)$

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

And $\sigma \circ (\tau \circ \phi)(a) = \sigma((\tau \circ \phi)(a)) = \sigma(\tau(\phi(a))) = (\sigma \circ \tau) \circ \phi(a)$, the identity thus holds. □

Theorem. *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 $\boxed{\circ}$ map. S_A is called the permutation group of set A.

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

Proof. *Note that $(\sigma \circ \imath) = \sigma(\imath(a)) = \sigma(a)$, this proves $\sigma \circ \imath = \sigma$.*

Also, $(\imath \circ \sigma) = i(\sigma(a)) = \sigma(a)$, this proves that $\imath \circ \sigma = \sigma$-

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

By lemma above, we have the associativity holds.

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

Note that $\sigma \circ \sigma^{-1} = \imath$ and $\sigma^{-1}\sigma = \imath$, 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.

Let $A = \mathbb{R}^2$, let g to be a 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.

Example. Theorem.

Let $A = \{1, 2, \ldots, n\}$. The $S_A = S_n$ is called the symmtric group on n letter.

We use a two-row matrix to present $\sigma \in S_n$. Then

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

For example, for $\sigma \in S_3$, we have

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

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

The identity element

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

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

Theorem. *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.

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

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. 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.

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

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. 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, then

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

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

7 Orbits, Cycles, Alternating Groups

Definition. ***Theorem.***

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: we may 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* $c = \tau^m(b) = \tau^m \circ \tau^n(a) = \tau^{m+n}(a)$ □

Theorem. *A can be written as disjoint union of equivalence class.*

Example. *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*.*

***Answer* 1.**

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.

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

———————————[END OF 2023-09-26]———————————

Definition. ***Cycle***

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

That is, σ *can only have one orbit with more than 1 element, all other orbits must have 1 element only.*

Definition. ***Length***

If σ *is a cycle,* $\sigma = e$ *has a length of 1. Otherwise, the length is defined by cardinality of its unique orbit with more than one element.*

Example.

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. 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 will use one row notation to denote a cycle with length not equal to e.

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

Example.

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, $(7,8,9) * 3 = 3$

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

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

Also the 3 cycles are disjoint.

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

In fact, 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 $(i_1,\ldots,i_s) \cap (j_1,\ldots,j_t) = \varnothing$. 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. *Every permutation is a product of disjoint cycles.*

Example. 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 $\sigma = (1,7,8,9)(4,5)$

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

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

Proof. *Let $\sigma = (a_1,\ldots,a_k)$. We can 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 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, let $i \in a_1$. Then:

LHS $= (a_1,\ldots,a_k) a_1 = a_2$, RHS $= (a_1,a_k),(a_1,a_{k-1}),\ldots,(a_1,a_2) a_1 = (a_1,a_k),(a_1,a_{k-1}),\ldots,(a_1,a_3) a_2 = a_2$ □

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

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

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

Case 2: $i\in\{2,7,1,9\}$, *say,* $i\in 9$. *Then* $(2,7,1,9)i=2$, *RHS*$=(2,9)(2,1)(2,7)i=(2,9)(2,1)9=(2,9)9=2$

Case 3 can be done in a similar way. □

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

Example. 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. Note that 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. *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. *(With a simpler, linear algebra version 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.* …

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

If we write $\sigma=r_1r_2\ldots r_s$ *as a product of s transposition, then we have*

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

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. □

Review

Theorem. *Every permutation in S_n is a product of disjoint cycles.*

Example. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 5 & 8 & 7 \end{pmatrix} \in S_8$. Then σ is a product of 3 disjoint cycles. Namely:

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

Definition. *A cycle of length 2 is called transposition.*

Example. *Let $\sigma = (3,5,6,7,8)$ be a cycle of length 5. We may represent $\sigma = (3,8),(3,7),(3,6),(3,5)$.*

Corollary. *Any permutation in S_n can be written as a product of transposition.*

Example. *Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 5 & 8 & 7 \end{pmatrix} \in S_8$. Then $\sigma = (1,4),(1,3),(1,2),(5,6),(7,8)$*

Theorem. *No permutation in S_n can be written as a product of even number of transposition and as a product of odd number of transposition.*

Example. *Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 6 & 5 & 1 & 2 & 4 \end{pmatrix}, \sigma = (1,3,8,2,7)(4,9)(5,6) = (1,7)(1,2)(1,8)(1,3)(4,9)(5,6)$.*

Theorem. *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 :*

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

Note that there are $2k-1$ transposition. Thus σ is odd. □

Theorem.

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 $\sigma = s_1 \ldots s_{2m}, \tau = t_1 \ldots t_{2n}$ in their transposition form.*

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

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

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

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

Proof. *Let σ be even. Then*

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

By similar proof, if σ is odd, we can also prove that σ^{-1} is also odd. □

Definition. ***Alternating Groups***

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

Proof. *(On A_n is a subgroup of S_n)*

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. *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. *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. as

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

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

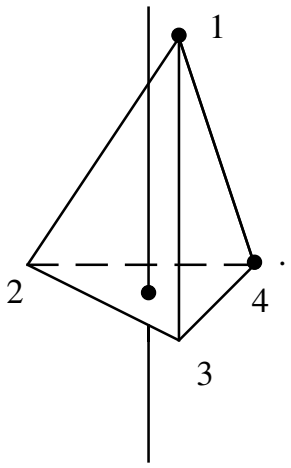
$$\begin{aligned} f((1,2)\tau) &= (1,2)(1,2)\tau \\ &= \tau \end{aligned}$$

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

How to find the elements in A_4?

Consider regular tetrahedron 

.

Note that tetrahedron have $120°, 240°$ 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. 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 $(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$.

8 Cosets, Theorem of Lagrange

Theorem. *Lagrange theorem*

If H is a subgroup of finite group G, then the order of H is a divisor of order of G.

Example.

A_3 is a subgroup of S_3. Note that $|S_6|=6, |A_3|=3$, then 3 is such divisor.

$(\mathbb{Z}_9,+)$ is a finite group, note that $<3>$ is a subgroup. Note that $|\mathbb{Z}_9|=9, |<3>|=3$. 3 is such divisior.

Definition 2. *Coset*

The left coset of H containing $a, a\in G$ is $aH=\{ah: h\in H\}$.

The right coset of H containing a os $Ha=\{ha: h\in H\}$.

Example 3. Let $H=\{h_1,\ldots,h_k\}$, then $aH=\{ah_1,\ldots,ah_k\}$.

———————————[END OF 2023-10-03]———————————

Review

Theorem 4. *Lagranian theorem*

If H is a subgroup of G, then $|G|$ is a multiple of $|H|$.

Definition 5. *Cosets*

Let $H\subset G$ be a subgroup. If $a\in G$, then $aH=\{ah: h\in H\}$. This is called the left coset of H containing a.

Example 6. 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 7. 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 lefts such as $1+3\mathbb{Z}$ and $2+3\mathbb{Z}$ have empty intersection.

Example 8. 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.

Example 9.

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: $\begin{cases} aH=bH \\ aH\cap bH=\varnothing \end{cases}$.

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

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

$\boxed{aH\subset bH}$

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. *Lagrange theorem*

If H is a subgroup of 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 11. 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 12. Everything proven for left coset also holds for right cosets.

Corollary 13. *If $|G|=p$ is prime, then G is cyclic group.*

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

Corollary 14. *If G is finite, $a\in G$, then order of a is a divisor of order of G.*

Review

***Definition* 15.** *Order*

The order of a is the smallest positive integer n, s.t. $a^n=e$, also, it can be defined as $|<a>|$.

***Example* 16.** *Let $G=\{e,a,b,c\}$ be a group. Note that the order of $e=1$, order of a,b,c are divisors of 4 by the Lagrange theorem. If one of a,b,c has order of 4, then G is cyclic. It proves that none of a,b,c has order 4 so that all of them have order of 2. Now one may construct the table of G.*

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Example 17. (As exericise)

If H_1, H_2 are subgroup of G, $|G|<\infty$, and $|H_1|$ and $|H_2|$ are relatively prime, prove that $H_1\cap H_2=\{e\}$.

Theorem 18. *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 19. Let $U_n=\{z\in\mathbb{C}: z^n=1\}=\left\{e^{\frac{2\pi i}{n}k}: k=1,2,...,k-1\right\}$. 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 $U_2\cap U_5=\{e\}$.

[END OF 2023-10-05]