

Some special symbols, notations and functions used in this note

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

Sections with square brackets are mostly proofs, reviews, and additional informations about the courses.

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 symmetrical (In both rotational and reflexional means).

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

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

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

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

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.

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

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 $x \in (A \cap C) \cup (B \cap C)$

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

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,

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

Definition. Map(Function)

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

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

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 $A \rightarrow B$ is given by n^m .

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

For a map $f: A \rightarrow B$

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** $f: A \rightarrow B$ exists.

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

If there is a **surjection** $h: A \rightarrow B$, 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 impossible to find a map which is one to one because the cardinality $|A| > |B|$

[END OF 2023-09-05]

However some strange phenomenon 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 $f(x) = \frac{2}{\pi}x, f: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \rightarrow (-1, 1)$ is bijective. Thus both have equal cardinality.

Definition. Partition

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

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

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

Example.

If $f: A \rightarrow B$ 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 $A = A_1 \sqcup A_2 \dots \sqcup A_n$ is a partition of A , we define relation \sim on A as follow.

$a \sim b$, if and only if a and b 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 $\tilde{a}_1 \cap \tilde{a}_2 = \emptyset$

Theorem.

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

Definition. Partial Order

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

$$1. a \leq a$$

$$2. a \leq b \text{ and } b \leq a \text{ implies } a = b$$

$$3. a \leq b \text{ and } b \leq c \text{ implies } a \leq c$$

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

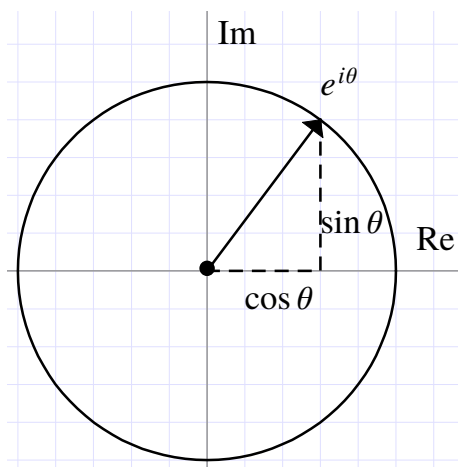
$$\begin{aligned}(a + bi) \cdot (c + di) &= ac + adi + bci + bd(i \cdot i) \\ &= (ac - bd) + (ad + bc)i\end{aligned}$$

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

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

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

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 $z^n = 1$,

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

Proof.

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

□

Definition. Binary Operation

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

For example, the addition $\boxed{+}$ we used is an example of binary operation, where

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

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,

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

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

- 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 $n \times n$ matrices, 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 a matrix with $|A| = 0$, for such a 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 a set is called $GL(n, \mathbb{R})$.

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

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

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

Thus the set is closed.

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

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

Thus $GL(n, \mathbb{R})$ 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 an infinite set.

Example.

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

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

- There is an 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 $U_n = \left\{e^{\frac{2\pi i}{n}k} | k=0, 1, \dots, n-1\right\}$, 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,

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

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,

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

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, $a * c = b * a \nRightarrow c = b$.

Proof for L-R cancellation:

<p>Left cancellation:</p> $a * b = a * c$ $a^{-1}(a * b) = a^{-1}(a * c)$ $(a^{-1}a) * b = (a^{-1}a) * c \quad \text{(Associative)}$ $e * b = e * c \quad \text{(Definition of identity element)}$ $b = c \quad \text{(Definition of identity element)}$	
<p>Right cancellation can be proved by similar method.</p>	

Proof of $a * c = b * a \nRightarrow c = b$

<p>Pick two element from $GL(\mathbb{Z}, 2)$, where $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$.</p> <p>(Remark: Lower triangle matrix and Upper triangle matrix do not commute)</p> <p>Define $C = ABA^{-1} \Rightarrow CA = AB$ (By multiplying A on both side)</p> <p>Find the inverse of A: (Trick)</p> $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ thus inverse } A^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ <p>As a result, we have $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$</p> <p>Thus $CA = AB$ does not implies that $C = B$, thus $a * c = b * a \nRightarrow c = b$.</p>
--

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 definition, 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 $S = \{n | n \notin \mathbb{Q} \text{ and } n \in \mathbb{R}\}$ 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 .

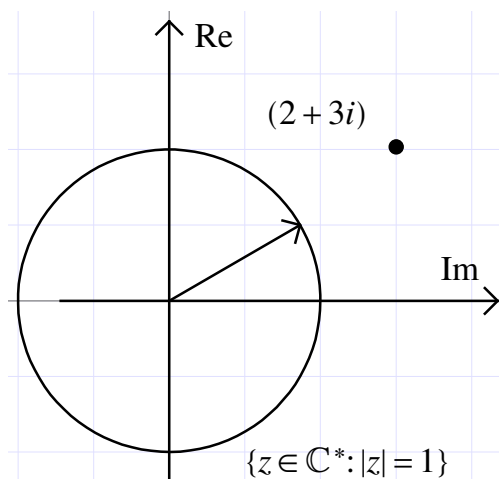
Then we check whether the inverse element exists.

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

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

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

$$a * b: ab$$

$$\underbrace{a * a * a * \dots * a}_n = a^n$$

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

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

$$a^0 = e$$

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 $e \in H$
- $\forall a \in H, a^{-1} \in H$

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

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

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 $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ to be a subgroup of G .

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

Moreover, $\langle a \rangle$ is the smallest subgroup.

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

Proof.

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

The identity element e exists in $\langle a \rangle$ 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. □

Example.

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

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

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

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

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

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

$$\langle 3 \rangle = \{0, 3, 3+3=6=0, \dots\} = \{0, 3\}$$

$$\langle 5 \rangle = \langle 5 \rangle = \{0, 5, 5+5=10=4, 5+5+5=15=3, 5+5+5+5=20=2, \dots\} = \{0, 1, 2, 3, 4, 5\}$$

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. $\langle a \rangle = G$.

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 generate \mathbb{Z}_n .

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

Example.

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

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

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

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

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

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

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

Proof. If $a \neq 0$, then $\frac{1}{2}a \notin \langle a \rangle$, contradiction! □

Example. (Extra)

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

A cyclic group is abelian group.

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

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

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

□

For arbitrary group G , $a \in G$, sometimes $\langle a \rangle$ is infinite, sometimes it is finite.

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

Theorem.

If $\langle a \rangle$ 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 $\{e, a, a^2, \dots, a^n\}$ could already form a subgroup, which contradicts the fact that $\langle a \rangle$ 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

$$\text{ord}(2) = \infty$$

$$\text{ord}(-1) = 2$$

$$\text{ord}(i) = \text{ord}(-i) = 4$$

$$\text{ord}(1) = 1$$

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

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

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

$\langle 8 \rangle = \{8, 16, 24 \rightarrow 0\}$ thus order of 8 = 3

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

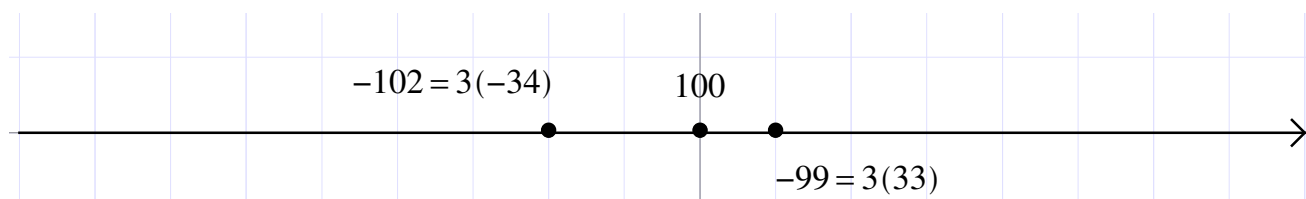
Lemma. Division algorithm for \mathbb{Z}

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 $G = \langle a \rangle$. 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 $\exists b \in H$, 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 $H = \langle a^m \rangle$

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

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

Consider $n \div m$ by division algorithm

$$n = mq + r$$

$$r = n - mq$$

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

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

□

Corollary. 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. $\because (m_1s + n_1r) + (m_2s + n_2r) = (m_1 + m_2)s + (n_1 + n_2)r \in H$.

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 $d = \text{GCD}(r, s) = ms + nr$ 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

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

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. $G = \langle a \rangle$.

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

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

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

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

Proof.

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

For any element g, h in G ,

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

□

Example.

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

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 $\langle a \rangle$.

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

Thus we have $\langle a \rangle$ 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

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

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 $GL(2, \mathbb{R})$, compute the order of the following element.

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

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 $0 \leq r < n$. $r = m - nq$. $a^r = a^{m-nq} = a^m a^{-nq} = a^m (a^n)^{-q} = e \times e^{-q} = e$

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 $(ab)(ab)(ab)\dots(ab) = e$

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

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 $\{a, a^2, a^3, \dots, a^N, a^{N+1}\}$ have $N + 1$ element. Then there exists 2 element which are not unique from the pigeonhole 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, $|G| = n$, $G = \{a_1, a_2, \dots, a_n\}$. For $a \in G$, $\{aa_1, aa_2, \dots, aa_n\}$ is a distinct list.

Proof. Assume that two terms in the list are equal, by cancellation law,

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

then $\{aa_1, aa_2, \dots, aa_n\}$ 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, $G = \{a_1, \dots, a_n\}$, then aa_1, aa_2, \dots, aa_n is a permutation of the list.

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

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

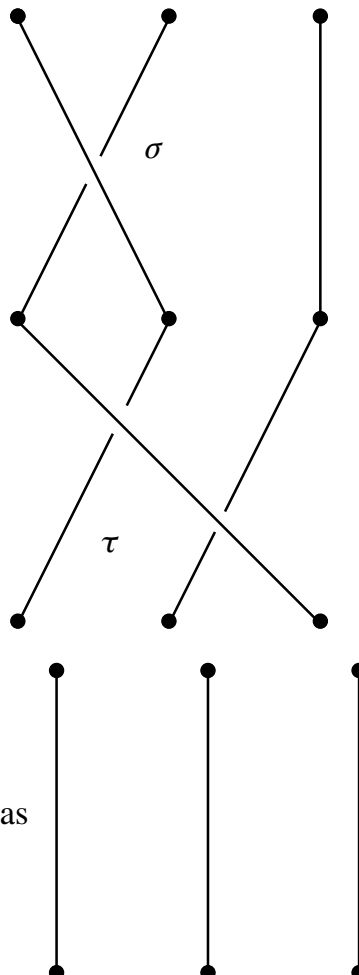
Note that the table is of permutation, and only hold for 2 and 3 element group.

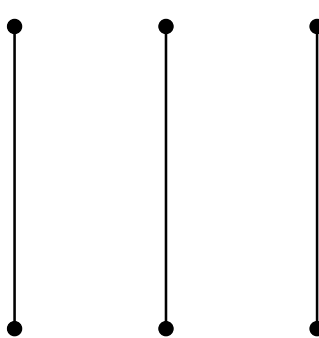
Example.

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



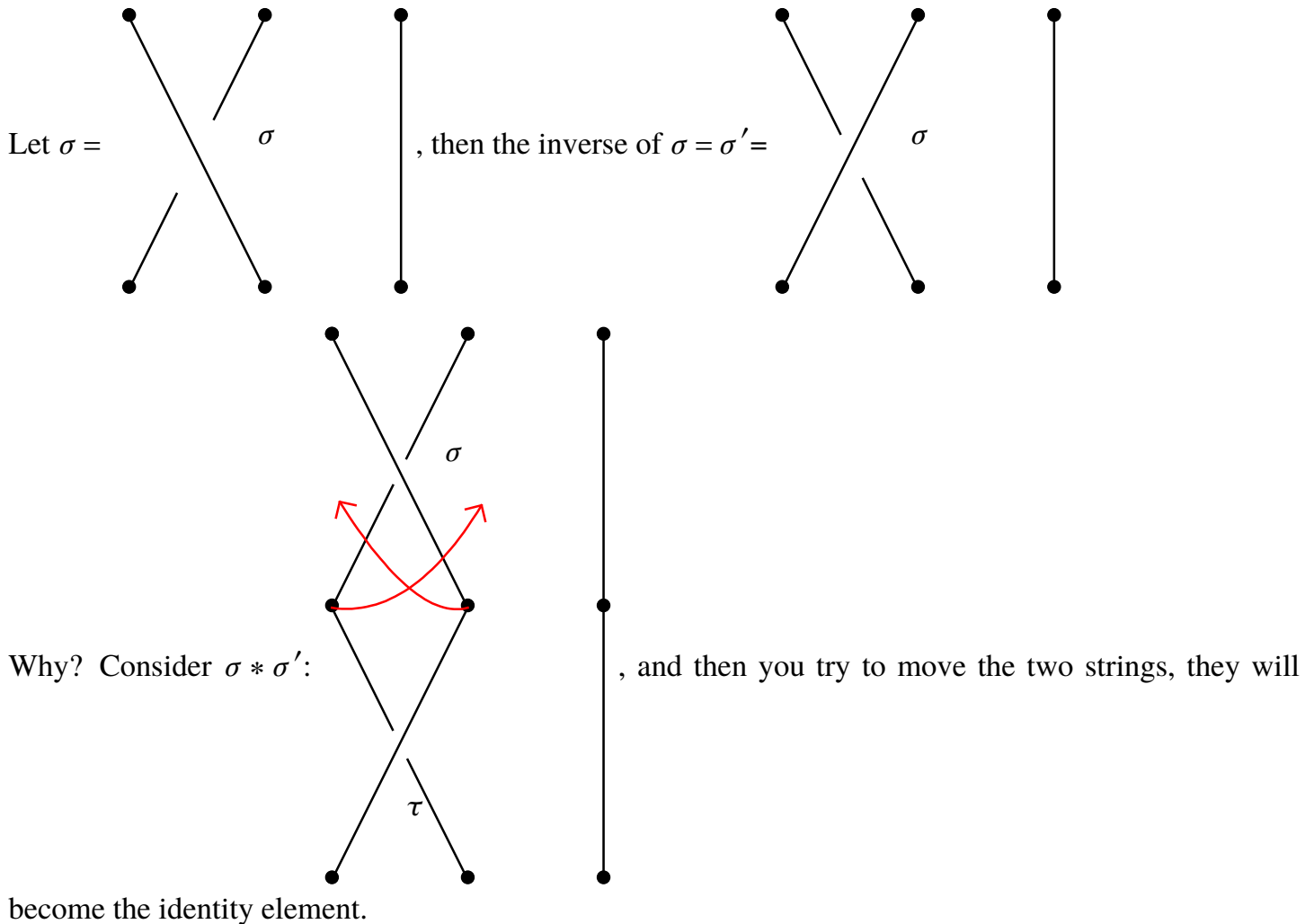
One may define the multiplication, $\sigma * \tau$, by joining the graph together with σ 's bottom and τ 's top. For example, $\sigma * \tau$ will be



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!



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 $\phi: A \rightarrow A$ is called a permutation of A , if it is one to one and onto.

Example.

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

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

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

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

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

Is a permutation.

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

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

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 \square map. S_A is called the permutation group of set A .

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

Proof. Note that $(\sigma \circ \iota) = \sigma(\iota(a)) = \sigma(a)$, this proves $\sigma \circ \iota = \sigma$.
 Also, $(\iota \circ \sigma) = \iota(\sigma(a)) = \sigma(a)$, 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 $\exists! a \in A$, 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.

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

Example. Theorem.

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

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

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

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

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

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, \dots, 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 $n(n-1)(n-2)\dots(2)(1) = n!$ permutations in S_n . \square

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 $\sigma^7(1) = \sigma^6(4) = \sigma^5(2) = \sigma^4(7) = \dots = \sigma(5) = 1$

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 $A = \{1, 2, \dots, n\}$ 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 $c = \tau^m(b) = \tau^m \circ \tau^n(a) = \tau^{m+n}(a)$ \square

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.

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

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 $i = 1, \dots, 9$. 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 $\sigma = (i_1, \dots, i_s)$ with length s , let $\tau = (j_1, \dots, j_t)$ with length τ . where $s, t > 1$.
 Then $(i_1, \dots, i_s) \cap (j_1, \dots, j_t) = \emptyset$. We want to prove that $(i_1, \dots, i_s) \circ (j_1, \dots, j_t) k = (j_1, \dots, j_t) \circ (i_1, \dots, i_s) k$.
 Case 1: $k \in (i_1, \dots, i_s)$. Then LHS = $(i_1, \dots, i_s)i$, RHS = $(i_1, \dots, i_s)k = \text{LHS}$.
 Case 2: $k \in (j_1, \dots, j_t)$: Similar proof as Case 1.
 Case 3: $k \notin (j_1, \dots, j_t) \notin (i_1, \dots, i_s)$: 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) interchanges 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 $\sigma = (a_1, \dots, a_k)$. We can write $\sigma = (a_1, a_k), (a_1, a_{k-1}), \dots, (a_1, a_2)$.
 Then $|(a_1, a_k), (a_1, a_{k-1}), \dots, (a_1, a_2)| = k - 1$.
 Now we prove that $(a_1, \dots, a_k)i = (a_1, a_k), (a_1, a_{k-1}), \dots, (a_1, a_2)i$.
 If $i \notin \{a_1, \dots, a_k\}$, then LHS = RHS = i .
 Otherwise, let $i \in a_1$. Then:
 LHS = $(a_1, \dots, a_k)a_1 = a_2$, RHS = $(a_1, a_k), (a_1, a_{k-1}), \dots, (a_1, a_2)a_1 = (a_1, a_k), (a_1, a_{k-1}), \dots, (a_1, a_3)a_2 = a_2$ □

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 $A = (a_1, \dots, a_n)$ 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 columns, and by linear algebra, by interchanging two columns, determinant is multiplied by -1 .

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

$$A \xrightarrow{r_s} r_s A \xrightarrow{r_{s-1}} r_s r_{s-1} A \rightarrow \dots \rightarrow \sigma A$$

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

We may also write $\sigma = \tau_1 \dots \tau_m$ 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. □

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 :

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

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 $\sigma = s_1 \dots s_{2m}, \tau = t_1 \dots t_{2n}$ 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. 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 $(g_1 \dots g_n)(g_1 \dots g_n)^{-1} = g_1 \dots g_n g_n^{-1} g_{n-1}^{-1} \dots g_1^{-1} = g_1 \dots e \dots g_1^{-1} = e$ □

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

Proof. Let σ be even. Then

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

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

Definition. Alternating Groups

If $n \geq 2$, then the set of all even permutations of $\{1, 2, \dots, n\}$ forms a subgroup of order of symmetric group of order $\frac{1}{2}n!$ of symmetric group S_n . 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 $f: A_n \rightarrow B_n$, 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

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

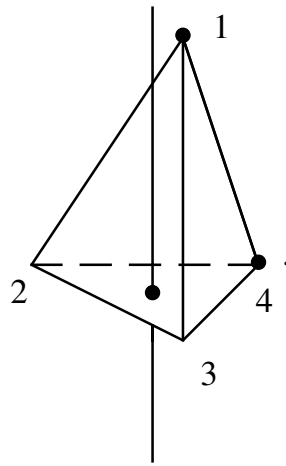
This proves that f is both onto and one-to-one. Hence f is a bijection. This implies that $|A_n| = |B_n|$.

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

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

How to find the elements in A_4 ?

Consider regular tetrahedron



Note that tetrahedron have $120^\circ, 240^\circ$ of rotational symmetry. Thus totally there are 8 elements related to this symmetry. And there are 3 more elements, that are obtained by rotating with 180° . 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) clockwise, 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.

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 $|S_3| = 6, |A_3| = 3$, then 3 is such divisor.

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

Definition. *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. Let $H = \{h_1, \dots, h_k\}$, then $aH = \{ah_1, \dots, ah_k\}$.

[END OF 2023-10-03]

Review

Theorem. *Lagrange theorem*

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

Definition. *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. 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. 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. 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.

Let $H = \{h_1, \dots, h_n\}$, and $|H| = n$. Then $|aH| = |\{ah_1, \dots, ah_n\}| = n$.

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 $c \in bH = bh_2, h_2 \in H$.

$$\boxed{aH \subset bH}$$

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. *Lagrange theorem*

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

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

Then $|G| = |a_1H| + \dots + |a_nH| = |H| + \dots + |H| = n|H|$ □

Example. 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. 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 $\langle a \rangle = G$. \square

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

Review

Definition. Order

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

Example. 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

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

Proof. Left as exercise. \square

Theorem. 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 subgroup of H .

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

Review

Theorem. Lagrange theorem

If H is a subgroup of finite group G , then $|H|$ is a divisor of $|G|$.

From this, we also have $\frac{|G|}{|H|} = n$, which is the number of left cosets of H .

Proof. Let a_1H, \dots, a_nH be a list of all left cosets of H . Then $G = a_1H \sqcup \dots \sqcup a_nH$.

Then $|G| = |a_1H| + \dots + |a_nH| = n|H|$ □

Example. Let $G = S_n$, then $H = A_n$ is a subgroup of G . We have $\frac{|S_n|}{|A_n|} = 2$, thus there are 2 left cosets, namely A_n and B_n , where B_n is the set of all odd permutations.

Example. Let $H \subset G$ be a subgroup. Prove that $aH = bH$, if and only if $b^{-1}a \in H$.

For example, we have $10\mathbb{Z} \in \mathbb{Z}$. Then $a + 10\mathbb{Z} = b + 10\mathbb{Z}$, if and only if $a - b \in 10\mathbb{Z}$.

Proof. (\Rightarrow)

If $aH \subset bH$, because $b \in bH (b = b \times e)$, then $b \in aH \Rightarrow b \in ah$ for some $h \in H$. Then

$$\begin{aligned} b^{-1}b &= b^{-1}ah \\ e &= b^{-1}ah \\ h^{-1} &= b^{-1}a \in H \end{aligned}$$

OR

If $a \in aH = bH$, then $a = bh_1, h_1 \in H$, thus $b^{-1}a = h_1 \in H$.

(\Leftarrow)

Suppose:

$$\begin{aligned} b^{-1}a &\in H \\ b^{-1}a &= h \in H \\ bb^{-1}a &= bh \\ a &= bh \\ a &= ae \in aH \\ bh &\in bH \\ a &\in aH \cap bH \end{aligned}$$

□

9 Direct Product, Finitely Generated Abelian Groups

Definition. 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

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

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

Example.

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. 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 $e_1 \in G_1, \dots, e_n \in G_n$ are the identity elements, then identity element is (e_1, \dots, e_n) .

Associativity: We prove 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. If G_1, \dots, G_n are Abelian group, then $G_1 \times \cdots \times G_n$ is also Abelian group.

Example. HW#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 $(a, b) + \dots + (a, b) = (5a, 5b) = (0, 0)$. Thus (a, b) will generate a group of 5 elements, but never 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 $\underbrace{(1, 1) + \dots + (1, 1)}_n = (n, n) = (0, 0)$ 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. 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.

Definition. 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 $k_1, \dots, k_m \in \mathbb{Z}$.

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

Also, let $S' = \{(1, 2), \dots, (n-1, n)\}$. This interchange two integers. Then S' can generate S_n . (Not required)

Consider $GL(3, \mathbb{R})$, 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:

$$\begin{aligned} (A|I) &\xrightarrow{\text{1st row operation}} (E_1 A_1 | E_1 I_3) \\ &\xrightarrow{\text{2nd row operation}} (E_2 E_1 A_1 | E_2 E_1 I_3) \\ &\vdots \\ &\xrightarrow{\text{mth row operation}} (E_m E_{m-1} \dots E_2 E_1 A_1 | E_m E_{m-1} \dots E_2 E_1 I_3) \end{aligned}$$

$$\begin{aligned} (E_m E_{m-1} \dots E_2 E_1) A &= I \\ A^{-1} &= (E_m E_{m-1} \dots E_2 E_1) \end{aligned}$$

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

Definition. Let G be a group, let $S \subset G$ be a subset. S generates G , if every $g \in G$ can be expressed as

$$g = a_1^{k_1} \dots a_n^{k_n}$$

for some $a_1, \dots, a_n \in S, k_1, \dots, k_n \in \mathbb{Z}$.

Example. 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:

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

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

Example.

Consider $\mathbb{Z} \times \mathbb{Z} = \{(m, n) : m, n \in \mathbb{Z}\} \subset \mathbb{R}^2$. 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 $T = \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$ 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. A group G is called a finitely generated group, if there is finite subset S that generates G .

Example.

A finite group is finitely generated.

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

$\mathbb{Z}_{k_1} \times \dots \times \mathbb{Z}_{k_n} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_m$ is finitely generated.

Definition. Isomorphic (Brief introduction)

G and G' is isomorphic, if there is $\phi: G \rightarrow G'$, where ϕ is bijective, and ϕ preserves group structure, i.e. $\phi(ab) = \phi(a)\phi(b)$.

Theorem. **★ 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, \dots, p_n are primes, r_1, \dots, r_n are positive integers. $m > 0$.

Definition. Vector Space

A vector space is a set with two operation: addition, $+: V \times V \rightarrow V$, and scalar multiplication, $\cdot: \mathbb{R} \times V \rightarrow V$, 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.

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.

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

Section 12 (Symmetry) is skipped

10 Homomorphisms

Definition. A map $\phi: G \rightarrow G'$ 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. $\phi: G \rightarrow G'$ 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 $\phi: G_1 \rightarrow G_2$

Example.

Let \mathbb{R} is a group under $+$, and $\mathbb{R}_{>0}$ is a group under multiplication. Find an isomorphism $\phi: \mathbb{R} \rightarrow \mathbb{R}_{>0}$. Take $\phi: \mathbb{R} \rightarrow \mathbb{R}_{>0} = e^x$. Then $\phi(x)$ is actually a bijection. And also $e^{a+b} = e^a e^b$. This implies that actually \mathbb{R} and $\mathbb{R}_{>0}$ are isomorphic, even under the different operations.

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

Example. Consider the regular tetrahedron again, there are totally 12 symmmtries, 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. Consider a regular triangle. There are rotational symmetry, which are $\{120^\circ, 240^\circ, 360^\circ = 0^\circ\}$, and also there are 3 reflections. Thus $|G| = 6$. Thus such group is isomorphic to S_3 .

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

—————[END OF 2023-10-12]—————

Review

Definition. A map $\phi: G \rightarrow G'$ is called a homomorphism if:

$$\phi(ab) = \phi(a)\phi(b), \forall a, b \in G$$

Note that if G has binary operation $*$, while G' has binary operation \star , then $\phi(a, b) = \phi(a)\phi(b)$ means

$$\phi(a * b) = \phi(a) \star \phi(b), \forall a, b \in G$$

Definition. An isomorphism $\phi: G \rightarrow G'$ is a homomorphism and is bijective.

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

Proof. We aim to prove that $\phi(x + y) = \phi(x) \cdot \phi(y)$.

Note that

$$\begin{aligned} \text{LHS} &= e^{x+y} \\ \text{RHS} &= e^x \cdot e^y \\ &= e^{x+y} \\ &= \text{LHS} \end{aligned}$$

□

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

Definition. Two groups G_1, G_2 are isomorphic, if there exists an isomorphism $\phi: G_1 \rightarrow G_2$.

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

Proof. (1) By contradiction

Suppose S_3 and \mathbb{Z}_6 are isomorphic. Then we have an isomorphism $\phi: S_3 \rightarrow \mathbb{Z}_6$.

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

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

Note that by homomorphism property,

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

By the property of homomorphism,

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

Contradiction! □

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

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

Proof. Note that

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

By cancellation law, we have

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

□

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

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

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

Proof.

(\Rightarrow)

If $a^n = e$, apply ϕ on both sides, we have

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

(\Leftarrow)

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

□

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

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

Case 1: $|G| = |G'| = n \in \mathbb{Z}_{>0}$

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

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

Theorem.

Let $\phi: G \rightarrow G'$, $\phi(x) = x$ is always isomorphic.

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

Proof. Trivial.

□

Example.

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

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

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

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

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

Example. Let $\phi: \mathbb{R}_{>0} \rightarrow \mathbb{R}, \phi(x) = \log_a(x)$ 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:

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

Thus ϕ is strictly increasing, ϕ is one-to-one.

onto

As:

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

And ϕ is continuous, thus ϕ is onto.

□

Example. (HW #4) Find a homomorphism $\phi: \mathbb{R} \rightarrow \mathbb{R}^*$ such that $\phi(2) = 3$

Note that:

$$\begin{aligned} a^2 &= 3 \\ a &= \sqrt{3} \end{aligned}$$

Thus one possible map $\phi(x) = (\sqrt{3})^x$.

Example. (HW #4)

If $\phi_1: G_1 \rightarrow G_2$ is a homomorphism, $\phi_2: G_2 \rightarrow G_3$ is a homomorphism, then $\phi_1 \circ \phi_2: G_1 \rightarrow G_3$ is also a homomorphism.

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

Note that:

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

□

Example. Find a homomorphism

$$f: \text{GL}(2, \mathbb{R}) \rightarrow \mathbb{R}$$

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

Consider:

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

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

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

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

[END OF 2023-10-17]

Review

Definition. Homomorphism

A map $\phi: G \rightarrow G'$ is a homomorphism if $\phi(ab) = \phi(a)\phi(b)$

Example. $\phi: \mathbb{R}^* \rightarrow \mathbb{R}$, where $\phi \mapsto \log_{10} |a|$ is a homomorphism.

Proof.

$$\log_{10} |ab| = \log_{10} |a| + \log_{10} |b|$$

□

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

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

Proof.

(1)

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

(2)

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

(3)

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

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

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

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

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

(4)

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

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

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

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

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

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

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

Definition. Kernal

If $T: V \rightarrow V'$ is a linear map, then $\ker(T) = T^{-1}(0)$.

Example. Consider:

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

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

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

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

Midterm review note is stored separately.

See <https://smokingpuddle58.github.io/#course> for more details.

[END OF 2023-10-19]

Review

Definition. Kernel

If $T: V \rightarrow V'$ is a linear map, then $\ker(T) = T^{-1}(0)$.

Definition. Kernel

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

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

Then

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

Theorem.

Let $\phi: G \rightarrow G'$ be a homomorphism of groups, $\ker(\phi) = H$.

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

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

Example.

Let $\phi: \mathbb{R}^* \rightarrow \mathbb{R}^*$, and $\phi(x) = |x|$. As $|xy| = |x||y|$, thus ϕ is a homomorphism.

Then $\ker(\phi) = \{a \in \mathbb{R}^*: \phi(a) = 1\} = \{a \in \mathbb{R}^*: |a| = 1\} = \{1, -1\}$

Let $b \in \mathbb{R}^*$. Then

$$\begin{aligned} \phi^{-1}(b) &= \{x \in \mathbb{R}^*: \phi(x) = b\} \\ &= \{x \in \mathbb{R}^*: |x| = b\} \end{aligned}$$

Then $b = -2$.

Case 1: If $b < 0$

Proof.

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

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

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

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

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

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

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

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

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

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

This proves such theorem. □

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

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

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

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

Theorem.

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

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

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

- $(*)$ has no solution

- If $x = a \in \mathbb{R}^m$ is a solution, then every other solution can be written as :

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

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

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

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

Corollary.

A group of homomorphism $\phi: G \rightarrow G'$ is a one to one map iff $\ker(\phi) = \{e\}$.

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

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

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

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

Example. Let $\phi: U_4 = \{1, -1, i, -i\} \rightarrow U_2 = \{1, -1\}$, let $\phi(z) = z^2$.

Then

$$\phi^{-1}(1) = \{1, -1\}$$

Definition. Normal Subgroup (13.19)

A subgroup H of a group G is a normal subgroup if $\forall g \in G, gH = Hg$

Example.

If G is abelian, then every subgroup is normal.

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

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

$$(1, 3)H = \{(1, 3), (1, 2, 3)\}$$

$$H(1, 3) = \{(1, 3), (1, 3, 2)\}$$

H is thus not a normal subgroup.

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

$$gbg^{-1} \in H$$

Proof.

\Rightarrow

Suppose H is normal, then $gH = Hg$, then $gh \in gH = Hg$, then $gh = h'g$ for some $h' \in H$. Then $ghg^{-1} = h' \in H$, hence $\forall g \in G, b \in H, gb g^{-1} \in H$.

\Leftarrow

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

$gH \subset Hg$

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

Thus $gH \subset Hg$

$Hg \subset gH$

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

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

Example. Prove that A_n is a normal subgroup of S_n .

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

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

Theorem.

If $\pi: G \rightarrow G'$ is a homomorphism, then $\ker(\pi)$ is a normal subgroup of G .

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

Thus $ghg^{-1} \in \ker(\pi)$. □

Example. Define special linear group as:

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

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

Quiz results and answers have been released. Details please see the canvas files. Thanks

11 Factor Groups

Theorem.

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

1. Binary operation on G/H defined by:

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

is well defined.

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

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

Proof.

(1)

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

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

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

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

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

(2)

Associativity:

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

Thus the associativity holds in G/H .

Identity

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

Inverse

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

Thus G/H is a group. □

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

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

In general, $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_n$

Theorem.

- If G is finite, then $|G/H| = \text{number of cosets of } H = \frac{|G|}{|H|}$.
- Let H be a normal subgroup of G , G/H be the factor group of G by H . Then the map $\gamma: G \rightarrow G/H, \gamma(a) = aH$ is a homomorphism and $\ker(\gamma) = H$.
- If $\phi: G \rightarrow G'$ is a group homomorphism, then $\ker(\phi) = \{x \in G: \phi(x) = e'\}$ is a normal subgroup of G .

Proof.

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

Thus γ must be a homomorphism.

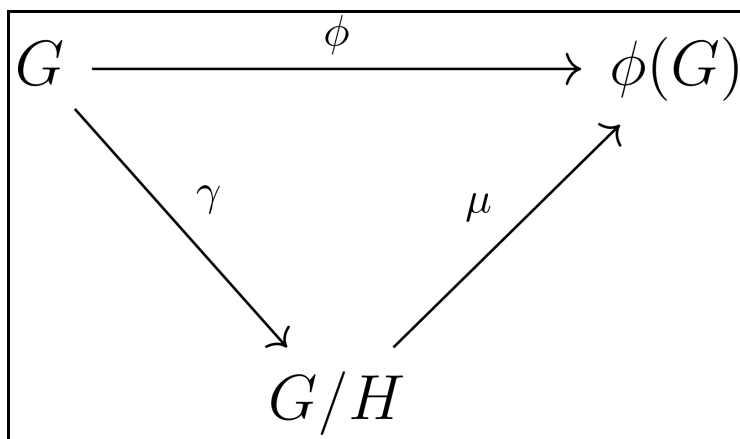
$$\begin{aligned}\ker(\gamma) &= \{a \in G: \gamma(a) = eH\} \\ &= \{a \in G: aH = eH\} \\ &= \{a \in G: a \in H\} \\ &= H\end{aligned}$$

□

Theorem. *The Fundamental Homomorphism Theorem for Groups*

Suppose that $\phi: G \rightarrow G'$ is a group homomorphism, with $\ker(\phi) = H$, then:

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



Proof.

We only prove the second property.

Well-definedness

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

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

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

This proves the well-definedness.

μ is homomorphism

Note that

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

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

μ is one-to-one

Note that μ is clearly onto.

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

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

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

□

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

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

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

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

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

Proof.

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

□

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

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

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

Theorem. The linear algebra version of 1st fundamental theorem for linear maps

If $\phi: V \rightarrow V'$ is a linear map, $S = \ker(\phi) = \{x \in V: \phi(x) = 0\}$, then $\mu: V/S \Rightarrow \phi(V')$ given by $\mu(a + S) = \phi(a)$ is well-defined, moreover, it is linear isomorphism.

Proof.

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

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

[END OF 2023-10-31]

12 Group action on a set

Intuition

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

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

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

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

Definition. Group Action

Let G be a group, X be a set. An group action of G on X is a map:

$$G \times X \rightarrow X$$

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

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

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

Then σx is the image of x under permutation σ .

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

Note. If A is a 2×2 matrix, then A introduces a linear map from $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ for $v \in \mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\}$

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

Proof.

The identity element is given by $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $I_2 v = v$

Moreover, $(AB)v = A(Bv)$ as matrix multiplication is associative. \square

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

Example.

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

Let R_a be the rotation along the centre anticlockwisely by a° .

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

Let L_M be the reflexion along the axis M .

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

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

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

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

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

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

Proof.

Closeness

If $g_1 g_2 \in G_x$, then $(g_1 g_2)x = g_1(g_2 x) = g_1(x) = x$, thus $g_1 g_2 \in G_x$, thus G_x is closed in operation.

Identity

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

Inverse

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

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

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

Thus G_x is the subgroup. □

Example.

Let $G = GL(2, \mathbb{R})$ acts on \mathbb{R}^2 .

Then $G_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} = \left\{ g \in GL(2, \mathbb{R}) : g \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0 \right\} = GL(2, \mathbb{R})$

For $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{R}^2$, we have $G_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \left\{ g \in GL(2, \mathbb{R}) : g \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0 \right\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : d \in \mathbb{R}^*, b \in \mathbb{R} \right\}$.

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

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

Definition.

Let G act on X , $x \in X$, then define:

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

This is called the orbit of x .

Intuition

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

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

Example.

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

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

Example.

Consider $G = S_5$ acts on $X = \{1, \dots, 5\}$. Then $G1 = \{\sigma(1) : \sigma \in S_5\} = X$.

In fact, $G1 = G2 = G3 = G4 = G5 = X$.

Theorem.

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

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

Example. Consider a cube, where X is the set of 6 faces, G is the symmetry group of the cube. G acts on X , and $X = \{1, 2, 3, 4, 5, 6\}$.

Then $G1 = X$, and as $|G_1| = 4$ (The rotation symmetry is 4), thus $|G| = 4 \times 6 = 24$.

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

REVIEW

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

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

G_x is called the isotropy subgroup or stabilizer of x , and Gx is called orbit of x .

Theorem.

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

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

Proof.

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

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

$$\varphi(gG_x) = gx$$

Note that φ is well defined, i.e.

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

Onto

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

Obviously φ is a onto map.

One-to-one

Suppose

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

Hence φ is one-to-one

This implies φ is a bijection

Thus

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

□

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

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

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

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

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

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

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

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

Proposition. *If G acts on X , then:*

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

Example.

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

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

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

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

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

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

13 Ring and Fields

Here, we give some informal definition of a ring:

A ring is a set with two binary operation, $+$, \cdot .

Then the following are considered as rings:

$$\begin{array}{ll} (\mathbb{Z}, +, \cdot) & (\mathbb{Q}, +, \cdot) \\ (\mathbb{R}, +, \cdot) & (\mathbb{C}, +, \cdot) \end{array}$$

Definition. A ring is a set R with an addition and a multiplication following the axioms below:

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

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

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

Example.

For a positive integer n , let $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$.

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

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

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

Definition. Commutative Rings

A ring R is a commutative ring, if the multiplication is commutative. i.e.

$$ab = ba$$

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

Example.

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

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

However, such ring is not a commutative ring.

Example.

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

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

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

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

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

Example.

If R_1, \dots, R_n are rings, then the product set $R_1 \times \dots \times R_n$ is a ring under

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n), \text{ and}$$

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

Theorem.

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

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

Proof.

1

Note that:

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

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

2

Note that:

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

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

3

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

□

Review

Definition. A ring is a set R with an addition and a multiplication following the axioms below:

1. $(R, +)$ is an abelian group
2. \times is associative.
3. Distributive law holds.

Definition. Ring Homomorphism

Let R, R' be two rings, Define $\phi: R \rightarrow R'$ is called a ring homomorphism if:

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

Example.

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

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

Example.

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

Proof.

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

Thus ϕ gives a ring homomorphism. □

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

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

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

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

Note that

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

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

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

□

Definition. Ring Isomorphism

An isomorphism $\phi: R \rightarrow R'$ from ring R to ring R' is a homomorphism that is bijective.

Example.

Let $\phi: \mathbb{C} \rightarrow A$, where $A = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a ring,

and $\phi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ gives a ring **isomorphism**.

Definition.

A ring R with multiplicative identity element (unity) is a ring with unity. It is usually denoted by 1 , which satisfies $1 \times a = a \times 1 = a, \forall a \in R$.

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

Why $1 \neq 0$?

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

Example.

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

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

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

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

For $C[0, 1]$, then f is a unit iff $f(a) \neq 0, \forall a \in [0, 1]$.

Definition. Division Ring and Field

Let R be a ring with unity 1 , we call R a division ring if every nonzero element $a \in R$ is a unit.

A commutative division ring is called a field.

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

- R is commutative
- R has a unity 1

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

Example.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. However, \mathbb{Z} is not a field.

14 Integral Domain

Intuition

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

Example. In $\mathbb{Z}_{10}, 4 \neq 0, 5 \neq 0$, however, $4 \times 5 = 20 = 0!!!$

Definition.

Let R be a commutative ring. $a \in R$ is called a zero divisor if $a \neq 0$, and there is $b \neq 0, ab = 0$.

Example.

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

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

Theorem.

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

Proof.

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

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

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

Example. Consider $C[0, 1]$, let:

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

Then $f(x)g(x) = 0$

(P.S. $f(x)$ actually has the shape of a “ReLU” activation function.)

Definition.

A ring D is a integral domain, if it satisfies:

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

Example.

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

$C[0, 1]$ is not integral domain. (As it does not satisfies 3)

\mathbb{Z}_{10} is not a integral domain.

In general, if n is not prime number, then \mathbb{Z}_n is not a integral domain.

Proof.

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

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

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

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

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

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

[END OF 2023-11-09]

Review

A ring R is called a field, if and only if:

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

Example.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. However, \mathbb{Z} is not a field.

A ring D is a integral domain, if it satisfies:

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

Theorem.

Every field is an integral domain.

Proof.

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

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

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

Which leads to contradiction.

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

□

Example. \mathbb{Z} is an integral domain but is NOT a field.

From this we can see such relation:

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

Theorem. \mathbb{Z}_n is a integral domain if and only if n is prime.

Proof. See above.

□

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

$$ab = ac \Rightarrow b = c$$

Proof.

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

as a is not a zero-divisor.

□

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

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

We list all element in D :

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

where $|D| = n + 1$.

Consider the following list

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

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

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

15 Fermat's and Euler's Theorem

Theorem. *Fermat's theorem*

If p is prime, $a \in \mathbb{Z}$, then $a^p - a$ is a multiple of p .

Proof.

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

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

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

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

Now we prove by MI.

Let $a = 1$, then

$$a^p - a = 0$$

The result holds.

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

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

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

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

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

Thus $\binom{p}{j}$ is a multiple of p . So Δ is a multiple of p . The results holds for $a = n + 1$. □

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

Theorem. Equivalent Formulation of Fermat's Theorem

If p is a prime, a is **NOT** a multiple of p , then $a^{p-1} - 1$ is a multiple of p .

Proof. Note that

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

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

Conversely, we have:

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

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

Definition. Euler's phi function

Define $\varphi(n)$ for some positive integer n , where it satisfies:

$$\varphi(1) = 1$$

$$\varphi(mn) = \varphi(m)\varphi(n)$$

$$\varphi(p^k) = p^k - p^{k-1}$$

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

Example.

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

Theorem. Euler's Theorem

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

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

Proof.

From the corollary: If G is a finite group, $a \in G$, then $a^{|G|} = e$.

One can produce two groups from \mathbb{Z}_n , namely $(\mathbb{Z}_n, +)$ and (G_n, \times) where G_n is the set of elements in \mathbb{Z}_n having inverse.

Then $|G_n| = \varphi(n)$.

Anyway, professor claims there is no time, so I skip the remaining proof for now. □

Anyway here are somethings that is not in syllabus, but fun ☺

Theorem. Fermat's Theorem

A prime p is a sum of two squares, iff $p \equiv 1 \pmod{4}$

Theorem. Fermat's Last Theorem

For $n \geq 3$, the following equation:

$$a^n + b^n = c^n$$

has only trivial solution. (i.e. $b = 0, a = c$).

Proof. I have a proof of this theorem, but there is not enough space in this margin.

(No, actually the proof is quite not trivial so I'll not include this) □

[END OF 2023-11-14]

This part is not completed. Author of this note will complete this part tomorrow, with the help from the lecture notes.

If F is a field, i.e. F is commutative, $1 \in F, 1 \neq 0, \forall a \in F, a \neq 0, a^{-1}$ exists, then $G(F) = F - \{0\}$.

Consider the group $\mathbb{Z}_n, n > 2$, then the zero-divisors are $a \in N$

Example.

$$G_2 = \{1\}$$

$$G_3 = \{1, 2\}$$

$$G_4 = \{1, 3\}$$

$$G_5 = \{1, 2, 3, 4\}$$

$$G_6 = \{1, 5\}$$

$$G_7 = \{1, 2, \dots, 6\}$$

$$G_8 = \{1, 3, 5, 7\}$$

Define $|G_n| = \varphi(n) = \#$ of positive integers $j, j \in [1, n), j$ is relatively prime to n following the properties below.

- If a, b are relatively prime, then $\varphi(ab) = \varphi(a)\varphi(b)$
- For $n = p^k$ for some primes p , we have $\varphi(p^k) = p^k - p^{k-1}$.

Proof.

(2)

Consider:

$$\begin{array}{c} 1, 2, \dots, p \\ p+1, p+2, \dots, 2p \\ \vdots \\ (p-1)p^{k-1} + 1, \dots, p^k \end{array}$$

As p is a prime number, an positive integer b is relatively prime to p^k iff b is not a multiple of p .

In the list $1, 2, 3, \dots, p^k$, $\frac{p^k}{p} = p^{k-1}$ of them are a multiples of p .

Then $(p^k - p^{k-1})$ of them are relatively prime to p .

This implies $\varphi(p^k) = p^k - p^{k-1}$.

(1)

Consider \mathbb{Z}_{nm} , note that it is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$, provided that they are relatively prime.

Then the unit of \mathbb{Z}_{nm} , $G(\mathbb{Z}_{nm}) \cong G(\mathbb{Z}_m) \times G(\mathbb{Z}_n)$. □

Theorem. Generalization of Fermat's theorem

Let n be a positive integer greater than 2, b is relatively prime to n , then $b^{\varphi(n)} - 1$ is a multiple of n .

Proof.

Consider the group $G(n)$, then $|G(n)| = \varphi(n)$.

As b is relatively prove to n , $b \in G(n)$, thus $b^{\varphi(n)} = 1$ in $G(n)$.

Then $b^{\varphi(n)-1}$ is a multiple of n . □

Example.

$$\begin{aligned} \varphi(1000) &= \varphi(2^3 5^3) \\ &= (2^3 - 2^2)(5^3 - 5^2) \\ &= 400 \end{aligned}$$

Can we evaluate the last digit of 3^{400} without applying the Fermat's theorem? Yes!

$$\begin{aligned} 3^{400} &= (3^2)^{200} \\ &= (10 - 1)^{200} \\ &\equiv \sum_{i=0}^{200} \binom{200}{i} 10^i (-1)^{200-i} \\ &\equiv 1 - \binom{200}{1} 10 + \binom{200}{2} 10^2 \\ &\equiv 1 \pmod{1000} \end{aligned}$$

Let's discuss some HW problems.

(5) Let R be a commutative ring with unity 1, suppose $a \in R$ with $a^2 = 0$, prove that the set $S = \{1 + ax | x \in R\}$ is a group under the multiplication.

(Something extra not in HW) Suppose R is finite, prove that $|G|$ is divisor of $|R|$.

Proof. Pick arbitrary two elements $(1 + ax), (1 + ay) \in G$, then we have

$$\begin{aligned}(1 + ax)(1 + ay) &= 1 + ay + ax + a^2xy \\ &= 1 + a(x + y)\end{aligned}$$

This implies that G is closed under multiplication.

$$1 = 1 + a0 \in G,$$

S is associative by the axiom of rings.

For any $1 + ax \in G$, $1 + a(-x) \in G$.

$$(1 + ax)1 + a(-x) = 1$$

Therefore all element in G has an inverse in G . So G is a group. □

Proof.

Wrong proof for Suppose R is finite, prove that $|G|$ is divisor of $|R|$. □

As G is a subgroup of $(R, +)$, by Lagrange theorem, then $|G|$ is a divisor of R .

Correct proof for Suppose R is finite, prove that $|G|$ is divisor of $|R|$.

As $(1 + ax)(1 + by) = 1 + a(x + y)$, therefore the map defined by

$$\phi: R \rightarrow G, \phi(x) = 1 + ax$$

is a group homomorphism. Note that ϕ is surjective, therefore $\phi(R) = G$.

By homomorphism theorem, $R/\ker(\phi)$ is isomorphic to G .

Therefore, $|G| = \frac{|R|}{|\ker(\phi)|} \Rightarrow |R| = |G||\ker(\phi)|$. $|G|$ is a divisor of R .

Now, we modify the condition, such that $a^n = 0$.

(1)

$$\begin{aligned}(1 + ax)(1 + by) &= 1 + ax + ay + a^2xy \\ &= 1 + a(x + y + axy) \in G \\ (1 + ax)(1 - ax + (ax)^2 - (ax)^3 + \dots + (-1)^{n-1}(ax)^{n-1}) &= 1\end{aligned}$$

(2)

Did not prove. Left as exercise.

Review

Let R be a commutative ring with unity 1, suppose $a \in R$ with $a^n = 0, n > 0$.

1. Prove that the set $S = \{1 + ax | x \in R\}$ is a group under the multiplication.
2. Suppose R is finite, prove that $|G|$ is divisor of $|R|$.

Proof.

(1)

We have, for any commutative ring, that

$$1 - y^n = (1 - y)(1 + y + y^2 + \cdots + y^{n-1})$$

Proof:

$$\begin{aligned} \text{RHS} &= 1 + y + y^2 + \cdots + y^{n-1} - y(1 + \cdots + y^{n-1}) \\ &= 1 + y + \cdots + y^{n-1} - (y + y^2 + \cdots + y^n) \\ &= 1 - y^n \end{aligned}$$

Now we let $y = -ax$, we then have:

$$\begin{aligned} 1 - (-ax)^n &= (1 - (-ax))(1 + (-ax) + \cdots + (-ax)^{n-1}) \\ 1 - (-1)^n a^n x^n &= (1 - (-ax))(1 + (-ax) + \cdots + (-ax)^{n-1}) \\ (1 - (-ax))(1 + (-ax) + \cdots + (-ax)^{n-1}) &= 1 \end{aligned}$$

Note that $(1 - (-ax))$ has inverse of $1 + (-ax) + \cdots + (-ax)^{n-1} \in G$, as

$$1 + (-ax) + \cdots + (-ax)^{n-1} = 1 + a(-x + \cdots - a^{n-2}x^{n-1})$$

(2)

Wrong proof for Suppose R is finite, prove that $|G|$ is divisor of $|R|$.

As G is a subgroup of $(R, +)$, by Lagrange theorem, then $|G|$ is a divisor of R .

Correct proof for Suppose R is finite, prove that $|G|$ is divisor of $|R|$.

Let $A = \{ax : x \in R\}$. As A is a group under $+$, therefore $a0 = 0 \in R$.

$(ax + ay) = a(x + y)$ implies A is closed under $+$.

$(ax) + a(-x) = 0$ implies $a(-x) \in A$ has additive inverse exists in A . Therefore A is a group under $+$.

A is therefore a subgroup of R .

By Lagrange theorem $|A|$ is a divisor of R .

Therefore we have $G = 1 + A \Rightarrow |G| = |1 + A| = |A|$

□

16 The field of quotients of an integral domain

Recall

Definition.

A ring D is a integral domain, if it satisfies:

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

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

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

Example. \mathbb{Z} is a integral domain but \mathbb{Z} is not a field.

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

Example. \mathbb{Z}_7 is a field.

Example.

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

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

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

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

Let's consider the following:

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

Proof.

(1) R is commutative obviously.

(2) R contains an unity, by definition.

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

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

Contradiction!

□

Let's consider the following with the help of above theorem.

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

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

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

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

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

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

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

We note that:

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

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

Example.

For arbitrary positive integer d , define

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

is a subring of \mathbb{R} .

Note that:

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

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

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

Note it is closed under $+$.

And

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

Note that $d^{\frac{2}{3}}$ is not in A therefore A is not a subring. However, if we modify the condition s.t.

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

then A is a subring.

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

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

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

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

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

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

We can do the following:

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

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

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

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

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

However, we notice that

$$\begin{aligned} [(a_1, b_1) + (a_2, b_2)](c, d) &= ((a_1 b_2 + a_2 b_1)c, b_1 b_2 d) \\ (a_1, b_1)(c, d) + (a_2, b_2)(c, d) &= (a_1 c b_2 d + b_1 d a_2 c, b_1 b_2 d d) \\ [(a_1, b_1) + (a_2, b_2)](c, d) &\neq (a_1, b_1)(c, d) + (a_2, b_2)(c, d)!!!! \end{aligned}$$

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

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

$$(a, b) \sim (a', b') \text{ iff } ab' = ba'$$

Proof. Skipped, left as exercise. □

NOT FINISHED

After checking (1) and (2). we can have $+$, \times on \hat{F} descends to $+$ and \times on F .

(3) Check $(F, +, \times)$ is a field.

That is, if

$$(4) D \subset F$$

Definition. Field F is called the field of quotients of integral domain D .

The concepts after this becomes too abstract that the author have some difficulties to understand, therefore author refuses to include this part. But don't worry this part is not that important. We are just proving the fact that $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ which is quite real analysis.

17 Homomorphism and factor rings

Definition. Let R and R' be rings. A map $\phi: R \rightarrow R'$ is called ring homomorphism if

$$\phi(a+b) = \phi(a) + \phi(b)$$

$$\phi(ab) = \phi(a)\phi(b)$$

for any $a, b \in R$.

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

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

Proof.

$$1 \times 1 = 1$$

$$\phi(1 \times 1) = \phi(1)$$

$$\phi(1)^2 = \phi(1)$$

$$\phi(1) = 0 \text{ or } \phi(1) = 1$$

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

$$\phi(x) = \phi(1 \times x)$$

$$= \phi(1)\phi(x)$$

$$= 0$$

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

$$\phi(2) = \phi(1+1)$$

$$= 2$$

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

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

Exercise 1. If $\phi: \mathbb{R} \rightarrow \mathbb{R}$ is ring homomorphism, then $\phi(x) = x$, or $\phi(x) = 0$ for all $x \in \mathbb{R}$.

Definition. Let R and R' be rings. A map $\phi: R \rightarrow R'$ is called ring homomorphism if

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

for any $a, b \in R$.

Example. If R_1, \dots, R_n are rings, then $R_1 \times \dots \times R_n$ is the product ring.

For each $i \in [1, n]$, consider projection map $\pi_i: R_1 \times \dots \times R_n \rightarrow R_i$, $\pi_i(a_1, \dots, a_n) = a_i$ is a ring homomorphism.

Example. $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n$, where $\pi(a) = a \bmod n$ is a ring homomorphism.

For example, consider for $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_3$, then $\pi(0) = 0, \pi(1) = 1, \pi(2) = 2, \pi(3) = 0, \dots$,

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

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

Proof.

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

□

Theorem.

If $\phi: R \rightarrow R', \varphi: R' \rightarrow R''$ are ring homomorphism, then their composition:

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

is also a ring homomorphism.

Proof. Left as exercise

□

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

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

Definition. Subring

If R is a ring, a nonempty subset $S \subset R$ is called a subring if S is closed under addition and multiplication, and S is a ring under $+$ and \times .

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

Proof. If a set S is closed under addition and multiplication, to check S is a subring, it is enough to check 0 is in S and $a \in S \Rightarrow -a \in S$.

Reason: Associativity holds if R is a ring. Distributive law also holds given that R is a ring.

□

Theorem. Let $\phi: R \rightarrow R'$ is a ring homomorphism, then

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

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

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

□

Definition. Theorem. Kernal

Let $\phi: R \rightarrow R'$ be a ring homomorphism. Then

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

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

Moreover, $\ker(\phi)$ is a subring of R .

Example. Consider $\phi: C[0, 7] \rightarrow \mathbb{R}, \phi(f) = f(3)$ is a ring homomorphism. Moreover, the kernal

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

Definition. Let R be a ring, a subset $I \subset R$ is called an ideal, if

1. I is a subgroup of $(R, +)$

2. For all $a \in R, b \in I$, then $ab \in I, ba \in I$

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

Example. $3\mathbb{Z}$ is an ideal of \mathbb{Z} .

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

Proof.

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

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

□

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

Proof.

Since ϕ is an additive group homomorphism from $R \rightarrow R'$, therefore $\ker(\phi)$ is an additive subgroup of R .

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

Check:

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

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

□

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

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

(Proof of multiplication is well-defined)

Proof.

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

Note that:

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

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

Theorem.

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

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

Example.

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

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

Theorem. Fundamental homomorphism theorem for Rings

If $\phi: R \rightarrow R'$ is a ring homomorphism with $\ker(\phi) = N$, then the map given by $\mu: R/N \rightarrow \phi(R')$

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

is well defined and is isomorphism of rings.

All topics that will appear in the final exam have been finished.

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

In the following, we will talk about:

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

18 Jordan Canonical form of square matrices over \mathbb{C}

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

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

Example. $GL(n, \mathbb{R})$ acts on $M_n(\mathbb{R})$ by $g * A = gAg^{-1}$.

Thus we can claim that A, B are similar, if A, B are in the same orbit.

Theorem. If A, B are similar, then $|A| = |B|$

Proof.

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

□

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

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

□

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

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

Proof.

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

□

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

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

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

If A, B are similar, then

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

Therefore A is only similar to itself. Contradition!

□

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

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

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

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

Question. Given A_1 , find T , s.t. TAT^{-1} is as simple as possible. i.e. in ideal case, we should have diagonal matrix.

[END OF 2023-11-23]

Example. The matrix

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

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

Example. The matrix

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

is **not** diagonalizable even over \mathbb{C} !

Proof. Suppose it is diagonalizable. Then

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

Note that the matrix has eigenvalue with multiplicity 2, and $\begin{bmatrix} \lambda_1 & \\ & \lambda_2 \end{bmatrix}$ has eigenvalues of λ_1, λ_2 .

Therefore $\lambda_1 = \lambda_2 = 2$. Thus:

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

Contradiction!

□

Definition. Jordan block

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

Example.

Any 1×1 matrix is a Jordan block.

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

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

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

Definition.

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

Example. Consider a 5×5 matrix,

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

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

The matrix

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

is also blockwise diagonal matrix but not in Jordan block.

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

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

Proof.

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

Recall:

Theorem. ★ *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, \dots, p_n are primes, r_1, \dots, r_n are positive integers. $m > 0$.

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

19 Polynomial Rings

Definition. *Polynomials*

A polynomial over \mathbb{R} is an expression

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

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

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

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

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

Suppose $f \mapsto a_n x^n + \cdots + a_1 x + a_0$. Suppose $g \mapsto b_m x^m + \cdots + b_1 x + b_0$.

Then

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

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

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

We therefore have the following theorem:

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

Definition. Let R be a commutative ring with unity 1, then a polynomial over R is an expression of

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

where all coeff are element in the ring R .

Let $R[x]$ be the set of polynomial in variable x with coeff in R .

Then this is a commutative ring with unity 1. Moreover, R is a subring of $R[x]$.

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

False! Consider $R = \mathbb{Z}_6$. Let $f \mapsto 3x^2 + 1, g \mapsto 2x + 1$. Then $fg = 6x^3 + 3x^2 + 2x + 1 = 3x^2 + 2x + 1$. Then the degree for $fg = 2$ while $\deg(f) + \deg(g) = 3$!

Proposition. If R is an integral domain. $f, g \in R[x]$, $f \neq 0, g \neq 0$, then $fg \neq 0$, therefore $R[x]$ is a integral domain. Moreover, $\deg(f) + \deg(g) = \deg(fg)$.

Definition. *Derivative in R*

If $f \mapsto a_n x^n + \cdots + a_1 x + a_0$, we define $f' \mapsto n a_n x^{n-1} + \cdots + a_1$. (Just like the usual formula for derivative.)

The usual definition (First principle) for derivative on \mathbb{R} does not hold. However, we have the formula in \mathbb{R} holds in R also.

If f is a constant, $f = a_0$, then $f' = 0$. However, the converse is not always true.

Proposition. *If F is a field, $f \in F[x]$, then we say $c \in F$ is a root of f if $f(c) = 0$.*

For example, can we find all the roots of $x^5 - x + 1 \in \mathbb{Z}_5[x]$.

Yes, we can plug in $x = 1, \dots, 5$. We then have f have no roots in \mathbb{Z}_5 .

Are there any simpler ways? Also yes! By Fermat Little theorem, $x^5 - x = 1$, therefore $x^5 - x + 1 \neq 0$.

Proposition. *If $f \in F[x]$, $\deg(f) = n > 0$, then we have*

- $c \in F$ is a root of f iff $f(x) = (x - c)g(x)$ for some $g \in F[x]$, and $\deg(g) = n - 1$.
- f has at most n roots in F .

Proof.

$$\begin{aligned} f(x) &= (x - c)g(x) \\ f(c) &= (c - c)g(x) \\ &= 0g(x) = 0 \end{aligned}$$

Conversely, if c is a root of f , i.e. $f(c) = 0$, then

$$a_n c^n + \dots + a_0 = 0$$

We then have

$$\begin{aligned} f(x) &= f(x) - f(c) \\ &= (a_n x^n + \dots + a_1 x + a_0) - (a_n c^n + \dots + a_1 c + a_0) \\ &= (a_n)(x^n - c^n) + \dots + a_1(x - c) \end{aligned}$$

Note that $x^n - c^n = (x - c)(x^{n-1} + \dots + c^{n-1})$, hence $f = (x - c)g(x)$ for some $g(x)$. □

[END OF 2023-11-28]

20 Introduction to field theory

Review

A field is a ring, F satisfying three properties

1. F is commutative
2. F has 1 as unity, where $1 \neq 0$
3. Every nonzero element $a \in F$ has a multiplicative inverse $a^{-1} \in F$.

For arbitrary number $\alpha \in \mathbb{C}$, α generates a field $\mathbb{Q}(\alpha)$ in \mathbb{C} .

$$\mathbb{Q}(\alpha) = \left\{ \frac{a_n \alpha^n + \cdots + a_1 \alpha + a_0}{b_m \alpha^m + \cdots + b_1 \alpha + b_0} \mid a_0, \dots, a_n, b_1, \dots, b_m \in \mathbb{Q}, m, n \in \mathbb{Z}_{\geq 0}, b_m \alpha^m + \cdots + b_1 \alpha + b_0 \neq 0 \right\}$$

We pick $\alpha = 0$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(0) = \left\{ \frac{a_0}{b_0} \mid a_0, b_0 \in \mathbb{Q}, b_0 \neq 0 \right\} = \mathbb{Q}$

Pick $\alpha = 1$, then $\mathbb{Q}(\alpha) = \mathbb{Q}$. For any rational number α , we have $\mathbb{Q}(\alpha) = \mathbb{Q}$ also.

Pick any $\alpha \notin \mathbb{Q}$, but $\alpha \in \mathbb{Q}(a)$, for example, we can pick $\alpha = \frac{\alpha + 0}{0\alpha + 1} \in \alpha$.

Pick $\alpha = i$, we then have $\mathbb{Q}(i) = \{ ai + b \mid a, b \in \mathbb{Q} \}$

Proof. Since

$$\begin{aligned} a_n i^n + a_{n-1} i^{n-1} + \cdots + a_1 i + a_0 &= ci + d, (c, d) \in \mathbb{Q}^2 \\ b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0 &= vi + s, (v, s) \in \mathbb{Q}^2 \end{aligned}$$

And therefore,

$$\begin{aligned} \mathbb{Q}(i) &= \left\{ \frac{ci + d}{vi + s} \mid c, d, v, s \in \mathbb{Q}, v, s \text{ not both zero} \right\} \\ &= \{ ai + b \mid a, b \in \mathbb{Q} \} \end{aligned}$$

□

Note that $\mathbb{Q}(\pi)$ is a very large set, however, $\mathbb{Q}(\pi) \subsetneq \mathbb{R}$, since $\mathbb{Q}(\pi)$ is countably finite, however \mathbb{R} itself is not countable.

Definition. *Field Extension*

If F is a field, an extension of F is a field E with $F \subset E$. We say F is a subfield of E , and E is a extension of F .

For example, \mathbb{Q} is the smallest subfield in \mathbb{C} .

Proof. If F is a subfield in \mathbb{C} , then $1 + 1 + \cdots + 1 = n \in F$. We have $-n \in F$, and $n^{-1} \in F$, and $\frac{m}{n} = mn^{-1} \in F$. Hence $\mathbb{Q} \subset F$. □

Definition. If F is a field, a vector space over F is a set V with addition and scalar multiplication s.t.

1. $(V, +)$ is a abelian group. (This implies 0 exists, a^{-1} exists, and operation is associative)
2. $(k_1 k_2)v = k_1(k_2 v), \forall k_1, k_2 \in F, v \in V$. Also $1 \times v = v$
3. $(k_1 + k_2)v = k_1 v + k_2 v, k(v_1 + v_2) = k v_1 + k v_2$

Almost all results and concepts in linear algebra course can be generalized to a linear algebra over F . For example, linearly independence, basis, ...

Example.

Consider $F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$. Define $+$ and scalar multiplication as same in \mathbb{R}^2 .

Then F^2 has a basis of $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Definition.

A vector space V over F has a dimension n , $n \in \mathbb{Z}_{\geq 0}$, written as $\dim_F V = n$, if V has a basis consisting of n vector spaces. If V has no finite basis, then $\dim_F V = \infty$.

Example. $\mathbb{R}^\infty = \{(a_1, \dots, a_n) : a_1, \dots, \in \mathbb{R}\}$ is a vector space with infinitely dimension.

Theorem. If $F \subset E$, E is a field extension of field F , then E is automatically a vector space over F .

Definition. The degree of the extension $F \subset E$ is $[E:F] = \dim_F E$.

Example. $[\mathbb{C}:\mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2$.

Taking back the example

For arbitrary number $\alpha \in \mathbb{C}$, α generates a field $\mathbb{Q}(\alpha)$ in \mathbb{C} .

$$\mathbb{Q}(\alpha) = \left\{ \frac{a_n \alpha^n + \dots + a_1 \alpha + a_0}{b_m \alpha^m + \dots + b_1 \alpha + b_0} \mid a_0, \dots, a_n, b_1, \dots, b_m \in \mathbb{Q}, m, n \in \mathbb{Z}_{\geq 0}, b_m \alpha^m + \dots + b_1 \alpha + b_0 \neq 0 \right\}$$

again, then $[\mathbb{Q}(\alpha):\mathbb{Q}] = \begin{cases} 1, \alpha \in \mathbb{Q} \\ 2, \alpha = i \\ \vdots \end{cases}$

Definition.

α is called an algebraic number if there is $f(x) \in \mathbb{Q}(x)$, s.t. $f(\alpha) = 0$. We say α is transcendental if α is not algebraic.

Theorem.

e, π are transcendental number.

Moreover, let $\bar{\mathbb{Q}}$ be the set of all algebraic number, then $\bar{\mathbb{Q}}$ is a subfield of \mathbb{C} .

$\mathbb{C} - \bar{\mathbb{Q}}$ is the set of transcendental number, moreover, this set is uncountable.

Theorem. \mathbb{R} can be classifield into two types: Construstible number and non-constructible number

Definition. A real number $\alpha \in \mathbb{R}$ is called a constructible number if we can constructible a line segment with length $|\alpha|$ in a finitely number of steps from the given segment of length 1 by using a straight edge and a compass.

Example. All integers are constructable. All rational numbers are constructable.

Lemma. If γ is constructable, then $\gamma^{\frac{1}{2}}$ is constructable as well.

Proof. Consider



□

Theorem.

In the following, we let C be the set of constructible. Then

1. C is a subfield of \mathbb{R}
2. Any element in C is algebraic
3. $[\mathbb{Q}(\alpha): \mathbb{Q}] = 2^k, k \in \mathbb{Z}_{\geq 0}$, for any $\alpha \in C$.

Example. $2^{\frac{1}{3}}$ is not constructible.

Proof. $[\mathbb{Q}(2^{\frac{1}{3}}): \mathbb{Q}] = 3 \notin 2^k$

□

In general, given $a \in \mathbb{Z}_{>0}$, if $a \notin \mathbb{Z}$, then $a^{\frac{1}{3}}$ is never constructible.

Theorem. It is not possible to trisect a given angle using straight edge and compass.

Proof. If such statement is true, then one may construct 20° from 60° . But

$$[\mathbb{Q}(\cos 20^\circ): \mathbb{Q}] = 3$$

Then $\cos 20^\circ$ is not constructible.

□

Final

Dec 9 12:30-14:30

Covering 1,4,5,6,8,9,10,11,13,14,16,18,19,20,26

Closed book, but you have some important theorem page. Access on page of canvas

60~70% similar to homework problem.