Group Isomorphisms

Kimsie Phan

Mathematics Undergraduate from KU
phankimsie03@gmail.com

Mathematical Association of Cambodia

April 17, 2021

Group Isomorphisms

Review:

Definition (Groups)

A group is a nonempty set G with a binary operation $* : G \times G \to G$,$(x, y) \mapsto x * y$ satisfying the following conditions:

1. G is associative: $(a * b) * c = a * (b * c), \quad \forall a, b, c \in G$.

Review:

Definition (Groups)

A group is a nonempty set G with a binary operation $*: G \times G \to G, (x, y) \mapsto x * y$ satisfying the following conditions:

2. There is an element e in G such that $a * e = a$ and $e * a = a, \quad \forall a \in G$.

Review:

Definition (Groups)

A group is a nonempty set G with a binary operation $* : G \times G \to G, (x, y) \mapsto x * y$ satisfying the following conditions:

3. $\forall a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = e$ and $a^{-1} * a = e$.
   If G be a group but it is also commutative i.e.,
   $\forall a, b \in G, \quad a * b = b * a$, that is called Abelian group.

Review:

Definition (Groups)

A group is a nonempty set G with a binary operation $* : G \times G \to G, (x, y) \mapsto x * y$ satisfying the following conditions:

Definition (Subgroups)

Let G be a group and H a nonempty subset of G i.e.,

$$\varnothing \neq H \leq G \iff \begin{cases} h_1 h_2 \in H \\ h_1^{-1} \in H \end{cases}, \forall h_1, h_2 \in H$$

$$\iff \forall h_1, h_2 \in H, \quad h_1 h_2^{-1} \in H$$

Definition (Order of Groups and elements)

Let G be a group. A number of elements in G is called the **order** of G and denoted by $|G|$. When G is infinite, we write $|G| = \infty$. Let $x \in G$ and $n \in \mathbb{N}$. We denote

$$x^n = x \cdot x \cdot x \cdots x \quad (n \text{ times of } x)$$

$$x^{-n} = (x^{-1})^n = x^{-1} \cdot x^{-1} \cdot x^{-1} \cdots x^{-1} \quad (n \text{ time of } x^{-1})$$

$$x^0 = e$$

The smallest positive integer n such that $x^n = e$ is called the **order of the element** x in G and denoted by $|x| = n$. If no such integer exists, we say that x has **infinite order** and denoted by $|x| = \infty$.

Definition (cyclic group)

Let G be a group. G is a **cyclic group** if there exists $x \in G$ such that $G = \langle x \rangle$. The group $\langle x \rangle$ is called the **group generated by** x and x is called the **generator** of $\langle x \rangle$.

Example

We give some examples of groups.

I. Infinite Groups

1. Matrix groups: $\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{R}), \mathrm{SO}(n), \mathrm{U}(n)$ and $\mathrm{SU}(n)$, ... with multiplication operation.
2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian group.
3. $(S_X, \circ), S_X = \{f : X \to X, X \neq \varnothing | f \quad \text{is bijective}\}$ is called permutation groups.

II. Finite Groups

1. $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$ with addition operation modulo n.
2. $\mathbb{Z}_n^\times = \{m \in \mathbb{Z}_n | (m, n) = 1\}$ with multiplication operation modulo n. Example: $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$
3. $G = \{1, -1, i, -i\}$ is a group under usual multiplication of complex number and it is an abelian group.
4. If the set $X = \{1, 2, ..., n\}$ we denote S_n is symmetric groups.

Operation Table of Groups

- Table of $\mathbb{Z}_8^\times$

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

- Table of $(G, \times)$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Table of $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table of $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

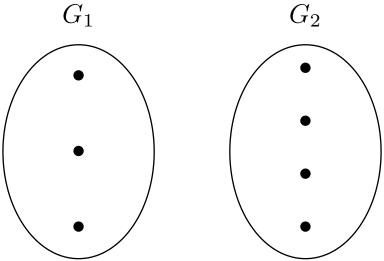
Table of G after changing order of element

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

By transformation

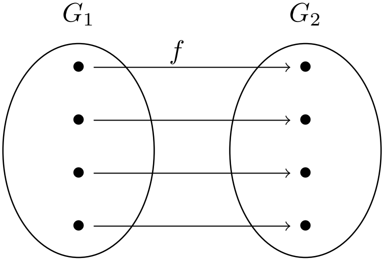
$0 \longleftrightarrow 1, 1 \longleftrightarrow i, 2 \longleftrightarrow -1$ and $3 \longleftrightarrow -i$.

Remark: We cannot use table of operations to check whether two groups are the same or not.
Now consider:

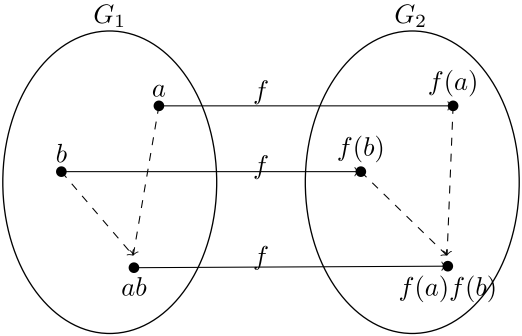


G_1 can not be the same as G_2 since $\text{card}(G_1) \neq \text{card}(G_2)$.

Consider if $\text{card}(G_1) = \text{card}(G_2)$, then



1. There exists $f : G_1 \to G_2$ such that f is bijective.



2. $\forall a, b \in G, \quad f(ab) = f(a)f(b)$.

Definition (isomorphism groups)

Let G_1 and G_2 be two groups. We say that G_1 is **isomorphic** to G_2 there exists a function $f : G_1 \longrightarrow G_2$ which satisfies:

1. f is bijection.
2. f preserves operator, that is $f(ab) = f(a)f(b)$ for any $a, b \in G$.

We symbolize this fact by writing,

$$G_1 \cong G_2 \quad \text{or} \quad G_1 \approx G_2.$$

1. Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

Proof.

Let $G = \langle x \rangle$ where $|x| = \infty$.
Consider the map $f : G \to \mathbb{Z}$ given by $x^n \mapsto n$ where $n \in \mathbb{Z}$.
This map is well-defined and injective since for any $x^m, x^n \in G$

$$x^m = x^n \iff m = n$$

where $m, n \in \mathbb{Z}$.
Now f is surjective since for any $n \in \mathbb{Z}$, $\exists x^n \in G$ such that $f(x^n) = n$.
And f is operation preserving since for any $x^m, x^n \in G$, we have

$$f(x^m x^n) = f(x^{m+n}) = m + n = f(x^m) + f(x^n).$$

□

2. Any finite cyclic group $\langle x \rangle$ such that card$(\langle x \rangle) = n$ is isomorphic to $\mathbb{Z}_n$.
Proof: Let $G = \langle x \rangle$ where $|x| = n$.
Consider the map $f : G \longrightarrow \mathbb{Z}_n$ given by

$$f(x^p) = p \quad \text{mod } n$$

where $p \in \mathbb{Z}$.
Now f is injective since $\forall p, q \in \mathbb{Z}$

$$p(\mod n) = q(\mod n) \Longleftrightarrow x^p = x^q.$$

And f is surjective since $\forall p(\mod n) \in \mathbb{Z}_n, \exists x^p \in G$ such that $f(x^p) = p$ mod n.
Furthermore f preserve group operation: Let $x^p, x^q \in G$ then

$$\begin{aligned} f(x^p x^q) &= f(x^{p+q}) \\ &= (p+q) \mod n \\ &= (p \mod n) + (q \mod n) \\ &= f(x^p) + f(x^q) \end{aligned}$$

Therefore, $G \cong \mathbb{Z}_n$.

How does one recognize if two groups are isomorphic to each other?

1. Make a smart guess on a function $f : G_1 \longrightarrow G_2$ which might be an isomorphism.
2. Check that f is injective and surjective, that is bijective.
3. Check that f satisfies the preserve operation $f(ab) = f(a)f(b)$.

How does one recognize when two groups are not isomorphic to each other?

Show that two groups G_1 and G_2 are not isomorphic by observing:

- card$(G_1) \neq$ card(G_2)
- $|G_1| \neq |G_2|$
- G_1 is cyclic but G_2 is not.
- G_1 is abelian but G_2 is not.

Cayley's Theorem

Theorem

Every group is isomorphic to a group of permutations.

Proof: Let G be an arbitrary group. Consider the permutation group S_G and for each $g \in G$, we define a map

$$\begin{aligned} f_g : G &\to G \\ x &\mapsto gx \end{aligned}$$

First, observe that $f_g \in S_G$ for all $g \in G$. Indeed,

$$f_g(x) = f_g(y) \Longleftrightarrow gx = gy \Longleftrightarrow x = y, \quad \forall x, y \in G.$$

$$\forall y \in G, \exists x = g^{-1}y \in G, f_g(x) = f_g(g^{-1}y) = gg^{-1}y = y.$$

In addition, the set $\overline{G} := \{f_g | g \in G\}$ is a subgroup of S_G since for any $g_1, g_2 \in G$ and $x \in G$, we have

$$\left(f_{g_1} \circ f_{g_2}\right)(x) = f_{g_1}(g_2 x) = g_1 g_2 x = f_{g_1 g_2}(x) \Longleftrightarrow f_{g_1} \circ f_{g_2} = f_{g_1 g_2} \in \overline{G}.$$

$$f_{g_1} \circ f_{g_1^{-1}}(x) = f_{g_1}(g_1^{-1}x) = g_1 g_1^{-1} x = x.$$

$$\iff f_{g_1} \circ f_{g_1}^{-1} = Id \iff f_{g_1}^{-1} = f_{g_1^{-1}} \in \overline{G}.$$

We will prove that $G \cong \overline{G}$. Consider a map:

$$f : G \to \overline{G}$$
$$g \mapsto f_g$$

This map is well-defined and injective.
Let $g_1, g_2 \in G$,

$$g_1 = g_1 \iff g_1 x = g_2 x, \forall x \in G \iff f_{g_1} = f_{g_2}$$

Now f is clearly surjective because $\forall y \in \overline{G}, \exists x = g^{-1}y \in G$ such that

$$f_g(x) = f_g(g^{-1}y) = gg^{-1}y = y.$$

And f preserves the operation: for any $g_1, g_2 \in G$, we have

$$f(g_1 g_2) = f_{g_1 g_2} = f_{g_1} \circ f_{g_2} = f(g_1) \circ f(g_2).$$

Therefore,

$$G \cong \overline{G} \leq S_G.$$

Properties of Isomorphism

Properties of Isomorphism Acting on Elements

Theorem

Suppose that f is an isomorphism from a group G onto a group $\overline{G}$.

1. *f carries the identity of G to the identity of $\overline{G}$.*
2. *For every integer n and for every group element a in G, $f(a^n) = [f(a)]^n$.*
3. *For any element a and b in G, a and b commute if and only if $f(a)$ and $f(b)$ commute.*
4. *$G = \langle a \rangle$ if and only if $\overline{G} = \langle f(a) \rangle$.*
5. *$|a| = |f(a)|$ for all a in G (isomorphism preserves orders).*
6. *For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same numbers of solutions in G as does the equation $x^k = f(b)$ in $\overline{G}$.*
7. *If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.*

Properties of Isomorphism Acting on Groups

Theorem

Suppose that f is an isomorphism from a group G onto a group $\overline{G}$.

1. f^{-1} is an isomorphism from $\overline{G}$ onto G.
2. G is abelian if and only if $\overline{G}$ is abelian.
3. G is cyclic if and only if $\overline{G}$ is cyclic.
4. If K is a subgroup of G, then $f(K) = \{f(k) | k \in K\}$ is a subgroup of $\overline{G}$.
5. $f(Z(G)) = Z(\overline{G})$ where $Z(G)$ denotes the center of the group G.

Note: $Z(G) = \{x \in G | xg = gx, \forall g \in G\}$.

Application of Isomorphism

- In mathematics
  1. Studying abstract groups via isomorphisms with simple/familiar/readable groups.
     Example: Suppose V is vector space on $\mathbb{R}$ and finite-dimensional.
     Let $G = \{T : V \to V | T \quad \text{is bijective}, T, T^{-1} \quad \text{is linear}\}$.
     Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear transformation defined by

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

We get

$$T \circ T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = T \begin{pmatrix} x_1 + 3x_2 - x_3 \\ 3x_1 - x_2 + 4x_3 \\ 2x_1 - 4x_2 + x_3 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 + 3x_2 - x_3 + 3(3x_1 - x_2 + 4x_3) - (2x_1 - 4x_2 + x_3) \\ 3(x_1 + 3x_2 - x_3) - (3x_1 - x_2 + 4x_3) + 4(2x_1 - 4x_2 + x_3) \\ 2(x_1 + 3x_2 - x_3) - 4(3x_1 - x_2 + 4x_3) + (2x_1 - 4x_2 + x_3) \end{pmatrix}.$$

We must instead again, it is too hard. But we can find $T \circ T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ by using multiplication of matrix.

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

Then $T(T(x)) = \begin{pmatrix} 1 & 3 & -1 \\ 3 & -1 & 4 \\ 2 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & -1 \\ 3 & -1 & 4 \\ 2 & -4 & 1 \end{pmatrix} = T \circ T$.

References

1. Charles C. Pinter, A BOOK OF ABSTRACT ALGEBRA. Second Edition, McGraw-Hill Publishing Company, Inc., New York, 1982.
2. Joseph A. Gallian, Contemporary Abstract Algebra. Eight Edition, CENGAGE Learning, United State of America, 2017.
3. Vinod Moreshwar Vaz, A Comparative Study of Graph Isomorphism Applications, International Journal of Computer Applications (0975-8887), March 7 2017.
4. Stephen H. Friedberg, Linear Algebra, Four Edition, Pearson Education, Inc., 2003.
5. Ellis, Properties of group isomorphism, 2011.
6. Wikipedia, Group Isomorphism. 1 April 2021.
7. Wikipedia, Isomorphism. 10 April 2021.

THANK YOU FOR YOUR PAYING ATTENTION !

Mathematics is the art of giving the same name to different things.
Henri Poincaré (1854-1912)

The basis for poetry and scientific discovery is the ability to comprehend the unlike in the like and the like in the unlike.
Jacob Bronowski

Moreover, I would like to thank my two advisors Seng Monyrathanak and Deom Vanny for providing me guidance and feedback throughout this project work.

Last but not least, I also would like to thank all MAC members who has discussed with me during this project work period.

Q & A !