Group Isomorphisms

Srishti Patel(Roll no 23)

Delhi Technological University

October 2019

Definition

An isomorphism Φ from a group G to a group G' is one-one ,onto mapping that preseves the group operation,i.e
$\Phi(xy) = \Phi(x) \cdot \Phi(y)$

Notation: If G is isomorphic to G' then we denote it by $G \cong G'$

Examples of Isomorphisms I

1. Let $G = (\mathbb{R}, +)$ and $G' = (\mathbb{R}^+, \cdot)$ be two groups then $\Phi : G \to G'$ as $\Phi(x) = 2^x$ is an isomorphism
   • Φ is one-one -
   Let $\Phi(x) = \Phi(y) \Rightarrow 2^x = 2^y \Rightarrow 2^{x-y} = 1 \Rightarrow x - y = 0 \Rightarrow x = y$
   • Φ is onto -
   Let y $\in \mathbb{R}^+$, then $\exists x = \log_2 y$ such that $\Phi(x) = 2^x = 2^{\log_2 y} = y$
   therefore, Φ is onto
   • Φ is homomorphism -
   $\Phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \Phi(x)\Phi(y)$
   therefore Φ is an isomorphism.

Examples of Isomorphisms II

2. Let $G = SL(2\mathbb{R})$
Define $\Phi : G \to G$ as
$\Phi(A) = MAM^{-1} \forall A \in G$ where M is a fixed 2×2 matrix in $SL(2, \mathbb{R})$
then Φ is an isomorphism
• ϕ is one one -
Let $\phi(A) = \phi(B) \Rightarrow MAM^{-1} = MBM^{-1} \Rightarrow A = B$ (by pre and post multiplying by M^{-1} and M^{1} respectively)
• ϕ is onto -
Let A $\in$ G.Then $\exists$ $M^{-1}AM \in G$ such that
$\Phi(M^{-1}AM)$= $M(M^{-1}AM)M^{-1} = A$
• ϕ is homomorphism-
$\Phi(A.B) = MABM^{-1} = (MAM^{-1})MBM^{-1} = \Phi(A).\Phi(B)$
Therefore Φ is an isomorphism called the **conjugation** by M

Examples of Isomorphisms III

3. Let $G = \{1, \omega, \omega^2\}$,the group of cube roots of unity and $G' = \{R_0, R_1, R_2\}$ the group of rotations in the plane through 0°,120° and 240° respectively.
   The mapping $\theta : G \to G'$ given by $\theta(1) = R_0$,$\theta(\omega) = R_1$ and $\theta(\omega^2) = R_2$ defines an isomorphism of G onto G'.

Properties of isomorphism I

Let $\theta : G \to G'$ be an isomorphism of G onto G'.Let e and e' be the identity elements of G and G' respectively.Then

1. $\theta(e) = e'$
   proof:
   Let $\theta(e) = a' \in G'$.Then $a' = \theta(e) = \theta(e.e) = \theta(e) \cdot \theta(e) = a'.a'$.
   Thus $a'a' = a' = a'e'$,by left cancellation law $a' = e'$.Hence $\theta(e) = e'$
2. $\theta(a^{-1}) = \{\theta(a)\}^{-1}$ for all $a \in G$
   proof:
   $\theta(a^{-1}) \cdot \theta(a) = \theta(a^{-1}.a) = \theta(e) = e'$ and
   $\theta(a) \cdot \theta(a^{-1}) = \theta(a.a^{-1}) = \theta(e) = e'$ .Hence by uniqueness of inverse in G',$\theta(a^{-1})$ is the inverse of $\theta(a)$
   Remark: in the above properties the result is valid even if θ is one-one and homomorphism .It need not be onto.

Properties of isomorphism II

3. $\forall n \in \mathbb{Z}$ and $\forall a \in G, \theta(a^n) = [\theta(a)]^n$

Proof:

Case1:

When n=0 then $\theta(a^0) = \theta(e) = e'$,also $[\theta(a)]^n = [\theta(a)]^0 = e'$
therefore , $\theta(a^n) = [\theta(a)]^n$

Case 2:

When $n \in \mathbb{Z}^+$

$$\theta(a^n) = \theta(a \cdots a)\{ntimes\}$$

$$= \theta(a) \cdot \theta(a) \cdots \theta(a)\{ntimes\}$$

$$= [\theta(a)]^n$$

Case 3:

When $n \in \mathbb{Z}^-$, Let $n = -m; m \in \mathbb{Z}$

$$\theta(a^n) = \theta(a^{-m}) = [\theta(a^{-1})]^m = [\theta(a)]^{-m}$$

$$= [\theta(a)]^n$$

Theorems I

Theorem

Let G and G' be isomorphic.If G is abelian ,so is G'

Proof:

Let $\theta : G \to G'$ be isomorphism of G onto G'.Let $a', b' \in G'$.Since θ is onto ,there exists $a \in G$ and $b \in G$ such that $\theta(a) = a'$ and $\theta(b) = b'$.Now $a' \cdot b' = \theta(a) \cdot \theta(b) = \theta(ab) = \theta(ba)$ (Since G is abelian)$= \theta(b) \cdot \theta(a) = b'a'$.

Thus G' is abelian.

Remark 1: The above theoram is also true if θ is an onto homomorphism.

Remark 2: If G is abelian and G' is non abelian then G and G' cannot be isomorphic.

Theorem

Any infinite cyclic group is isomorphic to Z and any finite cyclic group of order n is isomorphic to Z_n

Theorems II

Proof:
Case1: Let $G =< a >$ be an infinite cyclic group.Define $f : Z \to G$ given by $f(n) = a^n$
then $f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$.
Therefore f is homomorphism.Since all the powers are distinct in G therefore f is one-one.By definition it is onto .
Hence $G \cong Z$
Case 2: Let G be a finite cyclic group of order n. $G =< a >$ such that $0(a) = n$. Let $f : Z_n \to G$ is defined by $f(k') = a^k$ f is well defined.
$l' + m' = k' \Leftrightarrow l + m \equiv k(modn) where 0 \leq k \leq n-1$
$\Leftrightarrow (l + m - k) \mid n \Leftrightarrow (l + m - k) = np \Leftrightarrow a^{l+m-np} = a^k$
$\Leftrightarrow a^{l+m}.(a^n)^{-p} = a^k \Leftrightarrow a^{l+m} = a^k$
$f(l' + m') = f(k') = a^k = a^{l+m} = a^l.a^m = f(l').f(m')$
f is homomorphism.
$l' \neq m' \Rightarrow l \neq m \Rightarrow a^l \neq a^m \Rightarrow f(l') \neq f(m')$
Therefore f is one-one. Clearly f is onto hence f is an isomorphism $G \cong Z_n$

Theorems III

Corollary1

Any two cyclic groups of the same order are isomorphic

Proof: **Case 1:**Let G and G' be finite cyclic groups of order n ,then $G \cong Z_n$ and $G' \cong Z_n$ (by the above theorem)therefore, $G \cong G'$
Case 2: Let G and G' be infinite cyclic groups.By previous theorem $G \cong Z$ and $G' \cong Z$ therefore, $G \cong G'$

Remark

For each prime p,there exists only one group(upto isomorphism) of order p i.e the cyclic group of order p

First theorem of Isomorphism

Theorem

Let $f : G \rightarrow G'$ be a homomorphism of G onto G'and kernel of f is K then
$\bullet$ *K is normal in G*
$\bullet \frac{G}{K} \cong G'$

Proof: Let $f' : \frac{G}{K} \rightarrow G'$ be defined as $f'(aK) = f(a)$ for $a \in G$
Let $aK = bK \Leftrightarrow a^{-1}b \in K \Leftrightarrow f(a^{-1}b) = e' \Leftrightarrow f(a^{-1}) \cdot f(b) = e'$
$\Leftrightarrow f(a^{-1}) \cdot f(b) = e' \Leftrightarrow f(a) = f(b) \Leftrightarrow f'(aK) = f'(bK)$
Therefore f is well defined and one-one
Since f is onto hence f' is also onto
$f'(aKbK) = f'(abK) = f(ab) = f(a).(b) = f'(aK).f'(bK)$
Therefore f' is homomorphism and since f' is one-one and onto as well hence f is isomorphism

$$\frac{G}{K} \cong G'$$

Lemma

Let $f : G \to G'$ be a homomorphism then,

- if $H < G$,then $f(H) = H' < G'$
- if H is normal in G anf f is onto then H' is normal in G'
- if $H' < G' \Rightarrow f^{-1}(H') = H < G$
- if H' is normal in G'$\Rightarrow$ H is normal in G ,further if f is onto then $\frac{G}{H} \cong \frac{G'}{H'}$

Second Theorem of Isomorphism

Theorem

Let H and K be normal in G such that $K \subset H$ then

- $\frac{H}{K} \lhd \frac{G}{K}$
- $\frac{G/K}{H/K} \cong \frac{G}{H}$

Proof: Consider the projection map

$$p : G \to \frac{G}{K} = G'$$

by $p(a) = aK$ where $a \in G$. Since H is normal in G ,$p(H) = \frac{H}{K} = H'$
Consider

$$G/K = \{aK | a \in G\}$$

$$H/K = \{aK | a \in H\}$$

$$H' \lhd G'$$

also from previous lemma, we have $\frac{G'}{H'} \cong \frac{G}{H}$ that is $\frac{G/K}{H/K} \cong \frac{G}{H}$

Third theorem of Isomorphism I

Theorem

Let $H, K < G$ with K is normal in G

- *$H \cap K$ is normal in H*
- $\frac{H}{H \cap K} \cong \frac{HK}{K}$

Proof: Since K is normal in G and $K \leq G$ therefore HK is a subgroup of G $\Rightarrow HK = KH$.
As K is normal in G and $HK \leq G$ thus K is normal in HK $\Rightarrow \frac{HK}{K}$ well defined.
Also $H \cap K$ is normal in H.
Let $x \in H \cap K$
$\Rightarrow x \in H$and $x \in K$, since $h \in H$ therefore $hxh^{-1} \in H$
also since K is normal in G and $x \in K$ therefore $hxh^{-1} \in K$ and hence $hxh^{-1} \in H \cap K$

Third theorem of Isomorphism II

define $f : H \to \frac{HK}{K}$ by

$$f(a) = aK$$

then $xK \in \frac{HK}{K}$ then $xK = (hk)K = hK = f(H)$ (for some $h \in H$ and $k \in K$)
Therefore f is onto

$$f(ab) = abK = aK.bK = f(a).f(b)$$

f is a homomorphism $Kerf = \{a \in H | f(a) = K\} = \{a \in H | aK = K\} = \{a \in H | a \in K\} = H \cap K$
From first isomorphism theorem we have

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

Questions I

Question 1

Show that $< Q, + >$ cannot be isomorphic to $< Q^*, \cdot >$ where $Q^* = Q - \{0\}$

Solution: Suppose f is an isomorphism from Q to Q^*.Then $2 \in Q^*$,f is onto therefore,$\exists \alpha \in < Q^* >$,s.t. $f(\alpha) = 2$

$$\Rightarrow f(\frac{\alpha}{2} + \frac{\alpha}{2}) = 2$$

$$\Rightarrow f(\frac{\alpha}{2}).f(\frac{\alpha}{2}) = 2$$

$\Rightarrow x^2 = 2$ where $x = f(\frac{\alpha}{2}) \in Q^*$
But that is a contradiction as there is no rational number x such that $x^2 = 2$.Hence the result follows

Questions II

Question 2

Show that any finite cyclic group of order n is isomorphic to the quotient group $\frac{\mathbb{Z}}{N}$ where $<\mathbb{Z},+>$ is a group of integers and $N=<n>$

Solution: Let $G=<a>$ be of order n
Define $f:\mathbb{Z}\to G$ s.t. $f(m)=a^m$ then f is clearly well defined and onto map.
Since $f(m+k)=a^{m+k}=a^m.a^k=f(m).f(k)$
f is a homomorphism and therefore by First theorem of Isomorphism, $G\cong\frac{\mathbb{Z}}{kerf}$
We show ker $f=N=\langle n\rangle$
Now $m\in$ Ker $f=N=\langle n\rangle$

$$\Leftrightarrow f(m)=e$$

$$\Leftrightarrow a^m=e$$

Questions III

$$\Leftrightarrow O(a)|m$$

$$\Leftrightarrow n|m$$

$$\Leftrightarrow m \in < n >$$

Hence $G \cong \frac{\mathbb{Z}}{<n>}$

Question 3

If G is the additive group of reals and N is the subgroup of G consisting of integers ,prove that $\frac{G}{N}$ is isomorphic to the group H of all complex numbers of absolute value under multiplication.

Solution: Define a map
$f(\alpha) = e^{2\pi i\alpha}$
$|e^{2\pi i\alpha}| = |cos2\pi\alpha + isin2\pi\alpha| = \sqrt{cos^2(2\pi\alpha) + sin^2(2\pi\alpha)} = 1$
We show f is onto
Let $h \in H$ be any element then $h = a + ib$

Questions IV

where $|a+ib| = 1 = \sqrt{a^2+b}$
$a+ib = r(cos\theta + isin\theta)$
$|(a+ib| = 1 \Rightarrow r = 1$
$a+ib = cos\theta + isin\theta = e^{i\theta}$
$f(\frac{\theta}{2\pi}) = e^{\frac{\theta}{2\pi}\cdot 2\pi i} = e^{i\theta}$
$\Rightarrow \frac{\theta}{2\pi}$is the required pre image
Now we will show that f is a homomorphism as

$$f(\theta_1+\theta_2) = e^{2\pi(\theta_1+\theta_2)i}$$

$$= e^{2\pi\theta_1 i}\cdot e^{2\pi\theta_2 i} = f(\theta_1)f(\theta_2)$$

By first theorem of isomorphism $H \cong \frac{G}{kerf}$
We claim that ker f$= N$
Let $\alpha \in Kerf$

$$\Leftrightarrow f(\alpha) = 1$$

$$\Leftrightarrow e^{2\pi i\alpha} = 1$$

Questions V

$$\Leftrightarrow cos2\pi\alpha + isin2\pi\alpha = 1 + i0$$

$$\Leftrightarrow cos2\pi\alpha = 1, sin2\pi\alpha = 0$$

$$\Leftrightarrow 2\pi\alpha = 2\pi\alpha n \pm 0$$

$$\Leftrightarrow \alpha = n$$

$$\Leftrightarrow \alpha \in N$$

Hence Ker f $= N$