Isomorphisms

Idea: To develop a formal method to see if two groups in different terms are really the same.

Def Group Isomorphism:

An isomorphism ϕ from a group G to a group $\overline{G}$ is a one-to-one onto mapping from G to $\overline{G}$ that preserves the group operation. That is

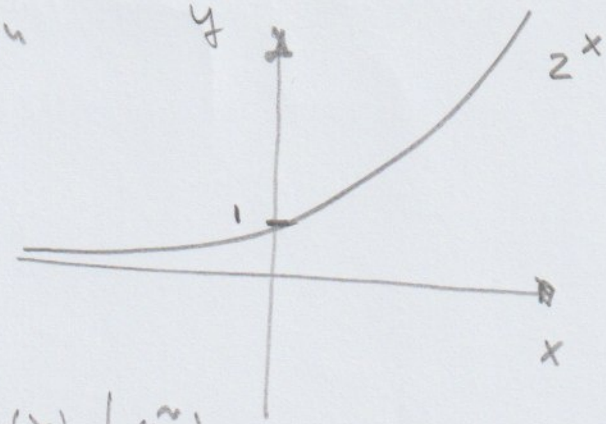
$$\phi(ab) = \phi(a)\phi(b) \quad \forall a,b \in G$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are isomorphic and write $G \approx \overline{G}$.

Example: G: real numbers under addition

$\bar{G}$: positive real numbers under multiplication

$\phi(x) = 2^x$



$$\phi(x+\tilde{x}) = 2^{x+\tilde{x}}$$
$$= 2^x 2^{\tilde{x}} = \phi(x)\,\phi(\tilde{x})$$

Example: Any infinite cyclic group is isomorphic to $\mathbb{Z}$. If a generates G, then $a^k \to k$ is an isomorphism $G \to \mathbb{Z}$.

Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ under the mapping $a^k \to k \bmod n$.

Example: The mapping from $\mathbb{R} \to \mathbb{R}$ under addition given by $\phi(x) = x^3$ is not an isomorphism.

It is not operation-preserving as

$\phi(x+y) = (x+y)^3 = x^3 + y^3$ is <u>not</u> true

for all $x, y \in \mathbb{R}$.

<u>Example:</u> There is no isomorphism from $\mathbb{Q}$, the group of rational numbers under addition, to $\mathbb{Q}^*$, the group of nonzero rational numbers under multiplication. If there were such a mapping, there would be $a \in \mathbb{Q}$ such that $\phi(a) = -1$. But then

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

but there is no $b = \phi\left(\frac{a}{2}\right)$ in $\mathbb{Q}^*$ such that $b^2 = -1$.

<u>Example</u> Let $G = SL(2,\mathbb{R})$, the group of 2×2 matrices with determinant 1.
Let $M \in SL(2,\mathbb{R})$, define ϕ_M via

$$\phi_M(A) = MAM^{-1} \quad (\text{"conjugation by } M\text{"}).$$

To verify that ϕ_M is an isomorphism, we need

1. Show that $\phi_M(A) \in G$
2. ϕ_M is one-to-one.
3. ϕ_M is onto.
4. ϕ_M is operation preserving

Theorem Properties of Isomorphisms Acting on Elements

Suppose that ϕ is an isomorphism from $G \to \overline{G}$. Then

1/ ϕ carries the identity of G to the identity of $\overline{G}$.

2/ $\phi(a^n) = (\phi(a))^n$ (additive: $\phi(na) = n\phi(a)$)

3/ $a, b \in G$ commute if and only if $\phi(a)$ and $\phi(b)$ commute.

4/ $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$

5/ $|a| = |\phi(a)|$ for all $a \in G$

6/ $x^k = b$ has the same number of solutions in G as $x^k = \phi(b)$ in $\overline{G}$.

7. If G is finite, then G and $\bar{G}$ have exactly the same number of elements of every order.

Proof: 1./ Let e be the identity in G, and $\bar{e}$ the identity in $\bar{G}$.

$e = ee \Rightarrow \phi(e) = \phi(e)\phi(e) \Rightarrow \bar{e} = \phi(e)$
(cancellation)

2./ positive integers, use induction.

If n is negative, then $-n$ is positive.

$$e = \phi(e) = \phi(a^n a^{-n}) = \phi(a^n)\,\phi(a^{-n})$$
$$= \phi(a^n)\,\phi(a)^{-n} \Rightarrow \phi(a)^n = \phi(a^n)$$

Property 1 takes care of $n = 0$.

4./ Let $G = \langle a \rangle$, clearly $\langle \phi(a) \rangle \subseteq \bar{G}$.
Since ϕ is onto, for any $b \in \bar{G}$

there exists $a^k \in G$ such that $\phi(a^k) = b$, thus $b = (\phi(a))^k \in \langle \phi(a) \rangle$. Hence $\overline{G} = \langle \phi(a) \rangle$.

Now suppose $\overline{G} = \langle \phi(a) \rangle$, clearly $\langle a \rangle \subseteq G$. For any $b \in G$ we have $\phi(b) \in \langle \phi(a) \rangle$, so $\phi(b) = (\phi(a))^k = \phi(a^k)$
$\Rightarrow b = a^k$ since ϕ is one-to-one.
This implies $G = \langle a \rangle$ $\square$

Theorem: Properties of Isomorphisms Acting on Groups

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

1./ ϕ^{-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

$\phi(K) = \{ \phi(a) \mid a \in K \}$ is a subgroup of $\overline{G}$.

5./ If $\overline{K}$ is a subgroup of $\overline{G}$, then

$\phi^{-1}(\overline{K}) = \{ g \in G \mid \phi(g) \in \overline{K} \}$ is a subgroup of G.

6./ $\phi(Z(G)) = Z(\overline{G})$

Note: We can use these theorems to show that groups are not isomorphic, for example if $|G| \neq |\overline{G}|$.

MTH 339

9/9

Cayley's Theorem: Every group is isomorphic to a group of permutations.

Proof: Given G, use it to construct $\overline{G}$.

For any $g \in G$, define $T_g : G \to G$

$T_g(x) = gx$ (multiplication by g on the left)

Clearly, T_g is a permutation on the set of elements of G. Set $\overline{G} = \{T_g \mid g \in G\}$.

$\overline{G}$ is a group under the operation of function composition. Define $\phi(g) = T_g$

(1) ϕ is one-to-one: $T_g = T_h \Rightarrow T_g(e) = T_h(e) \Rightarrow g = h$

(2) ϕ is onto by construction.

(3) Operation-preserving:

$$\phi(ab) = T_{ab} = T_a T_b = \phi(a)\phi(b)$$

$T_{ab}(x) = (ab)x = a(bx) = aT_b(x) = T_aT_b(x)$ $\square$

MTH 339 - Do Now

1./ Verify claims (1)-(4) to show that ϕ_M is an isomorphism.

2./ Prove property 3: If $\phi : G \to \overline{G}$ is an isomorphism then $a, b \in G$ commute if and only if $\phi(a)$ and $\phi(b)$ commute.

3./ Prove that T_g is a group under the operation of function composition.

MTH 339 - HW

1./ Show that $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$ under multiplication.

2./ In the proof of Cayley's Theorem, prove that T_e is the identity and $(T_g)^{-1} = T_{g^{-1}}$.

3./ Let G be a group under multiplication, $\overline{G}$ a group under addition and ϕ an isomorphism $G \to \overline{G}$. If $\phi(a) = \overline{a}$ and $\phi(b) = \overline{b}$, find an expression for $\phi(a^3 b^{-2})$ in terms of $\overline{a}$ and $\overline{b}$.

4/ Let $r \in U(n)$. Prove that the mapping $\alpha: \mathbb{Z}_n \to \mathbb{Z}_n$, defined by $\alpha(s) = sr \bmod n$ for $s \in \mathbb{Z}_n$ is an automorphism of $\mathbb{Z}_n$

5/ Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.