Isomorphism.

Definition

Let G and G' be two groups. A map $f : G \to G'$ is called an isomorphism if

(i) f is a bijection.

(ii) $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Two groups G and G' are said to be isomorphic if there exist an isomorphism $f : G \to G'$.

If two groups are isomorphic we write $G \cong G'$.

Example : See book

Theorem 3.44.

Isomorphism is an equivalent relation among groups.

for any group G.

$i_G : G \to G$ is clearly an isomorphism

Hence $G \cong G$. Therefore the relation is reflexive.

Now, let $G \cong G'$ and let $f : G \to G'$ be an isomorphism.

Then f is a bijection.

$\therefore f^{-1} : G' \to G$ is also a bijection

let $x', y' \in G'$.

Let $f^{-1}(x') = x$ and $f^{-1}(y') = y$

$f(x) = x$ and $f(y) = y$

$f(xy) = f(x)\, f(y)$

$= x'y'$.

$\therefore f^{-1}(x'y') = xy = f^{-1}(x')\, f^{-1}(y')$.

Hence f^{-1} is an isomorphism

Thus $G' \cong G$ and hence the relation is symmetric

Now, let $G \cong G'$ and $G' \cong G''$

Then there exist isomorphisms

$f : G \longrightarrow G'$ and $g : G' \longrightarrow G''$.

Since f and g are bijections;

$gof : G \longrightarrow G''$ is also bijection.

Now let $x, y \in G$, then

$(gof)(xy) = g[f(xy)]$

$= g[f(x)\, f(y)]$ (since f is an isomorphism.)

$= g[f(x)]\, g[f(y)]$

$= (gof)(x)\, (gof)(y)$

Hence gof is an isomorphism.

Thus $G \cong G''$ and hence the relation is transitive.

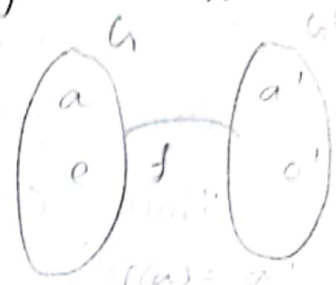
Isomorphism is an equivalence relation among groups.

Theorem 3.45

Let $f : G \to G'$ be an isomorphism. Then

(i) $f(e) = e'$ where e and e' are the identity elements of G and G' respectively. (ie) In an isomorphism identity is mapped on to indentity.

(ii) $f(a^{-1}) = [f(a)]^{-1}$



(i)

Let $a' \in G'$ since $f : G \to G'$ is a bijection, there exists such that $a \in G$ such that $f(a) = a'$

$$a' f(e) = f(a) f(e)$$
$$= f(ae)$$
$$= f(a)$$
$$= a'$$

Similarly,

$$f(e)\, a' = a'$$

Hence, $f(e) = e'$

(ii) To prove $f(a) f(a^{-1}) = f(a^{-1}) f(a) = e'$

Now, $f(a) f(a^{-1}) = f(aa^{-1})$
$= f(e)$
$= e'$.

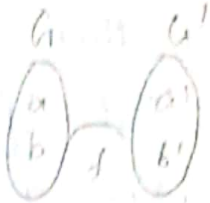
$f(a^{-1}) f(a) = f(a^{-1}a)$
$= f(e)$
$= e'$

Hence $f(a) f(a^{-1}) = e' = f(a^{-1}) f(a)$

$$f(a^{-1}) = [f(a)]^{-1}.$$

Theorem 3.46.

Let $f : G \longrightarrow G'$ be an isomorphism. If G is abelian, then G' also abelian.



Let $a', b' \in G'$. Then there exist $a, b \in G$ such that $f(a) = a'$ and $f(b) = b'$

Now, to prove G' is abelian

$a'b' \in G'$ then $a'b' = f(a)f(b)$ (by homomorphism)

$= f(ab)$ (since G is abelian $ab = ba$)

$= f(ba)$

$= f(b)f(a)$

$= b'a'$

$\therefore a'b' = b'a'$.

Hence G' is abelian.

Theorem 3.47.

Let $f : G \longrightarrow G'$ be an isomorphism. Let $a \in G$. Then the order of a is equal to the order of $f(a)$.

Let the order of a is n.

$o(a) = n$ such that $a^n = e$. n is least positive integer

Now, to prove the order of $f(a)$ is n such that $[f(a)]^n = e'$. n is least positive integer

Now, $[f(a)]^n = f(a), \ldots\ldots, f(a)$

$= f(a^n)$

$= f(e)$

$= e'$.

Now, if possible let m be a positive integer such that $0 < m < n$ and $[f(a)]^m = e'$.

Then $[f(a)]^m = f(a^m) = f(e) = e'$

But $f(e) = e'$

Since f is 1-1, Then $f(a^m) = f(e)$

$a^m = e$

But the definition of order of a is $a^n = e$ which is contradicts.

Hence n is must least positive integer such that $[f(a)]^n = e$.

$\therefore$ The order of $f(a)$ is n.

Theorem 3.48

Let $f : G \longrightarrow G'$ be an isomorphism If G is cyclic then G' is also cyclic.

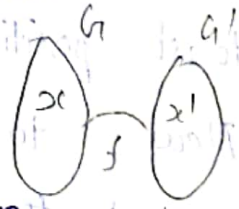
Let a be a generator of group G.

$G = \langle a \rangle$, $a^n = x$ for some integer n.

To prove that $f(a)$ is generator of the group G'.

Let $x' \in G'$. since f is bijection, there exists $x \in G$ such that

$f(x) = x'$



Now, TPT $x' = [f(a)]^n$

$x' = f(x) = f(a^n) = [f(a)]^n$.

Since $x' \in G'$ is arbitrary every element of G' is of the form $[f(a)]^n$

so that $G' = \langle f(a) \rangle$

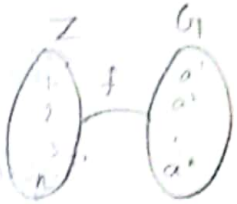
Hence G' is cyclic.

Theorem 3.44

Any infinite cyclic group G is isomorphic to $(\mathbb{Z}, +)$

Let G be an infinite cyclic group generated by a.

$$G = \{ a^n / n \in \mathbb{Z} \}$$



We defined map $f : \mathbb{Z} \to G$ by $f(n) = a^n$.

Since G is infinite $n \neq m$

$$f(n) \neq f(m)$$

$$a^n \neq a^m$$

Hence f is 1-1.

Let $a^n \in G$ for some $n \in \mathbb{Z}$

$$f(n) = a^n.$$

Hence f is onto.

Now, $f(n+m) = a^{n+m} = a^n \cdot a^m = f(n) f(m)$.

Hence f is an isomorphism.

$\therefore (\mathbb{Z}, +) \cong G$.

Corrollary

Any two infinite cyclic groups are isomorphic to each other.

Let G and G' be two infinite cyclic groups.

By our known Theorem $G \cong (\mathbb{Z}, +)$ and $(\mathbb{Z}, +) \cong G'$.

Thus $G \cong G'$. (since $\cong$ is an equivalence relation)

Theorem 3.50.

Any finite cyclic group of order n with is isomorphic to Z_n. ①

Let G_1 be a cyclic group of order n with generator a. such that $o(G_1) = n$

$G_1 = \langle a \rangle \quad a^n = e$

The $G_1 = \{e, a, a^2, \ldots a^{n-1}\}$

Define $f : Z_n \longrightarrow G_1$ by $f(r) = a^r$

Cleary f is a bijection.

Now, let $r, s \in Z_n$, let $r \oplus s = t$.

$r + s = qn + t$

where $0 \leq t < n$

$f(r \oplus s) = a^{r \oplus s} = a^t \longrightarrow ①$

let $r, s \in Z_n$

$r \neq s$

$a^r \neq a^s$

$f(r) \neq f(s)$. f is 1-1

take $a^r \in G_1$

$r \in Z_n$

$f(r) = a^r$. f is onto.

Also,

$f(r) f(s) = a^r \cdot a^s$

$= a^{r+s}$

$= a^{qn+t}$

$= (a^n)^q \cdot a^t$

$= e^q \cdot a^t$

$= a^t \longrightarrow ②$

from ① and ② we get $f(r \oplus s) = f(r) f(s)$

Hence f is an isomorphism.

$\therefore Z_n, \oplus \cong G_1$.

Corollary

Any two finite cyclic groups of the same order are isomorphic.

Let G and G' be two finite cyclic group of same order.

To prove $G \cong G'$

By known theorem $G \cong (\mathbb{Z}_n, \oplus)$ and $(\mathbb{Z}_n, \oplus) \cong G'$.

We know that $\cong$ is transitive.

Hence $G \cong G'$.

Theorem 3.51

Cayley's theorem.

Any finite group is isomorphic to a group of permutations.

We shall prove this theorem in 3 steps. we shall first find a set G' of permutations and finally we exhibit an isomorphism $\phi : G \to G'$.

Step-01. Let G be a finite group of order n.

Let $a \in G$.

Define $f_a : G \to G$ by $f_a(x) = ax$

Now, $f_a(x) = f_a(y)$

$ax = ay$ (by cancellation law)

$x = y$

Hence f is 1-1.

Now, $y \in G$ $a \in G$ $a^{-1} \in G$

$f_a(a^{-1}y) = a(a^{-1}y)$ Hence f_a is onto

$= (aa^{-1})y$.

$f_a(a^{-1}y) = y$.

This f_a is bijection.

Since G has n elements, f_a is just a

permutation on n symbols.

Let $G' = \{ f_a / a \in G \}$

Step-2.

Now, we prove G' is a group.

Let $f_a . f_b \in G'$.

$$(f_a \circ f_b) x = f_a(f_b(x)) = f_a(bx)$$
$$= a(bx)$$
$$= (ab)x$$
$$= f_{ab}(x).$$

Hence $f_a \circ f_b = f_{ab}$.

G' is closed under composition of mappings.

$$[(f_a \circ f_b) \circ f_c] x = (f_a \circ f_b)[f_c(x)]$$
$$= (f_a \circ f_b)(cx)$$
$$= f_a[f_b(cx)]$$
$$= f_a(bcx)$$
$$= a(bcx)$$
$$= a(bcx)$$
$$[(f_a \circ f_b) \circ f_c] x = [f_a \circ (f_b \circ f_c)] x.$$

G' is associative.

$$(f_a \circ f_e) x = f_a(ex)$$
$$= aex$$
$$= ax$$
$$= f_a(x)$$

Hence $f_e \in G'$ is the identity element.

The inverse of f_a in G' is f_a^{-1}.

step-3- we prove $G \cong G'$.

Define $\phi : G \to G'$ by $\phi(a) = f_a$

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

$f_a = f_b$

$f_a(x) = f_b(x)$

$ax = bx$

$a = b$

Hence ϕ is 1-1. obviously ϕ is onto.

Also $\phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$

Hence, ϕ is homomorphism.

Hence ϕ is an isomorphism.

Theorem 3.52.

For any group G,

(i) Aut G is a group under composition of functions.

(ii) $I(G)$ is a normal subgroup of Aut G.

(i) Let $f, g \in$ Aut G.

$\therefore f$ and g are isomorphisms of G to itself

$\therefore fog$ is an isomorphism of G to itself

$\therefore fog \in$ Aut G.

$f \in$ Aut $G \Rightarrow f^{-1} \in$ Aut G

Clearly Composition of functions is associative

Hence Aut G is a group.

(ii) Let $\phi_a, \phi_b \in I(G)$. Then

$(\phi_a \phi_b)(x) = \phi_a(bxb^{-1})$

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

$= (ab)x(ab)^{-1}$

$= \phi_{ab}(x)$

Hence $\phi_a \phi_b = \phi_{ab} \in I(G)$

ϕ_e is the identity element of $I(G)$

the inverse of ϕ_a is $\phi_{a^{-1}}$.

$\therefore I(G)$ is a subgroup of Aut G.

We now prove that $I(G)$ is a normal in Aut (G).

Let $\alpha \in \text{Aut}(G)$ and $\phi_a \in I(G)$ Then

$$\begin{aligned} \alpha\phi_a\alpha^{-1}(x) \in &= \alpha\phi_a(\alpha^{-1}(x)) \\ &= \alpha\left(a\,\alpha^{-1}(x)\,a^{-1}\right) \\ &= \alpha(a)\,\alpha\alpha^{-1}(x)\,\alpha(a^{-1}) \\ &= \alpha a\, x\, [\alpha a]^{-1} \\ &= \phi_{\alpha(a)}(x). \end{aligned}$$

$\alpha\phi_a\alpha^{-1} = \phi_{\alpha(a)} \in I(G)$

Hence $I(G)$ is a normal subgroup of Aut G.