Isomorphisms

Definition. Let $f: (G, \circ) \to (H, *)$ be a homomorphism. f is called an isomorphism if it is one-to-one and onto. In this case, G and H are called isomorphic groups. We write in this case $G \cong H$.

Ex. $(\mathbb{R}_+, \cdot)$ and $(\mathbb{R}, +)$ are isomorphic groups since $\exists$ isomorphism $f: \mathbb{R}_+ \to \mathbb{R}$ given by $f(x) = \ln x$. Evidently, $f(x)$ is one-to-one and onto. Also f is a homomorphism from $(\mathbb{R}_+, \cdot)$ to $(\mathbb{R}, +)$ since

$$f(a \cdot b) = \ln(a \cdot b) = \ln a + \ln b = f(a) + f(b).$$

Theorem. Let G be a cyclic group.

(a) If $|G| = \infty$ then G is isomorphic to $(\mathbb{Z}, +)$

(b) If $|G| = n < \infty$, $n > 1$, then G is isomorphic to $(\mathbb{Z}_n, +)$, where $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ and $[a] + [b] = [c]$, $a + b = kn + c$, $0 \le c \le n-1$, $k \in \mathbb{Z}$.

Proof:

(a) We have $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

Define $f(a^k) = k$. Then $f(a^k \circ a^m) = f(a^{k+m}) = k + m = f(a^k) + f(a^m)$, i.e. f is a homomorphism.

Let us show that f is one-to-one.

If $f(a^k) = f(a^m)$, then $k = m$, i.e. $a^k = a^m$.

f is clearly onto since $\forall k \in \mathbb{Z}$, $k = f(a^k)$.

(b) $G = \{a, a^2, \dots, a^{n-1}, a^n = e\}$ for some $a \in G$.

Define $f(a^k) = [k]$.

HW. Prove that $f(a^k) = [k]$ is a group homomorphism from G to $\mathbb{Z}_n$.

Properties of Isomorphisms

We consider isomorphic groups to be "the same". For our use of the word "same" to be reasonable, we should prove that the relation $\cong$ has properties similar to $=$, i.e. we need to prove that $\cong$ is an equivalence relation.

Theorem. Let G, H, K be groups. Then

(1) $G \cong G$.

(2) If $G \cong H$ then $H \cong G$.

HW (3) If $G \cong H$ and $H \cong K$, then $G \cong K$.

Proof:

(1) To prove that $G \cong G$, consider function $id: G \to G$ given by $id(a) = a \ \forall a \in G$. It is one-to-one and onto. Also $id(a \circ b) = a \circ b = id(a) \circ id(b)$, i.e. id is a homomorphism, then id is an isomorphism from G to G, i.e. $G \cong G$.

(2) Let $G \cong H$, then $\exists$ isomorphism $f: G \to H$, i.e. f is (i) one-to-one and (ii) onto and a homomorphism. From (i), (ii) it follows that $\exists\, f^{-1}: H \to G$ s.t. $f(f^{-1}(a)) = a \ \forall a \in H$ and $f^{-1}(f(b)) = b \ \forall b \in G$.

The inverse of f, f^{-1}, is one-to-one and onto. Also, $\forall a, b \in H$, $\exists\, x, y \in G$ s.t. $a = f(x)$, $b = f(y)$ and then

$$f^{-1}(a * b) = f^{-1}(f(x) * f(y)) = f^{-1}(f(x \circ y)) = x \circ y = f^{-1}(a) \circ f^{-1}(b), \quad \forall a, b \in H.$$

It yields that f^{-1} is an isomorphism from H to G, i.e. $H \cong G$.

(3) HW $\square$

Since isomorphic groups are supposed to be the same, they should have many of the same properties. Moreover, the isomorphism should send an element to one with the same properties.

Theorem: Let $G \cong H$. Then

(1) G and H have the same number of elements.
(2) G is commutative iff H is commutative.
(3) G is cyclic iff H is cyclic
HW (4) If $g \in G$, $T: G \to H$ is an isomorphism, then $ord(g) = ord(T(g))$.

Proof:

(1) $G \cong H \iff \exists$ one-to-one and onto function $T: G \to H \Rightarrow |G| = |H|$.

(2). Let G be commut, $T: G \to H$ be an isomorphism. Let $a, b \in H$, then $\exists x, y \in G$ s.t. $a = T(x)$, $b = T(y)$

$$a * b = T(x) * T(y) = T(x \circ y) = T(y \circ x) = T(y) * T(x) = b * a,$$

(T is homom; G is commut; T is homom.)

i.e. $a * b = b * a$ $\forall$ $a, b \in H$. Hence, H is commut. groep. Similar, if H is commut., $T^{-1}: H \to G$ is a homom, then G is commut.

(3) Let G be cyclic, $T: G \to H$ be an isomorphism, $G = \langle a \rangle$ for some $a \in G$. Then $H = \langle T(a) \rangle$. Indeed, $\langle T(a) \rangle \subset H$. On the other hand, $\forall$ $x \in H$ $\exists$ $b_x \in G$ s.t. $T(b_x) = x$. Since $G = \langle a \rangle$, then $b_x = a^{n_x}$ for some $n_x \in \mathbb{Z}$. Therefore,

$$x = T(b_x) = T(a^{n_x}) = (T(a))^{n_x} \subset \langle T(a) \rangle,$$

It implies that $H \subset \langle T(a) \rangle$ and proves $H = \langle T(a) \rangle$. □

Ex. Let G be a group. Define a binary relation on G by

$$R = \{(x,y): \exists g \in G \text{ s.t. } y = g \circ x \circ g^{-1}\}$$

Show that R is an equivalence relation.

Solution:

Clearly, R is reflexive since $x = e \circ x \circ e^{-1}$, i.e. $(x,x) \in R \ \forall x \in G$.

R is symmetric. Indeed,

if $(x,y) \in R$, i.e. $\exists g$ s.t. $y = g \circ x \circ g^{-1}$, then

$g^{-1} \circ y = x \circ g^{-1}$, or $g^{-1} \circ y \circ g = x$, or $g^{-1} \circ y \circ (g^{-1})^{-1} = x$.

Hence $(y,x) \in R$.

R is transitive. Indeed,

Let $(x,y) \in R$, $(y,z) \in R$. Then $\exists g, p \in G$ s.t.

$y = g \circ x \circ g^{-1}$, $z = p \circ y \circ p^{-1}$. Hence

$z = p \circ y \circ p^{-1} = p \circ g \circ x \circ g^{-1} \circ p^{-1} = (p \circ g) \circ x \circ (p \circ g)^{-1}$, i.e. $(x,z) \in R$.

As reflexive, symmetric, transitive binary relation, R is an equivalence relation.

Ex. Let G be a group and H a subgroup. Show that $R_H = \{(x,y): x \circ y^{-1} \in H$, i.e., $x \in yH\}$ is an equivalence relation on G.

Solution:

- Reflexivity: $(x,x) \in R_H \ \forall x$ since $x \circ x^{-1} = e \in H$.
- Symmetry: Let $(x,y) \in R_H$, i.e. $x \circ y^{-1} \in H \Rightarrow$ $(x \circ y^{-1})^{-1} \in H$, i.e. $y \circ x^{-1} \in H \Rightarrow (y,x) \in R_H$

Transitivity: Let $(x,y) \in R_H$, $(y,z) \in R \Rightarrow x \circ y^{-1} \in H$, $y \circ z^{-1} \in H \Rightarrow$ $x \circ z^{-1} = (x \circ y^{-1}) \circ (y \circ z^{-1}) \in H \Rightarrow (x,z) \in R_H$

Thus, R_H is an equivalence relation on G.

Denote the number of distinct equivalence classes on G induced by R_H, by $[G:H]$. We call this number the index of H in G.

Theorem (Lagrange's Theorem). Let G be a finite group and H a subgroup. Then $|G| = [G:H] \cdot |H|$.
In particular, if G is a finite group, the number of elements in H divides the number of elements in G.

Proof.
Assume that G is finite. It is clear that $|G|$ is equal to the sum of the elements in all distinct equivalence classes of R_H, since

$$G = A_1 \cup A_2 \cup \dots \cup A_{[G:H]}$$

If we show that every equivalence class A_i has $|H|$ elements then we will add $|H|$ to itself $[G:H]$ times and get the number of elements in G.
Thus we need to show that $|aH| = |H|$.
To show this let us show that function $f: H \to aH$ defined by $f(x) = a \circ x$ is a one-to-one and onto:

one-to-one: $f(x) = f(y) \iff a \circ x = a \circ y \Rightarrow x = y$

onto: Take $y \in aH \Rightarrow \exists x \in H$ s.t. $y = ax \Rightarrow f(x) = ax = y$, i.e. For $y \in aH \; \exists x \in H$ s.t. $f(x) = y$. □

Corollary 1. Let G be a finite group, $g \in G$. Then order of g divides $|G|$. Therefore, $g^{|G|} = e$.

Proof:
$\langle g \rangle$ is a subgroup of $G \Rightarrow |\langle g \rangle|$ divides $|G|$ by Lagrange's Theorem. But $|\langle g \rangle| = \text{ord}(g)$. Hence, $\text{ord}(g) \cdot k = |G|$ for some $k \in \mathbb{N}$. Therefore,

$$g^{|G|} = g^{\text{ord}(g)\,k} = \left(g^{\text{ord}\,g}\right)^k \overset{(5)}{=} e^k = e. \quad \square$$

Corollary 2. Let G be a group and $|G|$ is a prime number. Then G is cyclic and hence $G \cong \mathbb{Z}_{|G|}$.

Proof: Take arbitrary element $g \in G$, $g \neq e$. Consider $\langle g \rangle$. We know that $\langle g \rangle$ is a subgroup of G. Then, by Lagrange's Theorem, $|\langle g \rangle|$ divides $|G|$. Since $|G|$ is prime then $|\langle g \rangle| = |G|$. Hence, $G = \langle g \rangle$ and then G is cyclic. □

For example, groups with 17 elements are all cyclic.

Corollary 3 (Fermat Theorem). Let p be a prime number. Then for any integer x, we have $x^p - x$ is divisible by p.

To prove Corollary 3, consider

set $\mathbb{Z}_p$, where p is a prime number.

(p is prime if it is divisible only by 1 and p. For example, 3, 5, 7, 11 are prime numbers).

Let $\mathbb{Z}_p^* = \{[1], [2], \dots, [p-1]\}$ be the set of classes by modulo p except class $[0]$.

Define the following binary operation on $\mathbb{Z}_p^*$:

$[a] \circ [b] = [c]$, where $ab = kp + c$, $0 \leq c \leq p-1$, $k \in \mathbb{Z}$.

Then $(\mathbb{Z}_p^*, \circ)$ is a group. Indeed,

1) $\forall [a], [b] \in \mathbb{Z}_p^*$, $[a] \circ [b] \in \mathbb{Z}_p$ and $[a] \circ [b] \neq [0]$.
Assume contrary, $[a] \circ [b] = [0]$, then $ab = kp$. Since $1 \leq a \leq p-1$ and $1 \leq b \leq p-1$ then and p is prime it is impossible to have $ab = kp$.
Hence, $[a] \circ [b] \in \mathbb{Z}_p^*$

2) $([a] \circ [b]) \circ [c] \stackrel{?}{=} [a] \circ ([b] \circ [c])$
$[ab] \circ [c] \stackrel{?}{=} [a] \circ [bc]$
$[abc] = [abc]$. O.K

3) $\exists e = [1]$ s.t. $[a] \circ [1] = [a]$

4) $\forall [a] \exists [a]^{-1}$ s.t. $[a] \circ [a]^{-1} = [1]$. Indeed,

Let $[a]^{-1} = [b]$. Then we must have

$$ab = kp + 1$$

Consider $a\cdot 1, a\cdot 2, \ldots, a\cdot(p-1)$. Assume that all of them do not have remainder 1 after division by p. Then there are two numbers, say $a\cdot i$ and $a\cdot j$, $1 \le j < i \le p-1$ that have the same remainder after division by p, i.e.

$$a\cdot i - aj = kp, \quad k \in \mathbb{Z}.$$

$$\Downarrow$$

$$a(i-j) = kp, \text{ i.e. } [a]\circ[i-j] = [0].$$

This is impossible since $\mathbb{Z}_p^*$ is closed under $\circ$ and do not contain $[0]$.

Hence $\mathbb{Z}_p^*$ is a group under multiplication.

Proof of Fermat Theorem (Corollary 3)

There are two possibilities:

(i) x is divisible by p and (ii) x is not divisible by p.

In first case if $x = pk$, then clearly

$x^p - x = p^p k^p - pk = p(p^{p-1}k^p - k)$ is divisible by p.

Consider second case – when x is not div. by p.

$x = pk + r$, $1 \le r \le p-1$. By Corollary 1 (applying to $(\mathbb{Z}_p^*, \circ)$) we have $r^{p-1} = e$, i.e. $r^p = r$. Hence $(x-pk)^p = x - pk$, i.e.

$$(x-pk)(x-pk)\ldots(x-pk) = x - pk$$

$$x^p + yp = x - pk, \text{ where } y \in \mathbb{Z}.$$

Then $x^p - x = p(-y-k)$ is divisible by p.