Homomorphisms

Definition: Let $\langle G, * \rangle$ and $\langle H, \diamond \rangle$ be groups.
A function $\varphi: G \to H$ s.t.

$$\varphi(x * y) = \varphi(x) \diamond \varphi(y) \quad \forall\ x, y \in G$$

is a homomorphism.

When the group operations are clear, we write $\varphi(xy) = \varphi(x)\varphi(y)$

operation on G   operation on H

Examples:

1.) The function $f: \mathbb{Z} \to \mathbb{Q}$ defined $f(x) = x$ is a homomorphism.
$f(a+b) = a + b = f(a) + f(b)$.

In fact, if $H \leq G$, then the embedding $f: H \to G$ is a homomorphism.

2.) Define $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}_+, \cdot \rangle$ by

$$f(x) = e^x.$$

Then $f(x+y) = e^{x+y} = e^x e^y = f(x) f(y)$. Thus, f is a homomorphism.

3.) Let $f: \mathbb{Z}_4 \to D_8$ be defined
$f(a) = r^a$.

Then $f(a+b) = r^{a+b} = r^a r^b = f(a)f(b)$.

We have to be careful though! This only works because the additions are both "mod 4", and $a+b \in \{0,1,2,3\}$.

i.e. $r^x = r^{x \pmod 4}$. From now on, write $+_n$ to mean addition mod n

4.) Define $f: \mathbb{Z}_3 \to D_8$ by $f(a) = r^a$

Then $f(0) = r^0 = e$
$f(1) = r^1 = r$
$f(2) = r^2$

Then $f(a +_3 b) = r^{a +_3 b} = r^a r^b = f(a)f(b)$? <u>No</u>

These $+$'s are supposed to be different! One should be be mod 3 and one is mod 4!

This equality <u>doesn't</u> hold

e.g. $f(1 +_3 2) = f(0) = e$, but $f(1)f(2) = r^1 r^2 = r^3 \neq e$.

What's going on? $3 \equiv 0 \pmod 3$ and $3 \equiv 3 \pmod 4$

5.) Define $f: \langle \mathbb{Q} - \{0\}, \cdot \rangle \to \langle \mathbb{Q}, + \rangle$ by $f(x) = x$.

Then $f(1 \cdot 1) = 1$, but $f(1) + f(1) = 1+1 = 2$, so

f is <u>not</u> a homomorphism.

<u>Thm</u>: If $f: G \to H$ is a homomorphism, then $\forall\ x \in G$, $f(x^n) = f(x)^n \ \forall\ n \in \mathbb{Z}$. (In particular, $f(e) = e$, $f(x^{-1}) = f(x)^{-1}$)

Pf: First we prove the statement for $n \geq 0$.

If $n=0$, then $f(e) = f(e \cdot e) = f(e)f(e) \Rightarrow f(e) = e = x^0$.

Now assume the statement holds for k.

Then $f(x^{k+1}) = f(x^k x) = f(x^k)f(x) = f(x)^k f(x) = f(x)^{k+1}$.

Now we show $f(x^{-1}) = f(x)^{-1}$:

$e = f(x x^{-1}) = f(x) f(x^{-1}) \Rightarrow f(x^{-1}) = f(x)^{-1}$.

Now, we show the statement holds for $n<0$:

If $n<0$, then $x^n = (x^{-n})^{-1}$, so $f(x^n) = f((x^{-n})^{-1}) = f(x^{-n})^{-1}$

But $-n>0$, so $f(x^{-n})^{-1} = \left(f(x)^{-n}\right)^{-1} = f(x)^n$. $\square$

Def: If $\varphi: G \to H$ is a homomorphism and also a bijection, then φ is an <u>isomorphism</u>, and we say that G and H are <u>isomorphic</u>, denoted $G \cong H$.

Ex:

1.) The homomorphism $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}_+, \cdot \rangle$ defined $f(x) = e^x$ is an isomorphism:

Injectivity: If $f(x) = f(y)$, then

$$e^x = e^y$$

$$\Rightarrow \ln(e^x) = \ln(e^y) \Rightarrow x = y.$$

surjectivity: If $x \in \mathbb{R} - \{0\}$, then $f(\ln x) = e^{\ln x} = x$.

2.) The function $f: \mathbb{Z} \to 2\mathbb{Z}$ defined $f(x) = 2x$ is an isomorphism:

$\forall\, a,b \in \mathbb{Z}$, $f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b)$, so f is a homomorphism.

If $f(x) = f(y)$, then $2x = 2y \Rightarrow x = y$, so f is injective.

If $x \in 2\mathbb{Z}$, then $x = 2y$ for some $y \in \mathbb{Z}$, so $f(y) = x$, so f is surjective.

If φ is an isomorphism, it preserves the structure of the group:

Theorem: If $\varphi: G \to H$ is an isomorphism, then

a.) $|G| = |H|$
b.) G is abelian $\Leftrightarrow$ H is abelian
c.) $\forall\, x \in G$, $|x| = |\varphi(x)|$

Pf: a.) Since φ is an isomorphism, it's a bijection, so G and H have the same cardinality, so $|G| = |H|$.

b.) Assume G is abelian. Then if $a, b \in H$, $\exists$ $a', b' \in G$ s.t. $\varphi(a') = a$, $\varphi(b') = b$. Then $ab = \varphi(a')\varphi(b') = \varphi(a'b') = \varphi(b'a') = ba$.

So H is abelian. If H is abelian, then $\varphi^{-1}: H \to G$ is an isomorphism, so G is abelian as well, by the above argument.

c.) Case 1: x has finite order.

If $|x| = n$, then $\varphi(x)^n = \varphi(x^n) = \varphi(e) = e$,

so $\varphi(x)$ has finite order $m \leq n$.

$\varphi(x^m) = \varphi(x)^m = e = \varphi(e)$. Since φ is an isomorpism, $x^m = e$, so

$m \geq n \implies m = n$

Case 2: x has infinite order. Assume $\varphi(x)$ has finite order.

Then, by the above, x has finite order, which is a contradiction.

Thus, $\varphi(x)$ has infinite order as well. $\square$

Ex: $\langle \mathbb{Q}, + \rangle$ is not isomorphic to $\langle \mathbb{R}, + \rangle$ since $\mathbb{Q}$ and $\mathbb{R}$ have different cardinalities — $\mathbb{Q}$ is countable, while $\mathbb{R}$ is not.

Ex: $D_6 \not\cong \mathbb{Z}_6$ since D_6 is not abelian, while $\mathbb{Z}_6$ is.

Ex: $\mathbb{Z} \times \mathbb{Z}_2 \not\cong \mathbb{Z}$, since $(0, 1)$ has order 2, while all nonzero elements of $\mathbb{Z}$ have infinite order.

Images and Kernels of homomorphisms

Def: Let $\varphi: G \to H$ be a homomorphism. The kernel of φ, denoted $\ker \varphi$ is the set $\{g \in G \mid \varphi(g) = e\}$

Theorem: $\ker \varphi$ is a subgroup of G.

Pf: $\varphi(e) = e$, so $e \in \ker\varphi$, so $\ker\varphi \neq \emptyset$.

Let $x, y \in \ker\varphi$. Then $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = e \cdot \varphi(y)^{-1} = e$.

Thus, $xy^{-1} \in \ker\varphi$.

Ex: Consider (let $n \in \mathbb{Z}_+$) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined $\varphi(x) = x \pmod{n}$.

Then $\ker\varphi = \{x \in \mathbb{Z} \mid x = 0 \pmod{n}\} = n\mathbb{Z}$.

Ex: Consider $\varphi : n\mathbb{Z} \to \mathbb{Z}$ defined $\varphi(x) = x$.
Then $\ker\varphi = \{x \in n\mathbb{Z} \mid \varphi(x) = 0\} = \{0\}$

Theorem: If $\varphi : G \to H$ is a homomorphism, then φ is injective $\Longleftrightarrow$ $\ker\varphi = \{e\}$.

Proof: Assume φ is injective. Let $x \in \ker\varphi$. Then
$\varphi(x) = e = \varphi(e)$, so $x = e$. $\Rightarrow \ker\varphi = \{e\}$.

Now assume $\ker\varphi = \{e\}$. Suppose $\varphi(x) = \varphi(y)$ for some $x, y \in G$. Then $\varphi(x)\varphi(y)^{-1} = \varphi(y)\varphi(y)^{-1} = e$

$$\Rightarrow \varphi(xy^{-1}) = e$$
$$\Rightarrow xy^{-1} \in \ker\varphi$$
$$\Rightarrow xy^{-1} = e \Rightarrow x = y.$$

So φ is injective. $\square$

Recall that the image of $\varphi: G \to H$, or $\varphi(G)$, is

$$\{ y \in H \mid \varphi(x) = y, \text{ some } x \in G \}$$

Theorem: $\varphi(G) \leq H$.

Pf: $\varphi(e) = e$, so $e \in \varphi(G) \Rightarrow \varphi(G) \neq \emptyset$.

Let $x, y \in \varphi(G)$. Then $\varphi(a) = x$, $\varphi(b) = y$ for some $a, b \in G$

Then $xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1})$, so $xy^{-1} \in \varphi(G)$

Thus, $\varphi(G) \leq H$, as desired. $\square$

Thm: If $\varphi: G \to H$ is injective, then $G \cong \varphi(G)$.

Define $\psi: G \to \varphi(G)$ by $\psi(g) = \varphi(G)$.

Then ψ is a homomorphism, since φ is, and

$\ker \psi = \ker \varphi = \{e\}$, so ψ is injective.

By construction, ψ is surjective. Thus, ψ is an isomorphism, so $G \cong \varphi(G)$, as desired. $\square$