Isomorphisms: Basics

Definition: Let G and H be groups. An isomorphism from G to H is a function

$$f : G \to H$$

in G in H

which is bijective and which satisfies $\boxed{f(g_1 g_2) = f(g_1)f(g_2)}$ for all $g_1, g_2 \in G$. If an isomorphism exists between two groups G and H, they are called *isomorphic*.

Example: $\mathbb{R}$ **and** $\mathbb{R}^{\star}_{+}$**,** e^x **and** $\log(x)$**.**

$G = \mathbb{R}$ with addition

$H = \mathbb{R}^*_+ = \{x \in \mathbb{R},\ x > 0\}$ with multiplication.

$f : \mathbb{R} \longrightarrow \mathbb{R}^*_+$

$f(x) = e^x$ is an isomorphism.

Remember: inverse function theorem says f is bijective $\Leftrightarrow$ it has an inverse.

$\ln : \mathbb{R}^*_+ \longrightarrow \mathbb{R}$ $\quad e^{\ln(x)} = \ln e^x = x$

$\underbrace{f(g_1 g_2)}_{\text{in } \mathbb{R}.} = f(g_1)f(g_2)$ in $\mathbb{R}^*_+$

$x = g_1$

$y = g_2$

$e^{\underset{\text{in } \mathbb{R}}{x+y}} = \boxed{e^x \cdot e^y}$ (true!)

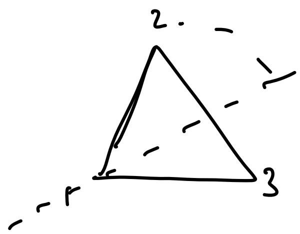
$\ln : \mathbb{R}^*_+ \longrightarrow \mathbb{R}$

$\ln(xy) = \ln(x) + \ln(y)$

$0 \in \mathbb{R}$

$e^0 = 1 \in \mathbb{R}^*_+$ $\quad 1 \in \mathbb{R}^*_+ \quad \ln(1) = 0 \in \mathbb{R}$

Example: S_3 and the triangle group



f: triangle group $\longrightarrow S_3$

symmetry $\longrightarrow$ corresponding permutation of vertices.

$$\mathrm{id} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\text{rotation right} \longrightarrow (1\,2\,3)$$

$$\text{rotation left} \longrightarrow (1\,3\,2)$$

$$\text{reflections} \longrightarrow (2\,3),\ (1\,3),\ (1\,2)$$

(reflection fixing 1)(rotation right) = reflection fixing 2

$$(2\,3)(1\,2\,3) = (1\,3)$$

reflection fixing 2 =

f(reflection fixing 1) f(rotation right) = f((reflection fixing 1)(rotation right))

Example: $U(7)$ and $\mathbb{Z}_6$ are isomorphic

$U(7) = \{1, 2, 3, 4, 5, 6\}$ with multiplication

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with addition.

$3 \in U(7)$ 3 has order 6 mod 7

$\langle 3 \rangle = U(7) \cong \mathbb{Z}_6$

$3^1 = 3$

$3^2 = 9 = 2$

$3^3 = 6$

$3^4 = 4$

$3^5 = 5$

$3^6 = 1$

$U(7)$		$\mathbb{Z}_6$
3	$\longrightarrow$	1
2	$\longrightarrow$	2
6	$\longrightarrow$	3
4	$\longrightarrow$	4
5	$\longrightarrow$	5
1	$\longrightarrow$	$6 = 0$

$$f(\underbrace{6 \cdot 4}_{\text{in } U(7)}) = f(3^3 \cdot 3^4) = f(3^7) = f(3^6 \cdot 3) = f(3) = 1$$

$f(6) = 3$

$f(4) = 4$

$f(6) + f(4) = 3 + 4 = 7 = 1$

$f(6 \cdot 4) = f(6) + f(4)$

$g : \mathbb{Z}_6 \longrightarrow U(7)$

$g(a) = 3^a$

$g(a) = g(\underline{a+6}) = 3^{a+6} = 3^a \cdot \underline{3^6} = 3^a$ g is "well defined" on $\mathbb{Z}_6$.

$g(a+b) = 3^{a+b} = 3^a \cdot 3^b = g(a)g(b)$. g is isomorphism.

g is bijective. $g(1) = 3$ $g(2) = 2$ $g(3) = 6$ $g(4) = 4$ $g(5) = 5$ $g(6) = 1$

$\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic.

$\mathbb{Z}_4$ have four elements.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \to (0,0), (1,0), (0,1), (1,1)$ $\quad (1,1)+(1,1) = (1+1, 1+1) = (0,0)$

Suppose $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ is an isomorphism.

every elt of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2.

But $1 \in \mathbb{Z}_4$ has order 4.

$f(1) = \underline{a} \in \mathbb{Z}_2 \times \mathbb{Z}_2$

$f(1+1) = f(2) = f(1) + f(1) = a + a = 0$

$f(2) = 0.$

also $f(0) = 0$: Proof

$\underline{a} = f(1) = f(1+0) = f(1) + f(0) = a + f(0)$

$a = a + f(0) \Rightarrow f(0) = 0.$

So f not bijective.

No isomorphism exists.

$\mathbb{Q}$ and $\mathbb{Z}$ are not isomorphic

$\mathbb{Q}$ additive $\qquad \mathbb{Z}$ additive.

Suppose

$$f : \mathbb{Z} \longrightarrow \mathbb{Q}$$

is an isomorphism.

$$\rightarrow f(1) = a \in \mathbb{Q}. \qquad \underline{a \neq 0}$$

if $\begin{cases} f(1) = 0 & \text{then } f(1+1) = f(2) = f(1)+f(1) \\ f(2) = 0 & \text{so } f \text{ not bijective} \quad = 0+0 \\ & \quad = 0 \end{cases}$

$$\frac{a}{2} \in \mathbb{Q}$$

there must be $x \in \mathbb{Z}$ so that $f(x) = \frac{a}{2}$.

$$f(2x) = f(x+x) = f(x)+f(x) = \frac{a}{2} + \frac{a}{2} = a$$

$$f(2x) = a.$$

$$2x = f^{-1}(a) = 1 \quad \text{in } \mathbb{Z}$$

But there is no $x \in \mathbb{Z}$ such that

$$2x = 1.$$

So f cannot exist.

Some theorems

Proposition: If $f : G \to H$ is an isomorphism, then $f(e_G) = e_H$.

Proof: we will check that $f(e_G)$ has the property that $f(e_G)h = hf(e_G) = h$ for all $h \in H$.

Since there is only one element like this, $f(e_G) = e_H$.

Choose $h \in H$. $h = f(g)$ for some $g \in G$.

$hf(e_G) = f(g)f(e_G) = f(ge_G) = f(g) = h$

$f(e_G)h = f(e_G)f(g) = f(e_Gg) = f(g) = h.$

$f(e_G)$ has the identity property so it must $= e_H$.

$f(x) = e^x$

$e^0 = 1$

$\ln(1) = 0.$

$f : \mathbb{Z}_6 \to U(7)$

$f(a) = 3^a$

$f(0) = 3^0 = 1$

Theorem: Let $f : G \to H$ be an isomorphism between G and H. Then:

- G and H have the same number of elements. (same cardinality)

  ~~Consequence of f~~ being bijective.

- f^{-1} is an isomorphism from H to G.

  Proof: Need to check that $f^{-1}(h_1 h_2) = f^{-1}(h_1) f^{-1}(h_2)$ for all $h_1, h_2 \in H$. $f^{-1} : H \to G$.

  Given $h_1, h_2 \in H$.

  $h_1 = f(g_1)$ $g_1 = f^{-1}(h_1)$

  $h_2 = f(g_2)$ $g_2 = f^{-1}(h_2)$

  $h_1 h_2 = f(g_1) f(g_2) = f(g_1 g_2)$ $g_1 g_2 = f^{-1}(h_1 h_2)$

  $f^{-1}(h_1) f^{-1}(h_2) =$

- if one of G or H is abelian, so is the other.

$f: G \to H$ is an isomophism.

G abelian

$H \ni h_1 = f(g_1)$

$H \ni h_2 = f(g_2)$

$$h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1)$$
$$= f(g_2)f(g_1)$$
$$= h_2 h_1$$

$f^{-1}: H \to G$ is an isomophism

you can use same argument to show

H abelian $\Rightarrow$ G abelian.

- if one of G or H is cyclic, so is the other.

$f: G \to H$ isomophism

Suppoe G cyclic.

Then $G = \langle g \rangle$.

$h = f(g)$

Claim: $H = \langle h \rangle$.

we've shown $h_2 = h^i$ for some i

so H is cyclic.

Let $h_2 \in H$.

$h_2 = f(g_2)$

$g_2 = g^i$

$$h_2 = f(g^i) = \underbrace{f(g)f(g)f(g)\dots}^{i \text{ times}}$$
$$= (f(g))^i = h^i$$

$f: \mathbb{Z}_6 \to U(7)$

$1 \mapsto 3^1 = 3$

- if K is a subgroup of G, then $f(K)$ is a subgroup of H.

$K \subseteq G$ subgroup $\quad f: G \to H$ isomorphism

$f(K) = \{ h \in H \mid h = f(k)$ for some $k \in K \}$.

Proof: $f(K)$ contains $f(e_G) = e_H$

$e_G \in K$.

$f(K)$ not empty

$a, b \in f(K)$ $\quad a = f(k_1)$, $b = f(k_2)$

$ab = f(k_1)f(k_2) = f(k_1k_2)$

$k_1k_2 \in K \quad f(k_1k_2) \in f(K)$

$a \in f(K) \quad a = f(k), \quad a^{-1}? \quad f(k^{-1}) = a^{-1} \quad f(k^{-1})a = f(k^{-1})f(k) = f(e_G) = e_H$

$a^{-1} \in f(K)$

- if one of G or H has a subgroup of order n, so does the other.

follows from above

$K \subseteq G$ has n elements is a subgp.

$f(K) \subseteq H$ is a subgroup and

$f: K \to f(K)$ is bijective

so $f(K)$ has n elements.

Proposition: Isomorphism is an equivalence relation on groups.

- It is reflexive (G is isomorphic to itself)

Find $f: G \to G$ that is an isomorphism.

$f = id_G : G \to G.$

- It is symmetric (if G is isomorphic to H, then H is isomorphic to G)

if $f: G \to H$ is an isomorphism

then $f^{-1}: H \to G$ is, too

- It is transitive (if G is isomorphic to H, and H is isomorphic to K, then G is isomorphic to K)

if $f: G \to H$ $g: H \longrightarrow K$ are isomorphisms

then $g \circ f : G \longrightarrow K$ is too.

- $g \circ f$ is bijective.

$(g \circ f)(g_1 g_2) = g(f(g_1 g_2)) = g(f(g_1) f(g_2))$

$= g(f(g_1)) g(f(g_2))$

$= (g \circ f)(g_1)(g \circ f)(g_2)$