Class 11

February 13, 2024

Isomorphism

Often we might notice two groups seem to have very similar structure. When can we say that two groups have the same structure? If two groups have the same structure, we hope many important properties are preserved. Here are some:

- Have the same number of elements
- Have the same minimum number of generators
- Same number of commuting elements (ie, the center is the same size)
- Has the same number of cycles
- ...

If we look at two groups we have seen previously S_3, D_3, it seems like both groups share each of these properties? Can we say they are the same structure? To do so, we need the concept of Isomorphism. For groups G, H, we say G is **isomorphic** to H if there exists a bijection $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b)$. We denote this as $G \approx H$. Note, $a, b \in G$, so ab will be combined using the binary operation of G. Likewise, $\phi(a), \phi(b) \in H$, so we must take $\phi(a)\phi(b)$ using the binary operation of H.

Examples of Isomorphisms

As we have shown with **5** above, it is sufficient to show that the isomorphism $\phi : G \to H$ maps the generators of G to the generators of H as long as ϕ is bijective. If we use $G = D_3, H = S_3$, then we can use the isomorphism $\phi : G \to H$

$$\phi(x) = \begin{cases} (1) & e \\ (123) & r \\ (132) & r^2 \\ (12) & f \\ (13) & fr \\ (23) & fr^2 \end{cases}$$

To show this is an isomorphism, we need to show that the generators are mapped appropriately. This means we only need to check that $\phi(ab) = \phi(a)\phi(b)$ for every possible pair of generators a, b. We know ϕ is a bijection, as these are finite sets and each element in H gets mapped to exactly once.

$$(132) = \phi\left(r^2\right) = \phi(r)\phi(r) = (123)(123) = (132)$$

$$(23) = \phi\left(fr^2\right) = \phi(rf) = \phi(r)\phi(f) = (123)(12) = (23)$$

$$(13) = \phi(fr) = \phi(f)\phi(r) = (12)(123) = (13)$$

$$(1) = \phi(e) = \phi(ff) = \phi(f)\phi(f) = (12)(12) = (1)$$

As these all hold, then ϕ is an isomorphism and $D_3 \approx S_3$.

Isomorphism is an Equivalence Relation

Isomorphism forms an equivalence relation on the "set" of all groups. (Technically there is not a set of all groups. There is a category of all groups or a proper class of all groups. This gets far into the weeds of set theory, and the details are irrelevant to this class).

pf

To show that we have an equivalence relation, we need to show that for groups G, H, K

1. $G \approx G$ (Reflexivity)
2. $G \approx H \implies H \approx G$ (symmetry)
3. $G \approx H, H \approx K \implies G \approx K$ (transitivity)

1) Consider the identity function $\phi : G \to G$ such that $\phi(a) = a$. From a previous class, we know that the identity function is a bijection. As $\phi(ab) = ab = \phi(a)\phi(b)$, then ϕ is an isomorphism and $G \approx H$.

2) Suppose $G \approx H$. Then $\exists \phi : G \to H$ such that ϕ is an isomorphism. As ϕ is an isomorphism, then ϕ is bijective, thus ϕ^{-1} is bijective. As ϕ is an isomorphism, then $\phi(ab) = \phi(a)\phi(b)$. Applying ϕ^{-1} to both sides,

$$\phi^{-1}(\phi(a))\phi^{-1}(\phi(b)) = ab = \phi^{-1}(\phi(ab)) = \phi^{-1}(\phi(a)\phi(b))$$

As $\phi(a), \phi(b)$ are arbitrary elements of H, this combined with bijection implies ϕ^{-1} is an isomorphism from $H \to G$, thus $H \approx G$.

3) Suppose $G \approx H, H \approx K$. Then $\exists$ isomorphisms $\phi : G \to H, \theta : H \to K$. As ϕ, θ are isomorphisms, then both ϕ, θ are both bijections. Thus $\theta \circ \phi$ is a bijection. As ϕ, θ are isomorphisms, then

$$\theta(\phi(ab)) = \theta(\phi(a)\phi(b)) = \theta(\phi(a))\theta(\phi(b))$$

Thus $\theta \circ \phi$ is an isomorphism and $G \approx K$. As all three conditions are met, then isomorphism forms an equivalence relation.

Properties of Isomorphisms

Isomorphisms preserve all of the kinds of properties we usually care about. Here are some of the properties. For isomorphic groups, G, H, with isomorphism $\phi : G \to H$, the following properties hold:

1. $\phi(e)$ is the identity in H.
2. $\phi(a^n) = \phi(a)^n \ \forall n \in \mathbb{Z}$.
3. For all $a, b \in G$ such that $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$.
4. $G = \langle a \rangle$ iff $H = \langle \phi(a) \rangle$.
5. For $n > 0$, $a^n = e$ iff $\phi(a)^n = \phi(e)$.
6. ϕ^{-1} is an isomorphism.
7. G is abelian iff H is abelian.
8. G is cyclic iff H is cyclic.
9. If $K \leq G$, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of H.
10. If $J \leq H$, then $\phi^{-1}(J) = \{g \in G | \phi(g) \in J\}$ is a subgroup of G.
11. $\phi(Z(G)) = Z(H)$. The center is preserved under isomorphism.

We will prove 1-10, but will save 11 for a future homework problem.

pf

1. $\phi(e) = \phi(ee) = \phi(e)\phi(e)$. As the identity is unique, then $\phi(e)$ must be the identity in H.

2. We have 3 cases: First, suppose $n = 0$. Then $\phi(a^0) = \phi(e) = \phi(a)^0$. Suppose $n \geq 1$. Then we can use induction. For the base case, let $n = 1$. Then

$$\phi(a^1) = \phi(a) = \phi(a)^1$$

For the inductive step, suppose $\phi(a^k) = \phi(a)^k \;\; 1 \leq k \leq n$. Then

$$\phi(a^n) = \phi(a)^n$$

If we multiply both sides by $\phi(a)$, then

$$\phi(a^n)\phi(a) = \phi(a)^n \phi(a)$$

$$\phi(a^{n+1}) = \phi(a^n a) = \phi(a)^{n+1}$$

Thus the $n \geq 1$ case holds by induction. For case 3, suppose $n \leq -1$. We will use induction again. For the base case, let $n = -1$. Then

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e)$$

As the inverse is unique, this implies $\phi(a)^{-1} = \phi(a^{-1})$. Now, for the induction step, suppose $\phi(a^{-k}) = \phi(a)^{-k} \;\; 1 \leq k \leq n$. Then

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

Multiply both sides by $\phi(a)^{-1}$

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

Thus the inductive proof holds for case 3. As this holds for all three cases, we have proven the desired result.

3. First suppose $ab = ba$. Then $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$. Now suppose $\phi(a)\phi(b) = \phi(b)\phi(a)$. Then $\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a) = \phi(ba)$. Taking the inverse function of both sides

$$\phi^{-1}(\phi(ab)) = ab = ba = \phi^{-1}(\phi(ba))$$

4. For each $x \in G$, there exists $n \in \mathbb{Z}$ such that $x = a^n$. Pick some $\phi(x) \in H$. As ϕ is a bijection, then this is possible for every element of H. Thus $\phi(x) = \phi(a^n) = \phi(a)^n$ (Using **2**). As every element of Hcan be written is this form, then we say that H can be generated by $\langle \phi(a) \rangle$. Similarly, if $H = \langle \phi(a) \rangle$, then for any $\phi(x) \in H$, $\phi(x) = \phi(a)^n$ for some $n \in \mathbb{Z}$. Thus for any $x \in G$, $\phi(x) = \phi(a)^n = \phi(a^n)$. Taking the inverse of each side, $x = \phi^{-1}(\phi(x)) = \phi^{-1}(\phi(a^n)) = a^n$, thus each element of G can be written as a^n for some $n \in \mathbb{Z}$,and $G = \langle a \rangle$.

5. Recall from **1.** $\phi(e)$ is the identity in H. Thus $\phi(e) = \phi(a^n) = \phi(a)^n$, if $a^n = e$. Suppose $\phi(a)^n = \phi(e)$. Then $\phi(e) = \phi(a)^n = \phi(a^n)$. Taking the inverse of both sides $e = \phi^{-1}(\phi(e)) = \phi^{-1}(\phi(a^n)) = a^n$.

6. This was shown in the process of showing that isomorphism forms an equivalence relation.

7. G is abelian if $ab = ba$ for all $a, b \in G$. By **3**, we know $\phi(a)\phi(b) = \phi(b)\phi(a)$ iff $ab = ba$. Thus H is abelian. Similarly, if H is abelian, then $\phi(a)\phi(b) = \phi(b)\phi(a) \;\; \forall \phi(a), \phi(b) \in H$. By **3**, then $ab = ba$, thus G is abelian.

8. If G is cyclic, then $G = \langle a \rangle$ for some $a \in G$. By **4**, then $H = \langle \phi(a) \rangle$, thus H is cyclic. If H is cyclic, then $H = \langle \phi(a) \rangle$ for some $\phi(a) \in H$. By **4**, then $G = \langle a \rangle$, thus G is cyclic.

9. If $K \leq G$, then for all $a, b \in K$, $ab^{-1} \in K$, thus $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1}$. As $ab^{-1} \in K$, then $\phi(ab^{-1}) \in \phi(K)$, thus $\phi(a)\phi(b)^{-1} \in \phi(K)$, thus $\phi(K) \leq H$.

10. As ϕ^{-1} is an isomorphism from $H \to G$, and $J \leq H$, then by **9**, $\phi^{-1}(J) \leq G$.