

MATH 30A, ABSTRACT ALGEBRA I: GROUP THEORY

6. ISOMORPHISMS

We often want to say that two groups G and H are essentially the same, i.e., representations of the same abstract concept. We say that they are *isomorphic*.

6.1. Definition.

Definition 6.1. An isomorphism $\phi : G \xrightarrow{\cong} H$ is a bijection satisfying the condition:

$$\phi(gh) = \phi(g)\phi(h)$$

for all $g, h \in G$. We write $G \cong H$ (G is isomorphic to H)

A *bijection* is 1-1 and onto. I gave this example:

Theorem 6.2. The additive group $G = (\mathbb{R}, +)$ with identity 0 is isomorphic to the multiplicative group $H = (\mathbb{R}_+, \cdot)$ with identity 1.

Proof. An isomorphism $\phi : G \rightarrow H$ is given by $\phi(x) = e^x$. We have to verify the three conditions:

ϕ is 1-1. This means that different elements of G go to different elements of H . If $x \neq y$ then we have to show that $\phi(x) \neq \phi(y)$. In this case we have to show that $e^x \neq e^y$. Suppose this were not true. Then we would have $e^x = e^y$. Taking natural log of both sides we get $x = y$ which is a contradiction.

ϕ is onto. This means that each element of H is equal to $\phi(g)$ for some $g \in G$. So, take $h \in H = \mathbb{R}_+$. This means h is a positive real number. So we can take the natural log: $\ln y \in G = \mathbb{R}$. This has the property that $\phi(\ln y) = e^{\ln y} = y$. So, ϕ is onto.

Finally, we have to show that $\phi(gh) = \phi(g)\phi(h)$. This says that the operation in G corresponds to the operation in H . I.e.,

$$\phi(g + h) = \phi(g)\phi(h)$$

Or:

$$e^{x+y} = e^x e^y$$

This is one of the rules of exponents. Therefore, ϕ is an isomorphism. \square

6.2. Consequences. A group has an identity and inverses. One of the consequences of the definition is that an isomorphism takes identity to identity and inverses to inverses. For the identity I wrote:

$$\phi(e_G) = e_H$$

For example $\phi : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot)$ takes 0 to 1. ($e^0 = 1$) Here is the proof using the fact that the identity is the only idempotent (the only solution of the equation $x^2 = x$).

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$$

So, $\phi(e_G)$ is an idempotent in H and therefore must be e_H .

Isomorphisms also carry inverses to inverses. (In the example this says $\phi(-x) = e^{-x} = (e^x)^{-1} = \phi(x)^{-1}$. The proof is simple:

$$e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

So, $\phi(g^{-1}) = \phi(g)^{-1}$.

Also, isomorphisms preserve orders of elements:

$$|\phi(g)| = |g|$$

6.3. cyclic groups.

Theorem 6.3. *A groups of order n is cyclic iff it is isomorphic to \mathbb{Z}_n .*

Proof. Suppose that G is cyclic of order n and generated by g . Then an isomorphism $\phi : \mathbb{Z}_n \rightarrow G$ is given by $\phi(i) = g^i$. \square

Note that there are several isomorphisms $\mathbb{Z}_n \xrightarrow{\cong} G$, one for each generator of the cyclic group G .

Theorem 6.4. *Any group with p element (p : prime) is cyclic.*

Corollary 6.5. *Any two groups of order p are isomorphic.*

6.4. inverse of an isomorphism. An isomorphism $\phi : G \rightarrow H$ is a bijection. So, it has an inverse $\phi^{-1} : H \rightarrow G$ which is also a bijection.

Lemma 6.6. *The inverse mapping ϕ^{-1} of an isomorphism $\phi : G \rightarrow H$ is an isomorphism $H \rightarrow G$.*

Proof. We already know that $\psi = \phi^{-1}$ is a bijection. We just have to verify the condition:

$$\psi(h_1 h_2) = \psi(h_1)\psi(h_2)$$

for all $h_1, h_2 \in H$. To show this use the fact that ϕ is onto. So, $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Then

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$$

So,

$$\psi(h_1h_2) = \psi\phi(g_1g_2) = g_1g_2 = \psi(h_1)\psi(h_2)$$

and we see that $\psi = \phi^{-1}$ is an isomorphism. \square

6.5. Automorphisms. When $G = H$, an isomorphism $\phi : G \rightarrow G$ is called an *automorphism* of G . Since automorphisms are bijections from G to G , the set of automorphisms is a subset of the group of permutations of G .

Theorem 6.7. *The set of automorphisms of G is a subgroup of the group of permutations of G .*

Proof. We have to show three things:

- (1) The subset contains the identity. I.e., the identity permutation of G is an automorphism. This is obvious.
- (2) The subset is closed under the binary operation. I.e, the composition of automorphisms is an automorphism. Here is the proof of that:

$$\phi\psi(gh) = \phi(\psi(gh)) = \phi(\psi(g)\psi(h)) = \phi\psi(g)\phi\psi(h)$$

- (3) The set is closed under inverse. I.e., the inverse ϕ^{-1} of an automorphism is an automorphism. We already showed that in the lemma.

\square

Corollary 6.8 (corollary of the proof). *Isomorphism of groups is an equivalence relation.*

The group of automorphisms of a group G is denoted $\text{Aut}(G)$.

Here are some examples.

Example 6.9. (1) \mathbb{Z}_3 has two automorphisms. Since 2 is prime,

$$\text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2.$$

(2) $\text{Aut}(\mathbb{Z}_5)$ is cyclic of order 4.

(3) $\text{Aut}(\mathbb{Z}_8)$ has 4 elements but is not cyclic.

Theorem 6.10. $\text{Aut}(\mathbb{Z}_n)$ is isomorphic to the group $U(n)$ of multiplicative units modulo n .

Proof. What does this theorem say? An isomorphism

$$\psi : U(n) \xrightarrow{\cong} \text{Aut}(\mathbb{Z}_n)$$

sends $k \in U(n)$ to $\psi_k \in \text{Aut}(\mathbb{Z}_n)$. But ψ_k is an automorphism of \mathbb{Z}_n so

$$\psi_k : \mathbb{Z}_n \xrightarrow{\cong} \mathbb{Z}_n$$

This is what the theorem claims is true. To prove it we write down the formula for ψ_k . It is just multiplication by k modulo n :

$$\psi_k(j) = jk$$

This is an automorphism of \mathbb{Z}_n since

$$\psi_k(i + j) = (i + j)k = ik + jk = \psi_k(i) + \psi_k(j)$$

And ψ is an automorphism because

$$\psi_{ab}(j) = jab = (jb)a = \psi_a\psi_b(j)$$

□

Theorem 6.11. $\text{Aut}(\mathbb{Z}^n) \cong GL(n, \mathbb{Z})$

6.5.1. *inner automorphisms.* When a group G is nonabelian, there are automorphisms ϕ_g for each element $g \in G$ called *inner automorphisms* of G . They are defined by

$$\phi_g(x) = gxg^{-1}$$

This is a bijection because it has an inverse mapping $\phi_{g^{-1}}$:

$$\phi_{g^{-1}}\phi_g(x) = g^{-1}gxg^{-1}g = x$$

It is an automorphism since

$$\phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y)$$

Here is an example where all the automorphisms are inner:

Theorem 6.12. $\text{Aut}(S_3) \cong S_3$.

The correspondence $g \leftrightarrow \phi_g$ gives the isomorphism $S_3 \xrightarrow{\cong} \text{Aut}(S_3)$. It takes some work to show that this is an isomorphism.