Class 12

February 16, 2024

Thm

All cyclic groups of order n are the same up to isomorphism.

Pf

Here, when we say up to isomorphism, we mean that all cyclic groups of order n are isomorphic. Suppose G, H are cyclic groups of order n. That is

$$G = \langle a | a^n = e \rangle, H = \langle b | b^n = e \rangle$$

for some $a \in G$, $b \in H$. Then we can take the isomorphism $\phi : G \to H$ such that $\phi(a^m) = b^m$. To show this is an isomorphism, we will show this function is bijective and obeys $\phi(aa') = \phi(a)\phi(a') \, \forall a, a' \in G$. First, let's show ϕ is bijective. To show ϕ is onto, suppose $c \in H$. Then $c = b^m$ for some m such that $0 \le m < n$, thus for some $d \in G$

$$\phi(d) = c = b^m = \phi(a)^m = \phi(a^m)$$

Thus $\forall c \in H$ there exists $d = a^m \in G$ such that $\phi(d) = c$, so ϕ is onto. To show ϕ is one to one, suppose

$$\phi(x) = \phi(y)$$

for $x, y \in H$. Then

$$\phi(x) = b^m = \phi(y)$$

For some m such that $0 \le m < n$, thus

$$\phi(x) = \phi(y) = b^m = \phi(a^m)$$

And

$$x = y = a^m$$

Thus ϕ is one-to-one. As ϕ is onto and one-to-one, then ϕ is a bijection. For $x, y \in G$, $x = a^m, y = a^r$ for some r, s such that $0 \le r, s < n$.

$$\phi(xy) = \phi(a^m a^r) = \phi\left(a^{m+r}\right) = b^{m+r} = b^m b^r = \phi(a^m)\phi(a^r) = \phi(x)\phi(y)$$

Thus G, H are isomorphic. We could have also proven this result by noting that ϕ maps the generator of G to H, and then applied the properties from last class.

Automorphisms

There are a couple of special types of isomorphisms we will focus on now. The first is automorphisms. Informally, these are isomorphisms from a group onto itself. Formally, we say $\phi : G \to G$ is an automorphism if ϕ is an isomorphism. These automorphisms represent symmetry structures within a group.

Ex 1

Let $G = (\mathbb{C}, +)$, and let $\phi : G \to G$ such that $\phi(z) = \bar{z}$. Equivalently, $\phi(a + bi) = a - bi$. Then ϕ is an automorphism on G.

Pf

First, let's show ϕ is bijective. To do this, we start by showing ϕ is onto. Let $a+bi, c+di \in \mathbb{C}$. Then

$$\phi(c+di) = a+bi$$

$$= c-di = a+bi$$

Thus $a=c, d=-b$. For any $a+bi \in \mathbb{C}, \exists c+di \in \mathbb{C}$ such that $\phi(c+di) = a+bi$. Now to show ϕ is one-to-one. Suppose $a+bi, c+di \in \mathbb{C}$ s.t. $\phi(a+bi) = \phi(c+di)$. Then

$$a-bi = \phi(a+bi) = \phi(c+di) = c-di$$

Thus

$$a=c, -b=-d$$

$$a=c, b=d$$

so

$$a+bi = c+di$$

Therefore ϕ is one-to-one. As ϕ is both onto and one-to-one, then ϕ is bijective. Now, to show ϕ is an isomorphism. Let $x, y \in \mathbb{C}$ such that $x = a+bi, y = c+di$

$$\phi(x+y) = \phi((a+bi)+(c+di)) = \phi((a+c)+(bi+di))$$

$$= \phi((a+c)+(b+d)i) = (a+c)-(b+d)i$$

$$= a+c-bi-di = (a-bi)+(c-di) = \phi(a+bi)+\phi(c+di) = \phi(x)+\phi(y)$$

Thus ϕ is an isomorphism from $G \to G$, and thus an automorphism on G. This automorphism corresponds to the symmetry in the complex plane found by reflecting over the real axis.

Ex 2

Let $G = \mathbb{Z}_6$. Let $\phi : G \to G$ be an automorphism such that $\phi(1) = 5$. As 1 and 5 are generators, this is enough to uniquely define the automorphism. Equivalently, we can write this as $\phi(a) = -a \ \forall a \in \mathbb{Z}_6$. To show we have an isomorphism, let's show ϕ is an isomorphism. First, to show ϕ is a bijection. Suppose $a, b \in G$. To show ϕ is onto:

$$\phi(a) = -a = b$$

Thus

$$a = -b$$

and so each $b \in G$ has an $a \in G$ such that $\phi(a) = b$. Now, to show ϕ is one-to-one:

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

$$-a = -b$$

$$a = b$$

Thus ϕ is one-to-one. As ϕ is both onto and one-to-one, ϕ is bijective. Now, to show ϕ is an isomorphism.

$$\phi(a+b) = -(a+b) = -a-b = \phi(a)+\phi(b)$$

Thus ϕ is an isomorphism and an automorphism on $\mathbb{Z}_6$.

Inner Automorphisms

There is a special class of automorphisms called inner automorphisms. These are defined as follows: For group G with $a \in G$, $\phi_a : G \to G$ is an inner automorphism if

$$\phi_a(x) = axa^{-1}$$

First let's prove that inner automorphisms are actually automorphisms.

pf

We need to show $\phi_a(x)$ is bijective and obeys $\phi_a(xy) = \phi_a(x)\phi_a(y)$. First for bijection, let's show ϕ_a is onto. Pick some $y \in G$, such that

$$y = \phi_a(x) = axa^{-1}$$

Then multiplying by a^{-1}, a appropriately

$$a^{-1}ya = a^{-1}axa^{-1}a = exe = x$$

Thus $\forall y \in G, \exists x$ such that $\phi_a(x) = y$. Now to show ϕ_a is one-to-one. Suppose $x, y \in G$ such that

$$\phi_a(x) = \phi_a(y)$$

$$axa^{-1} = aya^{-1}$$

Multiplying both sides by a, a^{-1} appropriately:

$$a^{-1}axa^{-1}a = a^{-1}aya^{-1}a$$

$$exe = eye$$

$$x = y$$

This ϕ_a is both onto and one-to-one, thus bijective. Now, to show ϕ_a is an isomorphism:

$$\phi_a(xy) = axya^{-1} = axeya^{-1}$$

$$= axa^{-1}aya^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right) = \phi_a(x)\phi_a(y)$$

So ϕ_a is an isomorphism, thus ϕ_a is an automorphism on G.

Ex 1

A boring example comes from finding an inner automorphism on G when G is abelian. For any element a in G,

$$\phi_a(x) = axa^{-1} = aa^{-1}x = ex = x$$

So the only inner automorphism is the identity function.

Ex 2

A more interesting example can be shown for D_3. Suppose we take $\phi_f(x) = fxf^{-1} = fxf$. Then we can show what the automorphism looks like for each $x \in D_3$.

$$\phi_f(e) = fef = ff = e$$

$$\phi_f(r) = frf = r^2$$

$$\phi_f\left(r^2\right) = fr^2f = r$$

$$\phi_f(f) = fff = ef = f$$

$$\phi_f(fr) = ffrf = erf = rf = fr^2$$

$$\phi_f\left(fr^2\right) = ffr^2f = er^2f = r^2f = fr$$

Notice that this is a bijection. This is also an isomorphism, using the argument shown in the proof of this this section.

Automorphism Groups

We can define groups of automorphisms and inner automorphisms as groups of these functions under composition. We call the group of automorphisms on G,

$$\mathrm{Aut}(G) = \{\phi : G \to G | \phi \text{ is an automorphism}\}$$

Similarly, we define the inner automorphism group

$$\mathrm{Inn}(G) = \left\{\phi_a | \phi_a(x) = axa^{-1} \forall x \in G, a \in G\right\}$$

Let's prove that each of these form a group.

pf

Let $\mathrm{Aut}(G)$ be the set of all automorphisms on G. To show we have a group under function composition, we need to show we have closure, associativity identity, and inverses. First to show closure holds. Suppose ϕ, θ are automorphisms on G. Then ϕ, θ are bijective, thus $\phi \circ \theta$ is bijective. Now to show $\phi \circ \theta$ is an isomorphism. Let $x, y \in G$.

$$\phi \circ \theta(xy) = \phi(\theta(xy)) = \phi(\theta(x)\theta(y)) = \phi(\theta(x))\phi(\theta(y)) = (\phi \circ \theta(x))(\phi \circ \theta(y))$$

Thus $\phi \circ \theta$ is an isomorphism, and an automorphism of G. This implies $\mathrm{Aut}(G)$ is closed under function composition. As $\mathrm{Aut}(G)$ is a subset of the group of all invertible functions from $G \to G$ under composition, then $\mathrm{Aut}(G)$ has associativity, as composition of functions is associative. Now, to show identity, consider $\phi(x) = x$. This is a bijection as the identity function is a bijection. to show $\phi(x) = x$ is an isomorphism, let $x, y \in G$. Then

$$\phi(xy) = xy = \phi(x)\phi(y)$$

As $\phi(x) = x$ is an isomorphism, then $\phi(x) = x$ is an automorphism on G. As the identity function is the identity in the group of all invertible functions $G \to G$, then it will also be the identity of $\mathrm{Aut}(G)$. Finally, to show inverses hold, suppose ϕ^{-1} is the inverse of $\phi \in \mathrm{Aut}(G)$. We know the inverse ϕ^{-1} exists and is bijective as ϕ is bijective. Now, to show ϕ^{-1} is also an isomorphism:

$$\phi(xy) = \phi(x)\phi(y)$$

$$xy = \phi^{-1}(\phi(xy)) = \phi^{-1}(\phi(x)\phi(y))$$

$$\phi^{-1}(\phi(x))\phi^{-1}(\phi(y)) = \phi^{-1}(\phi(x)\phi(y))$$

For convenience, we may wish to set $X = \phi(x), Y = \phi(y)$.

$$= \phi^{-1}(X)\phi^{-1}(Y) = \phi^{-1}(XY)$$

Thus ϕ^{-1} is an isomorphism and thus an automorphism on G. As such, $\phi^{-1} \in \mathrm{Aut}(G)$. Now, let's show that $\mathrm{Inn}(G)$ is a group. To do so, we will note $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$, as each element of $\mathrm{Inn}(G)$ is an automorphism (as shown previously). Suppose we use subgroup test 2. First, we must show $\mathrm{Inn}(G)$ is closed under function composition. Let $\phi_a, \phi_b \in \mathrm{Inn}(G)$. Then

$$\phi_b \circ \phi_a(x) = \phi_b(\phi_a(x)) = \phi_b\left(axa^{-1}\right) = baxa^{-1}b^{-1} = (ba)x(ba)^{-1} = \phi_{ba}(x)$$

as G is a group, $ba \in G$. Now, let's show that $\mathrm{Inn}(G)$ contains the inverses of its elements. Suppose $\phi_a \in \mathrm{Inn}(G)$. Then $\phi_a^{-1} = \phi_{a^{-1}}$ as

$$\phi_{a^{-1}} \circ \phi_a(x) = \phi_{a^{-1}}(\phi_a(x)) = \phi_{a^{-1}}\left(axa^{-1}\right) = a^{-1}axa^{-1}a = exe = x$$

As $a^{-1} \in G$, then $\phi_{a^{-1}} \in \mathrm{Inn}(G)$. As both conditions are met for the second subgroup test, then $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$, and thus $\mathrm{Inn}(G)$ is a group under function composition. Next class with new content, we will give some examples of these groups.