MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's lecture on Mon, Mar 16, 2020

Chapter 6: Isomorphism's cont'd.

AUTOMORPHISMS:

Def'n: An automorphism is an isomorphism of a group onto itself ie ϕ is an automorphism of G if

$\phi: G \to G$, ϕ one-to-one, onto & operation preserving.

Theorem 1: Let $Aut(G)$ denote the set of Automorphisms of a group G. Then $Aut(G)$ is a group under composition.

Proof: The identity map $i: G \to G$ given by $i(g) = g, \forall g \in G$, is clearly an automorphism (it is bijective & operation preserving). Thus $Aut(G)$ is non-empty. Note that $Aut(G)$ is a subset of the group S_G of all permutations on G (under composition).

Now let $\phi: G \to G$ be an automorphism. Since this is an isomorphism, we know that $\phi^{-1}: G \to G$ exists and is an isomorphism. Thus ϕ^{-1} is an automorphism and $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = i$ (the identity map)). Hence for all $\phi \in Aut(G)$, we have $\phi^{-1} \in Aut(G)$.

Finally let $\phi, \psi \in Aut(G)$. Then

$$\phi: G \to G \quad \& \quad \psi: G \to G$$

are automorphisms. Since ϕ and ψ are bijections, so is

$$\phi \circ \psi: G \to G.$$

To establish that $\phi \circ \psi$ is operation preserving, consider any $g, h \in G$. Then since ϕ and ψ are operation preserving, we have

$$\phi \circ \psi(g \cdot h) = \phi(\psi(g \cdot h)) = \phi(\psi(g) \cdot \psi(h)) = \phi(\psi(g)) \cdot \phi(\psi(h)).$$

Thus $\phi \circ \psi$ is an automorphism $\forall\, \phi, \psi \in Aut(G)$. Hence $Aut(G)$ is a group - and is a subgroup of S_G.

We have seen some examples of isomorphisms between two different groups. Now well consider examples of automorphisms.

Examples of automorphisms.

1) (Generalization of problem 3, Ch. 6, page 132).

Let $G = \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ = group of positive real numbers under multiplication (identity is 1)

Let $\alpha \in \mathbb{R} - \{0\}$ and consider the map

$$\left.\begin{aligned} \phi_\alpha : \mathbb{R}_+ &\to \mathbb{R}_+ \\ x &\to x^\alpha \end{aligned}\right\} \quad \phi_\alpha(x) = x^\alpha$$

for ~~each~~ given α. Then ϕ is a bijection – it is strictly increasing if $\alpha > 0$ and strictly decreasing if $\alpha < 0$. Also

$$\phi_\alpha(xy) = (xy)^\alpha = x^\alpha y^\alpha = \phi_\alpha(x)\,\phi_\alpha(y).$$

Hence ϕ_α is an automorphism of $\mathbb{R}_+$.

2) (Example 11 on p 128).

Let $\mathbb{C}$ denote the set of complex numbers and let ϕ be the map

$$\left.\begin{aligned} \phi : \mathbb{C} &\to \mathbb{C} \\ a+ib &\to a-ib \end{aligned}\right\} \quad \phi(a+ib) = a-ib,$$

namely conjugation. Now $\mathbb{C}$ is a group under addition. Denote by $z = a+ib$ & $\bar{z} = a-ib$. Then we have

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \forall\, z_1, z_2 \in \mathbb{C}$$

and ϕ is a bijection. Hence $\phi : (\mathbb{C}, +) \to (\mathbb{C}, +)$ is an automorphism.

Note that $\mathbb{C} - \{0\} = \mathbb{C}^\times$ is a group under multiplication. Now

$$\begin{aligned} \phi : \mathbb{C}^\times &\to \mathbb{C}^\times \\ a+ib &\to a-ib \end{aligned}$$

is also an automorphism because complex conjugation satisfies

$$\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$$

This however is an automorphism under multiplication.

3) Inner Automorphism (Theorem)

Let G be a group and let $g \in G$. Consider the map i_g generated by g given by

$$\left.\begin{array}{l} i_g : G \to G \\ \quad x \to g x g^{-1} \end{array}\right\} \quad i_g(x) = g x g^{-1} \ \forall x \in G.$$

Then i_g is an automorphism.

Proof: First we prove that i_g is a bijection.

i_g is onto because given any $y \in G$, we can find $x \in G$ such that $i_g(x) = g x g^{-1} = y$, because

$$g x g^{-1} = y \iff x = g^{-1} y g$$

and this gives the value of $x \in G$. Hence i_g is onto

i_g is one-to-one because

$$i_g(x) = i_g(y) \iff g x g^{-1} = g y g^{-1} \Rightarrow x = y \text{ (by cancellation)}$$

Hence i_g is one-to-one.

Thus i_g is a bijection.

Finally we show that i_g is operation preserving because $\forall x, y \in G$,

$$i_g(xy) = g x y g^{-1} = (g x g^{-1})(g y g^{-1}) = i_g(x)\, i_g(y),$$

Hence i_g is an automorphism.

The automorphism i_g is called the inner automorphism generated by g. We denote by $Inn(G)$, the set of all inner automorphisms of G. That is

$$Inn(G) = \{ i_g \mid g \in G \}.$$

Theorem 2: $Inn(G)$ is a subgroup of $Aut(G)$. (under composition).

Proof: The identity map $i : G \to G$ given by $i(x) = x \ \forall x \in G$, can be viewed as the inner automorphism generated by the identity $e \in G$, because

$i_e(x) = exe^{-1} = x$, $\forall\ x \in G$. Thus $i = i_e \in Inn(G)$.

Next for each $g \in G$, and the inner automorphism i_g generated by g satisfies

$$i_g(x) = gxg^{-1} = y \iff x = g^{-1} \cancel{xy}\, y\, g = g^{-1} y (g^{-1})^{-1} = i_{g^{-1}}(y)$$

As x ranges over all of G, so will y. Thus i_g satisfies

$$i_g^{-1} = i_{g^{-1}}$$

and so $i_g^{-1} \in Inn(G)$, $\forall\ i_g \in \cancel{I}nn(G)$.

Finally, consider two inner automorphisms $i_g, i_h \in Inn(G)$. Then

$$i_g \circ i_h(x) = i_g(i_h(x)) = i_g(hxh^{-1}) = g\cancel{h}\ xh^{-1}g^{-1} = (gh)x(gh)^{-1}$$
$$= i_{gh}(x), \quad \forall\ x \in G, \quad \text{with } gh \in G.$$

$$\therefore\ i_g \circ i_h = i_{gh} \in Inn\ G$$

Hence $Inn(G) < Aut(G)$, proving the theorem.

Remark: (i) If G is Abelian, then there is only one inner automorphism of G, namely the identity i because for every $g \in G$, we have

$$i_g(x) = gxg^{-1} = g \cdot g^{-1} x = ex = x \ \forall\ x \in G$$
$$\therefore\ i_g = i.$$

Hence $Inn(G)$ is of interest only when G is non-Abelian.

(ii) Since each $g \in G$ generates an inner automorphism i_g, we may consider the map

$$G \longrightarrow Inn(G)$$
$$g \longrightarrow i_g$$

This map is onto but is not one-to-one. The next two problems tell us the extent to which this map is not one-to-one.

Problem 45, Ch 6, p 135:

Let G be a group and $Z(G)$, the center of G. Let $g \in G$ and $z \in Z(G)$. Then $i_g = i_{zg}$ (that is, the inner automorphisms generated by g and zg are the same).

Proof: Consider any $x \in G$. Then since $z \in Z(G)$, we have

$$i_{zg}(x) = zg \cdot x \cdot (zg)^{-1} = zgxg^{-1}z^{-1} = gxg^{-1}zz^{-1} = gxg^{-1} = i_g(x), \ \forall x \in G$$

$$\therefore \quad i_{zg} = i_g \ (= i_{gz}).$$

Problem 47, Ch 6, p 135

Let G be a group and $Z(G)$, the center of G. Let $g, h \in G$. Then

$$i_g = i_h \iff h^{-1}g \in Z(G) \iff g^{-1}h \in Z(G).$$

Proof: First note that $g^{-1}h = (h^{-1}g)^{-1}$, thus $h^{-1}g \in Z(G) \iff g^{-1}h \in Z(G)$, because $Z(G)$ is a group.

Note that

$$\begin{aligned}
i_g = i_h &\iff i_g(x) = i_h(x), \ \forall x \in G \\
&\iff gxg^{-1} = hxh^{-1}, \ \forall x \in G \\
&\cancel{\iff h^{-1}gxg^{-1}h = x, \ \forall x \in G} \text{ (not needed)} \\
&\iff h^{-1}gx = xh^{-1}g, \ \forall x \in G \\
&\iff h^{-1}g \in Z(G).
\end{aligned}$$

This proves the assertion in #47.

Remark: Note that $h^{-1}g \in Z(G) \iff h^{-1}g = z \in Z(G) \iff g = hz = zh$ and so Problem 47 and Problem 45 are saying the same thing. Thus the repetitions in the map

$$g \to i_g$$

are given precisely ~~by~~ via multiplication by elements of $Z(G)$.