Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

Let's recall our meta-examples for groups: symmetries of an object. What if the considered object is a group? A symmetry of G is a group isomorphism from G to G.

<u>Def.</u> A group isomorphism $f: G \to G$ is called an automorphism. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

. Following our meta-example, we have that $(\mathrm{Aut}(G), \circ)$ is a group. We have already mentioned that conjugation c_g by g is an automorphism of G.

<u>Theorem.</u> Suppose $(G, \cdot)$ is a group. For $g \in G$, let

$$c_g : G \to G, \quad c_g(x) := g \cdot x \cdot g^{-1}.$$

(a) For every $g \in G$, $c_g \in \mathrm{Aut}(G)$. (An automorphism of the form c_g is called an <u>inner automorphism</u>.)

(b) Let $c: G \to \mathrm{Aut}(G)$, $c(g) := c_g$. Then c is a group homomorphism and $\ker c = Z(G)$. (The image of c consists of all inner automorphisms of G and it is denoted by $\mathrm{Inn}(G)$.)

(c) $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ and $\mathrm{Inn}(G) \simeq G/Z(G)$.

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

Pf. (a) Group homomorphism. For every $x, y \in G$,

$$c_g(x)\cdot c_g(y) = g\cdot x\cdot \underbrace{g^{-1}\cdot g}_{e_G}\cdot y\cdot g^{-1} = g\cdot xy\cdot g^{-1} = c_g(x\cdot y).$$

Invertible. To show that c_g is an automorphism, we prove that c_g is invertible. In fact we show that $c_{g^{-1}}$ is the inverse of c_g. For every $x\in G$,

$$\begin{aligned}(c_g\circ c_{g^{-1}})(x) &= c_g(c_{g^{-1}}(x)) \\ &= g\cdot(g^{-1}\cdot x\cdot (g^{-1})^{-1})\cdot g^{-1} \\ &= (g\cdot g^{-1})\cdot x\cdot (g\cdot g^{-1}) = x\end{aligned}$$

$\Rightarrow c_g\circ c_{g^{-1}} = \overset{(I)}{id}$ for every $g\in G$. Hence $c_{g^{-1}}\circ c_{(g^{-1})^{-1}} = id$, and so $c_{g^{-1}}\circ c_g = \overset{(II)}{id}$.

By (I) and (II), c_g is invertible. Therefore $c_g \in \mathrm{Aut}(G)$.

(b) c is a group homomorphism. For $g_1, g_2 \in G$, we want to show that $c(g_1 g_2) = c(g_1)\circ c(g_2)$. For every $x\in G$,

$$(c_{g_1}\circ c_{g_2})(x) = c_{g_1}(c_{g_2}(x)) = g_1\cdot(g_2\cdot x\cdot g_2^{-1})\cdot g_1^{-1}$$

$$= (g_1\cdot g_2)\cdot x\cdot \underbrace{(g_2^{-1}\cdot g_1^{-1})}_{(g_1\cdot g_2)^{-1}} = (g_1\cdot g_2)\cdot x\cdot (g_1\cdot g_2)^{-1} = c_{g_1\cdot g_2}(x).$$

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

This means $c(g_1)\circ c(g_2) = c(g_1\cdot g_2)$, and so c is a group homomorphism. Notice that $g\in\ker c \iff c_g = \mathrm{id}$.

$c_g = \mathrm{id}. \iff \forall x\in G,\ c_g(x) = x \iff \forall x\in G,\ g\cdot x\cdot g^{-1} = x$

$$\iff \forall x\in G,\ g\cdot x = x\cdot g \iff g\in Z(G).$$

(d) By the 1st isomorphism theorem, $G/_{\ker c} = \mathrm{Im}\, c$. By the previous part, $\ker c = Z(G)$, and by definition $\mathrm{Im}\, c = \mathrm{Inn}(G)$.

Hence $G/_{Z(G)} \simeq \mathrm{Inn}(G)$.

To show $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, we prove that $f\circ c_g\circ f^{-1}$ is an inner automorphism for every $g\in G$ and $f\in \mathrm{Aut}(G)$. For every $x\in G$,

$$(f\circ c_g\circ f^{-1})(x) = f(c_g(f^{-1}(x))) = f(g\cdot f^{-1}(x)\cdot g^{-1})$$

$$= f(g).\ f(f^{-1}(x)).\ f(g)^{-1}$$

$$= f(g)\cdot x\cdot f(g)^{-1} = c_{f(g)}(x).$$

Hence $f\circ c_g\circ f^{-1} = c_{f(g)}$ is an inner automorphism. Thus

$f\circ \mathrm{Inn}(G)\circ f^{-1} \subseteq \mathrm{Inn}(G)$ (I) for every $f\in\mathrm{Aut}(G)$. Therefore

$f^{-1}\circ \mathrm{Inn}(G)\circ f \subseteq \mathrm{Inn}(G)$, which implies $\mathrm{Inn}(G)\subseteq f\circ \mathrm{Inn}(G)\circ f^{-1}$ (II)

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

By (I) and (II), $f \circ \mathrm{Inn}(G) \circ f^{-1} = \mathrm{Inn}(G)$ for every $f \in \mathrm{Aut}(G)$, and so $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. ∎

<u>Ex.</u> If G is abelian, then $\mathrm{Inn}(G) = \{id.\}$.

<u>Pf.</u> Since G is abelian, $G = Z(G)$. Hence $G \subseteq \ker c$, which means $c_g = id.$ for every $g \in G$. Therefore $\mathrm{Inn}(G) = \{id.\}$. ∎

<u>Ex.</u> For $n \geq 3$, $\mathrm{Inn}(S_n) \simeq S_n$.

<u>Pf.</u> By the previous theorem $\mathrm{Inn}(S_n) \simeq S_n/Z(S_n)$. We have proved that $Z(S_n) = \{id.\}$ if $n \geq 3$. Hence $\mathrm{Inn}(S_n) \simeq S_n/\{id.\}$. Notice that for every group G, $G/\{e_G\} \to G$, $x\{e_G\} \mapsto x$ is an isomorphism. Therefore $\mathrm{Inn}(S_n) \simeq S_n$. ∎

Next we find the group of automorphism of a cyclic group of order n. Let $C_n = \langle g \rangle = \{e, g, \ldots, g^{n-1}\}$ be a cyclic group of order n.

<u>Theorem</u> $\mathrm{Aut}(C_n) \simeq \mathbb{Z}_n^{\times}$.

We start with the following lemma.

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

Lemma. For $k \in \mathbb{Z}$, let $f_k : C_n \to C_n$, $f_k(x) = x^k$. Then

(a) If $[k_1]_n = [k_2]_n$, then $f_{k_1} = f_{k_2}$.

(b) For every k, f_k is a group homomorphism.

(c) If $[k]_n \in \mathbb{Z}_n^\times$, then $f_k \in \mathrm{Aut}(C_n)$.

Pf. (a) By Lagrange's theorem, for every $x \in C_n$, $x^n = e$. If $[k_1]_n = [k_2]_n$, then $k_1 \overset{n}{\equiv} k_2$, and so $k_2 = k_1 + n\ell$ for some $\ell \in \mathbb{Z}$. Therefore, for every $x \in C_n$,

$$f_{k_2}(x) = x^{k_2} = x^{k_1 + n\ell} = x^{k_1} \cdot (x^n)^\ell = x^{k_1} \cdot e^\ell = x^{k_1} = f_{k_1}(x).$$

(b) $f_k(xy) = (xy)^k = xy\,xy \cdots xy = x^k y^k = f_k(x) f_k(y)$.

cyclic groups are abelian

(c) $x \in \ker f_k \iff x^k = e_G$

$\iff o(x) \mid k$ (I)

By Lagrange's theorem, $\forall x \in C_n$, $o(x) \mid n$ (II)

By (I) and (II), $o(x) \mid \gcd(n,k)$ (III). If $[k]_n \in \mathbb{Z}_n^\times$, then $\gcd(k,n) = 1$, and so (III) implies that $o(x) = 1$.

Therefore $\ker f_k = \{e_G\}$. In your HW assigment, you have

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

seen that a group homomorphism $f: G \to H$ is injective if and only if $\ker f = \{e_G\}$. Because it is an important result I go over its proof:

. Suppose f is injective.

$$x \in \ker f \Rightarrow f(x) = e_H = f(e_G) \xRightarrow{f \text{ injective}} x = e_G.$$

. Suppose $\ker f = \{e_G\}$.

$$f(x_1) = f(x_2) \Rightarrow f(x_2)^{-1} * f(x_1) = e_H$$

$$\Rightarrow f(x_2^{-1} \cdot x_1) = e_H$$

$$\Rightarrow x_2^{-1} \cdot x_1 \in \ker f$$

$$(\ker f = \{e_G\}) \Rightarrow x_2^{-1} \cdot x_1 = e_G \Rightarrow x_1 = x_2.$$

. (Going back to the proof of $f_k \in \mathrm{Aut}(C_n)$ if $[k]_n \in \mathbb{Z}_n^\times$.)

By the above result and $\ker f_k = \{e\}$, we deduce that $f_k : C_n \to C_n$ is injective. Hence $|\mathrm{Im}\, f_k| = |C_n| = n$, which implies that f_k is surjective. Therefore $f_k \in \mathrm{Aut}(C_n)$. ∎

Next we show that every automorphism of C_n is of the form f_k for some $[k]_n \in \mathbb{Z}_n^\times$.

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

<u>Lemma</u>. For $f \in Aut(C_n)$, there is $[k]_n \in \mathbb{Z}_n^\times$ such that $f = f_k$.

<u>Pf</u>. Suppose $C_n = \{e, g, \ldots, g^{n-1}\}$. Then $f(g) = g^k$ for some $0 \le k \le n-1$. We have proved that an isomorphism does not change order of elements, this implies $o(f(g)) = o(g) = n$. Therefore $o(g^k) \overset{(I)}{=} n$. We have seen that $o(g^k) = \frac{o(g)}{\gcd(o(g), k)} = \frac{n}{\gcd(n,k)}$ (II).

Thus by (I) and (II), we obtain that $\gcd(n,k) = 1$, and so $[k]_n \in \mathbb{Z}_n^\times$. Notice that, for every $m \in \mathbb{Z}$,

$$f(g^m) = f(g)^m = (g^k)^m = (g^m)^k = f_k(g^m).$$

Therefore $f = f_k$. ∎

<u>Pf of Theorem: $Aut(C_n) \simeq \mathbb{Z}_n^\times$.</u>

- Let $\theta: \mathbb{Z}_n^\times \to Aut(C_n)$, $\theta([k]_n) := f_k$. By the "3-part" lemma, θ is a well-defined function:

$$[k_1]_n = [k_2]_n \Rightarrow f_{k_1} = f_{k_2} \text{ and } f_k \in Aut(C_n).$$

- By the previous lemma θ is surjective.
- <u>Group homomorphism</u>. We have to show that

$$\theta([k]_n \cdot [\ell]_n) = \theta([k]_n) \circ \theta([\ell]_n).$$

Group of automorphisms

Tuesday, June 29, 2021 3:29 PM

This means we have to argue why

$$f_{k\ell} \overset{?}{=} f_k \circ f_\ell .$$

For every $x \in C_n$, $f_k \circ f_\ell(x) = f_k(f_\ell(x)) = f_k(x^\ell)$

$$= (x^\ell)^k = x^{k\ell}$$

$$= f_{k\ell}(x).$$

<u>θ is injective</u>. Let's recall that

$$\theta \text{ is injective} \iff \ker\theta = \{[1]_n\}.$$

$[k]_n \in \ker\theta \implies f_k = id. \implies f_k(g) = g$

$$\implies g^k = g \implies g^{k-1} = e$$

$$\implies o(g) \mid k-1 \implies n \mid k-1$$

$$\implies k \overset{n}{\equiv} 1 \implies [k]_n = [1]_n .$$

Altogether $\theta : \mathbb{Z}_n^\times \to Aut(C_n)$ is an isomorphism. ∎