Theorem 6.2 Properties of Isomorphisms Acting on Elements.
Let G, $\overline{G}$ be groups with respective identities e, $\overline{e}$. Let $k, n \in \mathbb{Z}$ and $a, b \in G$. Then
1. $\phi(e) = \overline{e}$;
2. $\phi(a^n) = [\phi(a)]^n$;
3. $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$;
4. $G = \langle a \rangle$ iff $\overline{G} = \langle \phi(a) \rangle$;
5. $|a| = |\phi(a)|$; and
6. $|\{x \in G \,|\, x^k = b\}| = |\{x \in \overline{G} \,|\, x^k = \phi(b)\}|$.

Proof of 1.
We have

$$\begin{array}{rcll} e & = & ee & \text{by identity in } G \\ \phi(e) & = & \phi(ee) = \phi(e)\phi(e) & \text{by operation preservation} \\ \overline{e}\phi(e) & = & \phi(e)\phi(e) & \text{by identity in } \overline{G} \\ \overline{e} & = & \phi(e) & \text{by right cancelation. } \square \end{array}$$

Proof of 2. (Induction)
For $n = 0$, $\phi(a^0) = \phi(e) = \overline{e} = [\phi(a)]^0$.
For $n = 1$, $\phi(a^1) = \phi(a) = [\phi(a)]^1$.
For $n = -1$, $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(e) = \overline{e}$, and therefore $\phi(a^{-1}) = [\phi(a)]^{-1}$.
Now assume $\phi(a^n) = [\phi(a)]^n$ for some positive integer n and consider $\phi(a^{n+1})$:

$$\begin{array}{rcll} \phi(a^{n+1}) & = & \phi(a^n a) = \phi(a^n)\phi(a) & \text{by operation preservation} \\ & = & [\phi(a)]^n \phi(a) & \text{by inductive assumption} \\ & = & [\phi(a)]^{n+1}. & \end{array}$$

Therefore by induction $\phi(a^n) = [\phi(a)]^n$ for all positive integers n.
Now assume $\phi(a^n) = [\phi(a)]^n$ for some negative integer n and consider $\phi(a^{n-1})$:

$$\begin{array}{rcll} \phi(a^{n-1}) & = & \phi(a^n a^{-1}) = \phi(a^n)\phi(a^{-1}) & \text{by operation preservation} \\ & = & [\phi(a)]^n [\phi(a)]^{-1} & \text{by inductive assumption and base case } n = -1 \\ & = & [\phi(a)]^{n-1}. & \end{array}$$

Therefore the statement holds for negative integers n, and thus for all $n \in \mathbb{Z}$. $\square$

Theorem 6.2 Properties of Isomorphisms Acting on Elements.
Let G, $\overline{G}$ be groups with respective identities e, $\overline{e}$. Let $k, n \in \mathbb{Z}$ and $a, b \in G$. Then
1. $\phi(e) = \overline{e}$;
2. $\phi(a^n) = [\phi(a)]^n$;
3. $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$;
4. $G = \langle a \rangle$ iff $\overline{G} = \langle \phi(a) \rangle$;
5. $|a| = |\phi(a)|$; and
6. $|\{x \in G \,|\, x^k = b\}| = |\{x \in \overline{G} \,|\, x^k = \phi(b)\}|$.

Proof of 3. We have that

$$\begin{aligned} ab = ba \quad &\text{if and only if} \quad \phi(ab) = \phi(ba) && \text{since } \phi \text{ is a bijective function} \\ &\text{if and only if} \quad \phi(a)\phi(b) = \phi(b)\phi(a) && \text{since } \phi \text{ is operation preserving.} \end{aligned}$$ $\square$

Proof of 4. ($\Rightarrow$)
Assume that $G = \langle a \rangle$. We must show $\overline{G} = \langle \phi(a) \rangle$.
($\supseteq$) By definition $\phi(a) \in \overline{G}$, so by closure $\langle \phi(a) \rangle \subseteq \overline{G}$.
($\subseteq$) Let $b \in \overline{G}$.
Since ϕ is onto and $G = \langle a \rangle$, there exists some $k \in \mathbb{Z}$ with $\phi(a^k) = b$.
By **2**, $[\phi(a)]^k = b$, and so $b \in \langle \phi(a) \rangle$.

($\Leftarrow$)
Assume that $\overline{G} = \langle \phi(a) \rangle$. We must show $G = \langle a \rangle$.
($\supseteq$) Since $a \in G$, by closure $\langle a \rangle \subseteq G$.
($\subseteq$) Let $b \in G$.
Since $\overline{G} = \langle \phi(a) \rangle$, there exists some $k \in \mathbb{Z}$ such that $\phi(b) = [\phi(a)]^k$.
By **2**, $\phi(b) = \phi(a^k)$. But ϕ is 1-1, so $b = a^k$.
Therefore $G = \langle a \rangle$. $\square$

Proof of 5. (Sketch)
Note that when $\phi : G \to \overline{G}$ is restricted in domain to $\langle a \rangle$, it is an isomorphism from $\langle a \rangle$ to $\langle \phi(a) \rangle$.
Then apply **4**. $\square$

Theorem 6.2 Properties of Isomorphisms Acting on Elements.
Let G, $\overline{G}$ be groups with respective identities e, $\overline{e}$. Let $k, n \in \mathbb{Z}$ and $a, b \in G$. Then
1. $\phi(e) = \overline{e}$;
2. $\phi(a^n) = [\phi(a)]^n$;
3. $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$;
4. $G = \langle a \rangle$ iff $\overline{G} = \langle \phi(a) \rangle$;
5. $|a| = |\phi(a)|$; and
6. $|\{x \in G \,|\, x^k = b\}| = |\{x \in \overline{G} \,|\, x^k = \phi(b)\}|$.

Proof of 6.
Without loss of generality, we show that $x \in G$ is a solution of $x^k = b$ in G iff $\phi(x) \in \overline{G}$ is a solution of $x^k = \phi(b)$ in $\overline{G}$.
This is because ϕ is a bijection.

Let $x, b \in G$, and let $k \in \mathbb{Z}$. Then

$$\begin{aligned} x^k = b \quad &\text{if and only if} \quad \phi(x^k) = \phi(b) && \text{since } \phi \text{ is a bijective function} \\ &\text{if and only if} \quad [\phi(x)]^k = \phi(b) && \text{by } \mathbf{2}. \qquad \square \end{aligned}$$

Proof of 7.
Let $\mathcal{O}$ be the set of orders of elements of G, and fix an order $o \in \mathcal{O}$.
(Note that $\mathcal{O}$ might include ∞. when $|G| = \infty$.)
Define $S = \{x \in G \,|\, |x| = o\}$ and $T = \{y \in \overline{G} \,|\, |y| = o\}$.
For all $x \in G$, by **5** we have $x \in S$ iff $\phi(x) \in T$.
Therefore ϕ with domain restricted to S is a bijection with range T, and $|S| = |T|$. $\square$

Theorem 6.4 Aut(G) and Inn(G) are Groups

Proof sketch

Use a subgroup test.

1. show the identity bijection is in both Aut(G) and Inn(G).
   (Hint: Compute φ_e)
2. Show closure:
   (i) $f, g \in Aut(G) \Rightarrow fg \in Aut(G)$
   (ii) $\varphi_x, \varphi_y \in Inn(G) \Rightarrow \varphi_x \varphi_y \in Inn(G)$
3. Show inverses are present:
   (i) $f \in Aut(G) \Rightarrow f^{-1} \in Aut(G)$
   (ii) $\varphi_x \in Inn(G) \Rightarrow \varphi_y \in Inn(G)$
   where $(\varphi_x)^{-1} = \varphi_y$

Theorem 6.5 When $n \in \mathbb{Z}^+$, $Aut(\mathbb{Z}_n) \approx U(n)$

Lemma An automorphism $\alpha \in Aut(\mathbb{Z}_n)$ is completely determined by $\alpha(1)$.

Proof $\mathbb{Z}_n$ is cyclic. So for any $x \in \mathbb{Z}_n$,

$$\begin{aligned} \alpha(x) &= \alpha(x \cdot 1) \\ &= x \cdot \alpha(1) \quad \text{Theorem 6.2 Part 2.} \end{aligned}$$

Therefore $\alpha(1) = \beta(1) \Rightarrow \alpha = \beta$.

Proof of Thm 6.5 (sketch)

Define

$$T : Aut(\mathbb{Z}_n) \to U(n)$$

by

$$T(\alpha) = \alpha(1)$$

T 1-1: By the lemma.

T onto: if $r \in U(n)$ then

$$\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$$

$$\alpha(1) = r$$

$$\alpha(s) = sr \pmod n$$

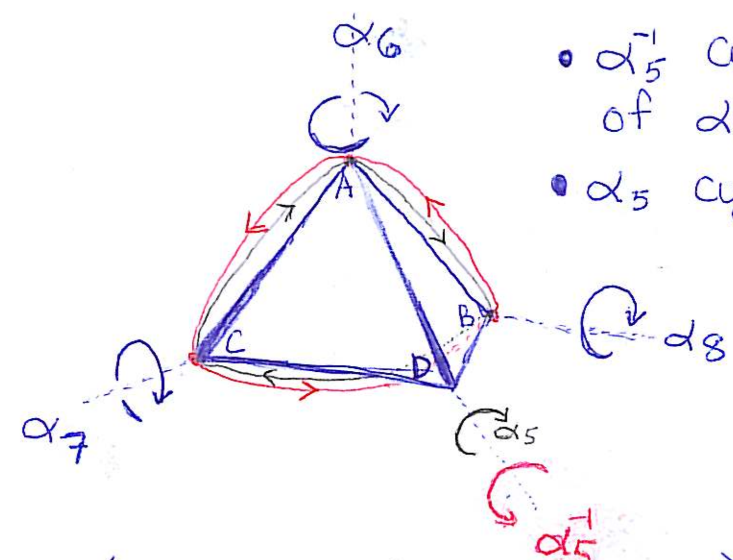
is an automorphism of $\mathbb{Z}_n$ with $T(\alpha) = r$.

T operation preserving:

$$\begin{aligned} T(\alpha\beta) = (\alpha\beta)(1) &= \alpha(\beta(1)) \quad \text{fxn composition} \\ &= \alpha(\underbrace{1+1+\cdots+1}_{\beta(1) \text{ times}}) \\ &= \underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{\beta(1) \text{ times}} \quad \text{Thm 6.2 Part 2} \\ &= \alpha(1)\beta(1) = T(\alpha)T(\beta) \end{aligned}$$

$\square$

Inner Automorphism $\varphi_{\alpha_5} : x \to \alpha_5 x \alpha_5^{-1}$ on A_4



- α_5^{-1} cycles the axes of α_6, α_7, and α_8
- α_5 cycles them back

$$\varphi_{\alpha_5} = (\alpha_6 \alpha_8 \alpha_7)\underbrace{(\alpha_6^{-1} \alpha_8^{-1} \alpha_7^{-1})}_{(\alpha_{11} \alpha_{10} \alpha_{12})}(\alpha_2 \alpha_4 \alpha_3)$$

$\alpha_2 = (AB)(CD)$

$\alpha_3 = (AC)(BD)$

$\alpha_4 = (AD)(BC)$