

Theorem 6.2 Properties of Isomorphisms Acting on Elements.

Let G, \overline{G} be groups with respective identities e, \bar{e} . Let $k, n \in \mathbb{Z}$ and $a, b \in G$. Then

1. $\phi(e) = \bar{e}$;
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. $|\{x \in G \mid x^k = b\}| = |\{x \in \overline{G} \mid x^k = \phi(b)\}|$.

Proof of 1.

We have

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

Proof of 2. (Induction)

For $n = 0$, $\phi(a^0) = \phi(e) = \bar{e} = [\phi(a)]^0$.

For $n = 1$, $\phi(a^1) = \phi(a) = [\phi(a)]^1$.

For $n = -1$, $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(e) = \bar{e}$, and therefore $\phi(a^{-1}) = [\phi(a)]^{-1}$.

Now assume $\phi(a^n) = [\phi(a)]^n$ for some positive integer n and consider $\phi(a^{n+1})$:

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

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 $\phi(a^{n-1})$:

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

Therefore the statement holds for negative integer 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, \bar{e} . Let $k, n \in \mathbb{Z}$ and $a, b \in G$.

Then

1. $\phi(e) = \bar{e}$;
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. $|\{x \in G \mid x^k = b\}| = |\{x \in \overline{G} \mid x^k = \phi(b)\}|$.

Proof of 3. We have that

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

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. The key is to note that when $\phi : G \rightarrow \overline{G}$ 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, \bar{e} . Let $k, n \in \mathbb{Z}$ and $a, b \in G$. Then

1. $\phi(e) = \bar{e}$;
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. $|\{x \in G \mid x^k = b\}| = |\{x \in \overline{G} \mid x^k = \phi(b)\}|$.

Proof of 6. It suffices to 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

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