To show that ψ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Pick m, $m' \in \mathbb{Z}_n$. Then, since $m +_n m' = m + m' - kn$ for some non-negative integer k,

$$\begin{aligned}\psi\left(\omega^m \omega^{m'}\right) &= \psi\left(\omega^{m+m'}\right) = \psi\left(\omega^{m+_n m'+kn}\right) = \psi\left(\omega^{m+_n m'}\omega^{kn}\right) \\ &= \psi\left(\omega^{m+_n m'}\left(\omega^n\right)^k\right) = \psi\left(\omega^{m+_n m'} \cdot 1^k\right) = \psi\left(\omega^{m+_n m'}\right) = m +_n m' \\ &= \psi\left(\omega^m\right) +_n \psi\left(\omega^{m'}\right),\end{aligned}$$

where the first, third and fourth equalities follow from the properties of powers.

Remark 7.4. Let G be a group. Then the identity mapping

$$\begin{array}{rccl} i_G : & G & \mapsto & G \\ & g & \mapsto & i_G(g) = g \end{array}$$

is a homomorphism. It is called the *identity homomorphism.*

Proposition 7.5. *If G, H and K are groups and*

$$\varphi : G \mapsto H \quad \textit{and} \quad \psi : H \mapsto K$$

are homomorphisms, then the composite mapping

$$\begin{array}{rccl} \psi \circ \varphi : & G & \mapsto & K \\ & g & \mapsto & (\psi \circ \varphi)(g) = \psi(\varphi(g)) \end{array}$$

is a homomorphism.

Proof This is left as an exercise. □

Definition 7.6. An *isomorphism*

$$\varphi : G \mapsto H$$

from a group G to a group H is a homomorphism from G to H for which there exists a homomorphism

$$\psi : H \mapsto G$$

such that

$$\psi \circ \varphi = i_G \quad \text{and} \quad \varphi \circ \psi = i_H,$$

where i_G and i_H are the identity isomorphisms of the groups G and H respectively (i.e.

$$\psi(\varphi(g)) = g \quad \forall g \in G \qquad \text{and} \qquad \varphi(\psi(h)) = h \quad \forall h \in H.)$$

If φ is an isomorphism, then ψ is called the *inverse homomorphism* of φ.