

**Remark 7.7.** It is easy to see that  $\psi$  is also an isomorphism with inverse homomorphism  $\varphi$ .

**Example 7.8.** Let  $n$  be a positive integer and take

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right),$$

the primitive  $n^{\text{th}}$  root of unity. Take  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  to be the group of integers mod  $n$  under addition mod  $n$ , and  $C_n$  to be the group of the  $n^{\text{th}}$  roots of unity under complex multiplication. From Example 7.3 (4), the mapping

$$\begin{aligned} \varphi : \mathbb{Z}_n &\mapsto C_n \\ m &\mapsto \varphi(m) = \omega^m. \end{aligned}$$

and its inverse

$$\begin{aligned} \psi : C_n &\mapsto \mathbb{Z}_n \\ \omega^m &\mapsto \psi(\omega^m) = m \quad \text{for } m \in \mathbb{Z}_n. \end{aligned}$$

are both homomorphisms. Hence  $\varphi$  and  $\psi$  are isomorphisms.

**Proposition 7.9.** Let  $G$  and  $H$  be groups and

$$\varphi : G \mapsto H$$

be a homomorphism. Then the following are equivalent:

- (i)  $\varphi : G \mapsto H$  is an isomorphism;
- (ii)  $\varphi : G \mapsto H$  is bijective.

**Proof** Let  $G$  and  $H$  be groups.

To show that (i)  $\Rightarrow$  (ii), suppose that  $\varphi : G \mapsto H$  is an isomorphism.

Then  $\varphi$  is an invertible mapping from  $G$  to  $H$  (with inverse given by the inverse homomorphism  $\psi : H \mapsto G$  of  $\varphi$ ). Hence  $\varphi : G \mapsto H$  is bijective.

To show that the (ii)  $\Rightarrow$  (i), suppose that  $\varphi : G \mapsto H$  is a bijective mapping. Then it is invertible. So there exists a mapping  $\psi : H \mapsto G$  such that

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

i.e.

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

where  $i_G$  and  $i_H$  are the identity isomorphisms of  $G$  and  $H$  respectively.

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