

(3) 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  $\mathbb{Z}$  to be the group of integers under addition, and  $C_n$  to be the group of the  $n^{\text{th}}$  roots of unity under complex multiplication. Consider the mapping

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

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

Pick  $m, m' \in \mathbb{Z}$ . Then

$$\varphi(m + m') = \omega^{m+m'} = \omega^m \omega^{m'} = \varphi(m) \varphi(m'),$$

where the second equality follows from the properties of powers.

(4) 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. Consider the mapping

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

To show that  $\varphi$  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  $k$ ,

$$\begin{aligned} \varphi(m +_n m') &= \omega^{m+_n m'} = \omega^{m+m'-kn} = \omega^m \omega^{m'} \omega^{-kn} = \omega^m \omega^{m'} (\omega^n)^{-k} = \omega^m \omega^{m'} \mathbf{1}^{-k} \\ &= \omega^m \omega^{m'} = \varphi(m) \varphi(m'), \end{aligned}$$

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

Consider now the inverse mapping  $\psi$  of  $\varphi$ :

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