

Abstract Algebra: Section 19

David Joseph Stith

19.17 Problem. Prove that if G is a cyclic group of order n , then $G \cong \mathbf{Z}_n$.

Suppose G is a cyclic group of order n . Then $G = \langle a \rangle$ for some $a \in G$. Therefore $G = \{a^0 = e, a^1, a^2, \dots, a^{n-1}\}$. We need to show that there exists an isomorphism $\theta : G \rightarrow \mathbf{Z}_n$. To do this we will show that the mapping θ defined by $\theta(a^x) = [x]$ is an isomorphism by showing that both of the following are true:

- (i) θ is well-defined, one-to-one, and onto.
- (ii) $\theta(pq) = \theta(p) \oplus \theta(q)$ for all $p, q \in G$.

We proceed as follows.

Suppose $p, q \in G$. Then $p = a^{k_1}$ and $q = a^{k_2}$ for some $k_1, k_2 \in \mathbf{Z}$.

- (i) To show that θ is well-defined we will show that $p = q \implies \theta(p) = \theta(q)$. Conversely, we will show that θ is one-to-one by showing that $\theta(p) = \theta(q) \implies p = q$ using the following bidirectional conditionals:

$$\begin{aligned}\theta(p) = \theta(q) &\iff \theta(a^{k_1}) = \theta(a^{k_2}) \\ &\iff [k_1] = [k_2] \\ &\iff n \mid k_1 - k_2 \\ &\iff a^{k_1 - k_2} = e \quad \text{since the order of } a \text{ is } n \\ &\iff a^{k_1} a^{-k_2} = e \\ &\iff a^{k_1} = a^{k_2} \\ &\iff p = q\end{aligned}$$

Therefore θ is well-defined and one-to-one. To see that θ is onto, simply note that for any $[x] \in \mathbf{Z}_n$, a^x exists in G and $\theta(a^x) = [x]$ by our definition of θ .

- (ii) It remains only to show that $\theta(pq) = \theta(p) \oplus \theta(q)$. We have,

$$\begin{aligned}\theta(pq) &= \theta(a^{k_1} a^{k_2}) \\ &= \theta(a^{k_1 + k_2}) \\ &= [k_1 + k_2] \\ &= [k_1] \oplus [k_2] \\ &= \theta(a^{k_1}) \oplus \theta(a^{k_2}) \\ &= \theta(p) \oplus \theta(q)\end{aligned}$$

Therefore $\theta(pq) = \theta(p) \oplus \theta(q)$.

Therefore θ is an isomorphism from G to \mathbf{Z}_n . Therefore $G \cong \mathbf{Z}_n$.

Q.E.D.