

Proof.

(\Rightarrow) Let G be a finite cyclic group. Then there exists $g \in G$ such that any element in G can be written g^n for some $n \in \mathbb{Z}$.

Let $N = |G|$ and define $\phi : G \rightarrow \mathbb{Z}(N)$ such that $\phi(g^n) = \bar{n}$, where \bar{m} is the class of integers congruent to m modulo N .

We first show that ϕ is well-defined. Consider the set $\{1, g, \dots, g^{N-1}\}$. If $g^n = g^m$ for any $0 \leq n < m < N$, then $g^{m-n} = 1$ while $m - n < N$. The cycle would have length less than N and g would not generate G , which is a contradiction. Thus the elements are unique and $G = \{1, g, \dots, g^{N-1}\}$. We also observe that $g^N = 1$, because for all $0 \leq n < N-1$, $0 < 1+n < N$, implying that $gg^n \neq 1$, leaving only g^{N-1} as the inverse of g . Let $n, m \in \mathbb{Z}$ be such that $g^n = g^m$. Then $n - m$ is an integer multiple of N , so $\phi(g^n) = \phi(g^m)$, as desired.

It is clear that ϕ is a homomorphism because for all $n, m \in \mathbb{Z}$, $\phi(g^n g^m) = \phi(g^{n+m}) = \overline{n+m} = \bar{n} + \bar{m} = \phi(g^n) + \phi(g^m)$. Finally, ϕ is a bijection because $|\{g^0, g^1, \dots, g^{N-1}\}| = |\{\bar{0}, \bar{1}, \dots, \overline{N-1}\}| = N$.

(\Leftarrow) Let G be a finite abelian group that is isomorphic to $\mathbb{Z}(N)$ for some N with $\phi : \mathbb{Z}(N) \rightarrow G$ as the isomorphism.

Observe that $|G| = |\mathbb{Z}(N)| = N$ since ϕ is a bijection. Since ϕ is a homomorphism, $\{\phi^0(1), \phi^1(1), \dots, \phi^{N-1}(1)\} = \{\phi(0), \phi(1), \dots, \phi(N-1)\}$. The right-hand side set has cardinality N since ϕ is a bijection. Thus, the left-hand side also has cardinality N and it is equal to G .

□