PSET3

Student: Ryan Baldwin, `rbaldwi2@swarthmore.edu`
Professor: Dr. Hsu
Collaborators: Ara
Peer Reviewers: Ara, Adil
Due Date: February 14, 2025

Artin Chapter 2: 6.2

♢ *Describe all homomorphisms $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective, and which are isomorphisms.*

Proof. Let $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ be a homomorphism. Since $\mathbb{Z}^+$ is generated by 1, the homomorphism φ is completely determined by $\varphi(1)$. Let $\varphi(1) = K$ for some $K \in \mathbb{Z}^+$. Then for any $n \in \mathbb{Z}^+$, we have

$$\varphi(n) = \varphi(1 + 1 + \cdots + 1) = \varphi(1) + \varphi(1) + \cdots + \varphi(1) = nK.$$

Similarly, if we were to take the negation of n, it is true then that

$$\varphi(-n) = \varphi(-1 - 1 - \cdots - 1) = -\varphi(1) - \varphi(1) - \cdots - \varphi(1) = -nK.$$

Thus, every homomorphism φ must be of the form $\varphi(n) = \pm nK$ for some $K \in \mathbb{Z}^+$.

Given that the general structure of the homomorphism φ is $\pm nK$, we can further characterize φ based on the value of K.

Case I: $K = 0$.

If $K = 0$, then $\varphi(n) = n \cdot 0 = 0$ for all $n \in \mathbb{Z}^+$. This is a trivial homomorphism.

Case II: $K > 0$.

If $K > 0$, then $\varphi(n) = nK$. Which leads us to investigate the value of $\varphi(a) = \varphi(b)$. Since $\varphi(a) = \varphi(b)$ is equivalent to $aK = bK$, for $K > 0$ we can divide by K to get $a = b$. This argument holds for $K < 0$ as the characterization of the homomorphism is not dependent on the sign. Thus, φ is indeed injective.

For φ to be surjective implies that for every $m \in \mathbb{Z}^+$, there must exist an $n \in \mathbb{Z}^+$ such that $\varphi(n) = \pm nK = m$. The only nonzero integer K that would satisfy $\pm nK = m$ is $K = 1$ which would further imply that $\pm n = m$, making φ surjective. However, for all $K > 1$ there is no nonzero n that would guarantee in $\pm nK = m$. Thus, φ is surjective if and only if $K = 1$.

Therefore, due to the restrictions of K, our homomorphism φ can only be isomorphic if and only if it is both injective and surjective. This means that φ is an isomorphism if and only if $K = 1$ (when φ is $\varphi(n) = \pm n$).

Therefore, the homomorphisms of $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ are of the form $\varphi(n) = \pm nK$ for some $K \in \mathbb{Z}^+$.φ is the *trivial homomorphism* when $K = 0$. φ is *injective* if $K > 0$. φ is *surjective* if and only if $K = 1$. And finally, φ is an *isomorphism* if and only if $K = 1$.

□

Artin Chapter 2: 6.9

$\Diamond$ *Prove that a group G and it's opposite group G° are isomorphic.*

Proof. Construct a bijective homomorphism $\varphi : (G, *) \to (G^\circ, \circ)$ such that $\varphi(z) = z^{-1}$ for all $z \in G$, and the operation of G° is defined as $x \circ y = y * x$ for all $x, y \in G^\circ$.

Consider the elements $a, b \in G$ which must also be in G°. We prove that the map between the two groups is indeed a homomorphism under φ.

$$\begin{aligned}\varphi(a * b) = (a * b)^{-1} = b^{-1} * a^{-1} = \\ &= a^{-1} \circ b^{-1} = \varphi(a) \circ \varphi(b) \\ \varphi(a * b) &= \varphi(a) \circ \varphi(b).\end{aligned}$$

With both sides being equal, φ is indeed a homomorphism.

Furthermore, the map $\varphi(a) = a^{-1}$ must be bijective as every element in G has a unique inverse, and the inverse function is itself its own inverse.

Therefore, φ is indeed homomorphic and bijective, proving that $G \cong G^\circ$.

$\square$

Artin Chapter 2: M.2(a)

$\Diamond$ *Prove that every group of even order contains an element of order 2.*

Proof. Assume we have a group G such that it has an even number of elements.

Consider the set $G - \{e\}$, which has an odd number of unique elements.

We partition this set as follows. Have each subset contain either an element that is its own inverse or a pair of two distinct elements with its corresponding inverse.

Since there are an odd number of elements in $G - \{e\}$, if we remove all pairs of elements with a corresponding inverse that is distinct we will have a remainder of one element. That is, removing an even number of elements from an odd number of elements leaves a leftover element we shall denote as a. Let a be the element that is its own inverse other than the identity such that

$$G = \{e\} \cup \{a\} \cup \{b, b^{-1}, c, c^{-1}, d, d^{-1}, \ldots\}.$$

Further considering the element a that is its own inverse, we see that

$$\begin{aligned} a &= a^{-1} \\ (a)a &= (a)a^{-1} \\ a^2 &= e. \end{aligned}$$

Thus, every group of even order contains an element of order 2. $\square$

Artin Chapter 2: Additional Problem 1

$\Diamond$ *Show that a group with no proper nontrivial subgroups is cyclic.*

Proof. To prove that the above statement holds, we shall divide this investigation into two cases where our group G is of different orders.

Case I: $|G| = 1$.

Consider the case where the order of G is 1. The only element of G must be the identity element. The identity element is indeed a generator that can generate the whole group comprised of the identity element.

Case II: $|G| \geq 2$.

Furthermore, consider the case where the order of G is greater than or equal to 1. There must then exists a nontrivial $a \in G$ that can serve as a generator for multiple elements including the identity element in G. This element $a \in G$ must generate the entire group G given that the group cannot have a nonproper nontrivial subgroup. Thus, $G = \langle a \rangle$ is indeed cyclic. $\square$