Elliott Daimler
MATH 4010
Dr. Chastkofsky
MWF 10:20am
February 4, 2022

Homework 3, Section 7.4 Solutions

1

Claim: The automorphism group of the additive group $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^*$.

Proof. We will show that an isomorphism exists from $\mathbb{Z}_n^*$ to $\mathrm{Aut}(\mathbb{Z}_n)$. Let $f : \mathbb{Z}_n^* \to \mathrm{Aut}(\mathbb{Z}_n)$ be the map $k \to \varphi_k$ for $k \in \mathbb{Z}_n^*$, defined such that for $[a] \in \mathbb{Z}_n$, $\varphi_k([a]) = [ka]$.

1) We must first show that φ_k is a well-defined bijective homomorphism from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. Let $[a] = [b]$ for $[a], [b] \in \mathbb{Z}_n$. We have $\varphi_k([a]) = [ka]$ and $\varphi_k([b]) = [kb]$. In the ring $\mathbb{Z}_n$, $[ka] = [k][a]$ and $[kb] = [k][b]$. Since $[a] = [b]$, it follows that $[k][a] = [k][b]$, so φ_k is well-defined.

Next, let $\varphi_k([a]) = \varphi_k([b])$. Then $\varphi_k([a]) = [ka] = [kb] = \varphi_k([b])$. By the cancellation property, $[ka] = [k][a] = [k][b] = [kb]$ implies $[a] = [b]$, so φ_k is injective.

To show that φ_k is surjective, let $[c] \in \mathbb{Z}_n$ and $[k] \in \mathbb{Z}_n^*$ be given. We must show that there is some $[a] \in \mathbb{Z}_n$ such that $\varphi_k([a]) = [c]$. Since k is relatively prime to n, there exist some $u, v \in \mathbb{Z}_n$ where $ku + vn = 1$. Multiplying both sides of this equation on the right by c yields $(ku + vn)c = kuc + vnc = c$. Now we can choose some $a \in \mathbb{Z}_n$ where $a = uc$. Since $vnc = 0$ in $\mathbb{Z}_n$, we have

$$\begin{aligned} kuc + vnc &= c \\ \to ka + 0 &= c \\ \to ka &= c, \end{aligned} \tag{1}$$

so the map φ_k is surjective.

Now let $a, b \in \mathbb{Z}_n$ be given. Then $\varphi_k([a+b]) = [k(a+b)] = [k][a+b]$. Similarly, $\varphi_k([a]) + \varphi_k([b]) = [ka] + [kb] = [k]([a] + [b]) = [k][a + b]$. Since the group operation of $\mathbb{Z}_n$ is addition, and $\varphi_k([a + b]) = \varphi_k([a]) + \varphi_k([b])$, the map φ_k is a homomorphism to $\mathbb{Z}_n$.

2) Next, we must show that the map f defined as $k \to \varphi_k$ is a well-defined bijective homomorphism from $\mathbb{Z}_n^*$ to $\mathrm{Aut}(\mathbb{Z}_n)$. To show that f is well-defined, let $k = j \in \mathbb{Z}_n^*$ be given. We have $\varphi([a]) = [ka] = [k][a]$ and $\varphi([a]) = [ja] = [j][a]$. Since $[k] = [j]$, it follows that $[k][a] = [ka] = [ja] = [j][a]$, so the map f is well-defined.

To show that f is injective, let $\varphi_j = \varphi_k \in \mathrm{Aut}(\mathbb{Z}_n)$ be given. Then for some $a \in \mathbb{Z}_n$, we have $\varphi_j([a]) = \varphi_k([a])$ and so $[ja] = [j][a] = [k][a] = [ka]$. By the cancellation property, $[j][a] = [k][a]$ implies $[j] = [k]$, so the map f is injective.

We will now show that f is surjective. Let $\varphi_c \in \mathrm{Aut}(\mathbb{Z}_n)$ be given. Then for some $b \in \mathbb{Z}_n$, $\varphi_c([b]) = [cb]$. There is some $[a] \in \mathbb{Z}_n$ where $[a] = [cb]$. Using a similar argument used for equation (1), we can be given some $k \in \mathbb{Z}_n^*$ and choose some $[d] \in \mathbb{Z}_n$ where $[kd] = [a] = [cb]$. So for any $\varphi_c \in \mathrm{Aut}(\mathbb{Z}_n)$, there is some $k \in \mathbb{Z}_n^*$ such that $\varphi_k = \varphi_c$, so f is surjective.

Finally, let $k, j \in \mathbb{Z}_n^*$ be given. Then for some $a \in \mathbb{Z}_n$, $\varphi_{kj}([a]) = [kja]$. Similarly, the composition $\varphi_k \circ \varphi_j([a])$ yields $\varphi_k([ja]) = [kja]$. The group operation of $\mathrm{Aut}(\mathbb{Z}_n)$ is composition, so the map f is a homomorphism to $\mathrm{Aut}(\mathbb{Z}_n)$.

we have shown that for each $k \in \mathbb{Z}_n^*$, φ_k is isomorphic from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, and we have shown that the f, the map $k \to \varphi_k$ is isomorphic from $\mathbb{Z}_n^*$ to $\mathrm{Aut}(\mathbb{Z}_n)$, so we have constructed an isomorphism from $\mathbb{Z}_n$ to $\mathrm{Aut}(\mathbb{Z}_n)$ and we are done. $\square$