Elliott Daimler
MATH 4010
Dr. Chastkofsky
MWF 10:20am
January 27, 2022

Homework 2, Section 7.3 Solutions

1

Claim: If a is the only element of a group G whose order is 2, then a is in the center G.

Proof. Let $b \in G$ be given. By the closure property, there is some $c \in G$ such that $c = b^{-1}ab$. Then for c^2 we have

$$\begin{aligned} c^2 &= (b^{-1}ab)^2 \\ &= b^{-1}abb^{-1}ab \\ &= b^{-1}aeab \\ &= b^{-1}aab \\ &= b^{-1}eb \\ &= b^{-1}b \\ &= e. \end{aligned}$$

The order of c is 2, and only $a \in G$ has order 2, so $c = a$ and $a = b^{-1}ab$. Applying the group operation with b on the left of both terms of this equation gives

$$\begin{aligned} ba &= bb^{-1}ab \\ &= eab \\ &= ab, \end{aligned}$$

so the equation $c = b^{-1}ab$ implies $ba = ab$, and a is in the center of G. □

2

Claim: Let p be a prime integer. Then for any integer a, $a^p \equiv a \mod p$.

Proof. First we will show that for any b in $\mathbb{Z}_p^*$, $b^{p-1} = 1$. Since $\mathbb{Z}_p^*$ is a finite multiplicative group, by Theorem 7.16 $\mathbb{Z}_p^*$ is cyclic. So there is some $c \in \mathbb{Z}_p^*$ that generates $\mathbb{Z}_p^*$, or $< c >= \mathbb{Z}_p^*$. Since p is prime, every nonzero element of $\mathbb{Z}_p$ is relatively prime to p, so $\mathbb{Z}_p^*$ has $p-1$ elements and $|c| = p-1$ is the highest order of an element in $\mathbb{Z}_p^*$.

Being a cyclic group, $\mathbb{Z}_p^*$ is abelian, so by Corollary 7.10, $|b|$ divides $p-1$. If follows that $b^{p-1} = 1$.

Now let b be the congruence class of a in $\mathbb{Z}_p^*$. Then $a^{p-1} \equiv 1 \mod p$ and $aa^{p-1} = a^p \equiv a \mod p$. □