MTH 316 Homework 6

Evan Fox (efox20@uri.edu)

April 6, 2022

Question 1.

Let G be a group and define $H = \{(g, g)|g \in G\}$

(a) Show $H \leq G \oplus G$

Proof. Note the the idenitity in $G \oplus G$ is (e, e) and since $e \in G$ we have $(e, e) \in H$. Then let $(a, a), (b, b) \in H$. Again since $b \in G$ we must have $b^{-1} \in G$ which implys $(b^{-1}, b^{-1}) \in H$ and this is clearly the inverse of $(b, b) \in H$. We note $(a, a)(b, b) = (ab, ab)$ Then similarly since $a, b \in G$ we have $ab \in G$ so $(ab, ab) \in H$. Hence by the two step subgroup test we have that H is a subgroup of $G \oplus G$. □

(b) Prove $H \cong G$.

Proof. Define $\phi : H \to G$ such that $(g, g) \mapsto g$. Injectivity is clear. For $h \in G$ we can see h is mapped to by $(h, h) \in H$. Hence ϕ is a bijection. Then

$$\phi((a, a)(b, b)) = \phi(ab, ab) = ab = \phi(a, a)\phi(b, b)$$

and this completes the proof. □

Question 2.

For prime p show that $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has $p + 1$ subgroups of order p

Proof. We start by counting the number of elements of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Each non-idenity element in $\mathbb{Z}_p$ has order p. Then an element of $\mathbb{Z}_p \oplus \mathbb{Z}_p$, say (a, b) has order p only if $\text{lcm}(|a|, |b|) = p$, but since the only possible orders for a and b are 1 and p, every case must give us an lcm of p unles both a, b have order 1 which can only occure when they are both the idenitity. That is, every element of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has order p except for the idenitity. Then since

$|\mathbb{Z}_p \oplus \mathbb{Z}_p| = p^2$, there must exist $p^2 - 1$ elements of order p. Every subgroup of order p is cyclic with $p - 1$ generators so we have counted each subgroup $p - 1$ times. Then the number of subgroups of order p is given by

$$\frac{p^2 - 1}{p - 1} = \frac{(p-1)(p+1)}{p-1} = p + 1$$

Hence there must be $p + 1$ distinct subgroups of order p. $\square$