Nathan Madsen
PERM: 5679642
madsen@ucsb.edu

HW Set 4
MATH 111A

2024-10-31

Problem 1

We want to show that

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \iff (m, n) = 1$$

We start by defining a homomorphism $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by saying that $f(x) = (x \mod m, x \mod n)$. We can verify this is a homomorphism.

$$\begin{aligned} f(xy) &= (xy \mod m, xy \mod n) \\ &= (x \mod m, x \mod n)(y \mod m, y \mod n) \\ &= f(x)f(y) \end{aligned}$$

We also know that if and only if $(m, n) = 1$ we have Bezout's Lemma that

$$am + bn = 1$$

Then we know we can define an inverse g for any $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$ where $g(x, y) = yma + xbn$. Testing we see $f(g(x, y)) \equiv (x, y)$ since $am \equiv 1 \mod n, bn \equiv 1 \mod m$.

Problem 2

We want to show that given some prime p for every integer $1 \leq n \leq m$, $\mathbb{Z}_{p^n}$ is isomorphic to some subgroup of $\mathbb{Z}_{p^m}$

We know that $\mathbb{Z}_{p^m}$ is the group of integers mod p^m. We also know that it suffices to show that there is some subgroup of $\mathbb{Z}_{p^m}$ of order p^n. We know that $\mathbb{Z}_{p^m}$ looks like

$$a, a^2, a^3, \ldots, a^{2p}, \ldots, a^{p^2}, \ldots, a^{p^3}, \ldots, a^{p^m}$$

So we are just looking for an element of order p^n since its cyclic subgroup is what we want. I claim that this element is $a^{p^m/p^n} = a^{p^{(m-n)}}$. We can easily verify this since $(a^{p^{(m-n)}})^{p^n} = a^{p^m} = e$.

Problem 3

We want to show that there are at least two automorphisms on $\mathbb{Z}_{20}$ such that $\phi(5) = 5$

Looking at an automorphism of $\mathbb{Z}_{20}$, say that $\phi(1) = x$ we then know that $\phi(5) = 5x$ by homomorphism rules. So it must be the case that $5x \equiv 5 \mod 20$, or equivalently that $x \equiv 1 \mod 4$. These means that $x \in \{1, 5, 9, 13, 17\}$, but 5 is not coprime to 20 so we get that $x \in \{1, 9, 13, 17\}$. And since homomorphisms on cyclic groups are determined by where they send the generator, the choice of x defined a unique automorphisms.

Problem 4

Let H and K be two subgroups of a group G. and let $a, b \in G$. We want to show that

$$aH = bK \implies H = K$$

Since H is a subgroup we know that $e \in H$.

$$\begin{aligned} aH &= bK \\ a &\in bK \\ b^{-1}a &\in K \end{aligned}$$

Since this is an element of K its inverse $a^{-1}b$ must also be in K. Now let $c_1 \in H$, we know we can find an element c_2 such that

$$\begin{aligned} aH &= bK \\ ac_1 &= bc_2 \\ c_1 &= a^{-1}bc_2 \end{aligned}$$

Here you can see that we have written c_1 as the product of elements in K so c_1 must be in K by closure, and thus every element in H is in K and every element in K is in H since $b^{-1}a$ must be in H.

Problem 5

We want to show that

$$H, G \text{ isomorphic} \implies \mathrm{Aut}(H), \mathrm{Aut}(G) \text{ isomorphic}$$

Let $\phi : G \to H$ be the isomorphism. We know want to define an isomorphism $\Phi : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$. Say $\alpha \in \mathrm{Aut}(G)$, lets define $\Phi(\alpha) = \phi \circ \alpha \circ \phi^{-1}$. We must now verify $\Phi(\alpha)$ is an automorphism in H. Let $h_1, h_2 \in H$

$$\begin{aligned} \Phi(\alpha)(h_1h_2) &= \phi \circ \alpha \circ \phi^{-1}(h_1h_2) \\ &= \phi \circ \alpha(\phi^{-1}(h_1)\phi^{-1}(h_2)) \\ &= \phi((\alpha \circ \phi^{-1}(h_1))(\alpha \circ \phi^{-1}(h_2))) \\ &= (\phi \circ \alpha \circ \phi^{-1}(h_1))(\phi \circ \alpha \circ \phi^{-1}(h_2)) \end{aligned}$$

And we must show its bijective, but this is trivial since ϕ, α are bijective so $\Phi^{-1} = \phi^{-1} \circ \alpha^{-1} \circ \phi$. Thus we have created an isomorphism between $\mathrm{Aut}(G)$ and $\mathrm{Aut}(H)$.

Problem 6

Let us think about some isomorphism $\phi : \mathbb{Q} \to H$

$$\phi\left(\frac{a}{b}\right) = \phi\left(\frac{1}{b} + \frac{1}{b} + \cdots + \frac{1}{b}\right) = a\phi\left(\frac{1}{b}\right)$$

By this we can write $\phi(1) = \phi\left(\frac{b}{b}\right) = b\phi\left(\frac{1}{b}\right)$ or that $\frac{1}{b}\phi(1) = \phi\left(\frac{1}{b}\right)$. And so

$$\phi\left(\frac{a}{b}\right) = \frac{a}{b}\phi(1)$$

If we say that $\phi(1) \neq 0 = c/d$. Then for any arbitrary $a/b \in \mathbb{Q}$ we have

$$\phi\left(\frac{ad}{bc}\right) = \frac{ad}{bc}\phi(1) = \frac{a}{b}$$

And so ϕ is surjective and cannot map onto a proper subgroup