Homework Eight

1. Orders and homomorphisms

(a) Let $g \in G$ be an element of order n. Let $\phi : G \to H$ be a homomorphism. Show that $\phi(g)$ must be an element whose order divides n.
(b) Let G and H be finite groups. If $gcd(|G|, |H|) = 1$, show that the only homomorphisms from G to H are trivial.
(c) Show that if $gcd(n, m) = 1$, then $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z}$. (Hint: what is the order of $([1], [1]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$?)

2. Build-up to the third isomorphism theorem

The third isomorphism theorem answers the following question: Let's say I have a nested sequence of subgroups, $A \subset B \subset G$. Well, I could quotient out all of B to get the orbit set G/B. (In the process, all of A is divided out, too, since A is contained in B.) Or I could try to quotient out step by step: First take G/A, and then divide out by what remains of B. Is the end result the same thing? The answer is yes, and if both A and B are normal in G (so that it makes to talk about quotient groups), the end result is the same thing *as groups*. We'll prove this eventually. Here, you'll establish the essential pieces for proving the Third Isomorphism Theorem.

(a) Suppose we have subgroups $A \subset B \subset G$. Exhibit an injection

$$f : B/A \to G/A.$$

(Neither of these are *groups*, these are just sets. After all, we haven't assumed that A is normal in G.)
(b) Let $A \subset B \subset G$ be subgroups. Suppose that A is normal in G. Prove that $A \triangleleft B$ as well. (Now it makes sense to talk about the *groups* G/A and B/A.)
(c) Prove that your injection f from above is a group homomorphism. This exhibits B/A as a subgroup of G/A.
(d) Exhibit a bijection

$$\psi : G/B \to (G/A)/(B/A).$$

(This just a function between two *sets*. To be clear, on the righthand side, we have made use of the action of B/A on G/A, since B/A is a subgroup. The quotient set $(G/A)/(B/A)$ is the usual orbit space of this action.)

(e) If G is finite, prove that

$$|G/B| = |G/A|/|G/B|.$$

3. Some Sylow-style fun

(a) Let $G = S_3$. List all the elements of $\mathrm{Syl}_3(G)$ and $\mathrm{Syl}_2(G)$. There should be one element in the former, and three elements in the latter.

(b) In class, we showed that if $|G| = pq$ with $q > p$ primes, then G must be a semidirect product

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

Assume that p does not divide $q - 1$. By considering the size of $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, and by considering Problem 1(b), show that G must be isomorphic to a *direct* product. Conclude using 1(c) that G must be a cyclic group.

(c) We prove the same result a different way. Assume you don't know (and could never know) the size of $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Using the Third Sylow Theorem, and assuming that p does not divide $q-1$, prove that G must be a direct product $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. (Hint: How did we do this in class for $pq = 15$?)

(d) Show that any group of the following orders are cyclic:

$$65, \qquad 221, \qquad 9797.$$

4. *Some fun with semidirect products

(The asterisk means you don't need to turn in this problem, but the problem may be turned in for extra credit.)

(a) Show that there are exactly two homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to itself.

(b) Show that there are exactly two homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$. (Hint: You know how big $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ is, based on the last homework. So what group must it be?)

(c) Recall that a semidirect product $L \rtimes_\phi R$ is determined by a homomorphism $R \to \mathrm{Aut}(L)$. Show that if ϕ is the dumb homomorphism (sending everything to the identity), $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

(d) If ϕ is the other homomorphism from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/3\mathbb{Z}$, show that $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong S_3$.

(e) In contrast, show that $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ must always equal $\mathbb{Z}/6\mathbb{Z}$. (The order of the semidirect product is reversed!) As a hint, you might again try to count how many elements are in $\mathrm{Aut}(L)$ for $L = \mathbb{Z}/2\mathbb{Z}$.