THIS WORKSHEET COVERS MATERIAL SIMILAR TO SOME HOMEWORK 2 (and HW 3) PROBLEMS. I RECOMMEND WORKING THROUGH THIS WORKSHEET BEFORE ATTEMPTING THE HW PROBLEMS ON NORMAL SUBGROUPS AND HOMOMORPHISMS.

Goals

- Know the definition of a Group Homomorphism and its kernal and image
- Understand the definition of a normal subgroup, and investigate their significance
- Investigate the connections between kernal of a group homorphism, normal subgroups, and the so called Quotient Groups

Introduction

We ended our discussion last week by providing some detailed computations involving Cosets for the integers. We described the collection of all cosets, $\mathbb{Z}/n\mathbb{Z}$ and hinted that it looked familiar to another group. Once and for all, we answer what group it looked similar to, and we make the similarity precise. Doing so involves first the definition of a Group Homomorphism- an idea of fundamental importance to Group Theory. Any time we have a definition of functions, whenever possible, we discuss the subset of objects that get "killed" (ie mapped to 0) by the function. This leads us to our definition of a kernal of a group homomorphism- and we will investigate some basic properties of kernals. In particular, we will show that they are the prototypical example of so called normal subgroups (and in fact are the only example of normal subgroups). Normal subgroups arise as the answer to the following two questions:

1. Suppose $(G, *)$ is a group. Then we will denote the set of LEFT cosets for H in G as $H\backslash G$. Note this looks different than the set of RIGHT cosets G/H. (We will see that in the case we are most interested in, the collection of left and right cosets coincide, so the most common notation will be G/H going forward). A typical coset looks like aH for some a in G. Then a question one could ask is, can we put a group structure on $H\backslash G$ by defining a product $\otimes$ on the set of Left Cosets as $aH \otimes bH := (a * b)H$?
2. Suppose $\phi : G \to H$ is a group homomorphism (to be defined below) between groups G and H. What can we say about the elements $g \in G$ such that $\phi(g) = e_H$? Does that

form a subgroup, and if so does it have any further "structure?"

1 Products of Cosets and Normal Subgroups

Last week we I briefly went over the definition of the integers modular n, which I denoted $\mathbb{Z}_n$ and described it as the set $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$ where $\overline{i}$ is the equivalence class of the number i subject to the equivalence relation $i \equiv x$ mod n. This set can be rather simply turned into an additive group by defining $\overline{a} + \overline{b} = \overline{a+b}$, after one checked that this addition rule is well defined. After that section, we took an interlude into cosets in general, and then did some concrete computations for left cosets for the integers $\mathbb{Z}$. In particular, we considered the subgroup $n\mathbb{Z}$ for an arbitrary n, and found that the collection of all left cosets for this subgroup, which we denoted $\mathbb{Z}/n\mathbb{Z}$ was a very simple set, $\mathbb{Z}/n\mathbb{Z} = \{0+\mathbb{Z}, 1+\mathbb{Z}, \ldots (n-1)+\mathbb{Z}\}$ This set looks almost identical to the set $\mathbb{Z}_n$- and since we just went through the process of showing that $\mathbb{Z}_n$ is actually a group, a natural question one might ask is:

1. Is $\mathbb{Z}/n\mathbb{Z}$ also a group?
   Solution: Yes, $\mathbb{Z}/n\mathbb{Z}$ is a group under the following addition rule: $(a + \mathbb{Z}) + (b + \mathbb{Z}) = (a + b) + \mathbb{Z}$. In making this definition, one must check however the following things:

   (a) If $a + \mathbb{Z}$, and $b + \mathbb{Z}$ are two left cosets, is $(a + b) + \mathbb{Z}$ again a left coset? (closure axiom)
   Solution: We shall come back to a full proof of this later, but first- **explain why the following "counter-example" is actually wrong.**

   Counter-Proof:
   Consider $\mathbb{Z}/4\mathbb{Z} = \{0 + \mathbb{Z}, 1 + \mathbb{Z}, 2 + \mathbb{Z}, 3 + \mathbb{Z}\}$. Then if we take the coset $2 + \mathbb{Z}$ and the coset $3 + \mathbb{Z}$ and try to add them together in the rule defined above, we would get $(2 + \mathbb{Z}) + (3 + \mathbb{Z}) = (2 + 3) + \mathbb{Z} = 5 + \mathbb{Z}$ which is not a left coset of $\mathbb{Z}/4\mathbb{Z}$. Hence this operation is not closed, and does not turn $\mathbb{Z}/4\mathbb{Z}$ into a group.

   Solution: This is an incorrect proof since the coset $5 + \mathbb{Z} = 1 + \mathbb{Z}$ so it remains in the set.

   (b) Think back to last week's example where you showed that the cosets $3 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$ for the group $\mathbb{Z}$ where the same. Indeed we used the fact that cosets are actually equivalence classes. So in defining addition this way, we again need to check that our choice of coset representative is well defined (just like in the case $\mathbb{Z}_n$): Show this-
   Solution: Again assume $a_1 + n\mathbb{Z} = a_2 + n\mathbb{Z}$ and $b_1 + n\mathbb{Z} = b_2 + n\mathbb{Z}$. Then you must show that $(a_1 + b_1) + n\mathbb{Z} = (a_2 + b_2) + n\mathbb{Z}$. Finish the proof:

Indeed we have that $(a_1 - a_2) \in n\mathbb{Z}$ and $(b_1 - b_2) \in n\mathbb{Z}$ so $(a_1 - a_2) + (b_1 - b_2) \in n\mathbb{Z}$ which is exactly what we needed to show.

(c) Now that we have shown addition is well defined and closed, finish the proof that $\mathbb{Z}/n\mathbb{Z}$ is a group. (You may have done this in class, if so try and re-do it for practice without looking at your notes)
Solution:

i. The Identity for the group is $n\mathbb{Z}$

ii. Let $a + n\mathbb{Z}$ be in $\mathbb{Z}/n\mathbb{Z}$. Then $(a + n\mathbb{Z})^{-1} = b + n\mathbb{Z}$ where b is the unique integer such that $a + b = n$

iii. Show that addition is associative. This follows since addition is associative in $\mathbb{Z}$

2. In showing above that $\mathbb{Z}/n\mathbb{Z}$ can be turned into a group, the real bulk of the work is in showing that the product of 2 cosets is again a coset, and that the choice of representative for the coset doesn't matter. Do you think that it is always the case that $H\backslash G$ can be turned into a group in this way? In other words, does the product $g_1H \otimes g_2H := (g_1 * g_2)H$ always turn $H\backslash G$ into a group? Jot down some thoughts about why you think it is true, or try coming up with a counter example, or reason why it would be false if you think it's false

(a) Solution: Let $G = S_3$ and let $H = \{e, (12)\}$ written in cycle notation. Then one can check that H is a subgroup of G. Now by Lagrange's theorem, H is of index 3 (since G is of order 6, and H is of order 2) so there are 3 left cosets of H in G. We always have the trivial coset eH- so, letting $\psi = (123)$, the three cosets are:

i. $\psi H = \{(123)e, (123)(12)\} = \{\psi, \psi(12)\}$

ii. $\psi^2 H = \{\psi^2 e, \psi^2(12)\} = \{\psi^2, \psi^2(12)\}$

iii. $eH = \{e, (12)\}$

Note $(12)H = \{(12), (12)^2\} = \{(12), e\} = eH$. However, consider the following two products

i. $(12)\psi H = \{(12)\psi e, (12)\psi(12)\} = \{(13), (132)\} = \psi^2 H$

ii. $e\psi H = \{e\psi e, e\psi(12)\} = \{(123), (23)\} = \psi H$

Therefore, even though (12)H=eH, we got different results doing the multiplication $eH\psi H$ and the multiplication $(12)H\psi H$ so it is not a well defined product.

3. If you think the answer above is no, what distinguishes between the cases $\mathbb{Z}/n\mathbb{Z}$ your counterexample? The former could be turned into a group (Good!) while the later could NOT be turned into a group (Bad!!)- what is the difference between these two situations? Well, consider the following **SUPER IMPORTANT THEOREM**

Thrm: Let N be a subgroup of G. Then G/N can be turned into a group (called the **Quotient Group**) under the rule $aN \circ bN = (ab)N$ if and only if $gNg^{-1} \subset N$ for all g in G (ie, for each $n \in N, g \in G,$ we have $gng^{-1} \in N$). Furthermore in this case $G/H = H\backslash G$ (that is the set of left cosets equals the set of right cosets)

4. We call such subgroups **Normal Subgroups** and we denote them as $N \trianglelefteq G$. Ok cool- so we have a new class of subgroups which would give us a new group, G/N to study- that's nice, we like groups here! A natural question to ask though is, when and how do these groups appear? How would I check that such a subgroup is Normal? We will say more about this next section, however, with this theorem above in mind let us prove:

   (a) Let $(G, *)$ be an abelian group. Then for any subgroup H of G, the set of cosets G/H is also an abelian group.
   Solution: (Hint- The above theorem tells us when G/H can be made into a group- why is it guaranteed in this case? Then recall how we defined the group product in G/H to conclude its abelian.)
   Solution: Since G is abelian, every subgroup H is normal in G (since $\forall g \in G, ghg^{-1} = h$ for any h in H). Thus we can form the group G/H with multiplication $aH \times bH = (ab)H = (ba)H = bH \times aH$ so it is abelian.

   (b) Corollary to the above: $\mathbb{Z}/n\mathbb{Z}$ is an abelian group (This is certainly the much quicker way of proving $\mathbb{Z}/n\mathbb{Z}$ is a group- but I believe the long way above is useful because you get some working familiarity with how cosets "work")
   Solution: Explain why the above result gives us this: Indeed $\mathbb{Z}$ is an abelian group, so $H = n\mathbb{Z}$ is abelian. Then by part a above the coset group $\mathbb{Z}/n\mathbb{Z}$ is also an abelian group.

2 Group Homomorphisms and Normal Subgroups

There's a general "schema" in Mathematics that says the following: we are in the business of constructing objects with certain properties (sets, groups, vector spaces, ect)- Once we have constructed these objects, we then ask how they interact, ie, what sort of functions are there between the objects. The functions we study between the objects should take into consideration the structure that exists on our objects. Consider for example:

1. In Math 21 (or intro Linear Algebra class) and Math 117 (or Upper Div Linear Alg course) we studied vector spaces. These were sets with an addition structure and a "scalar multiplication" structure- These structures were reflected in our definition of "linear transformations", Recall- A linear transformation $T : V \to W$ between vector spaces V,W is a function such that

   (a) $T(v_1 + v_2) = T(v_1) + T(v_2)$ for all $v_1, v_2 \in V$.

   (b) $T(rv) = rT(v)$ for all $r \in \mathbb{R}, v \in V$

We mentioned that the axioms for vector spaces actually made the set into an Abelian group under addition- Condition (a) of linear transformation guarantees the function "plays nice with" the addition in both V, and W. With this in mind, consider the definition below:

Def: Let $(G, *)$ and $(H, \circ)$ be two groups. Then a **Group Homomorphism** between G and H is a function $\psi : G \to H$ such that $\psi(g_1 * g_2) = \psi(g_1) \circ \psi(g_2)$.

1. Rephrase the definition of a linear transformation between two vector spaces in terms of group homomorphisms
   Solution: Let V, W be vector spaces. Then they are both abelian groups under addition. Therefore a Linear Transformation $T : V \to W$ is a group homomorphism such that T(rv)=rT(v) for all v.

2. Consider the map $\psi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\psi(x) = \overline{x}$. Is this a group homomorphism?
   Solution: Yes this is a group homomorphism since $\overline{a+b} = \overline{a} + \overline{b}$

3. Prove or disprove the following: "All group homomorphisms between two finite groups of the same cardinality are group isomorphisms"
   Solution: This is very false. For example, the so called 0 map (the map that sends every element to the identity element) is a group homomorphism.

4. Suppose you want to construct a group homomorphism $\psi : \mathbb{Z}_n \to G$ from $\mathbb{Z}_n$ to some other group G. Then there is actually one more step you need to do than just showing it splits up under the group operations. Keep in mind the steps needed in showing that addition was well defined in $\mathbb{Z}_n$, and jot down your idea for what other step we need to show
   Solution: You need to show the function is well defined- meaning it does not depend on choice of equivalence class representative. That is, if $a \equiv b$ mod n you must show that $\psi(\overline{a}) = \psi(\overline{b})$

5. **Explain why the following proof is Wrong**: We show the function $\psi : \mathbb{Z} \to \mathbb{R}^2$ defined by $\psi(z) = (z, z)$ is a group homomorphism.
   Solution: Indeed, we have that $\psi(1+1) = (1+1, 1+1) = (2, 2)$ and $\psi(1) + \psi(1) = (1, 1) + (1, 1) = (2, 2)$. Since $\psi(1 + 1) = \psi(1) + \psi(1)$ we have shown it is a group homomorphism.
   We only showed that ψ splits up under a specific element! To show it is a group homomorphism, we need to show it splits up under EVERY element, not just 1.

6. Come up with a function between two groups G,H that is NOT a group homomorphism.
   Solution: There are very many. Here is a simple one. Take $G = H = \mathbb{R}$ as a group under addition. Then $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not a group homomorphism since $f(1 + 1) = 4$ while $f(1) + f(1) = 2$

7. Challenge Problem: Let $m, n \in \mathbb{N}$. Take a guess about a sufficient condition for m and n for there to exist a group homomorphism $\psi : \mathbb{Z}_m \to \mathbb{Z}_n$

Solution: We need n to divide m. We will maybe prove this later in the course- it is a fun problem to think about- think about why this might be true!

Again, this is all well and good, yet it seems maybe a bit disconnected from the first half of this worksheet. The following definition is the bridge:
Def: Let $\psi : G \to H$ be a group homomorphism. Then

1. The **kernal of** ψ is the subset of G $ker(\psi) = \{g \in G : \psi(g) = e_H\} \subset G$
2. The **image of** ψ is the subset of H $im(\psi) = \{h \in H : \exists g \in G \text{ with } \psi(g) = h\} \subset H$, ie the set of all objects in H hit by some object in G under ψ

Let us explain why this provides a bridge:

1. Elementary lemma: Prove that $ker(\psi)$ is always non-empty. More specifically, prove that $e_G \in ker(\psi)$
   Solution: We have that $\psi(e_G) = \psi(e_G * e_G) = \psi(e_G) \times \psi(e_G)$ so multiplying on the right by $\psi(e_G)^{-1}$ gives $e_H = \psi(e_G)$
2. Prove that ker(ψ) and im(ψ) are subgroups of G and H respectively.
   Solution: We just showed $ker(\psi)$ is nonempty. Now let $g_1, g_2 \in ker(\psi)$. Then $\psi(g_1 * g_2) = \psi(g_1) \times \psi(g_2) = e_H \times e_H = e_H$ as desired. Now we show kernal is closed under inverses. Let $g \in ker(\psi)$. Then recall that for any g in G $\psi(g^{-1}) = \psi(g)^{-1}$, so in our case, we get $\psi(g^{-1}) = \psi(g)^{-1} = (e_H)^{-1} = e_H$ as desired.
   Now we show $im(\psi)$ is a subgroup. It is clearly nonempty, so we show closed under product and inverse. Let $h_1, h_2 \in im(\psi)$. That is, there exist some $g_1, g_2 \in G$ such that $\psi(g_1) = h_1, \psi(g_2) = h_2$. Then $h_1 \times h_2 = \psi(g_1) \times \psi(g_2) = \psi(g_1 * g_2)$ which says that $h_1 \times h_2$ is in the image. The fact that the image is closed under inverses is exactly the remark that $\psi(g^{-1}) = \psi(g)^{-1}$ again. So we are done.
3. Explain how the above definitions and results provide a connection between normal subgroups and group homomorphisms.
   Solution: This was purposely vague to get you all to think about it a bit. The connection will be that kernals are normal subgroups! In fact, keep reading and we will show that kernals are actually THE ONLY normal subgroups!
4. Consider the homomorphism $\psi : \mathbb{Z} \to \mathbb{Z}_n$ defined above as example 2. Find $ker(\psi)$ and $im(\psi)$
   Solution: The kernal of this map are all integers a such that $\overline{a} = \overline{0}$ which means that n divides a. Hence the kernal is $n\mathbb{Z}$.
   This map is surjective by construction, so the image is $\mathbb{Z}_n$.

5. Explain how $\mathbb{Z}/n\mathbb{Z}$ is related to the the example above
Solution: We have that $n\mathbb{Z} = ker(\psi)$ so the group $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/ker(\psi)$- in fact we will see next week that this identification actually shows that the two groups $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$ are "the same"

This above example actually provides an explicit characterization of how the groups $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ are related- Once we learn the "First Isomorphism" theorem next week, we can make this relation explicit and clear. For now, let us show one final example, which shows that every normal subgroup actually arises as the kernal of a group homomorphism. Remember that we have already shown that kernals are normal subgroups- this gives the converse.

1. Let $N \trianglelefteq G$ be a normal subgroup of G. Then recall that G/N can be made into a group. Consider the function $\pi : G \to G/N$ defined as $\pi(g) = gN$.
   (a) Show this is a group homomorphism.
   Solution: This is just another way of expressing that the product we defined in G/N is actually well defined. Indeed $\pi(g_1 * g_2) = (g_1 * g_2)N = g_1N \times g_2N = \pi(g_1) \times \pi(g_2)$
   (b) Find the kernal and image of this homomorphism.
   Solution: The image is all of G/N by construction. The kernal is the collection of all g such that gN=N. Remember that cosets are equivalence classes, so saying that gN=N forces g to be in N. Hence $ker(\pi) = N$.
   (c) Explain how this example justifies the claim "Normal subgroups and kernals to group homomorphisms are really the same thing"
   Solution: In the previous section, we showed that kernals of group homomorphisms are normal subgroups. The reverse question would be: Given a normal subgroup $N \trianglelefteq G$ does there exist some other group H, and a group homomorphism $\psi : G \to H$ that "realizes" N as the kernal (ie $ker(\psi) = N$). We have just shown that to be the case!! Given a normal subgroup $N \trianglelefteq G$ we saw that N is the kernal of the group homomorphism $\pi : G \to G/N$!

   This map $\pi : G \to G/N$ is called the "natural projection map" for G onto G/N. Fuzzily speaking what is happening in the group G/N is that we squish all of N to a single point and look what is happening outside of N. The following example shows some of the above vaguery in action.

2. Consider the additive abelian group $\mathbb{R}^2$, and let $N = \{(x, 0) : x \in \mathbb{R}\}$ (ie the x-axis). Then since $\mathbb{R}^2$ is abelian we get that N is normal.
   (a) Consider the projection map $\pi_y : \mathbb{R}^2 \to \mathbb{R}$ defined by $\pi_y(a, b) = b$. That is you project the element in $\mathbb{R}^2$ onto its y-component. Show that this a group homomorphism.
   Solution: $\pi_y(a_1 + a_2, b_1 + b_2) = b_1 + b_2 = \pi_y(a_1, b_1) + \pi_y(a_2, b_2)$ as desired.

(b) Find $ker(\pi_y)$ and $im(\pi_y)$
Solution: By definition, the kernal of π_y consists of all elements in $\mathbb{R}^2$ whose y-component is 0. In other words $ker(\pi_y) = \{(x, 0) : x \in \mathbb{R}\} = N$.
One can easily verify that $im(\pi_y) = \mathbb{R}$.

(c) How do you think the two projection $\pi_y : \mathbb{R}^2 \to \mathbb{R}$ and $\pi_N : \mathbb{R}^2 \to \mathbb{R}^2/N$ are connected? Under this connection, try and think of what the group $\mathbb{R}^2/N$ "is". That is, without proving anything, what group do you think $\mathbb{R}^2/N$ should look like.
Solution: Instead of viewing the projection $\pi_y : \mathbb{R}^2 \to \mathbb{R}$ one could instead consider the "natural projection" $\pi_N : \mathbb{R}^2 \to \mathbb{R}^2/N$ whose kernal is also N. One might suspect these group homomorphisms and in fact the groups themselves might be very similar. One would indeed be correct: When we learn about the first isomorphism theorem, and even the definition of "isomorphism" we will show that these two groups, $\mathbb{R}$ and $\mathbb{R}^2/N$ are "isomorphic", and we will identify the group $\mathbb{R}^2/N$ as really being the full image under π_y (that is, the group $\mathbb{R}^2/N$ is basically $\mathbb{R}^2$ where you squish all the x-axis to a single point)

3. **Challenge problem.** You can get some interesting geometrical shapes in this fashion. Again consider the additive Abelian group G=$\mathbb{R}$, but now let $N = \mathbb{Z}$. One can show this is a subgroup, so is again normal.

(a) Figure out what geometric object G/N is. (Hint, it is a very familiar geometric figure- This shows a rather neat fact that this familiar shape is actually a group in its own right!)
Solution: This group is actually the circle! See worksheet 4 for a more detailed explination!

(b) Instead let $G = \mathbb{R}^2$ and let $N = \mathbb{Z}^2 \trianglelefteq \mathbb{R}^2$. What is the geometric object G/N? (this one is much trickier- but it's still a very, very familiar shape)
Solution: This gives us the "torus" (that is, a donut!!) Again, see worksheet 4- to prove these claims one needs to use the "first isomorphism theorem."