"

THIS WORKSHEET COVERS MATERIAL SIMILAR TO SOME HOMEWORK 3 PROBLEMS. I RECOMMEND WORKING THROUGH THIS WORKSHEET BEFORE ATTEMPTING THE HW PROBLEMS ON QUOTIENT GROUPS AND ISOMORPHISMS.

Goals

- Investigate the definition of isomorphism
- Apply the definition of isomorphism to specific examples
- Recall the 1st isomorphism theorem, and investigate applications of it.

Introduction

Last week, we investigated the notion of Normal subgroups, group homomorphisms, and the kernal and image of group homomorphism. I mentioned that group homomorphisms are the way in which we can determine how groups can interact with one another. In this worksheet, we take that general goal further and investigate what we mean when we say two groups are the "same," so called isomorphic groups. Once we have a proper conception of what an isomorphism is- we can use it to exhibit a huge class of isomorphic groups. This will be the 1st isomorphism theorem, and is probably the most important and powerful theorem in Group Theory. We will conclude by providing some examples of the 1st Isomorphism theorem, and show that our intuition about certain groups being the same is well founded.

1 Group Isomorphisms

Let us first begin by recalling a few definitions. Throughout all of this, let $(G, *), (H, \circ)$ be two groups.

1. A function $\psi : G \to H$ is a **group homorphism** if, for every $g_1, g_2 \in G, \psi(g_1 * g_2) =$

$\psi(g_1) \circ \psi(g_2)$

2. The **kernal** of a group homorphism is $ker(\psi) = \{g \in G : \psi(g) = e_H\}$

3. The **image** of a group homorphism is $im(\psi) = \{h \in H : \psi(g) = h$ for some $g \in G\}$

4. We say a group homomorphism $\psi : G \to H$ is **injective** (or 1-1, read as "one to one") if whenever $\psi(g_1) = \psi(g_2)$ we must have $g_1 = g_2$ (that is, distinct elements in G get mapped to distinct elements in H)

5. We say a group homomorphism is **surjective** (or onto) if $im(\psi) = H$

In the background, we should be keeping in mind the definition of normal subgroups as defined last time. Specifically, remember that the kernal of any group homomorphism is a normal subgroup, which lets us consider the **Quotient Group** $G/ker(\psi)$. Let us first give a simple Lemma, and then we give some examples, and non-examples, of injective and surjective group homomorphism.

1. Lemma: Let $\psi : G \to H$ be a group homomorphism. Then ψ is injective iff $ker(\psi) = \{e_G\}$
   Solution: First, assume ψ is injective and suppose $g \in ker(\psi)$. Then $\psi(g) = e_H$, yet recall the lemma we showed last week gave us $\psi(e_G) = e_H$. Thus $\psi(g) = \psi(e_G)$ and since ψ is injective, we get that $g = e_G$. Hence the only element in the kernal is the identity.
   Prove the reverse implication:
   Now assume $ker(\psi) = \{e_G\}$ and assume that $\psi(g_1) = \psi(g_2)$ for some $g_1, g_2 \in G$. Then, multiplying on the right we get $\psi(g_1)\psi(g_2)^{-1} = e_H$. Since ψ is a group homomorphism, we can pull the inverse in to get $\psi(g_1 g_2^{-1}) = e_H$. Yet since the kernal is trivial we get $g_1 g_2^{-1} = e_G$ so $g_1 = g_2$.

2. Consider the identity map $id : G \to G$ defined by id(g)=g for all g in G. This is clearly injective and surjective.

3. Consider the map $\psi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\psi(x) = \overline{x}$. Is ψ injective? Is it surjective?
   Solution:
   (a) We found the kernal of this map last worksheet. For completion, find it here again to conclude this map is not injective.
   Solution: First, we note that the identity in $\mathbb{Z}_n$ is the equivalence class of 0, $\overline{0}$- that is, all integer multiples of n. Therefore $ker(\psi) = \{x \in \mathbb{Z} : \overline{x} = \overline{0}\} = \{x \in \mathbb{Z} : x = nk$ for some k $\in \mathbb{Z}\} = n\mathbb{Z}$. Therefore, this group is not injective.
   (b) Is ψ surjective?
   Yes this map is surjective. Given $\overline{a} \in \mathbb{Z}_n$ we get that $\psi(a) = \overline{a}$.

4. Let $\psi : \mathbb{Z} \to \mathbb{Z}$ be defined by $\psi(z) = 2z$. Is ψ injective? Surjective?

   (a) Surjective: (Hint- to show that something IS surjective, you need to show every element in the codomain is mapped to by at least one element in the domain. To show something is NOT surjective on the other hand, it suffices to show that a single element in the codomain is not mapped to. Think about which is the case here)
   This map is not surjective. The image is only the even integers, so no odd integers are mapped to. For example, 3 is not in the image.

   (b) Is ψ injective?
   Yes this map is injective. We can use the characterization of injectivity from above to show this. Namely, if $\psi(z) = 2z = 0$ then z=0 so $ker(\psi) = \{0\}$

5. **Important Example:** Let $N \trianglelefteq G$ be a normal subgroup. Recall we defined the "natural projection of G onto G/N" last section, $\pi : G \to G/N$ by $\pi(g) = gN$. Is π injective? Surjective?

   (a) Is π injective? The identity element of G/N is the trivial coset N. Now we have $g \in ker(\pi) \iff gN = N \iff g \in N$ so $ker(\pi) = N$ showing that π is not injective.

   (b) Prove that π is surjective.
   Recall that G/N consists of all left (or right) cosets of N in G. So let gN be such a coset for some g in G. Then $\pi(g) = gN$ showing that π is surjective.
   (compare to example 4 above).

The real power of the definitions injective, and surjective group homomorphisms come when we combine them: That is the following definition.

A group homomorphism $\psi : G \to H$ is a **Group Isomorphism** if ψ is both injective and surjective. We say the groups G and H are **Isomorphic** and write it $G \cong H$

The intuition one should build is that if two groups are isomorphic, they are "the same." That is, they should have the same group structure. Let us make that a little clearer hopefully with the following example:

1. Suppose $(G, *), (H, \circ)$ are two groups and $\psi : G \to H$ is an isomorphism. Then, given any $h_1, h_2 \in H$ and since ψ is an isomorphism, we know that there exists unique g_1, g_2 with $\psi(g_1) = h_1,$ and $\psi(g_2) = h_2$. Suppose we know that $g_1 * g_2 = g_3$ in G. Then this forces what $h_1 \circ h_2$ can be (that is, knowing the multiplication in G forces it in H).

Indeed, we claim $h_1 \circ h_2 = \psi(g_3)$
Solution: The only pieces of information we know are that the h's come from unique g's by a group homomorphism. Use that information to complete this proof:
We have that $h_1 \circ h_2 = \psi(g_1) * \psi(g_2)$ by assumption. Now ψ is a group homomorphism so we get that $h_1 \circ h_2 = \psi(g_1 * g_2) = \psi(g_3)$

Let us be careful about what the definition of isomorphism says and doesn't say. For example, **say what are wrong** about the following **Incorrect** proofs.

1. We prove that every group homomorphism between isomorphic groups is injective
   Solution: Suppose $G \cong H$. Then the homomorphisms between them are by definition both surjective and injective. Thus, every group homomorphism between G and H is in particular injective.
   Recall that G is isomorphic to H if THERE EXISTS a bijective group homomorphism between them. It emphatically does not say that every such group homomorphism between them is an isomorphism. For example, $G \cong G$ trivially (take the identity map) but the zero morphism $0 : G \to G$ defined by $0(g) = e_G$ is a (very much) non injective group homomorphism.

2. We show the groups $\mathbb{Z}$ and $2\mathbb{Z}$ are NOT isomorphic.
   Solution: We know that $2\mathbb{Z}$ is a proper subgroup of $\mathbb{Z}$ and since there are elements in $\mathbb{Z}$ that are not in $2\mathbb{Z}$ there is no way for the groups to be isomorphic.
   This is another example of why infinite sets are weird. The group homomorphism $\psi : \mathbb{Z} \to 2\mathbb{Z}$ defined by $\psi(z) = 2z$ is a group isomorphism!

2 Some Examples of Group Isomorphisms

In this section, we provide isomorphic groups. In each case, show why they are isomorphic. That is, exhibit a group isomorphism between them.

1. Let $(G, *) = (\mathbb{R}, +)$ and let $H = \{(x, 0) : x \in \mathbb{R}\} \trianglelefteq \mathbb{R}^2$. Show that $G \cong H$
   Solution: Define the map $\psi : G \to H$ by $\psi(r) = (r, 0)$. This is a bijective group homomorphism.

2. Let $(G, *) = (\mathbb{R}, +)$ and let $H = \{(0, y) : y \in \mathbb{R}\} \trianglelefteq \mathbb{R}^2$. Show that $G \cong H$
   Solution: Define the map $\psi : G \to H$ by $\psi(r) = (0, r)$. This is again a bijective group homomorphism.

3. Let $(G, *) = (\mathbb{R}^4, +)$ and let $(H, *) = (M_{2\times 2}(\mathbb{R}), +)$. Show that $G \cong H$
   Solution: Define a map $\psi\big((x_1, x_2, x_3, x_4)\big) = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$
   This is a group homomorphism since matrix addition is defined componentwise. It is surjective by construction since we can choose any real number in the domain. Finally, assume $\psi\big((x_1, x_2, x_3, x_4)\big) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ Then $x_1 = x_2 = x_3 = x_4 = 0$ so ψ has trivial kernal and is thus injective.

4. Does there exist two vector spaces V,W that are isomorphic as vector spaces such that their underlying abelian groups are **NOT** isomorphic? (recall a vector space isomorphism is a bijective linear transformation)
   Solution: No, all vector space isomorphisms are in particular abelian group isomorphisms. Remember a linear transformation is in particular a group homomorphism, so a bijective linear transformation will automatically be a bijective group homomorphism- and thus a group isomorphism.

With this notion of Isomorphism in mind, one might guess that we can finally answer how $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$ are related- namely that they are isomorphic! You would in fact be correct!! However, to construct an explicit isomorphism between those two groups involves an annoying subtlety: Both groups are comprised of equivalence classes- so in defining a function between them, one has to show the added step that the function is well defined (see example 3 in section 2 of last worksheet). In other words, you have to show that the function does not depend on choice of representative for the equivalence class (think back to how we showed addition is well defined for each case). Therefore, rather than showing explicitly that they are isomorphic, we will first rely on the powerful 1st isomorphism theorem of next section. After which, for practice in showing functions are well defined, we will give a second, more explicit proof of the fact they are isomorphic.

3 First Isomorphism Theorem

Consider the following two examples we have worked through:

1. We considered the additive abelian group $(\mathbb{R}^2, +)$, and let N be the normal subgroup $N = \{(x, 0) : x \in \mathbb{R}\} \trianglelefteq \mathbb{R}^2$ (ie the x-axis). We then considered the projection map onto the y-axis:
   (a) $\pi_y : \mathbb{R}^2 \to \mathbb{R}$ defined by $\pi_y(a, b) = b$.

(b) We showed this map was surjective, and that the kernal of this map was exactly N

(c) We then hinted that this map might have some connection to the other projection map $\pi_N : G \to G/N$ and, through that connection, might help us understand the group G/N.

2. We also considered the surjective group homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\pi(x) = \overline{x}$. We showed

   (a) That this map had kernal $n\mathbb{Z}$

   (b) We again also have the projection map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and we have been hinting that there is some connection between the groups $\mathbb{Z}_n$, and $\mathbb{Z}/n\mathbb{Z}$

In both cases we were given a surjective group homomorphism, and through that group homomorphism got some idea as to what the more complicated quotient group might look like (namely it should be the codomain of the surjective homomorphism). This is not a coincidence:

Theorem (1st Isomorphism Theorem): Let $\psi : G \to H$ be a group homomorphism. Then there is an isomorphism $G/ker(\psi) \cong im(\psi)$

1. Prove once and for all that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$
   (The proof will use the 1st iso theorem- At this point, I should really note- you will often find some textbooks don't even distinguish between the two groups $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$. In my opinion, this isn't great pedagogically- while one can show that the equivalence relation defining $\mathbb{Z}/n\mathbb{Z}$ is really at the end of the day, the same equivalence relation defining $\mathbb{Z}_n$, (see Worksheet 2), in my opinion, treating these as separate groups until this point provides a great deal of motivation for a lot of the tools we have built up- and really gives a great starting point example to build a framework around how one actually uses the 1st isomorphism theorem)

   Solution: Again consider the map $\psi : \mathbb{Z} \to \mathbb{Z}_n$. We showed in Section1 example 3 that this map was surjective with $\ker(\psi) = n\mathbb{Z}$. Thus by the first Isomorphism Thrm we get $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

2. Consider the case from example 1 above. Show that $\mathbb{R}^2/N \cong \mathbb{R}$
   Solution: As we mentioned above, this map is surjective with kernal N. Thus by the first iso thrm again we get $\mathbb{R}^2/N \cong \mathbb{R}$

3. Consider the circle $\mathbb{S}^1 = \{e^{iz} : z \in \mathbb{R}\}$ (this really is a way to describe the circle- if you haven't seen complex numbers before, let me know and I can give you a crash course)

(a) Show that $\mathbb{S}^1$ is a group under the usual multiplication $e^{iz_1} \times e^{iz_2} = e^{i(z_1+z_2)}$ (the circle is a group!! Pretty cool huh!)
Solution: The identity of this group is just the number $1 = e^{0i}$ and we have $(e^{iz})^{-1} = e^{-iz}$. With these two pieces of information, it is a nice exercise to show that $\mathbb{S}^1$ is a group.

(b) Show that $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.
Solution: You will use the first isomorphism theorem. Construct a surjective group homomorphism $\psi : \mathbb{R} \to \mathbb{S}^1$ with kernal $\mathbb{Z}$.
Such a map is given by $\psi : \mathbb{R} \to \mathbb{S}^1$ defined by $\psi(r) = e^{2\pi ri}$. This is surjective and the kernal is $\mathbb{Z}$ (remember the identity is just the number 1) so again we conclude by the 1st Iso Thrm.

4. **Challenge Problem:** Recall that the sets $GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) : A \text{ is invertible}\}$ and $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : det(A) = 1\}$ are groups under multiplication and that $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$. Use the first isomorphism theorem to find what the quotient group $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ is.
Solution: Define the map $\psi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ by $\psi(A) = det(A)$ the determinant of A. (where $\mathbb{R}^*$ is the group of nonzero real numbers under multiplication). Remember that $det(AB) = det(A)det(B)$ so this is a group homomorphism! Now let $r \in \mathbb{R}^*$. Then the diagonal matrix $A = diag(r, 1, \ldots, 1)$ has det(A)=r so the map is surjective.
Finally, the kernal of this map are the matrices with det=1, ie $ker(\psi) = SL_n(\mathbb{R})$. So by the 1st Iso Thrm again, we get $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$

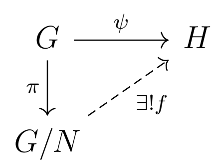
It is hard to overstate the importance and significance of this little theorem. For starters, all the other so called "Isomorphism Theorems" we will learn are proved using this theorem. More immediately though, we have just demonstrated its power in action. The general schema is the following:

1. Suppose you are given some normal subgroup $N \trianglelefteq G$ of your group G. Then we know we can turn this into a group G/N. However, this group is rather messy- its elements are equivalence classes and "doing" stuff on it therefore requires some care. So rather than trying to work out the group G/N from first principles we use the 1st Isomorphism Thrm.

2. Explain how the 1st isomorphism theorem gives us one line of attack in trying to determine what the group G/N is isomorphic to. Describe the steps one would take (think about the examples given above- what did we do for those cases?)
Solution: We should like to define a surjective group homomorphism from G to some other group H that has kernal precisely equal to N! If we can do so, then we conclude by the 1st Iso Thrm that $G/N \cong H$.

3. **Some extra information about quotient groups beyond the scope of the course**
There is a property of quotient subgroups that really gives the first isomorphism it's power- and really actually explains "why" the theorem is true. Recall that for $N \trianglelefteq G$ we denoted the natural projection map as $\pi : G \to G/N$, and we saw that this map has $ker(\pi) = N$. From the perspective of "Category Theory" (what I study), the pair $(G/N, \pi)$ convey the so called "universal property of the quotient group". What that means explicitly is the following:

   (a) Suppose you had some other group homomorphism $\psi : G \to H$ such that ψ "kills" everything in N, that is $N \subseteq ker(\psi)$. Then that morphism can be "factored" uniquely as follows



   , that is there exists a unique map $f : G/N \to H$ such that $f \circ \pi = \psi$.

   (b) To put this precisely, we have that the pair $(G/N, \pi)$ is "initial" amongst all pairs (H, ψ) with the property that N is contained in the kernal of ψ. Remember that defining morphisms out of quotient groups is tricky since the objects are equivalence classes- this universal property helps us get around that added difficulty! To define a map from $G/N \to H$ one must only give a map from $G \to H$ that contains N in the kernal. "Morally" what this says is that the group G/N is the "best possible" group in which every element from N "is zero"

As promised, to end it out- here is the "obvious" function that explicitly shows the isomorphism between $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$. I have mentioned before that much of higher mathematics is aesthetic driven- Cards on the table, so to speak, I find the following proof quite aesthetically ugly compared to the previous proof. However, to each their own:

1. Let $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ be defined by $\psi(x + n\mathbb{Z}) = \overline{x}$.

   (a) Show this is a well defined function-ie, does not depend on choice of coset representative.
   Solution: Suppose $(x_1 + n\mathbb{Z}) = (x_2 + n\mathbb{Z})$. Then we get that $x_1 - x_2 \in n\mathbb{Z} \implies x_1 = nl + x_2$. Thus $\psi(x_1) = \psi(nl + x_2) = \psi(nl) + \psi(x_2) = \psi(x_2)$ since $\psi(nl) = \overline{0}$. Thus this map is well defined.

   (b) Show furthermore that this is a group homomorphism.
   Solution: Note $\psi((x_1 + x_2) + n\mathbb{Z}) = \overline{x_1 + x_2} = \overline{x_1} + \overline{x_2} = \psi(x_1 + n\mathbb{Z}) + \psi(x_2 + n\mathbb{Z})$

(c) Show this is a group isomorphism
Solution: Let $\overline{a} \in \mathbb{Z}_n$. Then $\psi(a + n\mathbb{Z}) = \overline{a}$ so it is surjective.
Now assume that $\psi(a+n\mathbb{Z}) = \overline{0}$.This implies that $a \equiv 0$ mod n, ie $n|a$ so $a \in n\mathbb{Z}$. Hence $a + n\mathbb{Z} = n\mathbb{Z}$ which is the identity element in $\mathbb{Z}/n\mathbb{Z}$. This shows the only element that maps to the identity in $\mathbb{Z}_n$ is the identity in $\mathbb{Z}/n\mathbb{Z}$ so the map is injective. Combining it all we get that it is a group isomorphism.