MAT301H5Y

Week 5 Lecture 1: Introduction to homomorphisms

Tuesday Jun 6th, 2023

3-5pm instructed by Marcu-Antone Orsoni

Overview

We went over homomorphisms and propositions that arise from homomorphisms. We also went over kernel and image.

Homomorphisms

Definition: Homomorphism

Consider the groups $(G_1, *_1), (G_2, *_2)$, a map $\phi : G_1 \to G_2$ is said to be a homomorphism if the following is true:

$$\forall a, b \in G_1 \quad \phi(a *_1 b) = \phi(a) *_2 \phi(b)$$

As one may notice, the notion of homomorphism is similar to linear transformation between vector spaces in linear algebra. There are somewhat similar results that arise from there as well. Consider the proposition below:

Proposition: Composition of homomorphisms

Composition of homomorphisms are a homomorphism.

Proof

Suppose $\phi : G_1 \to G_2$ and $\gamma : G_2 \to G_3$ are homomorphisms. We see the following:

$$\begin{aligned} \gamma(\phi(ab)) &= \gamma(\phi(a)\phi(b)) \\ &= \gamma(\phi(a))\gamma(\phi(b)) \end{aligned}$$

Therefore we see that $\gamma \cdot \phi : G_1 \to G_2$ is a homomorphism as well, as required. ■

Proposition: identity for homomorphisms

Suppose we have a homomorphism $\phi : G \to G'$ with identity elements ϵ and ϵ' respectively. The following holds true:

1. $\phi(\epsilon) = \epsilon'$
2. $\forall x \in G \ \phi(x^{-1}) = \phi(x)^{-1}$

Proof for (1)

We see that the following series steps prove this proposition:

$$\begin{aligned} &\phi(\epsilon) = \phi(\epsilon\epsilon) = \phi(\epsilon)\phi(\epsilon) \text{ [Property of homomorphism]} \\ \implies &\cancel{\phi(\epsilon)}\cancel{\phi(\epsilon)^{-1}} = \phi(\epsilon)\cancel{\phi(\epsilon)}\cancel{\phi(\epsilon)^{-1}} \\ \iff &\epsilon' = \phi(\epsilon) \end{aligned}$$

Proof for (2):

Choose $x \in G$, computing the following:

$$\begin{aligned} & xx^{-1} = \epsilon \\ \implies & \phi(xx^{-1}) = \phi(\epsilon) = \epsilon' \text{ (As per (1))} \\ & = \phi(x)\phi(x^{-1}) \text{ [As per property of homomorphism]} \\ \implies & \phi(x)^{-1} = \phi(x^{-1}) \end{aligned}$$

■

Remark: A good check for whether a map is *not* a homomorphism is to check the contrapositive to (1) which is $\phi(e) \neq \epsilon' \implies \phi$ is not a homomorphism.

Below we consider some examples.

Example: non-homomorphism

The map $\phi : S_n \to S_n$ defined by $\sigma \to (1\ 2)\sigma$ is not a homomorphism.

Proof:
Observe that the identity of S_n written as the identity permutation ϵ, we see that $\phi(\epsilon) = (1\ 2)\epsilon \neq \epsilon$. This directly gives us that ϕ is not a homomorphism.

■

We went over other common examples in class as below:

Examples: common homomorphisms

1. Constant map $\phi : G \to G'$ defined as $x \to \epsilon'$
2. Given $H \preceq G$, an embedding map (such as the identity) is a homomorphism denoted by $H \hookrightarrow G$
3. Choose some $x \in G$, the map $\phi : \mathbb{Z} \to G$ given by $\phi(k) = x^k$
4. $\ln : (\mathbb{R}^+, *) \to \mathbb{R}$ the natural logarithm
5. $\det : GL(n, \mathbb{Z}) \to (\mathbb{R}^*,)$ the usual matrix determinant

Remark: Usually when the instructor just mentions $\mathbb{R}$ that means the default operation is addition. Likewise for $\mathbb{R}^*$ the operation would be multiplication by default. It also applies to other standard sets as well such as $\mathbb{Z}$.

An additional remark to consider is to ensure the function is well defined within its domain. This means that the representation of the element as the input should not change the output. For example, whenever constructing a homomorphism from $\mathbb{Z}_n$, it's important to see that the representation of the class does not change the output(for example $[1] = [11]$ in modulo 10 b ut $1 \neq 11$).

Kernel and Image

Definition: Kernel and image

Suppose we have a homomorphism $\phi : G \to G'$ the identities as ϵ, ϵ' respectively.

- **Kernel**, the kernel of ϕ denoted by $\ker(\phi)$ is defined as the set below:

$$\ker(\phi) = \phi^{-1}(\{\epsilon'\}) = \{x \in G : \phi(x) = \epsilon'\}$$

- **Image**: The denoted by $\text{Im}(\phi)$ or $\phi(G)$ is the following set:

$$\text{Im}(\phi) = \phi(G) = \{\phi(x) : x \in G\}$$

Remark: The notation for $\phi^{-1}(A)$ where A is some subset of G' is what we call the *pre-image*. That set is defined as follows for some map(not necessarily homomorphism):

$$\phi^{-1}(A) = \{x \in G : \phi(x) \in A\}$$

The following propositions arise as properties of kernel, image and pre image.

Proposition: Pre-image and image

Assuming $\phi : G \to G'$ is a homomorphism with identities ϵ, ϵ' respectively.

(1) $\forall H' \preceq G'$, $\phi^{-1}(H') \preceq G$

(2) $\forall H \preceq G$, $\phi(H) \preceq G$

Proof for (1):
Let us assume that $H' \preceq G'$. Let us prove the axioms of a subgroup.

1. $\phi^{-1}(H') \subseteq G$ is trivial by definition of pre-image
2. $\phi^{-1}(H') \neq \emptyset$: Observe that since H' is a subgroup, it must have ϵ'. Using a property of homomorism we see that $\phi(\epsilon) = \epsilon'$ and thus $\epsilon \in \phi^{-1}(H')$, making it non-empty
3. Closure: Choose $x, y \in \phi^{-1}(H')$. From this we see that $\phi(x), \phi(y) \in H'$. Computing $\phi(xy^{-1})$ we see that $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1}$. Since H' is a subgroup we know by assumption that $\phi(x), \phi(y)^{-1} \in H'$. From this it becomes clear that $\phi(xy^{-1}) \in H'$ and therefore $xy^{-1} \in \phi^{-1}(H')$. Using proposition 2.21 from the course notes(probably the cleanest proposition in existence) we see that $\phi^{-1}(H') \preceq G$

■

Proof for (2): Skipped in class but follows a very similar approach.

Similar to linear algebra, the kernel and injectivity of the function are related to each other.

Proposition: Injectivity and kernel

A homomorphism $\phi : G \to G'$ with identities as ϵ, ϵ' is injective if and only if $\ker(\phi) = \{\epsilon\}$.

Proof:
($\implies$) Want to show the forward direction first which is that an injective homomorphism implies that the kernel is the trivial subgroup. Assume ϕ is injective. We

need to show double inclusion of sets. We see trivially that $\{\epsilon\} \subseteq \ker(\phi)$ as $\phi(\epsilon) = \epsilon'$ as per the properties of homomorphisms.

Now wanting to show that $\ker(\phi) \subseteq \{\epsilon'\}$. Assume $x \in \ker(\phi)$. From this, the following steps follow:

$$\begin{aligned} x \in \ker(\phi) &\implies \phi(x) = \epsilon' = \phi(\epsilon) \\ &\implies x = \epsilon \text{ [Because } \phi \text{ is injective]} \\ &\implies x \in \{\epsilon\} \\ &\iff \ker(\phi) \subseteq \{\epsilon\} \end{aligned}$$

As per double inclusion we see that $\ker(\phi) = \{\epsilon\}$ which is what we needed to show for the forward direction.

($\Longleftarrow$) For the reverse direction, assume that $\ker(\phi) = \{\epsilon\}$. Let us start by assuming that $\phi(b) = \phi(a)$. We see the following steps follow:

$$\begin{aligned} \phi(b) = \phi(a) &\implies \phi(a)\phi(b)^{-1} = \epsilon' \\ &\implies \phi(ab^{-1}) = \epsilon' \\ &\implies ab^{-1} = \epsilon \text{ [As per our assumption that } \ker(\phi) = \{\epsilon\}] \\ &\implies a = b \end{aligned}$$

Which is sufficient to conclude that ϕ is injective. Having shown both directions we have shown the given proposition is true

■

We then analyzed kernels and images for certain homomorphisms in class as below:

Examples: Kernel and image

1. Constant function $\phi : G \to G'$ defined as $x \to \epsilon'$. We see that $\ker(\phi) = G$(all elements map to ϵ') and $\phi(G) = \{\epsilon\}$ as the image is just the identity.
2. Choose $x \in G$ define $\phi : \mathbb{Z} \to G$ such that $\phi(k) = x^k$. We have a couple cases.
   - If $|x| = n \neq \infty$, then $\ker(\phi) = n\mathbb{Z}$(This is because all integer multiples of the order equal the identity)
   - If $|x| = \infty$, then $\ker(\phi) = \{\epsilon\}$
   - $\text{Im}(\phi) = \langle x \rangle$
3. $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$: $\ker(\det) = SL(n, \mathbb{R})$ as all matrices that have determinant of 1(the identity in $\mathbb{R}^*$) defined by the group $SL(n, \mathbb{R})$. $\det(GL(n, \mathbb{R})) = \mathbb{R}^*$. This is the case for the image as we can just take the identity and set our last entry as our desired value in $\mathbb{R}^*$

There are more propositions that are useful when it comes to homomorphisms as below.

Proposition: order of homomorphisms

Assume that $\phi : G \to G'$ is a homomorphism.

(1) $\forall x \in G, \forall k \in \mathbb{Z}$, $\phi(x^k) = \phi(x)^k$

(2) $\forall x \in G$, $|x| = n \neq \infty \implies |\phi(x)| \Big| |x|$

Proof for (1):

This can be proved by via induction. We can also see that $\phi(g^n) = \phi(g \cdot g \dots g) = \phi(g) \cdot \phi(g) \cdot \phi(g) \dots \phi(g) = (\phi(g))^n$ informally.

Proof for (2):

Assume $|g| = n$, from this we know that $g^n = \epsilon$. Using this equation we get the following steps:

$$\begin{aligned} &\phi(g^n) = \phi(\epsilon) = \epsilon' \\ &\phi(g)^n = \epsilon' \text{ [Using (1) from earlier]} \\ \implies &|\phi(g)| \Big| n = |g| \end{aligned}$$

There is also a connection between cyclic subgroups and the image of cyclic subgroups.

Proposition: Cyclic subgroup images

Assume $\phi : G \to G'$ is a homomorphism $H \preceq G$ is cyclic $\implies$ $\phi(H) \preceq G'$ is also cyclic.

Proof:

We need to show that there exists $u \in \phi(H)$ such that $\phi(H) = \langle u \rangle$ in order to show it is cyclic. Assume that $H$is cyclic, that means that $H = \langle h \rangle$ for some $h \in H$. Claim is that $\langle \phi(h) \rangle = \phi(H)$. We can try to show this via double inclusion. First let us show $\phi(H) = \langle \phi(h) \rangle$.

Let $x \in \phi(H)$, that means that $x = \phi(u)$ for some $u \in H$. Since H is cyclic, there is some natural k for which $u = h^k$. This means that $x = \phi(h^k) = \phi(h)^k$(as per previous proposition). This means that $x \in \langle \phi(H) \rangle$ and thus we have shown that $\phi(H) \subseteq \langle \phi(h) \rangle$

Showing the reverse direction follows similar steps, however a student in class pointed out a clever trick when it comes to subspaces generated by elements. We know that $\phi(h) \in \phi(H)$ by definition, since $\langle \phi(h) \rangle$ is the smallest subgroup generated by $\phi(h)$, it directly follows that $\langle \phi(h) \rangle \subseteq \phi(H)$ which is what we wanted to show.

Having shown the double inclusion we may conclude that $\phi(H)$ is cyclic as well.

■

Proposition: uniqueness of generators

Suppose $G = \langle A \rangle$ for some $A \subseteq G$. A homomorphism $\phi : G \to G'$ can uniquely be determined by the elements of $a \in A$.

Proof

Let $A \subset G = \{a_1, a_2, a_3 \dots, a_m\}$. Assume $G = \langle A \rangle$ and choose $x \in G \iff x \in \langle A \rangle$. From this we conclude that $x = a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}$.

$$\begin{aligned} x &= a_1^{n_1} a_2^{n_2} \dots a_m^{n_m} \\ \phi(x) &= \phi(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}) = \phi(a_1^{n_1}) \phi(a_2^{n_2}) \dots \phi(a_m^{n_m}) \\ &= \phi(a_1)^{n_1} \phi(a_2)^{n_2} \dots \phi(a_m)^{n_m} \end{aligned}$$

Which shows us how to construct every element using our homomorphism.

■

We did an exercise in class as well. It is as below:

Exercise

Suppose we have a homomorphism $\phi : \mathbb{Q} \to \mathbb{Q}$. Show that for all $x \in \mathbb{Q}$, $\phi(x) = x\phi(1)$

Solution:

Assume $x \in \mathbb{Q}$, from this we realize that $x = \frac{p}{q}$ for integers p, q and non-zero q. Observe the following given our binary operation of addition.

$$\phi(\frac{p}{q})q = \phi(\frac{p}{q}) + \phi(\frac{p}{q}) + \dots \phi(\frac{p}{q}) = \phi(\frac{p}{q} + \frac{p}{q} + \cdots + \frac{p}{q}) = \phi(p)$$

Furthermore, observe that for any integer $k \in \mathbb{Z}$, we see that $\phi(k) = \phi(1 + 1 + \cdots + 1) = \phi(1) + \phi(1) + \cdots + \phi(1) = k\phi(1)$. Using this fact we see that $\phi(p) = p\phi(1)$. Using our equation from earlier we see that

$$\begin{aligned} \phi(\frac{p}{q})q = \phi(p) = p\phi(1) \\ \implies \phi(\frac{p}{q}) = \frac{p}{q}\phi(1) \\ \iff \phi(x) = x\phi(1) \end{aligned}$$

Which is what we needed to show

■