SEPTEMBER 12 NOTES

1. 1.6: Homomorphisms and Isomorphisms

A fundamental notion in abstract mathematics is the idea of a *morphism*, which is an allowed type of function in a *category* (collection) of objects that preserves whatever additional structure we have on these objects. For example, you've already seen *linear transformations* as the allowed functions from $\mathbb{R}^n$ to $\mathbb{R}^m$ in linear algebra, where the objects you're looking at are vectors, lines, or linear subspaces. The linear transformations are the functions that take linear subspaces to other linear subspaces.

Here, we will introduce morphisms of groups, which will 'preserve' the structure of a group.

Definition 1.1. Let $(G, \star_G)$ and $(H, \star_H)$ be groups. A **homomorphism** $\phi : G \to H$ is a function such that

$$\phi(a \star_G b) = \phi(a) \star_H \phi(b)$$

for all $a, b \in G$.

The homomorphism ϕ is called an **isomorphism** if it is a bijection (i.e. injective and surjective). In this case, we say G and H are **isomorphic** and write $G \cong H$.

Example 1.2. The function $\phi : \mathbb{R} \to \mathbb{R}^+$ given by $\phi(x) = e^x$ is a homomorphism and an isomorphism.

Let's prove this. To show it is a homomorphism, since the binary operation on $\mathbb{R}$ is $+$ and the binary operation on $\mathbb{R}^+$ is $\times$, we must show $\phi(x + y) = \phi(x) \times \phi(y)$. But this is true:

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x) \times \phi(y).$$

To show it is an isomorphism, we must show it is injective and surjective. To see injectivity, suppose $\phi(x) = \phi(y)$, so $e^x = e^y$. Taking the natural log of both sides, we see that $x = y$ so ϕ is injective. To see surjectivity, let $z \in \mathbb{R}^+$ be any element in the codomain. Then, if $x = \ln(z)$, then $x \in \mathbb{R}$ and we have $\phi(x) = e^{\ln z} = z$, so ϕ is surjective. Therefore, ϕ is an isomorphism.

By definition, a homomorphism of groups preserves the binary operation, but it also 'preserves' the identity and inverse elements as in the following proposition.

Proposition 1.3. *If $\phi : G \to H$ is a homomorphism, then:*

(1) $\phi(1_G) = 1_H$, where 1_G and 1_H are the identities in G and H, and
(2) for any $x \in G$, $\phi(x^{-1}) = \phi(x)^{-1}$.

Proof. We first prove (1). Because $1_G 1_G = 1_G$, we have

$$\phi(1_G 1_G) = \phi(1_G)$$

and by the homomorphism condition, we may write the left side as

$$\phi(1_G)\phi(1_G) = \phi(1_G).$$

Using the cancellation law that we have already proven, using that the right side is equal to $\phi(1_G)1_H$, we obtain

$$\phi(1_G) = 1_H.$$

(Alternatively, one could prove this without the cancellation law by multiplying both sides on the right or left by the inverse of $\phi(1_G)$.)

Now, we prove (2). Because we already know inverses are unique, it suffices to show that $\phi(x)\phi(x^{-1}) = \phi(x^{-1})\phi(x) = 1_H$ as this will show $\phi(x^{-1})$ satisfies the inverse property for the element $\phi(x)$.

But, using the homomorphism condition, we may write $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G)$, and by (1), we have $\phi(1_G) = 1_H$. Therefore, $\phi(x)\phi(x^{-1}) = 1_H$. By a similar argument for $\phi(x^{-1})\phi(x)$, we conclude $\phi(x)^{-1} = \phi(x^{-1})$. □

Typically, it is difficult to prove that two groups are isomorphic as you must actually construction an isomorphism between them. However, it is usually easier to prove that two groups are *not* isomorphic. For example:

Proposition 1.4. *If $\phi : G \to H$ is an isomorphism, then:*

(1) $|G| = |H|$,
(2) G is abelian if and only if H is abelian, and
(3) for all $x \in G$, $\mathrm{ord}(x) = \mathrm{ord}(\phi(x))$.

Proof. Exercise! □

Note that these are *not sufficient* to prove that two groups are isomorphic. They are mostly used to prove that groups cannot be isomorphic.

Example 1.5. $\mathbb{Z}$ and $\mathbb{R}$ are not isomorphic since $|\mathbb{Z}| \neq |\mathbb{R}\|$.

$\mathbb{Z}_6$ and S_3 are not isomorphic since $\mathbb{Z}_6$ is abelian but S_3 is not.

D_8 and Q_8 are not isomorphic since D_8 has two elements of order 4 but Q_8 has 6.

Some vocabulary:

Definition 1.6. The **kernel** of a homomorphism $\phi : G \to H$ is the set

$$\ker \phi = \{g \in G \mid \phi(g) = 1_H\}.$$

The **image** of a homomorphism $\phi : G \to H$ is the set

$$\mathrm{im}\phi = \{\phi(g) \mid g \in G\}.$$

Example 1.7. Let $\phi : \mathbb{Z} \to \mathbb{Z}_3$ be the map $\phi(n) = n \pmod 3$. We leave it as an exercise to show ϕ is a homomorphism. What is the kernel of ϕ? What is the image?

By definition, $\ker \phi = \{n \in \mathbb{Z} \mid \phi(n) = 0\}$ is the set of integers such that $n = 0 \pmod 3$. This is precisely the multiples of 3, i.e.

$$\ker \phi = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

The image of ϕ is the set of possible outputs of ϕ. The function is surjective and $\mathrm{im}\phi = \mathbb{Z}_3$.

2. 1.7: Group actions

Now, we come to a section that you may or may not have seen before. We aim to generalize one thing we saw for dihedral groups, symmetric groups, and matrix groups: they all *act* on certain objects. For instance, the dihedral group 'acts' on an n-gon by moving it to a new position. The symmetric group 'acts' on n cards by permuting them into a new order. Matrix groups act on vector spaces F^n by moving the vectors to new places. We now make the idea of a group action precise.

Definition 2.1. Let A be a set. An **action** of a group G on a set A is a map $G \times A \to A$, written as $(g, a) \mapsto g \cdot a$, such that:

(1) for all $g_1, g_2 \in G$ and $a \in A$, $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, and
(2) for all $a \in A$, $1 \cdot a = a$.

In this case, we say the group G **acts** on A.

Example 2.2. If $A = \mathbb{R}^n$ and $G = \mathrm{GL}_n(\mathbb{R})$, then G acts on A by $M \cdot \mathbf{v} = M\mathbf{v}$ for $M \in \mathrm{GL}_n(\mathbb{R})$ and $\mathbf{v} \in \mathbb{R}$. This satisfies the two properties:

$$M_1 \cdot (M_2 \cdot \mathbf{v}) = M_1 \cdot (M_2\mathbf{v}) = M_1(M_2\mathbf{v}) = (M_1M_2)\mathbf{v}$$

and

$$I \cdot \mathbf{v} = I\mathbf{v} = \mathbf{v}.$$

Example 2.3. If $A = \{1, 2, \ldots, n\}$, the group $S_A = S_n$ acts on A by $\sigma \cdot a = \sigma(a)$.

We introduce some notation and observations for a group G acting on a set A below.

For each fixed $g \in G$, there is a map $\phi_g : A \to A$ given by $\phi_g(a) = g \cdot a$.

Proposition 2.4. *If G acts on a set A, for any $g \in G$, $\sigma_g : A \to A$ is permutation of A.*

Proof. Recalling the definition of permutation, we must just show that σ_g is bijective. One way to do this is to show that σ_g has an inverse. We claim that $\sigma_{g^{-1}}$ is the inverse of σ_g. Indeed, for all $a \in A$,

$$\begin{aligned}
(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \quad \text{by definition of } \circ \\
&= g^{-1} \cdot (g \cdot a) \quad \text{by definition of } \sigma_g, \sigma_{g^{-1}} \\
&= (g^{-1}g) \cdot a \quad \text{by property (1) of being an action} \\
&= 1 \cdot a = a \quad \text{by property (2) of being an action}
\end{aligned}$$

Therefore, $\sigma_{g^{-1}} \circ \sigma_g$ is the identity function. Similarly, one can show $\sigma_g \circ \sigma_{g^{-1}}$ is the identity, so σ_g is bijective with inverse $\sigma_{g^{-1}}$ and hence a permutation of A. □

Proposition 2.5. *The map $\phi : G \to S_A$ given by $g \mapsto \sigma_g$ is a homomorphism.*

Proof. By the previous proposition, σ_g is indeed a permutation of A, so this map is well-defined. To show that it is a homomorphism, we must show

$$\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2)$$

for any $g_1, g_2 \in G$. As these are functions on A, they are equal if they have the same value for all $a \in A$. So, we compute:

$$\begin{aligned}
\phi(g_1g_2)(a) &= \sigma_{g_1g_2}(a) \quad \text{by definition of } \phi \\
&= (g_1g_2) \cdot a \quad \text{by definition of } \sigma \\
&= g_1 \cdot (g_2 \cdot a) \quad \text{by property (1) of being an action} \\
&= \sigma_{g_1}(\sigma_{g_2}(a)) \quad \text{by definition of } \sigma \\
&= (\sigma_{g_1} \circ \sigma_{g_2})(a) \quad \text{by definition of composition} \\
&= (\phi(g_1) \circ \phi(g_2))(a) \quad \text{by definition of } \phi.
\end{aligned}$$

Therefore, ϕ is a homomorphism.

□

Definition 2.6. The homomorphism $\phi : G \to S_A$ is called the **permutation representation** associated to the action of G on A.

In other words, we can 'represent' any action of G on A by permutations. We will make use of this often!

More vocabulary:

Definition 2.7. If G is a group and A is a set, the **trivial action** of G on A is the action $g \cdot a = a$ for all $g \in G$. The associated permutation representation $\phi : G \to S_A$ is the trivial homomorphism $\phi(g) = 1$ for all $g \in G$.

Definition 2.8. If G acts on a set B with permutation representation $\phi : G \to S_B$ such that $\phi_{g_1} \neq \phi_{g_2}$ for all $g_1 \neq g_2 \in G$, then the action is said to be **faithful**. In other words, a faithful action is one such that ϕ is injective.

Definition 2.9. If G acts on a set B, the **kernel** of the action is the set $\{g \in G \mid g \cdot b = b \forall b \in B\}$, namely the elements of G which fix *all* elements of B.

Exercise 2.10. Show that the kernel of the action is precisely the kernel of the permutation representation.

Example 2.11. Let us compute the permutation representation and the associated terminology for the elements of D_8.

Let $A = \{1, 2, 3, 4\}$ be the vertices of a square, numbered clockwise. The elements of D_8 act on A by permuting the vertices. For example, $r \cdot 1 = 2$, $r \cdot 2 = 3$, $r \cdot 3 = 4$, and $r \cdot 4 = 1$. The permutation representation is just the associated permutation $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 1$, which in cycle notation is just (1234). Therefore, $\phi(r) = \sigma_r = (1234)$.

By definition, $s \in D_8$ was reflection across the axis of symmetry through the vertex labeled 1. In this case, this is the axis connecting 1 and 3, so the action of s on A keeps 1 and 3 where they are, but switches 2 and 4, so the permutation representation is $\phi(s) = \sigma_s = (24)$.

We could do this for all 8 elements of D_4[1]:

$$\begin{aligned}
\phi(1) &= 1 \\
\phi(r) &= (1234) \\
\phi(r^2) &= (13)(24) \\
\phi(r^3) &= (1432) \\
\phi(s) &= (24) \\
\phi(sr) &= (14)(23) \\
\phi(sr^2) &= (13) \\
\phi(sr^3) &= (12)(34)
\end{aligned}$$

. We see that the map $\phi : D_8 \to S_4$ is injective, so action is faithful, and the kernel is only the identity element.

Example 2.12. Later in the course, we will often have a group G act *on itself*. The most common examples are the **left regular action** of G acting on G by $g \cdot a = ga$ for all $g, a \in G$ and **conjugation**: G acting on itself by $g \cdot a = gag^{-1}$ for all $g, a \in G$. You will explore these more in your homework!

[1]Note: here I follow the convention that sr means first do r, then do s.