3 Homomorphisms and Isomorphisms

3.1 Review

Last time, we discussed subgroups and cyclic groups. A subgroup of a group is essentially a subset of that group that is compatible with the group or multiplicative structure on it. A cyclic subgroup of an element g in a group is essentially the subgroup consisting of all the powers of g.

3.2 Homomorphisms

Now that we understand a little bit more about groups and their structures, the natural next step is to look at maps *between* groups.

Guiding Question
How can we understand groups by considering maps between different groups? What kinds of maps can provide useful insight into various groups?

First, we define a type of map that is compatible with the group structure on both groups.

Definition 3.1
Given groups G and G', a homomorphism between them is a map

$$f : G \longrightarrow G'$$

such that:

- For all $a, b \in G$, $f(ab) = f(a)f(b)$.
- The identity element is mapped to the identity: $f(e_G) = e_{G'}$.
- Inverses are preserved under the mapping: $f(a)^{-1} = f(a^{-1})$ for all $a \in G$.

Essentially, each of these conditions requires that the map preserve the group structure (multiplication, identity, inverse) from the domain G to the codomain G'. Either f can be applied to a product, or the product can be taken after f is applied, and it should yield the same element $f(ab) = f(a)f(b)$.[11] In fact, only the first condition is really necessary, and implies the second two.[12]

Proposition 3.2
If $f(ab) = f(a)f(b)$, then $f(e_G) = e_{G'}$ and $f(a)^{-1} = f(a^{-1})$.

Proof. For the first part, take $f(e_G \cdot e_G) = f(e_G) = f(e_G) \cdot e_{G'}$ by the definition of $e_{G'}$. Since f is a homomorphism, this will also be equal to $f(e_G)f(e_G)$. Multiplying on both sides by $f(e_G)^{-1}$[13] gives $f(e_G) = e'_G$.

The second part is similar. Take $a \in G$. Then $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e'_G$, and multiplying on the left by $f(a)^{-1}$ gives $f(a^{-1}) = f(a)^{-1}$. □

3.3 Examples

Let's see some examples.

Example 3.3
The determinant $\det : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^\times, \times)$ is a homomorphism from invertible matrices to the real numbers under multiplication, since $\det(AB) = \det(A)\det(B)$.

[11] In other words, a homomorphism will *commute* with multiplication in that they can be applied in either order. This results in a commutative diagram.

[12] In some way, this shows that the multiplication is the essential part of the group structure, and the identity and inverse properties are simply there to make sure nothing is able to go wrong with the multiplication.

[13] This must exist by the group property of invertibility.

Example 3.4
The exponential $\exp : (\mathbb{C}, +) \longrightarrow (\mathbb{C}^\times, \times)$ taking $z \longrightarrow e^z$ is a homomorphism, since $e^{a+b} = e^a e^b$.

Let the standard basis vectors of $\mathbb{R}^n$ be $\vec{e}_1 = (1, 0, \cdots, 0)^t, \vec{e}_2 = (0, 1, \cdots, 0)^t$, and so on, where $\vec{e}_i$ is the vector consisting of a 1 in the ith entry and 0s elsewhere.

For a permutation $p \in S_n$, let A_p be the permutation matrix taking $\vec{e}_i \longmapsto \vec{e}_{p(i)}$. In particular, the ith column of A_p will be $\vec{e}_{p(i)}$.

For example, for $p(123)$, $A_p = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Example 3.5
The mapping

$$\begin{aligned} \varphi : S_n &\longrightarrow GL_n(\mathbb{R}) \\ p \in S_n &\longmapsto A_p, \end{aligned}$$

where A_p is the permutation matrix, is a homomorphism. This is because $A_p(A_q(\vec{e}_i)) = A_p(\vec{e}_{q(i)}) = \vec{e}_{p(q(i))}$, and $A_{pq}(\vec{e}_i) = \vec{e}_{pq(i)} = \vec{e}_{p(q(i))}$, which matches, so $A_p A_q = A_{pq}$.

There is also another important homomorphism from S_n to another group.

Example 3.6
Let $\text{sign} = \det \circ \varphi$ take $S_n \longrightarrow \mathbb{R}^\times$ by taking the determinant of the permutation matrix. This mapping sign is also a homomorphism, since φ and det are both homomorphisms.

In fact, $\text{sign}(p) = \pm 1$. It is always possible to write any permutation as a composition of transpositions[14]: $p = \tau_1 \tau_2 \cdots \tau_r$ for transpositions τ_i. The determinant of a transposition matrix is -1, since $\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$, so $\text{sign}(p) = (-1)^r$ where r is the number of transpositions making up p. In fact, if $p = \tau_1 \cdots \tau_r = \tau'_1 \cdots \tau'_s$, $r = s$ modulo 2, since the sign homomorphism can be applied on either side. For example, for S_3, $e, (123)$, and (132) all have a sign of $+1$, while $(12), (13)$, and (23), the transpositions, all have a sign of -1.

Notice that $\mathbb{R}^\times = GL_1(\mathbb{R})$, since 1×1 invertible matrices are simply nonzero real numbers. These two examples provide a hint as to why homomorphisms are so useful: matrices/linear mappings and GL_n are generally well-understood, so if there is a homomorphism from a group to GL_n, the knowledge from GL_n can then be used to learn more about that particular group. This idea is the core theme of a branch of math called **representation theory.**[15]

Example 3.7
For any G and any $x \in G$, let

$$\begin{aligned} f_x : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto x^n. \end{aligned}$$

This is a homomorphism because $x^{a+b} = x^a x^b$, and is related to the cyclic subgroups of G.

Last time, in class, we studied cyclic subgroups $\langle g \rangle$ using $\mathbb{Z}$ and essentially used this homomorphism. In general, homomorphisms allow us to study complicated groups with simpler groups.

[14] Permutations that swap two elements and leave all other elements fixed.
[15] These examples actually provides the so-called *permutation representation* and *sign representation* of S_n.

Theorem 3.8
Let f be a homomorphism from $G \longrightarrow G'$. Then $\text{im}(f)$[a] is a subgroup of G'.

[a]The image of f consists of all the elements in G' that are mapped to by f.

This theorem is not surprising; the whole point of a homomorphism is that it plays nicely with the group structure, and the whole point of a subgroup is that it also plays nicely with the group structure.

Example 3.9
For example, $\text{im}(f_x)$ from Example 3.7 is $\langle x \rangle$.

Proof. Consider $y, y' \in \text{im}(f)$. Then there exist $x, x' \in G$ such that $y = f(x)$ and $y' = f(x')$. Then $yy' = f(x)f(x') = f(xx') \in \text{im}(f)$. The inverse and identity conditions are verified similarly.[16] □

Definition 3.10
The **kernel** of f is

$$\ker(f) \coloneqq \{x \in G : f(x) = e_{G'}\}.$$

Theorem 3.11
The kernel of a homomorphism f is also a subgroup.

Proof. If $x, x' \in \ker(f)$, then $f(xx') = f(x)f(x') = e_{G'}e_{G'} = e_{G'}$, so $xx' \in \ker(f)$. Also, $f(e_G) = e_{G'}$ so $e_G \in \ker(f)$. Lastly, if $x \in \ker(f)$, then $f(x^{-1}) = f(x)^{-1} = e_{G'}^{-1} = e_{G'}$, so $x^{-1} \in \ker(f)$ as well. □

The image and kernel of each of the previous examples can be seen to be subgroups. The fact that f is a homomorphism is imperative to the proofs of either fact, and these two theorems demonstrate that a homomorphism does in fact respect the group structure.

Example 3.12
Consider $\det : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^\times, \times)$. Since the determinant for invertible matrices can take on any nonzero value, the image of the determinant is all of $\mathbb{R}^\times$. The kernel of the determinant is $SL_n(\mathbb{R})$, the special linear group consisting of the $n \times n$ matrices with determinant 1.

Example 3.13
For $\exp : (\mathbb{C}, +) \longrightarrow (\mathbb{C}^\times, \times)$, the image is all of $\mathbb{C}^\times$, and the kernel is $2\pi i\mathbb{Z} \subseteq \mathbb{C}$, since $e^{2\pi ik} = 1$.

Example 3.14
For

$$\varphi : S_n \longrightarrow GL_n(\mathbb{R})$$
$$p \in S_n \longmapsto A_p,$$

the image is the set of permutation matrices in $GL_n(\mathbb{R})$, whereas $\ker(\varphi) = \{e\}$, the identity permutation.

Example 3.15
The image of the sign homoomorphism $\text{sign} = \det \circ \varphi$ is $\{\pm 1\} \in \mathbb{R}^\times$. The kernel defines a new group, called the **alternating group** $A_n \coloneqq \ker(\text{sign})$.

[16]For inverse, consider $y \in \text{im}(f)$. Then there exists x such that $y = f(x)$. From the definition of a homomorphism, $y^{-1} = f(x)^{-1} = f(x^{-1}) \in \text{im}(f)$. For identity, $f(e_G) = e_{G'}$, so $e_{G'} \in \text{im}(f)$.

For example, $A_3 = \{e, (123), (132)\} \subseteq S_3$.

Example 3.16
The kernel of f_x is $\{n : x^n = e_G\}$, which was used in the previous class, and is $d\mathbb{Z}$ where d is the order of x if it is finite, and $\{0\}$ if the order of x is infinite.

Definition 3.17
A mapping $f : G \longrightarrow G'$ is an **isomorphism** if it is a bijective homomorphism.

In some sense, if two groups are isomorphic (that is, if there exists an isomorphism between them), they are essentially the same group, because there are the exact same number of elements and the multiplication relationships between the elements will be exactly the same. Usually, in group theory, groups are considered with respect to the isomorphism classes.

Example 3.18
The exponential map from the real numbers under addition onto the positive real numbers under multiplication

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}_{>0}, \times) \\ t &\longmapsto e^t \end{aligned}$$

is an isomorphism.

Given an isomorphism $f : G \longrightarrow G'$, $f^{-1} : G' \longrightarrow G$ is also an isomorphism, since $f^{-1}(yy') = f^{-1}(y)f^{-1}(y')$. If there exists an isomorphism between G and G', this is denoted as $G \cong G'$.