Lecture 22

Group homomorphisms, kernels, and normal subgroups

22.1 Goals

1. Become familiar with more examples of group homomorphisms.
2. Understand the definition of kernel.
3. Understand that the triviality of the kernel is equivalent to a homomorphism being an injection.
4. Understand the definition and importance of normal subgroups (from the perspective of symmetry of a group).
5. Understand why kernels are normal subgroups.

22.2 Homomorphisms and their utility

Let's recall the definition of group homomorphism:

Definition 22.2.1 (Definition 15.4.1.)**.** Let G and H be two groups. A function $f : G \to H$ is called a *group homomorphism* if for every $g, g' \in G$, we have that $f(gg') = f(g)f(g')$.

In words, a group homomorphism is a function between two groups respecting the group operation of each (i.e., respecting "multiplication"). We have already seen that this barebones definition gives rise to some very nice properties:

Proposition 22.2.2 (Proposition 15.4.2.)**.** Suppose $f : G \to H$ is a group homomorphism. Then:

(a) Let $e_g \in G$ and $e_H \in H$ be the identity elements. Then $f(e_G) = e_H$. (Group homomorphisms respect identity elements.)

(b) For any $g \in G$, $f(g)^{-1} = f(g^{-1})$. (Group homomorphisms respect inverses.)

I originally introduced group homomorphisms as a natural way to try and compare two groups G and H. For example, a group homomorphism $f : G \to H$ could tell us a way in which multiplication in G translates into multiplication in H.

But now that we have some more tools lying around, I can begin to explore other ways in which homomorphisms are useful. Aside from the above motivation (comparing groups), interesting homomorphisms can help us understand deeply insightful structures. Now that we know about conjugation, we can actually link three different ideas:

- Measuring how far $f : G \to H$ is from being an injection. (Kernels.)
- How to destroy "redundancies" in a group action. (Quotient groups.)
- Finding subgroups of G that are preserved under conjugation. (Normal subgroups.)

The relation between these ideas will be the topic of today and next time.

22.3 Examples of group homomorphisms

Example 22.3.1. Let $G = D_{2n}$ be the symmetries of a regular n-gon, and let's label the vertices of the n-gon by numbers $1, 2, \ldots, n$. We let $H = \mathrm{Aut}(\underline{n}) = S_n$ be the set of bijections from $\underline{n}$ to itself. Then, because G acts on the set of vertices of the regular n-gon, we have a homomorphism

$$f : D_{2n} \to S_n.$$

(This is the content of Proposition 17.3.7.) Concretely, a symmetry g of a polygon is sent to the bijection from $\underline{n}$ to itself encoding how g transports the vertices of the polygon. For example, a reflection about the angle bisector at the ith vertex will result in a bijection $f(g)$ that fixes $i \in \underline{n}$.

Example 22.3.2. Fix an integer n. Let $G = \mathbb{Z}$ and $H = \mathbb{Z}/n\mathbb{Z}$. Then there is a group homomorphism

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

sending an integer a to its equivalence class modulo n. Just to get a feel for this: When $n = 3$, the elements $\ldots, -6, -3, 0, 3, 6, \ldots$ are all sent to the element $[0]$ of the codomain.

Example 22.3.3. Let $R \to S$ be a ring homomorphism. As you know, the collection of units $G = R^\times$ is a group. Moreover, because ring homomorphisms respect multiplication, we have an induced function

$$R^\times \to S^\times.$$

As an example, we studied the ring homomorphism $\mathbb{C} \to M_2(\mathbb{R})$ in Section 6.3, by observing that both complex numbers and 2-by-2 matrices act on $\mathbb{R}^2$. We thus have a group homomorphism

$$\mathbb{C} \setminus \{0\} \to GL_2(\mathbb{R})$$

from the set of non-zero complex numbers (under multiplication of complex numbers) to the set of invertible 2-by-2 real matrices (under matrix multiplication).

Here is a new-ish example we haven't discussed explicitly. Let's recall:

Definition 22.3.4. Given a 2-by-2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with real coefficients, define the *determinant of* A to be the number

$$\det(A) = ad - bc.$$

Proposition 22.3.5. Let A and B be two 2-by-2 matrices. Then

$$\det(AB) = \det(A)\det(B).$$

Proof. Let $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, and let's just compute:

$$\begin{aligned}
\det(AB) &= \det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) \\
&= \det\left(\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\right) \\
&= (aa'+bc')(cb'+dd') - (ab'+bd')(ca'+dc') \\
&= ad(a'd'-b'c') + bc(c'b'-d'a') + aa'cb' + bc'dd' - ab'ca' - bd'dc' \\
&= ad(a'd'-b'c') - bc(a'd'-b'c') \qquad (22.3.0.1) \\
&= (ad-bc)(a'd'-b'c') \\
&= \det(A)\det(B).
\end{aligned}$$

□

The fun thing is, the above proof is true regardless of whether a, b, c, d were real numbers, complex numbers, integers, or in any commutative. (We used that multiplication is commutative in the above proof.)

So, let R be any commutative ring. Note that if $A \in GL_2(R)$ is an invertible matrix, it must be that $\det(A)\det(A)^{-1} = \det(I) = 1$. (The determinant of the identity matrix is 1.) In particular, $\det(A) \in R^\times$. So we have:

Corollary 22.3.6. Let R be any commutative ring. Then the determinant is a group homomorphism

$$GL_2(R) \to R^\times.$$

Remark 22.3.7. In fact, one can define the notion of determinant for n-by-n matrices with $n \geq 1$. It remains true that $\det(AB) = \det(A)\det(B)$ in this generality, though the typical proof of this is far slicker than the brute-force computation of Proposition **??**. The usual proof of that det respects multiplication proceeds by proving that there exists exactly one function from $M_n(R) \to R$ that respects addition and scaling of columns in a matrix (i.e., is multilinear in the columns), and that sends the identity to 1, and that switches signs when columns are swapped (i.e., is skew-symmetric). It turns out to follow formally that the determinant must then be multiplicative.

Example 22.3.8. When $R = \mathbb{R}$, we have a group homomorphism

$$\det : GL_2(\mathbb{R}) \to \mathbb{R}^\times.$$

When $R = \mathbb{Z}$, we have a group homomorphism

$$\det : GL_2(\mathbb{Z}) \to \mathbb{Z}^\times = \{1, -1\}.$$

When $R = \mathbb{Z}/3\mathbb{Z}$, we have a group homomoprhism

$$\det : GL_2(\mathbb{Z}/3\mathbb{Z}) \to (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}.$$

22.4 How far is a group homomorphism from being an injection?

22.4.1 Kernels

As you know, for any function f (not necessarily a group homomorphism), we can ask whether f is an injection. Even before the idea of groups, whether f is an injection or not told us about potential "redundancies" of the function. For example, if f is not an injection, then there must exist two non-equal elements x, x' of the domain for which $f(x) = f(x')$. So in some sense, f wants to encode a loss of information: applying f makes the domain "forget" how to distinguish x from x'.

This intuition becomes even clearer when you think about a group action of G on X. As we've seen a few times now, if G acts on a set X, we auomatically have a group homomorphism

$$f : G \to \mathrm{Aut}(X).$$

Now, suppose that we have two elements g, g' that are sent to the same element of the codomain. This means that g and g' act *the exact same way* on elements of X. In other words, they encode the exact same symmetry of X. Thus, it appears that—when understanding symmetries of X—this group action has some redundancies.

A very special kind of redundancy is if a non-trivial element of G acts trivially on X. In other words, if $gx = x$ for all $x \in X$. Put judgmentally, g is useless. It performs the exact same action that e does, so why keep it around? Note that g is such a "useless" element of G precisely when $f(g) = e$; in other words, when f sends g to the identity element of $\mathrm{Aut}(X)$.

Of course, there are group homomorphisms that do not have target given by $\mathrm{Aut}(X)$. So let's more generally consider a group homomorphism

$$f : G \to H.$$

Again, we can ask whether some elements of G are rendered "useless" by f; in other words, whether if there is any $g \in G$ for which $f(g) = e_H$.

Note that whether there are non-trivial elements of G that are sent to e_H simultaneously measures: (i) whether some elements of G are rendered useless by f, and (ii) whether f is an injection (because if $f(g) = f(e)$ and $g \neq e$, we know f is not an injection).

We give a name for elements that map to e in the codomain:

Definition 22.4.1 (Kernel)**.** Let $f : G \to H$ be a group homomorphism. The *kernel* of f, denoted $\ker(f)$, is the set of all elements of G that are sent to e_H under f. Put another way, the kernel of f is the preimage of e_H. So

$$\ker(f) = f^{-1}(\{e_H\}) = \{g \in G \mid f(g) = e_H\}.$$

Remark 22.4.2. The kernel always contains the identity of G. Indeed, if f is a group homomorphism, we've already seen that $f(e_G) = e_H$.

22.4.2 Examples of kernels

Example 22.4.3. In the example of $f : D_{2n} \to S_n$, what would it mean for a symmetry of a polygon to do nothing on all vertices? Well, this would mean that the symmetry of the polygon does nothing on the entire polygon. In particular, the pre-image of e_{S_n} is exactly $e_{D_{2n}}$. So here, $\ker(f) = \{e_{D_{2n}}\}$ consists of exactly one element; this is an example of a *trivial* kernel, as kernels always have at least one element (Remark 22.4.2).

Example 22.4.4. In the example of $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, which integers are sent to 0 modulo n? Precisely the multiples of n. Thus,

$$\ker(f) = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}.$$

You may recognize this as the ideal $n\mathbb{Z}$. So this is an example where the kernel is not trivial (i.e., contains more than just the identity of the domain).

Example 22.4.5. For an arbitrary commutative ring R, the kernel of the determinant $\det : GL_2(R) \to R^\times$ may be hard to write down explicitly. Regardless, the kernel gets a special name (that you've seen in notes from previous lectures):

$$\ker(\det) = SL_2(R).$$

In other words, the kernel of the determinant is the set of all 2-by-2 matrices whose determinant equals 1. In the case of $R = \mathbb{Z}/3\mathbb{Z}$, there are 24 elements in this kernel. I am too lazy to write them all out, so please be content with the example of $R = \mathbb{Z}/2\mathbb{Z}$, where the special linear group has only 3 elements:

$$SL_2(\mathbb{Z}/2\mathbb{Z}) = \{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}.$$

22.4.3 Kernels detect whether a homomorphism is an injection

A priori, there may be other ways in which f could be not an injection (for example, perhaps there is only one element that maps to e, but multiple elements mapping to some other $h \in H$). But it turns out that when f is a group homomorphism, this cannot happen: Whether things map redundantly to e_H is enough to determine whether f is an injection:

Proposition 22.4.6. Let $f : G \to H$ be a group homomorphism. Then the following are equivalent:

(a) f is an injection.

(b) $\ker(f) = \{e_G\}$.

Proof. Suppose f is an injection. Then if $f(g) = f(e_G)$, we conclude that $g = e_G$. On the other hand, if f is a group homomorphism, we know that $f(e_G) = e_H$. Thus, the kernel of f consists only of e_G.

To prove the converse, suppose that $f(g) = f(g')$; we give this element a name, say h. Because f is a group homomorphism, we know that $f(g^{-1}) = h^{-1}$. Using that f is a group homomorphism again, we conclude

$$f(g^{-1}g') = f(g^{-1})f(g') = h^{-1}h = e_H.$$

In other words, $g^{-1}g' \in \ker(f)$. By assumption, this means $g^{-1}g' = e_G$. Multplying both sides on the left by g, we conclude $g' = g$. □

22.5 Kernels are subgroups

So kernels can be useful to see whether a function f is an injection (Proposition 22.4.6). It's nice when useful things are not just useful, but also have properties that make them easy to understand. Kernels are quite nice.

Proposition 22.5.1. Let $f : G \to H$. Then $\ker(f)$ is a subgroup of G.

Proof. We have already seen that $e_G \in \ker(f)$, so it remains to check that $\ker(f)$ is closed under multiplication and inverses. Every fact we'll need for the proof is found in Proposition 15.4.2.

If $g \in \ker(f)$, then $f(g) = e_H = (e_H)^{-1} = f(g^{-1})$. Thus $g^{-1} \in \ker(f)$.

If $g, g' \in \ker(f)$, then $f(gg') = f(g)f(g') = e_H e_H = e_h$. So $gg' \in \ker(f)$. □

22.6 Normal subgroups

Now, let's recall from our past lectures (Proposition 21.4.1) that every group acts on itself by conjugation:

$$C_g : G \to G, \qquad C_g(x) = gxg^{-1}.$$

(Now that there is a group H floating around in the background thanks to the homomorphism $f : G \to H$, I am writing x instead of h for the element of G being acted on.)

In particular, G acts on $\mathcal{P}(G)$ (Proposition 21.2.3). Concretely, this action takes any subset A and sends A to

$$C_g(A) = \{x' \in G \,|\, x' = gxg^{-1} \text{ for some } x \in A.$$

For simplicity, we will often write

$$C_g(A) = gAg^{-1}.$$

We caution that gAg^{-1} is a *subset* of G (not an element).

Let's think a little about what this action does when A is not just a subset of G, but a *subgroup* H.

Proposition 22.6.1. Let $H \subset G$ be a subgroup, and fix $g \in G$. Then

$$gHg^{-1}$$

is a subgroup of H.

Proof. gHg^{-1} contains e because H does ($geg^{-1} = e$) and gHg^{-1} is closed under inverses:

$$(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

where the last statement follows because H is a subgroup (hence contains h^{-1}). And gHg^{-1} is also closed under multiplication:

$$(ghg^{-1})(gh'g^{-1}) = g(hh')g^{-1} \in gHg^{-1}.$$

Again at the end, we have used that H is a subgroup (so $h, h' \in H \implies hh' \in H$). □

Definition 22.6.2. Let $H, H' \subset G$ be subgroups. If there exists some $g \in G$ for which $H' = gHg^{-1}$, we say that *H' is conjugate to H*.

Remark 22.6.3. As usual, H' is conjugate to H if and only if H is conjugate to H'. Indeed, whether two subgroups are conjugate determines an equivalence relation on the set of all subgroups of G.

Remark 22.6.4. Let's again remember that conjugation is a canonical symmetry of G. In other words, for every $g \in G$, the map $C_g : G \to G$ is some bijection of G that preserves all group-theoretic properties.

So if H and H' are conjugate subgroups, this means that H and H' look identical up to a natural symmetry of G itself; and they share all properties one could possibly dream of sharing. Put another way, up to symmetry of G, conjugate subgroups are indistinguishable.

So, a subgroup H is *very* special if it is not identical to any other. In other words, if H is only conjugate to itself, we know that H—as a subgroup of G—is incredibly unique. There is no natural symmetry of G that takes H to another group. Such subgroups are so special they have a name:

Definition 22.6.5. A subgroup $H \subset G$ is called *normal* if $gHg^{-1} = H$.

Remark 22.6.6. In analogy to symmetries of a polyhedron, finding a normal subgroup H of G is like finding a face of a polyhedron that is always taken to itself, regardless of the symmetry of the polyhedron. Certainly such a face occupies a special role in the geometry of the polyhedron. Note that the face need not be unmoved—it could be rotated into itself—and that there could be more than one such face.

Likewise, even if H is normal, it may be that conjugation *moves* elements of H—e.g., it is possible that $ghg^{-1} \neq h$—but the point is that $gHg^{-1} = H$ regardless. Likewise, one may have more than one normal subgroup in a group.

Warning 22.6.7. Being "normal" is not a property that makes sense to ask of an group H, normal is a property applying to subgroups of a given group G. That is, "being a normal subgroup" is a concept only meaningfully defined when we also specify the parent group. So, strictly speaking, we should always write "H is a normal subgroup of G" to be most explicit.

As you know, checking that two sets A and B are the same can be tedious—we have to check $A \subset B$ and $B \subset A$. When checking whether $H = gHg^{-1}$, there are some shortcuts. As you read the proposition below, note that these shortcuts are rather obvious if H is finite, so these shortcuts are mainly useful when H is not finite:

Proposition 22.6.8. Let $H \subset G$ be a subgroup, and fix $g \in G$. Then the following are equivalent:

(a) For every $g \in G$, $H = gHg^{-1}$.

(b) For every $g \in G$, $H \subset gHg^{-1}$.

(c) For every $g \in G$, $H \supset gHg^{-1}$.

Proof. It is obvious that the first condition implies the last two. So it suffices to show that (b) implies (a), and that (c) implies (a).

Assume (b). Fix $g \in G$. We seek to show that $gHg^{-1} \subset H$. For this, given some element $k = ghg^{-1} \in gHg^{-1}$, using (b) for g^{-1} to conclude $h = g^{-1}h'g$. This shows

$$k = g(g^{-1}h'g)g^{-1} = h' \in H.$$

The proof of (c) is similar. □

22.6.1 Examples of normal subgroups

Here are some examples of normal subgroups, straight from the definition.

Example 22.6.9. Let A be an abelian group. Then any subgroup of A is a normal subgroup. (Make sure you verify this.)

Example 22.6.10. Let G be a group. Then the trivial subgroup $\{e\}$ is normal. Likewise, G itself is a normal subgroups.

Finally, let Z be the center of G (Definition 21.4.8). Then Z is a normal subgroup of G.

22.7 Kernels are normal subgroups

Proposition 22.7.1. Let $f : G \to H$ be a group homomorphism. Then $\ker(f)$ is a normal subgroup of G.

Proof. It suffices to show that, for every $g \in G$, $g \ker(f) g^{-1} \subset \ker(f)$ (Proposition 22.6.8).

So, given $k \in \ker(f)$, observe:

$$f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g)e_H f(g)^{-1} = f(g)f(g)^{-1} = e_H.$$

This completes the proof. □

22.7.1 Not all subgroups are kernels

Let's just see some examples that not all subgroups are normal subgroups. In particular, not every subgroup arises as the kernel of a group homomorphism.

Example 22.7.2. Let $G = S_3$. Consider the subgroup generated by the element (12):

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

(Note this group only has two elements because (12) is an element of order 2.) Then H is not normal. For example, conjugation by $g = (23)$ takes H to

$$gHg^{-1} = \{e, (13)\}.$$

Evidently, H and gHg^{-1} are not the same subset. Note that, in a group like $G = S_n$, it is straightforward (if tedious) to check whether a given group is normal. The reason is that we have a very concrete description of what conjugation in G looks like (Theorem 19.5.1).

22.8 Exercises: All about the quaternion group

In math, the word "quaternions" can refer to two kinds of things: (i) A non-commutative ring isomorphic to $\mathbb{R}^4$ additively (see Section 6.8), and (ii) A group of 8 elements (which sits inside the group of units of the ring of quaternions). We will explore the latter in this exercise.

Definition 22.8.1. The quaternion group Q_8 is a set with 8 elements denoted by

$$\{1, -1, i, -i, j, -j, k, -k\}.$$

One endows Q_8 with a group operation for which 1 is the identity element, and for which the following relations hold:

$$i^2 = j^2 = k^2 = -1, \qquad ij = k, \qquad (-1)^2 = 1.$$

It is a tedious-to-verify result that there is a unique multiplication on Q_8 satisfying these relations.

Exercise 22.8.2. Fill in the multiplication table of Q_8:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1								
-1								
i								
$-i$								
j								
$-j$								
k								
$-k$								

Exercise 22.8.3. We are now going to write down every subgroup of Q_8.

(a) Let $\langle i \rangle$ denote the subgroup of Q_8 generated by i. Show this is a subgroup of order 4.

(b) Let $\langle j \rangle$ denote the subgroup of Q_8 generated by j. Show this is a subgroup of order 4.

(c) Let $\langle k \rangle$ denote the subgroup of Q_8 generated by k. Show this is a subgroup of order 4.

(d) Let $\langle -i \rangle$ denote the subgroup of Q_8 generated by i. Show that $\langle -i \rangle = \langle i \rangle$.

For the rest of this exercise, you may assume that $\langle -j \rangle = \langle j \rangle$ and $\langle -k \rangle = \langle k \rangle$.

(e) Let $\langle -1 \rangle$ denote the subgroup of Q_8 generated by -1. Show this is a subgroup of order 2.

(f) Now prove that any subgroup of Q_8 must be trivial, or be one of the subgroups above, or equal Q_8 itself. (Hint: Suppose $H \subset Q_8$ is a subgroup. If H is cyclic, it is equal to one of the group above, because you've classified every subgroup generated by one element. If H is not cyclic, argue that H must have order at least 5; now use Lagrange's Theorem to conclude H must have order 8.)

Exercise 22.8.4. (a) You wrote down all 6 subgroups of the quaternion group in the previous exercise. Which of these are normal subgroups?

(b) We've seen that if G is an abelian group, then every subgroup of G is normal. Show that the converse is false. (That is, show that there exists some non-abelian group G all of whose subgroups are normal.)

Exercise 22.8.5. Which of the 6 subgroups you determined is the center of Q_8?