Math 417 – Thirteenth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 23, 2020

We briefly talked about automorphisms on Monday, which are a special kind of isomorphism. Today, I want to talk about a generalization, the homomorphism. An isomorphism between two groups is a kind of mirror image. A homomorphism is more of a shadow. In addition, it has an unexpected connection with cosets.

Suppose $(G, *_G)$ and $(H, *_H)$ are two groups. The map $\phi : G \to H$ is called a *homomorphism* if, for all $g_1, g_2 \in G$, we have

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

We do not care about one-to-one or onto; if ϕ is a bijection between G and H, then it is also an isomorphism, but we do not assume this.

There is always a homomorphism between any two groups, but it might not be very interesting – if $\phi(g) = e_H$ for every $g \in G$, then ϕ is a homomorphism, because $e_h *_H e_H = e_H$.

If $G_1 < G$ is a subgroup of G, there is always a homomorphism from $G_1 \to G$ called the *inclusion* homomorphism, defined by $\phi(g) = g$. This isn't so interesting either.

Related to every homomorphism are two sets, which we'll later show are groups. The first is $Im(\phi) \subseteq H$, or the *image* of ϕ:

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

The second is $Ker(\phi) \subseteq G$, or the *kernel* of ϕ. (I'm not sure why it's called the kernel.) In matrix theory, this is the nullspace.

$$Ker(\phi) = \{g \in G \mid \phi(g) = e_H\}.$$

It will turn out that, not only is $Ker(\phi)$ a subgroup of G, but its cosets have a particularly nice property. More later.

First a few examples. Let $G_1 = (\mathbb{Z}/2\mathbb{Z}, \oplus)$ and $G_2 = (\mathbb{Z}/6\mathbb{Z}, \oplus)$. (Equivalently, G_1 is the cyclic group $C_2 = \langle a \rangle, a^2 = e$ and G_2 is the cyclic group $C_6 = \langle b \rangle, b^6 = e$.)

Define $\phi_1 : G_1 \to G_2$ as follows:

$$\phi_1([0]_2) = [0]_6, \quad \phi_1([1]_2) = [3]_6.$$

Since $[0]_2 \mapsto [0]_6$, the only thing you need to check is

$$\begin{aligned} \phi_1([1]_2 + [1]_2) = \phi_1([2]_2) = \phi_1([0]_2) = [0]_6 \\ = [3]_6 + [3]_6 = \phi_1([1]_2) + \phi_1([1]_2). \end{aligned}$$

So ϕ_1 is a homomorphism.

We have $Im(\phi) = \{[0]_6, [3]_6\}$ and $Ker(\phi) = \{[0]_2\}$.

Alternatively, $\phi(e) = e, \phi(a) = b^3, Im(\phi) = \{e, b^3\}, Ker(\phi) = \{e\}$.

Now define an unrelated homomorphism $\phi_2 : G_2 \to G_1$ as follows

$$\phi_2([0]_6) = \phi_2([2]_6) = \phi_2([4]_6) = [0]_2;$$
$$\phi_2([1]_6) = \phi_2([3]_6) = \phi_2([5]_6) = [1]_2.$$

That is, $\phi_2([i]_6) = [i]_2$. You should try to persuade yourself that this is a homomorphism, and we'll soon have an explanation why it always works.

The operation is "well-defined": $i \equiv j \mod 6 \implies i \equiv j \mod 2$. (This would not work with 6 replaced by 5: $\phi([i]_5) = [i]_2$ isn't even a function, because $[0]_5 = [5]_5$, but $[0]_2 \neq [5]_2$.)

We have $Im(\phi) = \{[0]_2, [1]_2\}$ and $Ker(\phi) = \{[0]_6, [2]_6, [4]_6\}$.

In the other version

$$\phi(e) = \phi(b^2) = \phi(b^4) = e, \quad \phi(b) = \phi(b^3) = \phi(b^5) = a,$$

$Im(\phi) = \{e, a\}$, $Ker(\phi) = \{e, b^2, b^4\}$.

Here is a more general and completely typical example of a homomorphism. Suppose G and H are groups and consider the direct product $G \times H$. Define *projection* maps $\phi_G : G \times H \to G$ and $\phi_H : G \times H \to H$ by:

$$\phi_G((g,h)) = g, \qquad \phi_H((g,h)) = h.$$

You are just taking the first (or second) component of the ordered pair. These are homomorphisms immediately from the definition of

$$(g_1, h_1) *_{G \times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

In this case, $Im(\phi_G) = G, Ker(\phi_G) = \{(e_G, h) : h \in H\}$, and similarly for ϕ_H. Always remember that the kernel is in the group you start with and the image is in the group you end with.

Two more examples: suppose $G = \mathbb{Z}$ and $H = \mathbb{Z}/n\mathbb{Z}$ as usual. Define ϕ by

$$\phi(m) = [m]_n$$

In other words, we map the integer m to m mod n. What is $Im(\phi)$? It's all of H, because $\phi(j) = [j]_n$ for $0 \leq j \leq n-1$, so we get everything. What is $Ker(\phi)$? Unpack this: what gets mapped to the identity in H; namely, $[0]_n$? It's the integers which are $\equiv 0$ mod n. That is, $Ker(\phi) = n\mathbb{Z}$.

Suppose $n \mid r$, and to be precise, $r = dn$. Then there is a homomorphism $\phi : \mathbb{Z}/(dn)\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, defined by $\phi([a]_{dn}) = [a]_n$. First, we have to check that this is well-defined:

$$[a]_{dn} = [b]_{dn} \implies dn \mid b-a \implies (b-a) = dns$$
$$\implies n \mid b-a \implies [a]_n = [b]_n$$

Once you know that this is well-defined, you only have to check the operation:

$$\phi([a]_{dn} + [b]_{dn}) = \phi([a+b]_{dn}) = [a+b]_n$$
$$= [a]_n + [b]_n = \phi([a]_{dn}) + \phi([b]_{dn}).$$

This is ϕ_2 above with $dn = 6$ and $n = 2$.

Now, a (probably unsurprising) general result.

THEOREM If ϕ is a homomorphism from G to H, then $\phi(e_G) = e_H$, and for every $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.

PROOF Since ϕ is a homomorphism, and e_G and e_H are the respective identities,

$$e_H *_H \phi(e_G) = \phi(e_G) = \phi(e_G *_G e_G) = \phi(e_G) *_H \phi(e_G).$$

By cancellation, $e_H = \phi(e_G)$. But now for $g \in G$,

$$e_H = \phi(e_G) = \phi(g *_G g^{-1}) = \phi(g) *_H \phi(g^{-1});$$

that is, $\phi(g)$ and $\phi(g^{-1})$ are inverses in H.

Using this information, we can quickly establish that $Im(\phi)$ and $Ker(\phi)$ are groups.

THEOREM If $\phi : G \to H$ is a homomorphism, then $Im(\phi)$ is a subgroup of H.

PROOF Since $e_H = \phi(e_G)$, $Im(\phi)$ contains the identity.
If $h_1, h_2 \in Im(\phi)$, then there exist $g_1, g_2 \in G$ so that $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$, hence

$$h_1 *_H h_2 = \phi(g_1) *_H \phi(g_2) = \phi(g_1 *_G g_2) \in Im(\phi).$$

Thus, $Im(\phi)$ is closed under $*_H$.
Finally, if $h \in Im(\phi)$, then $h = \phi(g)$, so $h^{-1} = \phi(g^{-1}) \in Im(\phi)$: that is, $Im(\phi)$ contains inverses. □

THEOREM If $\phi : G \to H$ is a homomorphism, then $Ker(\phi)$ is a subgroup of H.

PROOF First, $\phi(e_G) = e_H \in Ker(\phi)$. If $g_1, g_2 \in Ker(\phi)$, then $\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) = e_H *_H e_H = e_H$, so $g_1 *_G g_2 \in Ker(\phi)$ as well. Finally, if $g \in Ker(\phi)$, then $\phi(g^{-1}) = (\phi(g))^{-1} = e_H^{-1} = e_H$, so $g^{-1} \in Ker(\phi)$. □

Not only is $Ker(\phi)$ a subgroup of G, but its cosets have a very special property.

In the following, I write $K = Ker(\phi)$ and will no longer explicitly write $*_G$ and $*_H$; the correct subscript always can be found by context.

THEOREM Suppose $\phi : G \to H$ is a homomorphism with kernel K. Then for $a \in G$,

$$aK = Ka = \{g \in G \mid \phi(g) = \phi(a)\}.$$

In other words, the left coset aK and the right coset Ka are equal to the preimage of $\phi(a)$; those elements in G which are mapped to $\phi(a)$.

PROOF If $x \in aK$, then $x = ak$, for some $k \in K$. Since ϕ is a homomorphism,

$$\phi(x) = \phi(ak) = \phi(a)\phi(k) = \phi(a)e_H = \phi(a).$$

(If $x \in Ka$, then $x = ka$, and the same proof goes through.)

Conversely, if $\phi(x) = \phi(a)$, then we can write $x = a(a^{-1}x)$, and

$$\phi(a) = \phi(x) = \phi(a(a^{-1}x)) = \phi(a)\phi(a^{-1}x) \implies \phi(a^{-1}x) = e_H$$

Thus, $a^{-1}x \in Ker(\phi) = K$, so $x \in aK$.

Similarly, we can write $x = (xa^{-1})a$, show that $xa^{-1} \in K$, so $x \in Ka$. □

The coset decomposition of G by K is determined by the values taken by ϕ. The fact that $aK = Ka$ for all a will be very significant!

Let's return to two of the examples. We had $\phi_2 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by

$$\phi_2([0]_6) = \phi_2([2]_6) = \phi_2([4]_6) = [0]_2;$$
$$\phi_2([1]_6) = \phi_2([3]_6) = \phi_2([5]_6) = [1]_2.$$

As previously noted, $K = Ker(\phi_2) = \{[0]_6, [2]_6, [4]_6\}$, and the cosets of K are

$$[0]_6 + K = \{[0]_6, [2]_6, [4]_6\} = \phi_2^{-1}(0),$$
$$[1]_6 + K = \{[1]_6, [3]_6, [5]_6\} = \phi_2^{-1}(1).$$

We also had $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\phi(m) = [m]_n$, and saw that $Ker(\phi) = n\mathbb{Z}$. The cosets are $i + n\mathbb{Z} = [i]_n = \{m : m \equiv i \mod n\}$, as we've already seen.

Now a very important definition: if $G_1 \leq G$ is a subgroup, then G_1 is called a *normal* subgroup if $aG_1 = G_1a$ for every $a \in G$ (in words, "if every left coset of G_1 is also a right coset.") This does *not* mean that $ag = ga$ for every $g \in G_1$, but it does mean that the cosets are equal *as sets*.

The symbol for being a normal subgroup is $G_1 \trianglelefteq G$.

There are now three cases in which we know that $G_1 \trianglelefteq G$.

(i) If G is abelian, then $ag = ga$, so $aG_1 = G_1a$, element by element.

(ii) We just proved that if $\phi : G \to H$ is a homomorphism, then $Ker(\phi) \trianglelefteq G$.

What we will prove soon is the converse: if $G_1 \trianglelefteq G$, then there exists a group H and a homomorphism $\phi : G \to H$ so that $Ker(\phi) = G_1$. The group H will actually consist of the cosets of G_1.

(iii) There is one more case of normal subgroups that we've already discussed. Suppose $G_1 \leq G$ and $[G : G_1] = 2$. We've already seen a description of the two cosets of G_1:

$$G = eG_1 \cup aG_1 \implies aG_1 = G \setminus G_1;$$
$$G = G_1e \cup G_1a \implies G_1a = G \setminus G_1 \implies G_1a = aG_1.$$

The left cosets and the right cosets are each $\{G_1, G \setminus G_1\}$.

Can we find a homomorphism of G whose kernel is G_1? Sure! Let $H = C_2 = \{e, u\}, u^2 = e$ (fixed from the lecture!) and define:

$$\phi(g) = e \quad \text{if } g \in G_1, \qquad \phi(g) = u \quad \text{if } g \notin G_1$$

Write $G = G_1 \cup aG_1 = G_1 \cup G_1a$.

If $g_1, g_2 \in G_1$, then $g_1g_2 \in G_1$, and

$$e = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = ee. \qquad \checkmark$$

If $g_1 \in aG_1$ and $g_2 \in G_1$, then $g_1 = ag_3$, with $g_3 \in G_1$, so $g_1g_2 = (ag_3)g_2 = a(g_3g_2) \in aG_1$ and

$$u = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = ue. \qquad \checkmark$$

If $g_1 \in G_1$ and $g_2 \in aG_1 = G_1a$, then $g_2 = g_3a$, with $g_3 \in G_1$, so $g_1g_2 = g_1(g_3a) = (g_1g_3)a \in G_1a = aG_1$ and

$$u = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = eu. \qquad \checkmark$$

Finally, if $g_1 \in G_1a$ and $g_2 \in G_1a = aG_1$, then $g_1 = g_3a$ and $g_2 = ag_4$, with $g_3, g_4 \in G_1$, so

$$u^2 = e = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = u^2. \qquad \checkmark$$

You can also think of the multiplication table as being divided in two, with all the elements of G_1 in the left half and upper half, and the elements of aG_1 in the right half and lower half, and you get blocks like we've seen with S_3 and D_4.

It is helpful to have the following small result:

LEMMA If $a \in G$, $L = \{e, a\}$ is a normal subgroup of G if and only if $a^2 = e$ and, for every $g \in G$, $ag = ga$.

PROOF The condition $a^2 = e$ is necessary and sufficient for $\{e, a\}$ to be a subgroup, because by closure, $a^2 \in L$, and $a^2 = a = ae$ is impossible.

Now for $g \in G$, consider the left coset $gL = \{g, ga\}$ and the right coset $Lg = \{g, ag\}$. If these are equal, then $ga = ag$.

Conversely, if $ga = ag$ for all g, then every left coset of L is a right coset. □

Since every subgroup of an abelian group is normal, it's interesting to look at non-abelian groups. So far, we only know two of these: S_3 and D_4.

Through the miracle of cut and paste, here is S_3 again:

$$\rho_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (123),$$

$$\rho_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23),$$

$$\mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3).$$

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

We've already seen that the proper subgroups of S_3 are $\{\rho_0, \rho_1, \rho_2\}$, which has order $3 = \frac{6}{2}$, and so is normal, and $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$, which have order 2.

In the first case, the cosets of $\{\rho_0, \rho_1, \rho_2\}$ are itself and the remaining elements $\{\mu_1, \mu_2, \mu_3\}$. As a reminder, in a normal subgroup, a left and a right coset are considered equal, even if the products aren't equal as you go along:

$$(\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2) = (\mu_1, \mu_2, \mu_3)$$
$$(\rho_0\mu_1, \rho_1\mu_1, \rho_2\mu_1) = (\mu_1, \mu_3, \mu_2).$$

We actually already know a homomorphism from $S_3 \to C_2 = \{e, a\}$, defined by

$$\phi(\rho_i) = e, \qquad \phi(\mu_i) = a,$$

Since $\rho_i\rho_j = \rho_k$, $\mu_i\mu_j = \rho_\ell$, $\rho_i\mu_j = \mu_m$, $\mu_i\rho_j = \mu_n$, we have that ϕ is a homomorphism. As an interpretation, if you think of S_3 as a symmetry of the triangle, the μ_i's flip the front and the back, and the ρ_i's don't and a is the motion of the flip.

You may also vaguely remember that for the subgroups of order two, the left and right cosets are different. Here is an example with $G_1 = \{\rho_0, \mu_3\}$ and $a = \rho_1$:

$$aG_1 = \{\rho_1\rho_0, \rho_1\mu_3\} = \{\rho_1, \mu_2\}$$
$$G_1a = \{\rho_0\rho_1, \mu_3\rho_1\} = \{\rho_1, \mu_1\}.$$

These are different, so by our theorem, there is no homomorphism whose kernel is exactly $G_1 = \{\rho_0, \mu_3\}$. (Or, by (iv), because $\rho_1\mu_3 \neq \mu_3\rho_1$.)

I'll talk about D_4 in class, but here's something to think about. We already have found three subgroups of D_4 of order $4 = \frac{8}{2}$, and so they are normal. The question is: what is another way of describing these groups in terms of the motions of the square. We already know that $\{\rho_0, \rho_1, \rho_2, \rho_3\}$ represents the rotations, that keep the front and back in place. Can you describe the other two?