Math 417 – Fourteenth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 25, 2020

A couple more general things about homomorphisms.

THEOREM If $\phi : G \to H$ is a homomorphism from the group G to the group H, then for $n \geq 2$ and $g_j \in G$,

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

PROOF The proof is by induction on n. The base case is $n = 2$, and comes from the definition of homomorphism. Assuming the result is true for n, then

$$\begin{aligned}
&\phi(g_1 *_G g_2 *_G \cdots *_G g_n *_G g_{n+1}) = \\
&\phi((g_1 *_G g_2 *_G \cdots *_G g_n) *_G g_{n+1}) = \\
&\phi(g_1 *_G g_2 *_G \cdots *_G g_n) *_H \phi(g_{n+1}) \\
&= (\phi(g_1) *_H \phi(g_2) *_H \cdots *_H \phi(g_n)) *_H \phi(g_{n+1}) \\
&= \phi(g_1) *_H \phi(g_2) *_H \cdots *_H \phi(g_n) *_H \phi(g_{n+1}). \quad \square
\end{aligned}$$

There is a bit of confusion about the relationship between isomorphisms and homomorphisms, so here is the connection.

THEOREM If $\phi : G \to H$ is a homomorphism from the group G to the group H, then ϕ is an isomorphism if and only if $Ker(\phi) = \{e_G\}$ and $Im(\phi) = H$.

PROOF For ϕ to be an isomorphism, it needs to be a bijection from G to H and satisfy $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$.

The second criterion is automatic with a homomorphism. Also, by definition, ϕ is onto if and only if $Im(\phi) = G$. If ϕ is one-to-one, then, since $\phi(e_G) = e_H$, it must be the only element that goes to e_H; that is, $Ker(\phi) = \{e_G\}$.

Conversely, suppose $Ker(\phi) = \{e_G\}$ and $\phi(g_1) = \phi(g_2) \in H$. Then $\phi(g_1^{-1}) = \phi(g_1)^{-1} \in H$, and

$$\phi(g_1^{-1} *_G g_2) = \phi(g_1^{-1}) *_H \phi(g_2) =$$
$$\phi(g_1)^{-1} *_H \phi(g_2) = \phi((g_1)^{-1}) *_H \phi(g_1) = e_H,$$

so $g_1^{-1} *_G g_2 \in Ker(\phi)$. Thus $g_1^{-1} *_G g_2 = e_G$, and so, by multiplying on the left by g_1, we get $g_2 = g_1$. That is, $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2$, so ϕ is injective, or one-to-one. □

Suppose $\phi : G \to H$ is a homomorphism. Then it is relatively easy to show that ϕ preserves the subgroup structures of both G and H.

THEOREM If $G_1 < G$, then

$$\phi(G_1) := \{\phi(g) \ : \ g \in G_1\}$$

is a subgroup of H.

PROOF We know the drill. Since $e_G \in G_1$, $\phi(e_G) = e_H \in \phi(G_1)$. If $h_1, h_2 \in \phi(G_1)$, then there exist $g_1, g_2 \in G_1$ so that $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$. Since G_1 is a subgroup, $g_1 *_G g_2 \in G_1$, so $\phi(G_1)$ contains

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) = h_1 *_H h_2,$$

thus $\phi(G_1)$ is closed under the operation of H. Finally, if $h \in \phi(G_1)$, then $h = \phi(g)$ for some $g \in G_1$. Thus $\phi(g^{-1}) = (\phi(g))^{-1} \in \phi(G_1)$. □

THEOREM If $H_1 \leq Im(\phi)$, then the inverse image of H_1

$$\phi^{-1}(H_1) := \{g \in G \mid \phi(g) \in H_1\}$$

is a subgroup of G.

PROOF. Again, H_1 is a subgroup, so $e_H \in H_1$ and $\phi(e_G) = e_H$ implies that $e_G \in \phi^{-1}(H_1)$. If $g_1, g_2 \in \phi^{-1}(H_1)$, then $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$, with $h_1, h_2 \in H_1$. Since $h_1 *_H h_2 \in H_1$ and $\phi(g_1 *_G g_2) = h_1 *_H h_2 \in H_2$, it follows that $g_1 *_G g_2 \in \phi^{-1}(H_1)$. And if $g \in \phi^{-1}(H_1)$, then $\phi(g) \in H_1$, so $\phi(g)^{-1} = \phi(g^{-1}) \in H_1$, so $g^{-1} \in \phi^{-1}(H_1)$. □

The next theorem is one you will probably think is obvious, but it needs to be written. It's kind of boring, to be sure.

THEOREM If G, H, K are groups and $\phi_1 : G \to H$ is a homomorphism and $\phi_2 : H \to K$ are both homomorphisms, then the composition map $\phi : G \to K$ defined by $\phi(g) = \phi_2(\phi_1(g))$ is also a homomorphism.

PROOF For clarity, if $g \in G$, then $\phi_1(g) \in H$ so $\phi_2(\phi_1(g)) \in K$. All we have to do is check that products go through. This will be true because the intermediate maps are homomorphisms. For $g_1, g_2 \in G$,

$$\phi(g_1 *_G g_2) = \phi_2(\phi_1(g_1 *_G g_2)) = \phi_2(\phi_1(g_1) *_H \phi_1(g_2))$$
$$= \phi_2(\phi_1(g_1)) *_K \phi_2(\phi_1(g_2)) = \phi(g_1) *_K \phi(g_2).$$

Thus, ϕ is a homomorphism. □

As a remark, this result can be generalized to chain homomorphisms with more than three groups by an even-more boring induction that will be omitted.

COROLLARY Suppose G_1 and G_2 are groups with an isomorphism $\Phi_G : G_1 \to G_2$ and H_1 and H_2 are groups with an isomorphism $\Phi_H : H_1 \to H_2$. Suppose also that $\phi : G_1 \to H_1$ is a homomorphism, then there is an *induced* homomorphism $\phi' : G_2 \to H_2$, defined for $g \in G_2$

$$\phi'(g) = \Phi_H(\phi(\Phi_G^{-1}(g))).$$

PROOF Yes, I know this looks horrible, but let's keep track of things: $g \in G_2$ so $\Phi_G^{-1}(g) \in G_1$ (notice that $\Phi_G : G_1 \to G_2$ is a bijection, so it has an inverse $\Phi_G^{-1} : G_2 \to G_1$.) Once we know that $\Phi_G^{-1}(g) \in G_1$, then we can apply our homomorphism $\phi : G_1 \to H_1$ and $\phi(\Phi_G^{-1}(g)) \in H_1$. The last function is Φ_H which takes this to H_2. This is then an example of the last theorem, with a composition of three homomorphisms. □

By switching the indices, any homomorphism $\tilde{\phi} : G_2 \to H_2$ can be made to induce a homomorphism $\tilde{\phi}' : G_1 \to H_1$.

Why do we do this?

We have talked about homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$, but these are isomorphic to the cyclic groups C_n and C_m respectively, and I'd rather talk about homomorphisms with the cyclic groups, because later in the semester we'll be talking about *ring* homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$, and it can get confusing otherwise.

This turns out to be a number-theoretic question. What are the possible homomorphisms from one cyclic group to another? To be specific, suppose $G = C_n = \langle a \rangle, a^n = e_G$ and $H = C_m = \langle b \rangle, b^m = e_H$.

In any case, we know that $\phi(e_G) = e_H$. Define ϕ_k by $\phi_k(a) = b^k$, where $0 \leq k \leq m-1$. (Since $\phi(a) \in H$, it has to be a power of b.) Then the property of homomorphisms implies that

$$\phi_k(a^2) = \phi_k(aa) = \phi_k(a)\phi_k(a) = b^k b^k = b^{2k},$$
$$\phi_k(a^3) = \phi_k(a^2 a) = \phi_k(a^2)\phi_k(a) = b^{2k} b^k = b^{3k},$$

and so on. It is easy to establish by induction that

$$\phi_k(a^r) = b^{kr} \implies \phi_k(a^r * a^s) = \phi_k(a^{r+s})$$
$$= b^{k(r+s)} = \phi_k(a^r)\phi_k(a^s).$$

So we're fine, except that we have to check that we actually have a well-defined map. That is, is it true that

$$a^r = a^s \implies \phi(a^r) = \phi(a^s) \iff b^{kr} = b^{ks}?$$

Now $a^r = a^s \iff r \equiv s \mod n \iff n \mid s - r$, and $b^{kr} = b^{ks} \iff kr \equiv ks \mod m \iff m \mid ks - kr = k(s - r)$. This is a number-theory problem. When does $n \mid s - r$ imply $m \mid k(s - r)$?

The hypothesis is that $n \mid s - r$; that is, $s - r = nt$ for some integer t. The conclusion is

$$m \mid k(s - r) = knt$$

for all t. In particular, it holds for $t = 1$; that is, $m \mid kn$, and if $m \mid kn$, then $m \mid knt$ for all t.

Putting this together, we have now proved

THEOREM The homomorphisms from C_n to C_m are given precisely by $\phi(a^r) = b^{kr}$, under the condition that $m \mid kn$.

For example, if $n = 6$ and $m = 4$, the choice for k is $k \in \{0, 1, 2, 3\}$, and we want to know when $4 \mid 6k$.

Since C_k is isomorphic to $\mathbb{Z}/k\mathbb{Z}$, this will also tell us all homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$. We saw in Wednesday's Worksheet Problem with $n = 6$ and $m = 4$, that a homomorphism exists for $k = 0, 2$ and not $k = 1, 3$.

There is one special case with an interesting result.

COROLLARY If $gcd(m, n) = 1$, then the only homomorphism from C_n to C_m is the trivial one.

PROOF As we've seen, $\phi(a^r) = b^{kr}$, but we need $m \mid kn$. Since $gcd(m, n) = 1$, a property of relatively prime integers is that $m \mid kn \implies m \mid k$, so $k = um$, and for every r,

$$\phi(a^r) = b^{kr} = b^{umr} = (b^m)^{ur} = e_H^{ur} = e_H$$

In other words, the only homomorphism maps everything to the identity. □

The full story is a bit messy.

COROLLARY Suppose $gcd(m, n) = g$, then the homomorphisms from C_n to C_m are given precisely by $\phi(a^r) = b^{kr}$, under the condition that k is a multiple of m/g. There are exactly g such homomorphisms.

PROOF Write $m = gm'$ and $n = gn'$, where $gcd(m', n') = 1$. The condition $m \mid kn$ is equivalent to

$$\frac{kn}{m} \in \mathbb{Z} \iff \frac{kgn'}{gm'} \in \mathbb{Z} \iff \frac{kn'}{m'} \in \mathbb{Z} \iff m' \mid kn'.$$

But $gcd(m', n') = 1$, so this last condition is that k is a multiple of

$$m' = \frac{m}{g} = \frac{m}{gcd(m, n)}.$$

Since $0 \leq k < m$ and $k = im'$, $0 \leq im' < m = gm'$, so $0 \leq i < g$ and $i \in \{0, 1, \ldots, g-1\}$. □

On the last Worksheet, k is a multiple of $\frac{4}{gcd(4,6)} = 4/2 = 2$, as we saw. If we had wanted homomorphisms from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/6\mathbb{Z}$ instead, then k must be a multiple of $\frac{6}{gcd(6,4)} = 6/2 = 3$: $k = 0, 3$.

The final topic will continue on Monday. Suppose that A and B are subsets of a group $(G, *)$, which might be finite or infinite. The *set product* $A * B$ is defined as

$$A = \{a_i\}, \quad B = \{b_i\} \implies A * B = \{a_j * b_k\}.$$

Usually, G will be finite, but there will be one simple and important exception later.

Suppose now that G is a group and $N \trianglelefteq G$ is a normal subgroup: for every $a \in G$, $aN = Na$; that is, every left coset is a right coset.

LEMMA If $N \trianglelefteq G$ is a normal subgroup, then for every $g \in G$ and $x \in N$, there exists $y \in N$ so that $g * x = y * g$; that is, $g * x * g^{-1} = y \in N$.

PROOF Consider the coset gN. By hypothesis, $g * x \in gN$, but $gN = Ng$, so $g * x \in Ng$. This means that $g * x = y * g$ for some $y \in N$. We can solve for y by multiplying by g^{-1} on the right: $(g * x) * g^{-1} = (y * g) * g^{-1} = y * (g * g^{-1}) = y \in N$. □

If G is abelian, then $y = g * x * g^{-1} = g * g^{-1} * x = x$, and this is no big deal. Matrix fans will recognize conjugation.

THEOREM Under the definition of set products, if $N \trianglelefteq G$ and aN and bN are two cosets of N, then $(aN) * (bN) = (a * b)N$.

(This is an amazing theorem. If $|N| = t$, then aN and bN each have t elements, and we'd expect t^2 products, not t. Please note n is a group element, not a natural number!)

PROOF If $x \in (a * b)N$, then $x = (a * b) * n$ for some $n \in N$. Thus $x = (a * e_G) * (b * n) \in (aN) * (bN)$. This shows that $(a * b)N \subseteq (aN) * (bN)$.
To prove the other direction, suppose $x \in (aN) * (bN)$. Then there exist $n_1, n_2 \in N$ so that $x = (a * n_1) * (b * n_2)$. By the Lemma, $n_1 * b = b * n_3$ for some $n_3 \in N$, and we then use associativity:

$$(a * n_1) * (b * n_2) = a * (n_1 * b) * n_2 = a * (b * n_3) * n_1$$
$$= (a * b) * (n_3 * n_1) \in (a * b)N \quad \square$$

Here is an example from a friendly group. Let $G = C_6 = \langle a \rangle$, $a^6 = e$ and let $N = \langle a^3 \rangle = \{e, a^3\}$. Since G is abelian and N is a subgroup, it is a normal subgroup. The cosets of N are:

$$N = a^3N = \{e, a^3\},\ aN = a^4N = \{a, a^4\},\ a^2N = a^5N = \{a^2, a^5\}.$$

I won't do all the products, but I hope you can see that

$$N * aN = \{a, a^4, a^4, a^7\} = \{a, a^4, a^4, a\} = \{a, a^4\} = aN$$

and

$$aN * a^2N = \{a^3, a^6, a^6, a^9\} = \{a^3, e, e, a^3\} = \{e, a^3\} = a^3N = N$$

The next step is to prove that this definition can be used to define a group whose elements consist of the cosets of N with the operation done above. That will have to wait for Monday.

Back to D_4:

$$\rho_0 = \begin{pmatrix} 1234 \\ 1234 \end{pmatrix} = (1)(2)(3)(4) \quad \rho_1 = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix} = (1234),$$

$$\rho_2 = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix} = (13)(24) \quad \rho_3 = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix} = (1432),$$

$$\mu_1 = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} = (14)(23),$$

$$\delta_1 = \begin{pmatrix} 1234 \\ 3214 \end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix} 1234 \\ 1432 \end{pmatrix} = (1)(24)(3),$$

You may recall that we found that $N = \{\rho_0, \rho_2\}$ is a normal subgroup of D_4 and we had a special version of the multiplication table of D_4.

D_4	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_2	ρ_2	ρ_0	ρ_3	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_1	ρ_1	ρ_3	ρ_2	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_3	ρ_3	ρ_1	ρ_0	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	μ_2	δ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	μ_1	δ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	δ_2	μ_1	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	δ_1	μ_2	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

The cosets of N are N, $\rho_1 N$, $\mu_1 N$, $\delta_1 N$ and the elements in the products of the cosets occupy the 2×2 blocks of the 8×8 multiplication table. This is what the products look like

$\circ$	N	$\rho_1 N$	$\mu_1 N$	$\delta_1 N$
N	N	$\rho_1 N$	$\mu_1 N$	$\delta_1 N$
$\rho_1 N$	$\rho_1 N$	N	$\delta_1 N$	$\mu_1 N$
$\mu_1 N$	$\mu_1 N$	$\delta_1 N$	N	$\rho_1 N$
$\delta_1 N$	$\delta_1 N$	$\mu_1 N$	$\rho_1 N$	N

Each entry above represents a 2×2 square. If the coset is $\{x, y\}$, then the square is one of the following two entries

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \quad \text{or} \begin{pmatrix} y & x \\ x & y \end{pmatrix}.$$

This sure looks like V to me.