Math 31 Lesson Plan

Day 25: Quotient Groups and Homomorphisms

Elizabeth Gillaspy

November 7, 2011

Supplies needed:

- Colored chalk
- Quizzes
- Homework

Goals for Students:

Students will:

- Understand what a quotient group is (elements and operation)
- Gain more practice with isomorphisms
- See a novel use of induction (Theorem 11.7)
- See a connection between normal subgroups and kernels

[**Lecture Notes: Write everything in blue, and every equation, on the board. [Square brackets] indicate anticipated student responses. *Italics* are instructions to myself.**]

- *Quizzes!*
- *Return HW*

On Friday we started proving Theorem 11.7: If G is a finite abelian group, and p is a prime that divides $|G|$, then G has a cyclic subgroup of size p.

We will prove this Theorem using induction on the size of G. Last time, we proved that G has a normal subgroup $H = \langle x \rangle$ such that G/H and H are both smaller than G. We also proved that if p divides $|H|$, then H has a subgroup P of size p, and since $P \leq H \leq G$, it follows that $P \leq G$ is a subgroup of G.

Case 2: $p \mid |G/H|$ In this case, we use the inductive hypothesis: Since $|G/H| < |G|$, we know that G/H has a subgroup, $P \leq G/H$, of size p. Any group of prime order is cyclic by Theorem 10.5, so $P = \langle Hg \rangle$ for some $g \in G$. Since P has order p, we know that $(Hg)^p = Hg^p = He = H$, but this tells us that $g^p \in H$.

Since G is finite, we know that $o(g)$ is also finite. Write $o(g) = m$. Then, $o(g^p) = \frac{m}{(m,p)}$ must divide m. Write $o(g^p) = k$. I claim that $o(g^k) = p$. Why do you think I might want to prove this? *Think-pair-share* Showing this will prove that the cyclic subgroup $\langle g^k \rangle \leq G$ has size p by Corollary 4.7.

Since $o(g^p) = k$, we have $g^{pk} = e$, and hence $(g^k)^p = e$. Are we done? [no] Therefore, $o(g^k) \leq p$. So, suppose $o(g^k) = n < p$. Then $g^{kn} = e$ and $kn < kp = m = o(g)$, which contradicts the fact that $m = o(g)$. Therefore, $o(g^k) = p = |\langle g^k \rangle|$, so G has a cyclic subgroup of order p as claimed. $\square$

Looking back at this proof, why do we need p to be prime? [so that we can guarantee that

p divides one of $|G/H|$ or $|H|$.] Why do we need G to be abelian? [so that any subgroup of G will be normal.]

Any questions about Theorem 11.7?

Kernels and Normal Subgroups

Who remembers what the kernel of a homomorphism is?

DEFINITION: The *kernel* of a homomorphism $\phi : G \to H$ is

$$\ker \phi = \{g \in G : \phi(g) = e_H\}.$$

There's actually a connection between the normalizer of a subgroup, that set $N(H)$ htat you were working on for a starred problem last week, and normal subgroups.

In fact, PROPOSITION: Let G and H be groups, and let $\phi : G \to H$ be a homomorphism. The the normalizer $N(\ker \phi) = G$. skip if short on time

Who can remind me of the definition of the normalizer?

$$N(\ker \phi) = \{a \in G : aga^{-1} \in \ker \phi \ \forall \ g \in \ker \phi\}$$

So what do I have to show? **Proof:** If $a \in G$ is arbitrary, I want to show that $\phi(aga^{-1}) = e_H$ for any $g \in \ker \phi$. But,

$$\phi(aga^{-1}) = \phi(a)\phi(g)\phi(a)^{-1} = \phi(a)e_H\phi(a)^{-1} = e_H.$$

Therefore, $a \in N(\ker \phi)$, and since $a \in G$ was arbitrary, we have that $N(\ker \phi) = G$ as claimed. $\square$

There's another way to phrase this result in the terminology we've been using recently. Can anyone tell me how? [$\ker\phi \lhd G$]

Observe that $N(H)$ is the subgroup of G consisting of all elements of G that treat H as if it were a normal subgroup: $gHg^{-1} = H$. In other words, the normalizer $N(H)$ is the largest subgroup of G in which H is normal. So we have another criterion for normality:

A subgroup $H \leq G$ is normal iff $N(H) = G$.

Questions?

OK, back to Section 13.

What does the Fundamental Theorem of Homomorphisms say?

[Fund Thm Let G, K be groups. If $\phi : G \to K$ is an epimorphism, then $G/\ker\phi \cong K$.]

We want to use this Theorem to prove Theorem 13.3 Let $\phi : G \to K$ be an onto homomorphism. Then we have a one-to-one correspondence between subgroups of K, and subgroups of G that contain $\ker\phi$. Moreover, if $H \leq G$ contains $\ker\phi$, then $H \lhd G$ iff $\phi(H) \lhd K$.

Proof: To prove the first statement, we will prove that

1. If $H_1 \leq G$ contains $\ker\phi$, then $\phi(H_1) \leq K$
2. If $H_2 \leq K$, and we define $\phi^{-1}(H_2) := \{g \in G : \phi(g) \in H_2\}$, then $\phi^{-1}(H_2) \leq G$.

Questions?

Please grab a partner, or a group of three, and work on proving this. *Discuss at board afterwards?*

Therefore, every subgroup of K can be written as $\phi(H)$ for some $H \leq G$ such that H contains $\ker \phi$.

Questions?

Now, to prove the second statement, we must also prove two things: What are they? *Think-pair-share*

1. If $H_1 \lhd G$ contains $\ker \phi$, then $\phi(H_1) \lhd K$.
2. If $H_2 \lhd K$, then we know that $H_2 = \phi(H_1)$ for some $H_1 \leq G$ such that H_1 contains $\ker \phi$. We must show that $H_1 \lhd G$.

To prove (1), let $k \in K, h \in H_1$. We want to show that $k\phi(h)k^{-1} \in \phi(H_1)$. Since ϕ is onto, we can assume that $k = \phi(g)$ for some $g \in G$. But then,

$$k\phi(h)k^{-1} = \phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) = \phi(h_1),$$

for some $h_1 \in H_1$, because $H_1 \lhd G$.

To prove (2), suppose that $H_1 \leq G$ satisfies $\phi(H_1) = H_2 \lhd K$. We want to show that if $g \in G, h \in H_1$, then $ghg^{-1} \in H_1$. In other words, we want to show that $\phi(ghg^{-1}) \in H_2$. But,

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} \in H_2,$$

since $\phi(h) \in H_2$ and H_2 is normal. Hence $ghg^{-1} \in H_1$ so $H_1 \lhd G$ as claimed. $\square$

Skip pf if short on time

Note that if $H \leq G$ is *any* subgroup, and $\phi : G \to K$ is any homomorphism, then $\phi(H) \leq K$. This is Theorem 12.6(i). However, we only get the 1-1 correspondence indicated in Theorem 13.3 if H contains $\ker \phi$ and ϕ is onto.

do this!

For example, let $\rho : D_4 \to D_4/\langle 180 \rangle$ be the quotient projection. Since $\langle 180 \rangle H = \{H, V\} = \langle 180 \rangle V$, we see that ρ takes $\langle V \rangle = \{0, V\}$ and $\langle H \rangle = \{0, H\}$ to the same subgroup of $D_4/\langle 180 \rangle$:

$$\rho(\langle V \rangle) = \{\langle 180 \rangle, \langle 180 \rangle V\} = \rho(\langle H \rangle).$$

Also, $\rho(\{0, 180, H, V\}) = \rho(\langle V \rangle)$. So there are many subgroups of D_4 that map to the same subgroup of $D_4/\langle 180 \rangle$, but only one of them contains $\langle 180 \rangle = \ker \rho$.

The other point that a lot of people had questions about was Theorem 13.5.

Suppose $H \lhd K \lhd G$ and $H \lhd G$. Then $K/H \lhd G/H$, and

$$\frac{G/H}{K/H} \cong G/K.$$

Proof: So what are these things in question? [Note that G/H is the collection of right cosets of H by elements of G; K/H is the collection of right cosets of H by elements of K; and G/K is the collection of right cosets of K by elements of G.] *Draw a picture!*

Why is $K/H \leq G/H$? *Think-pair-share* Basically, $K/H \leq G/H$ because $K \leq G$. More precisely, recall that if $k_1, k_2 \in K$, then $k_1k_2 \in K$ because $K \leq G$; and also $k_1^{-1}, k_2^{-1} \in K$. Therefore,

$$Hk_1 * Hk_2 = Hk_1k_2 \in K/H.$$

Moreover, observe that if $k_1 \in K$, then $Hk_1^{-1} = (Hk_1)^{-1}$ in both K/H and G/H:

$$Hk_1^{-1} * Hk_1 = H(k_1^{-1}k_1) = He = H,$$

which is the identity element of G/H and of K/H.

Hence, if $Hk_1, Hk_2 \in K/H$, then so is their product and inverse. Therefore, $K/H \leq G/H$ as claimed.

To see that $K/H \lhd G/H$, what should we do? Let $g \in G$ and $k \in K$ and consider the element $HgHk(Hg)^{-1} \in G/H$. We want to show that this coset is actually in K/H. Skip if short on time

---

However, by our observations above,

$$HgHk(Hg)^{-1} = HgHkHg^{-1} = Hgkg^{-1}$$

by the definition of the multiplication in G/H. Since $K \lhd G$, what can we conclude? [$gkg^{1-} \in K$, and therefore $Hgkg^{-1} \in K/H$ as claimed.]

To see that $\frac{G/H}{K/H} \cong G/K$ as claimed, we will use the Fundamental Theorem. So in other words, what am I going to do? That means we need to define a homomorphism $\phi : G/H \to G/K$ and show that its kernel is K/H. This will imply that $K/H \lhd G/H$.

We define $\phi : G/H \to G/K$ by $\phi(Hg) = Kg$. What do we need to check? We must now check that:

1. ϕ is well defined: that is, if $Hg = Hg'$ then $Kg = Kg'$ too.
2. ϕ is a homomorphism.
3. ϕ is onto.
4. $\ker \phi = K/H$.

Please divide into four groups (so 5-6 people per group). *label each group with a number* Please work on figuring out your proof in your groups; make sure it's clear enough that you'll be able to present it at the board! If you finish early, work on the other proofs.

Example of Theorem 13.5: Let's return to the D_4 example.

Let $G = D_4, H = \langle 180 \rangle, K = \langle 90 \rangle$. Take a second to convince yourself that these subgroups satisfy the conditions of the theorem. Talk to your neighbor if you want.

- What are the elements of G/H? G/K? K/H?