Math 31 Lesson Plan

Day 24: Quotient Groups and Homomorphisms

Elizabeth Gillaspy

November 4, 2011

Supplies needed:

- Colored chalk

Goals for Myself:

- Watch the time!!

Goals for Students:

Students will:

- Understand what a quotient group is (elements and operation)
- Gain more practice with isomorphisms
- Get a deeper (visual) sense for why normal subgroups are desirable
- See a novel use of induction (Theorem 11.7)
- Begin to 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.**]

Announce reading for Monday; next homework

Agenda: Today I want to return to the quotient group $\mathbb{Z}/3\mathbb{Z}$ from Wednesday, and talk about a visual way to tell if a subgroup is normal. Then we'll have you guys look at some examples of factor groups.

I decided that I do want to prove Theorem 11.7 in class; yes it's long and hard, but it's good to do hard things sometimes. So we'll do that, then we'll talk about Kernels and normal subgroups to pave the way for Section 13, which we'll be discussing on Monday.

Any questions before we get started?

I want to return to the group $\mathbb{Z}/3\mathbb{Z}$ that we talked about on Wednesday.

- What are the elements of this group?
- What is the group operation?

Think-pair-share

While students are thinking, draw outline of Cayley table for $\mathbb{Z}/3\mathbb{Z}$ on board. This is going to be the Cayley table for $\mathbb{Z}/3\mathbb{Z}$. I'd like you guys to come up to the board and complete it. If you think you know what element should go into one of the boxes, please come up and write it on the board! 12:45

In general, if $H \lhd G$ then we can make the right cosets of H into a group, which we write G/H. The group operation is $Ha * Hb = Hab$.

In this case, What familiar group is $\mathbb{Z}/3\mathbb{Z}$ isomorphic to? [$\mathbb{Z}_3$] What's the isomorphism? *think-pair-share if necessary* The map $\phi : \mathbb{Z}_3 \to \mathbb{Z}/3\mathbb{Z}$ given by $\phi(n) = 3\mathbb{Z} + n$ is an isomorphism. To see this, what do we have to check?

Proof: We must check that ϕ is a 1-1 and onto homomorphism. To see that ϕ is a homomorphism, observe that

$$\phi(n+m) = 3\mathbb{Z} + (n+m) = (3\mathbb{Z} + n) + (3\mathbb{Z} + m) = \phi(n) + \phi(m).$$

Observe that if $n+m \geq 3$, then $n+m$ mod 3 is in the same coset as $n+m$ itself, so the above equations are still true even if $n+m \geq 3$.

To see that ϕ is 1-1, suppose that $\phi(n) = \phi(m)$. We want to show that $n = m$ in $\mathbb{Z}_3$. But if $\phi(n) = \phi(m)$, that means that $3\mathbb{Z} + n = 3\mathbb{Z} + m$, and therefore $n - m \in 3\mathbb{Z}$. In other words, $3|(n-m)$, and hence $n - m = 0$ in $\mathbb{Z}_3$. It follows that $n = m$ in $\mathbb{Z}_3$ as claimed.

To see that ϕ is onto, observe that $3\mathbb{Z} + 0, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2$ are the three different cosets of $3\mathbb{Z}$, and each of these is the image of some element (0, 1, and 2 respectively) of $\mathbb{Z}_3$. $\square$ 12:55

Your book explains in words and symbols why the right cosets of H in G only form a group if $H \lhd G$. I'd like to explain visually.

Recall that on Wednesday, we looked at the normal subgroup $H = \{e, (123), (132)\} \lhd S_3$ and showed that the cosets of H divided the Cayley table of S_3 into nice boxes. Moreover, the color-coding into boxes told us the Cayley table of the quotient S_3/H. *Draw a rough sketch of the picture; don't fill in all the elements of S_3.*

Look back in your notes from Wednesday – What familiar group is S_3/H isomorphic to? [S_3/H is isomorphic to $\mathbb{Z}_2$, because the Cayley tables are the same:] *Draw Cayley table for $\mathbb{Z}_2$*

Let's look at what happens when we try to do this same breakdown into boxes for a non-normal subgroup. Let $K = \langle (12) \rangle \leq S_3$. Is K normal? K is not a normal subgroup. What are the right cosets of K? The right cosets of K are

$$\{e, (12)\}, \{(13), (132)\}, \{(23), (123)\}.$$

If we color-code those cosets on the top and side of the Cayley table, can we also color-code the interior into boxes? *Highlight cosets inside Cayley table; show overlap*

The fact that in this case, we don't get a neat division into boxes, means that we can't make a group out of the cosets! if we zoom out, the color-coded picture doesn't look like the Cayley table of a group.

Your book explains in words and symbols why we can't make a group out of the cosets of a subgroup if the subgroup isn't normal; I'm not going to discuss that right now, so that we can move on to other things. But please come see me in office hours if it doesn't make sense after rereading it! 1:05

Questions about quotient groups?

Please get back into groups of 3 or 4. Please get up, stretch your legs, move around, and find a group with someone that you haven't worked with yet. In your groups, I want you to look at some Examples of quotient groups: In each case, what familiar group is G/H isomorphic to?

1. $H = \{e\} \times \mathbb{Z}_4, G = S_3 \times \mathbb{Z}_4$
2. $H = \langle 180 \rangle, G = D_4$
3. $H = \langle (2, 2) \rangle, G = \mathbb{Z} \times \mathbb{Z}$
4. $H = SL(2, \mathbb{R}), G = GL(2, \mathbb{R})$

Discuss first two examples as a class, but not others if pressed for time. 1:15.

THEOREM 11.7 *If G is a finite abelian group, and $p \mid |G|$ is a prime, then G has a subgroup of size p.*

Proof: We will prove the Theorem by induction on the size of G. If $|G| = 1$, then no primes divide the size of G, so the Theorem is trivially true.

Let $|G| = n$ and suppose that for any group K such that $|K| < n$, the statement of the Theorem holds. So, what are we assuming?

WLG we can suppose $|G| \geq 2$. Therefore, G has an element $x \neq e$. Consider $\langle x \rangle \lhd G$ — call it H. Why is $H \lhd G$? [Because G is abelian so any subgroup of G is normal.] Since $H \lhd G$, we can form the quotient group G/H.

By Lagrange's Theorem, $|G| = [G : H]|H| = |G/H|\,|H|$, since $|G/H|$ is the number of distinct cosets of H in G. Since $|H| > 1$, both G/H and H are groups that have fewer elements than G.

If p is prime, and $p \mid |G|$, then Euclid's Theorem (4.3) tells us that either $p \mid |H|$ or $p \mid |G/H|$.

Case 1: $p \mid |H|$ In this case, by Theorem 5.5, since H is cyclic it must have a cyclic subgroup of size p — call it P. Since $P \leq H$ and $H \leq G$, it follows that $P \leq G$.

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

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

We proved on Monday that the kernel of a homomorphism $\phi : G \to H$ is a subgroup of G.

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

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 $N(H) = G$.