Math 417 – Fifteenth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 28, 2020

We're going to continue with two of the main ideas from last week. Suppose $K \leq G$ is a subgroup, then K is a normal subgroup ($K \trianglelefteq G$) if $aK = Ka$ for every $a \in G$. By this, we mean that the sets are equal.

We've also proved that the cosets of a normal subgroup have the property that $aK * bK = (a * b)K$. This means that we can take the operation for the group and apply it to the cosets, and it makes sense.

A typical element in aK is $a * k_1$ for some $k_1 \in K$ and a typical element in bK is $b * k_2$ for some $k_2 \in K$. (Just to be clear here: it might be the case that $k_1 = k_2$, but they don't have to be equal.) A typical element in $aK * bK$ is then $(a * k_1) * (b * k_2)$, and we proved that this can be re-written as $(a * b) * k_0$ for some $k_0 \in K$, and so this element is also in $(a * b)K$.

The crucial part of the argument here is that $aK = Ka$, so $x * k_1 \in aK = Ka$ implies that $x * k_1 = k_2 * x$ for some $k_2 \in K$ and $k_3 * y \in Ka = aK$ implies that $k_3 * y = y * k_4$ for some $k_4 \in K$ We'll need this later today.

Every subgroup of an abelian group is a normal subgroup, because the operation is commutative. Also, if $[G : K] = 2$, then $K \trianglelefteq G$. Thus, even though S_3 is not abelian, the subgroup $\{\rho_0, \rho_1, \rho_2\}$ is a normal subgroup, because it has $|S_3|/2 = 6/2 = 3$ elements.

The other big idea from last week was the homomorphism. Suppose G and H are groups. Then ϕ is a homomorphism if it is a map from $G \to H$ with the property that for $g, g' \in G$,

$$\phi(g *_G g') = \phi(g) *_H \phi(g').$$

Associated to each homomorphism are two important sets which we proved were groups, the kernel and the image

$$Ker(\phi) = \{g \in G \mid \phi(g) = e_H\} \subseteq G, \quad Im(\phi) = \{\phi(g) \mid g \in G\} \subseteq H.$$

As we have seen, an isomorphism is a homomorphism from $G \to H$ with the additional conditions that $Ker(\phi) = \{e_G\}$ and $Im(\phi) = H$.

The fact combining these two ideas is that for any homomorphism ϕ from $G \to H$ the kernel is a normal subgroup: $K = Ker(\phi) \trianglelefteq G$. The cosets of K have two descriptions: as a coset, and as the preimage of an element from $Im(\phi)$:

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

One goal today is to prove the converse: that if $K \trianglelefteq G$, then there is a "natural" way to find a group H and a homomorphism ϕ from $G \to H$ such that $Ker(\phi) = K$.

As a simple example, suppose the group G is given and $K = \{e_G\}$. Then we could take $H = G$ and define $\phi(g) = g$ for $g \in G$. Then

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

by the definition above, but $\phi(g) = g$ and $H = G$, so

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

Time for new material. We need to return to normal subgroups. Suppose $K \trianglelefteq G$. Consider the set of cosets $\{aK\}$. . The name of this set is G/K. It is usually called a *quotient* group or a *factor* group.

We have already seen this in one case. Look at the group $G = \mathbb{Z}$, and the normal subgroup $K = n\mathbb{Z}$. (It's normal because G is abelian.) We have already seen the cosets of K in G: these are $\{[a]_n\}$, and I've been calling this $\mathbb{Z}/n\mathbb{Z}$ all semester. Now you know why!

Define an operation $*_{G/K}$ on $H = G/K$ by

$$aK *_{G/K} bK = (a *_G b)K.$$

(Yes, I know it's confusing, because it's basically the same operation on both sides, but it is on different objects.)

THEOREM Under these circumstances, $(G/K, *_{G/K})$ is a group.

PROOF The first thing I need to show is that the operation is well-defined. What do I mean here? Suppose $aK = a'K$ and $bK = b'K$; that is, the cosets are defined differently but are the same sets. Then I want to prove that

$$aK *_{G/K} bK = a'K *_{G/K} b'K$$

That is, $(a *_G b)K = (a' *_G b')K$ as cosets. Since these are both cosets and $a' *_G b' \in (a' *_G b')K$ ($e_G \in K$), if $a' *_G b' \in (a *_G b)K$, then the two cosets have an element in common and so are equal.

This isn't so hard. We've already seen that $xK = yK$ if and only if $y = x *_G k$ for some $k \in K$. So $a' = a *_G k_1$ and $b' = b *_G k_2$ for some $k_1, k_2 \in K$. Thus

$$a' *_G b' = (a *_G k_1) *_G (b *_G k_2) = a *_G (k_1 *_G b) *_G k_2 =$$
$$a *_G (b *_G k_3) *_G k_2 = (a *_G b) *_G (k_3 *_G k_2)$$

Since $k_3 *_G k_2 \in K$, this shows that $a' *_G b' \in (a *_G b)K$.

We have a set and an operation. What's left? Identity, inverses and associativity. These are much easier!

Recall that $K = e_G K \in G/K$, so for every $aK \in G/K$,

$$(e_G K) *_{G/K} (aK) = (e_G *_G a)K = aK,$$
$$aK *_{G/K} e_G K = (a *_G e_G)K = aK,$$

so K is the identity. We now have

$$(a^{-1}K) *_{G/K} aK = (a^{-1} * a)K = e_G K = K,$$

so the inverse of the coset aK is the coset $a^{-1}K$. Finally, and I'm not looking forward to this, for any three cosets aK, bK, cK,

$$(aK *_{G/K} bK) *_{G/K} cK = (a *_G b)K *_{G/K} cK = ((a *_G b) *_G c)K$$
$$aK *_{G/K} (bK *_{G/K} cK) = aK *_{G/K} (b *_G c)K = (a *_G (b *_G c))K.$$

Since G is a group, it is associative, so $(a *_G b) *_G c = a *_G (b *_G c)$, and so we have associativity here. □

We've already seen some examples. I'd like to write out a case I started to talk about last week.
Let $G = S_3$ and let $K = \langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$, which is a cyclic subgroup of order 3. In this case, the group G/K consists of the two cosets of K

$$K = \{\rho_0, \rho_1, \rho_2\}, \ \mu_1 K = \{\mu_1, \mu_2, \mu_3\}.$$

And taking the operation of multiplication as defined, here is the multiplication table of G/K, which is evidently isomorphic to C_2

G/K	$\{\rho_0, \rho_1, \rho_2\}$	$\{\mu_1, \mu_2, \mu_3\}$
$\{\rho_0, \rho_1, \rho_2\}$	$\{\rho_0, \rho_1, \rho_2\}$	$\{\mu_1, \mu_2, \mu_3\}$
$\{\mu_1, \mu_2, \mu_3\}$	$\{\mu_1, \mu_2, \mu_3\}$	$\{\rho_0, \rho_1, \rho_2\}$

A natural question suggested by the notation is that maybe, if we know K and G/K, we can "recover" G. It is true that $|G/K| = |G|/|K|$. Thus, if we take the product of the two groups $K \times G/K$, we get a group that has $|G|$ elements. However, there is no guarantee that it is isomorphic to G.

In this case K is isomorphic to C_3 and S_3/K is isomorphic to C_2 and so $K \times S_3/K$ is isomorphic to $C_3 \times C_2$. Since $gcd(2,3) = 1$, it follows that $C_3 \times C_2$ is isomorphic to $C_{2.3} = C_6$. Thus, in this example $K \times S_3/K$ is isomorphic to C_6 and is not isomorphic to S_3.

Let's throw homomorphisms back into the mix. Suppose $K \trianglelefteq G$ is a normal subgroup of G. Define the homomorphism ϕ_K from $G \to G/K$ by $\phi_K(g) = gK$. Let's check that it's a homomorphism. It takes an element of G and maps it to an element of G/K. What about the product?

$$\begin{aligned}\phi_K(g_1 *_G g_2) &= (g_1 *_G g_2)K = g_1K *_{G/K} g_2K \\ &= \phi_K(g_1) *_{G/K} \phi_K(g_2). \qquad \checkmark\end{aligned}$$

What is the kernel of ϕ_K? We have, from the definition, and the fact that $e_{G/K} = K$, that $Ker(\phi_K)$ is

$$\{g \in G \mid \phi_K(g) = e_{G/K} = K\} = \{g \in G \mid gK = K\} = K.$$

Thus, ϕ_K is a homomorphism whose kernel is K, as promised.

What is the image of ϕ_K?

$$Im(\phi_K) = \{gK \mid g \in G\} = G/K.$$

One final twist, which is the sort of thing you might see in graduate mathematics. Suppose we started with a homomorphism ϕ from $G \to H$ and $K = \ker(\phi)$.

A subtle but important point: ϕ and ϕ_K are not the same homomorphism! We have ϕ mapping $G \to H$ and ϕ_K mapping $G \to G/K$, so the images are different. But there is a natural connection.

Remember that K is defined by ϕ and we know that $aK = \{g \in G \mid \phi(g) = \phi(a)\}$. So let us define a map $\alpha : G/K \to H$ in the only way we could:
$\alpha(aK) = \phi(a) \in Im(\phi) \subseteq H$, which we know is well-defined.

THEOREM With the above definitions, α is an isomorphism from G/K to $Im(\phi)$ and $\phi(g) = \alpha(\phi_K(g))$.

PROOF Let's first do the formula. We have $\alpha(\phi_K(g)) = \alpha(gK) = \phi(g)$. OK, that's good. Now we have to prove that α is an isomorphism. Is it one-to-one?

$$\alpha(aK) = \alpha(bK) \iff \phi(a) = \phi(b) \iff aK = bK.$$

Is it onto? If $h \in Im(\phi)$, then there exists $g \in G$ so that $\phi(g) = h$, and so $\alpha(gK) = h$, so yes, α is onto.

Thus α is a bijection. Finally, we have to check the operation, and use the definitions and the fact that

$$\alpha(aK *_{G/K} bK) = \alpha((a *_G b)K) = \phi(a *_G b) =$$
$$\phi(a) *_H \phi(b) = \alpha(aK) *_H \alpha(bK).$$

We've checked everything, so α is an isomorphism. □

This is called the "Fundamental Homomorphism Theorem". The technical term is that the map from G to H "factors through" G/K.

Let me work it out in another somewhat familiar case. Suppose $G = C_6 = \langle a \rangle, a^6 = e_G$ and $H = C_4 = \langle b \rangle, b^4 = e_H$ and define ϕ by $\phi(a) = b^2$. What we found was that

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

Thus, $K = Ker(\phi) = \{e_G, a^2, a^4\}$ and $Im(\phi) = \{e_H, b^2\}$. So G/K consists of the two cosets $\{K, aK\}$:

$$K = \{e_G, a^2, a^4\}, \quad aK = \{a, a^3, a^5\}$$

Thus, G/K is a cyclic group of order 2, as is $Im(\phi) \subset H$. Here is a picture of the Fundamental Homomorphism Theorem, as it applies to the elements of G, with $g \mapsto \phi_K(g) \mapsto \alpha(\phi_K(g))$:

$$\begin{aligned} e_G &\mapsto K \mapsto e_H, & a &\mapsto aK \mapsto b^2, \\ a^2 &\mapsto K \mapsto e_H, & a^3 &\mapsto aK \mapsto b^2, \\ a^4 &\mapsto K \mapsto e_H, & a^5 &\mapsto aK \mapsto b^2. \end{aligned}$$

There is one more topic in Section 13 that I wanted to mention: a family of isomorphisms for any group, which is interesting only when the group is *not* abelian.

Given a group G and a fixed element $g \in G$. We define i_g or *conjugation by* g to be the map defined by

$$i_g(x) = gxg^{-1}.$$

(This is the book's notation, so I should keep it; I'm working with only one group here, so it's ok to use the juxtaposition ab for the operation $a *_G b$.)

THEOREM For a group G and $g \in G$, i_g is an automorphism of G.

PROOF We have to prove that $i_g : G \to G$ is one-to-one, onto and a homomorphism. First,

$$i_g(x) = i_g(y) \iff gxg^{-1} = gyg^{-1} \iff x = y.$$

The last $\iff$ comes from left cancellation and then right cancellation. Thus, i_g is one-to-one.

It is also easy to check that

$$i_g(g^{-1}xg)) = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1}) = x.$$

so i_g is onto. Finally,

$$i_g(xy) = g(xy)g^{-1} = (gx)(g^{-1}g)(yg^{-1}) = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y),$$

so it's a homomorphism as well. □

Any automorphism which can be defined as a conjugation by g is called an *inner automorphism*.

One limitation with this is that if G is an abelian group, then

$$i_g(x) = gxg^{-1} = xgg^{-1} = xe_G = x,$$

so i_g is the identity.