Lecture 23

Quotient groups and the first isomorphism theorem

23.1 Goals

1. Understand that a subgroup being normal emerges naturally when trying to define a multiplication on a quotient set.

2. Understand the group multiplication on a quotient group.

3. Understand the first isomorphism theorem.

23.2 Recollection of quotient rings

We've already see the idea of "quotient rings" when R is a commutative ring. Recall that when R is a commutative ring and I is an ideal, we could define a set

$$R/I$$

whose elements are equivalence classes of elements in R. Informally, you can think of an element of R/I as a symbol $[x]$ with $x \in R$, and we declare two symbols to be equal, $[x] = [x']$, when $x - x' \in I$. (This is the step at which we "declared" two elements to be equal so long as their difference ended up in some well-behaved subset; in this case, an ideal.)

Then, it turned out that R/I inherits the structure of a ring. One can naively write down

$$[x] + [x'] = [x + x'], \qquad [x][x'] = [xx'],$$

and the convenient result is that these naively written operations actually make sense (i.e., are well-defined). For example, if we replace $[x]$ by the equal $[x + y]$ for some $y \in I$, we find that

$$[x][x'] = [x + y][x'] = [(x + y)x'] = [xx' + yx'] = [xx']$$

where the very last equality follows because $y \in I \implies yx' \in I$ by definition of ideal.

Thus, there is only one part of this quotient ring story that is non-trivial: Verifying that some naively written formula actually makes sense. And this verification required that I be a well-behaved subset (an ideal).

A similar story will emerge for groups. Given a subgroup $H \subset G$, one can not only define a quotient set G/H, we can ask whether this quotient set inherits a multiplication by writing down a naive formula. It will turn out that this naively formula only makes sense when H is a *normal* subgroup of G.

So we see another way in which "normal" arises. (Last time, we saw that kernels had to be normal subgroups, and that normal subgroups were "very unique" subgroups of G.) This time, we see that normalcy is a natural condition that guarantees our ability to identify elements of G while still maintaining a group structure in the result.

23.2.1 Motivation for quotients

Why might we be interested in producing quotient groups? (For quotient rings, we had a natural motivation, called understanding the ring of algebraic functions on an algebraic subset.)

I advocate for the notion of "removing redundancies in a group action." For example, let's say you have a group action $G \times X \to X$. But let's say you learned that 20 elements of G act trivially on X—that is, there exists 20 elements g for which $gx = x$ regardless of $x \in X$. You probably have a feeling that this group action is somehow "inefficient." Quotienting G by those "useless" elements creates a new group, with a new group action on X.

As another motivation, consider a group homomorphism $f : G \to H$. As you know, the kernel of f is the collection of elements in G that are "crushed" by f; or that are all sent to the identity element in H. If we could "quotient out" the kernel, we could hope to retain only the features of G that remain relevant after applying f (because we will have removed all the elements that are sent to the do-nothing element of H).

23.3 Cosets

Let's get started. What do we mean by "declaring two elements of G to be equivalent up to H?"

Notation 23.3.1. Fix a subgroup $H \subset G$. For this lecture, we will define two natural equivalences relations on G. We say

$$g \sim_L g'$$

if and only if there exists some $h \in H$ for which $g = g'h$. (In other words, if g' can be made equal to g at the expense of multiplying by an element of H on the right.) Equivalently, we say $g \sim_L g'$ if and only if $(g')^{-1}g \in H$.

Finally, we write

$$g \sim_R g'$$

if and only if $g = hg'$ for some $h \in H$. Equivalently, we say $g \sim_L g'$ if and only if $g(g')^{-1} \in H$.

Remark 23.3.2. Why are $\sim_R$ and $\sim_L$ equivalence relations? Well, note that $g \sim_L g'$ means that g is in the orbit of g', where G is considered as a set with a *right* action from H:

$$G \times H \to G, \qquad (g, h) \mapsto gh.$$

Of course, "being in the same orbit as" is an equivalence relation.

Likewise, $g \sim_R g'$ means that g is in the orbit of g' under the *left* action of H on G;

$$H \times G \to G, \qquad (h, g) \mapsto hg.$$

We give these equivalences classes, or these orbits, the following names.

Definition 23.3.3. Let $H \subset G$ be a subgroup, and fix $x \in X$. We say that the set

$$xH = \{g \in G \,|\, g = xh \text{ for some } h \in H\} = \{xh \,|\, h \in H\}$$

is a *left coset* of H. Likewise, we say that

$$Hx = \{g \in G \,|\, g = xh \text{ for some } h \in H\} = \{hx \,|\, h \in H\}$$

is a *right coset* of H.

Warning 23.3.4. The left/right distinction is interminably confusing. One just has to get used to it, or look it up all the time. Indeed, a left coset gH can be explained as the orbit of g under a right action by H on G, or as the result of a left action of G on $\mathcal{P}(G)$. It is both a blessing and a curse that xH admits an interpretation in terms of both left and right actions (of different groups on different sets); the curse is that the terminology convention is arbitrary.

Notation 23.3.5. Fix a subgroup $H \subset G$. For this lecture only, we let $[x]_L$ denote the equivalence class of x under $\sim_L$. In other words,

$$[x]_L = [x']_L \iff x = x'h \text{ for some } h \in H.$$

Put another way,

$$[x]_L = xH$$

is the set of all elements obtained from x by multiplying by elements of H on the right (equivalently, by transporting the set H by multiplying by x on the left).

Likewise, we let $[x]_R$ denote the equivalence class of x under $\sim_R$.

Notation 23.3.6. For this lecture only, we define the quotient sets

$$G/_{\sim_L} = \{xH\}.$$

Likewise,

$$G/_{\sim R} = \{Hx\}.$$

Remark 23.3.7. I hope the notation is hammering home the point that, given some subgroup $H \subset G$, there is no single natural notion of quotient set; there is always a left- versus right-handed choice. Moreover, these quotient sets almost never have a natural multiplication on them, unless H is normal. This observation forms the crux of the next section.

23.4 Naive attempts at a product operation on quotient sets: the second coming of normalcy

So, let's try to naively define a multiplication on $G/\sim_L$. That is, can we define an operation as

$$\text{“}[x]_L[y]_L = [xy]_L''?$$

To check that this is well-defined, we must make sure it makes sense as follows: If $[x]_L = [x']_L$, is it still true that $[xy]_L = [x'y]_L$?

So, let $x = x'h$ for some $h \in H$. We are asking whether $xy = x'hy$ and $x'y$ are related by the relation $\sim_L$. This is true if and only if there exists some $h' \in H$ for which

$$x'hy = x'yh'.$$

That is (by multiplying both sides on the right by y^{-1} and dividing both sides on the left by x') we are asking whether, for a given h, there exists an h' for which

$$h = y^{-1}h'y.$$

Upshot: if the "naive" multiplication is to be well-defined on $G/\sim_L$, it must be true that H is a subset of yHy^{-1}. (Does this look familiar? See Proposition 22.6.9.)

Remark 23.4.1. You could ask whether the above multiplication is well-defined in the y variable; i.e., ask what happens when you replace y by some $\sim_L$-equivalent $y' = yh$. Then you would have found that the multiplication is well-defined in the y variable. So, we're seeing some interesting consequences: There really is a "one-sidedness" to this all, and the naive multiplication would be well-defined if the relation behaved well "on both sides."

Okay, well what if we try to define a naive multiplication on $G/\sim_R$ as follows:

$$\text{“}[x]_R[y]_R = [xy]_R.''$$

Is this well-defined? Again, let's check. We know $y \sim_R y' \iff y = hy'$; so we must try to verify that each time we are given some $h \in H$, we have:

$$xy = xhy' \sim_R xy'.$$

Again by definition of $\sim_R$, for the above to hold, there must exist some $h' \in H$ for which

$$xhy' = h'xy'.$$

Then, multiplying both sides on the left by $(y')^{-1}$ and then by x^{-1}, the above equality is equivalent to demanding that

$$xhx^{-1} = h'.$$

In other words, we must demand that, regardless of x and $h \in H$, there must exist some $h' \in H$ for which $xhx^{-1} = h'$. That is, for the naive multiplication to be well-defined, we must have that for every $x \in G$, $xHx^{-1} \subset H$. (Look familiar? See Proposition 22.6.9.)

What we have discovered is:

Proposition 23.4.2. For the naive multiplication on $G/\sim_L$ (or on $G/\sim_R$) to be well-defined, it must be true that—for every $x \in G$—

$$H \subset xHx^{-1} \qquad (\text{or } xHx^{-1} \subset H)$$

But let's now apply the shortcut we learned last time (Proposition 22.6.9). We can conclude the following:

Corollary 23.4.3. Let $H \subset G$ be a subgroup. The following are equivalent:

1. H is a normal subgroup of G.

2. The naive multiplication on $G/\sim_L$ is well-defined.

3. The naive multiplication on $G/\sim_R$ is well-defined.

Let's take a moment to re-cap what just happened. We embarked on journey to try and equate elements of G if they "differ" by an element of H. Here we already found that $\sim_L$ and $\sim_R$ presented two possible ways to make such an equivalence relation. Then we asked whether this journey will allow us to induce a multiplication on the quotient set. Very curiously, This answer was "yes" so long as H satisfies the *normalcy* condition.

There are a few remarkable facts about this discovery. First, I did not motivate the idea of "normal subgroup" by appealing to creating quotients. I motivated it by saying normal subgroups are very special subgroups, as they are always fixed by the natural conjugation action—they are like very special faces of a polyhedron. It is interesting that two questions of different motivations (appeals to symmetry, versus appeals to algebra) lead to a discovery of the same condition (normalcy).

Second, we have the feeling that $\sim_L$ and $\sim_R$ are different equivalence relations. (They are, in general.) So then why does a *single* condition (normalcy) guarantee that both equivalence relations make the naive multiplication well-defined?

Let's settle this once and for all.

Proposition 23.4.4. Let $H \subset G$ be a subgroup. The following are equivalent.

(a) H is a normal subgroup.

(b) $\sim_L = \sim_R$. That is, $x \sim_L x'$ if and only if $x \sim_R x'$.

(c) For every $x \in G$, we have an equality of sets $xH = Hx$.

Remark 23.4.5. In other words, H being normal doesn't just cure the algebraic headache of defining a multiplication on a quotient of G; it also cures the headache of having left- and right-asymmetries! Imagine being the first person to discover this. Things are working too well; so well that you'd be afraid for the whole theory to be trivial. But the fact that there exist normal subgroups in abundance signals that, in fact, this is just a miracle of Mother Nature, and not an idea that is only useful in trivial situations.

Remark 23.4.6. Take a moment to look at both Proposition 22.6.9 and Proposition 23.4.4. Being a normal subgroup is useful not for its consequences, but for the many different ways in which you can characterize it.

Proof of Proposition 23.4.4. Suppose H is a normal subgroup. Then

$$\begin{aligned}
x \sim_L x' &\iff x = x'h \text{ for some } h \in H \\
&\iff x(x')^{-1} = x'h(x')^{-1} \text{ for some } h \in H \\
&\iff x(x')^{-1} = h' \text{ for some } h' \in H \qquad \text{(because } H \text{ is normal)} \\
&\iff x = h'x' \text{ for some } h' \in H \\
&\iff x \sim_R x'.
\end{aligned}$$

This shows (a) implies (b).

Suppose (b) is true. We have already seen that $xH = [x]_L$ is the equivalence class of x under $\sim_L$. Likewise, we know that $Hx = [x]_R$ is the equivalence class of x under $\sim_R$. Thus, (b) implies that $xH = Hx$ for all $x \in X$ (because an equivalence relation determines its equivalence classes).

Finally, assume (c), which in particular means $xH \subset Hx$. This means that for every $x \in X$ and for every $h \in H$, there exists some $h' \in H$ so that $xh = h'x$. By multiplying both sides by x^{-1} on the right, this means that for every $x \in X$ and $h \in H$, we have that $xhx^{-1} = h' \in H$. In other words, $gHg^{-1} \subset H$. By Proposition-22.6.9, we conclude that H is normal. This proves (c) implies (a). □

23.5 Quotient groups

So we have seen that H being a normal subgroup of G is *necessary* to define a natural product on quotient sets of G, and moreover, it *removes the ambiguity* of right- versus left-cosets (because if H is normal, $xH = Hx$ for any $x \in G$). If it feels there is a lot to juggle, just rest assured that a subgroup being normal is first and foremost necessary to define quotient groups; this necessary condition also happens to be convenient.

Definition 23.5.1. Let $H \subset G$ be a normal subgroup. Then the quotient set

$$G/H$$

is defined to be the set of equivalence classes $[x]$ defines by the (equivalent) equivalence relations $\sim_L$ and $\sim_R$. In other words,

$$[x] = [x'] \iff xh = x' \text{ for some } h \in H \quad \iff hx = x' \text{ for some } h \in H.$$

(These relations are the same relation by Proposition 23.4.4.) Finally, we endow G/H with a binary operation as follows:

$$[x][y] := [xy]. \tag{23.5.0.1}$$

(This is well-defined by Corollary 23.4.3.)

We call G/H, together with this multiplication, the *quotient group of G by H* or just *the quotient of G by H*.

Let us justify the term quotient "group":

Proposition 23.5.2. G/H, endowed with the binary operation (23.5.0.1), is a group.

The proof is quite easy once we know that multiplication is well-defined.

Proof. Let $e \in G$ be the identity element of G. I claim $[e]$ is the identity of G/H. Indeed,

$$[x][e] = [xe] = [x], \qquad [e][x] = [ex] = [x].$$

Next, associativity:

$$([x][y])[z] = [xy][z] = [(xy)z] = [x(yz)] = [x][yz] = [x]([y][z]).$$

Finally, I claim that $[x^{-1}] = [x]^{-1}$. To see this, let's compute:

$$[x][x^{-1}] = [xx^{-1}] = [e], \qquad [x^{-1}][x] = [x^{-1}x] = [e].$$

This concludes the proof. □

Remark 23.5.3. Note that Section 23.5 is devoid of any L and R notation. This is because, once H is normal, there is no ambiguity in what we mean by $\sim$.

Notice also that "do x and x' differ by an element of the kernel" also becomes a well-defined question, precisely because $\sim_L = \sim_R$.

23.6 The first isomorphism theorem

One of the motivations of quotient groups was the following: Fix a group homomorphism $f : G \to H$. Then f might not be injective; equivalently, $\ker(f)$ may be non-trivial. We reasoned that, if we "kill off" this redundancy by identifying those elements of G that differ by an element of the kernel, we should be left with exactly the portion of H that f detects. Let's first give a name to this "portion."

Definition 23.6.1. Let $f : G \to H$ be a function. The *image* of f, written $\text{image}(f)$, is the set of all elements in H hit by f. Put another way,

$$\text{image}(f) = \{h \in H \mid \text{ there exists some } g \in G \text{ for which } h = f(g)\}.$$

Proposition 23.6.2. Let $f : G \to H$ be a group homomorphism. Then image(f) is a subgroup of H.

Proof. We know $e_H \in \text{image}(f)$ because $f(e_G) = e_H$.

Next, suppose $h \in \text{image}(f)$. Then there exists $g \in G$ so that $f(g) = h$. Hence $f(g^{-1}) = f(g)^{-1} = h^{-1}$ is also in the image of f. This shows that image(f) is closed under taking inverses.

Finally, if $h, h' \in \text{image}(f)$, choose $g, g' \in G$ for which $f(g) = h$ and $f(g') = h'$. Then

$$hh' = f(g)f(g') = f(gg')$$

so hh' is in the image of f. (It is hit by gg'.)

This completes the proof. □

The following theorem makes our intuition precise:

Theorem 23.6.3 (The first isomorphism theorem)**.** Let $f : G \to H$ be a group homomorphism. Then f induces an isomorphism

$$G/\ker(f) \xrightarrow{\cong} \text{image}(f).$$

Thus, whenever there is a group homomorphism from G to H, one can realize a quotient of G as isomorphic to some subgroup of H.

You will prove this theorem in the exercises.

Remark 23.6.4. Note that you know that $\ker(f)$ is a normal subgroup (Proposition 22.7.1). Thus, you know what we mean by the quotient group $G/\ker(f)$ (Section 23.5).

Example 23.6.5. Let $f : S_3 \to \mathbb{Z}/2\mathbb{Z}$ be the function sending two-cycles to $1 \in \mathbb{Z}/2\mathbb{Z}$, and sending e and three-cycles to 0. You can check that f is a group homomorphism.

Then $\ker(f) = \{e, (123), (132)\}$ and the first isomorphism theorem tells us

$$S_3/\ker(f) \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z}.$$

Example 23.6.6. Let $\det : GL_2(\mathbb{R}) \to \mathbb{R}^\times$ be the determinant homomorphism. The kernel is the set of all matrices with determinant 1, otherwise known as $SL_2(\mathbb{R})$. Note that det is a surjection—given any real number t, the diagonal matrix with diagonal entries $1, t$ has determinant t.

Thus, the first isomorphism theorem tells us that the map

$$GL_2(\mathbb{R})/SL_2(\mathbb{R}) \to \mathbb{R}^\times, \qquad [A] \mapsto \det(A)$$

is a group isomorphism.

(Note that all kinds of non-trivial things have happened here. First, it might not have been so obvious that $SL_2(\mathbb{R})$ is a normal subgroup of $GL_2(\mathbb{R})$. Second, it is even less obvious that one could compute the quotient by $SL_2(\mathbb{R})$ as such a concrete group!)

23.7 Exercises: The first isomorphism theorem

Exercise 23.7.1. Let $f : G \to H$ be a group homomorphism, and suppose $K \subset G$ a normal subgroup. Assume that for every $k \in K$, we have that $f(k) = e_H$.

(a) Show that the function

$$f_{modK} : G/K \to H, \qquad [g] \mapsto f(g)$$

is well-defined. (That is, if $g' \sim g$, prove that $f(g') = f(g)$. Here, $\sim$ is the equivalence relation determined by the normal subgroup K. See Section 23.4.)

(b) Show that image$(f) =$ image(f_{modK}).

(c) If $K = \ker(f)$, show that f_{modK} is an injection.

Exercise 23.7.2. Let $f : G \to H$ be a group homomorphism. Show that the induced function

$$G \to \text{image}(f), \qquad g \mapsto f(g)$$

is a surjection and a group homomorphism.

Exercise 23.7.3. Fix a group homomorphism $f : G \to H$. Prove the first isomorphism theorem (Theorem 23.6.3).