QUOTIENTS AND NORMAL SUBGROUPS

LEO GOLDMAKHER

ABSTRACT. An overview of quotient groups and the importance of normal subgroups.

The goal of this document is to describe how to 'divide' a group by a subgroup. Why would one wish to do this? The hope is that one can decompose big mysterious groups into smaller, simpler groups whose properties might tell us about the big group; in other words, exactly the same reason why we decompose substances into molecules, or whole numbers into products of primes.

As we shall see, given any group G and any subgroup $H \leq G$, one can always create a quotient set G/H. However, this set may or may not be a group. This is reminiscent of quotients of integers; sometimes the answer isn't so nice (e.g. $\frac{60}{7}$), but other times it is (e.g. $\frac{60}{6}$). Under this analogy, subgroups $H \leq G$ are like integers $n \leq N$, and *normal* subgroups $H \trianglelefteq G$ are like integers dividing N. We'll return to this below.

Remark. One comment before we begin. One of the most important breakthroughs in abstract algebra was the realization that the proper notion of two groups being the same is not literal equality, but isomorphism (denoted $\simeq$). For example, the group $\mathbb{Z}_4$ of integers (mod 4) under addition is not literally the same as the group $\{\pm 1, \pm i\}$ under multiplication – they have completely different elements, and even a different operation! But they are isomorphic, which means that any property we can prove about $\mathbb{Z}_4$ as a group can be translated into a property about $\{\pm 1, \pm i\}$, and conversely. This is one of the biggest strengths of abstract algebra: it allows us to ignore the special properties of the elements of a group and focus on the properties of the group as a whole, thus seeing the forest rather than a bunch of individual trees! Thus, whenever we decide that two groups G_1 and G_2 are 'the same', we will write $G_1 \simeq G_2$ rather than $G_1 = G_2$.

1. MOTIVATING EXAMPLES

Recall that the dihedral group of order 8 is

$$D_8 := \{e, r, r^2, r^3, f, rf, r^2f, r^3f\},$$

subject to the relations $r^4 = e, f^2 = e$, and $fr = r^3f$. Interpreted geometrically, these are the symmetries of the square: r represents counterclockwise rotation by $\pi/2$, and f represents reflection across the horizontal axis.

Example 1. Observe that as written above, the first four elements of D_8 form a nice subgroup $H := \{e, r, r^2, r^3\}$:

$$D_8 = \{\underbrace{e, r, r^2, r^3}_{H}, \underbrace{f, rf, r^2f, r^3f}_{Hf}\} = H \sqcup Hf,$$

where $\sqcup$ denotes the disjoint union. Thus we can "factor out H" and write

$$D_8/H = \{[e], [f]\}.$$

(I'm writing brackets around the elements to indicate that this isn't strictly speaking true: you can't *actually* divide one set by another set. We'll discuss a rigorous notion of quotient below.)

The quotient set on the right side looks a lot like the subgroup $K := \{e, f\}$ of D_8, so we might guess

$$D_8/H \simeq K. \tag{1}$$

We could have also factored out K, by writing D_8 in a different order:

$$D_8 = \{\underbrace{e, f}_{K}, \underbrace{r, rf}_{rK}, \underbrace{r^2, r^2 f}_{r^2K}, \underbrace{r^3, r^3 f}_{r^3K}\} = K \sqcup rK \sqcup r^2K \sqcup r^3K.$$

Thus we write $D_8/K = \{[e], [r], [r^2], [r^3]\}$, which leads to the guess

$$D_8/K \simeq H.$$

This is reassuring, in view of (1).

Remark. The process in this example is highly reminiscent of factoring polynomials: by writing the elements of the group in a certain order, we can see a common factor to pull out.

Example 2. Let $I := \{e, r^2\} \leq D_8$. What's D_8/I? Following the pattern set out in the first example, we write the elements of D_8 in an appropriate order:

$$\begin{aligned} D_8 &= \{e, r, r^2, r^3, f, rf, r^2 f, r^3 f\} \\ &= \{\underbrace{e, r^2}_{I}, \underbrace{r, r^3}_{rI}, \underbrace{f, r^2 f}_{fI}, \underbrace{rf, r^3 f}_{rfI}\} \\ &= I \sqcup rI \sqcup fI \sqcup rfI. \end{aligned}$$

(Note that these calculation rely on the fact that r^2 and f commute.) Factoring out I from each of these, we deduce

$$D_8/I = \{[e], [r], [f], [rf]\}.$$

By contrast with the first example, the corresponding set $\{e, r, f, rf\}$ isn't a subgroup of D_8. (For example, it doesn't contain r^2.) We'll discuss this below.

Exercise 1. Show that

$$D_8/J = \{[e], [r], [r^2], [r^3]\},$$

where $J := \{e, rf\}$.

Remark. In view of the exercise, one might naturally guess that $D_8/J \simeq H$. But in the first example we were led to guess $D_8/K \simeq H$! This becomes less surprising once we observe that $J \simeq K$.

2. Formalizing our intuition

Given a group G and a subgroup $H \leq G$, our first step in the examples above was to write G as a disjoint union of multiples of H:

$$G = H \sqcup g_1 H \sqcup g_2 H \sqcup \cdots \sqcup g_n H. \tag{2}$$

for some elements $g_i \in G$. Then we factored out H:

$$G/H = \{[e], [g_1], [g_2], \ldots, [g_n]\}. \tag{3}$$

Now, we can always do this. But there's a serious problem with this approach: the choice of the set on the right hand side is *very* badly-defined. For example, fix any nontrivial element $h \in H$. A bit of thought will convince you that $H = hH$. But this means we can rewrite (2) in the form

$$G = hH \sqcup g_1 H \sqcup g_2 H \sqcup \cdots \sqcup g_n H,$$

which would give us a different answer for the quotient:

$$G/H = \{[h], [g_1], [g_2], \ldots, [g_n]\}.$$

Even worse, if we pick a bunch of elements $h_i \in H$, we could similarly deduce

$$G/H = \{[h], [g_1 h_1], [g_2 h_2], \ldots, [g_n h_n]\}.$$

At first glance, this issue seems to destroy our prospects for making this approach rigorous – it turns out we haven't even come up with a proper definition of what G/H might be! But now we introduce a truly bizarre idea: rather than fixing this flaw in our definition, we embrace it. We saw above that $[e]$ is replaceable by $[h]$, and possibly by other things of the form $[x]$, too. Rather than thinking of $[e]$ as a single element, let's declare $[e]$ to be the set of all the objects it could be replaced by. In other words, set

$$[e] := \{x \in G : H = xH\}.$$

Similarly, for any $g \in G$, we set

$$[g] := \{x \in G : gH = xH\}. \tag{4}$$

This removes the ambiguity in (3) by fiat: no matter what we replace $g_1 H$ by in (2), the set $[g_1]$ contains it.

This fixes the potential ambiguity in our definition (3) of G/H, but at a cost: the elements of G/H are themselves sets. This might be unfamiliar in a mathematical context, but is not as strange as it may seem. For example, our body is composed of cells, but these are themselves composed of even smaller components (DNA, organelles, etc.). Same with G/H: it consists of some objects $[g]$, each of which is also composed of smaller objects (namely, certain elements of G).

We're almost ready to formalize this as a definition, but now we run into another problem. How do we formalize the decomposition (2)? How do we find one? And how do we even know such a decomposition exists? Thus, before we can write down a definition of G/H, we have to prove something.

Proposition 1. *Given $H \leq G$, there exists some set $S \subseteq G$ such that*

$$G = \bigsqcup_{g \in S} gH.$$

Proof. First, observe that we can write

$$G = \bigcup_{g \in G} gH.$$

(Stare at this until it becomes obvious to you.) Next, observe that any two sets gH are either the same or completely disjoint:

Exercise 2. Given any two elements $g, g' \in G$, we have that either $gH = g'H$ or $gH \cap g'H = \emptyset$.

Applying the exercise, we see that we can simply remove all redundant sets gH from the union above, until all the sets which remain are disjoint. This completes the proof. □

Now we know that a decomposition of the form (2) is always possible. This in turn implies that the expression in (3) is well-defined.

We are now in a position to formally define G/H, but before we do so we make one final observation that will make the definition much cleaner.

Exercise 3. For any $g \in G$, we have $[g] = gH$.

With this, we now arrive at the following

Definition. Given $H \leq G$, we define

$$G/H := \{[g] : g \in G\},$$

where $[g]$ denotes the set gH.

Note that we've employed a cheat here: by *definition* a set ignores repeated elements (e.g. $\{1, 2, 3\} = \{1, 2, 3, 2\}$), so the potentially redundant $[g]$'s in $\{[g] : g \in G\}$ can be safely ignored.

Remark. The sets $[g] = gH$ are called *(left) cosets*.

Exercise 4. Why do we require H to be a subgroup of G in this construction? In other words, what goes wrong in the definition of G/H when H is merely a subset of G?

3. Is G/H a group?

Now, the idea of all of this was to break a group down into simpler groups. This means we'd like the set G/H to be a group. Is there a natural binary operation which makes it into a group? In other words, what should we define $[a][b]$ to be? The most natural guess is

$$[a][b] := [ab]. \tag{5}$$

Exercise 5. Prove that G/H satisfies all the group axioms with respect to the binary operation defined in (5): closure, associativity, existence of identity, and existence of inverses.

What might throw you a bit is that sometimes G/H doesn't look like a group. For instance, in Example 2 we found that

$$D_8/I = \{[e], [r], [f], [rf]\},$$

which doesn't look like it's closed under our operation: $[r]^2 = [r^2]$, which doesn't look like any of the four elements of D_8/I. However, a bit more thought shows that $[r^2] = [e]$, which *is* listed.

Thus, a quotient G/H might not look like a group and still be one. But there is something much worse that can happen: G/H **might look like a group and yet *not* be one**. How is this possible? Didn't we just check that all the group axioms are satisfied?

To see what's going on, we go back to a different example. In Exercise 1 we saw that

$$D_8/J = \{[e], [r], [r^2], [r^3]\},$$

which looks like a perfectly nice group under the binary operation (5). But there's a horrible surprise in store: *the binary operation* (5) *isn't well-defined* on this set. For example, we have $[e] = [rf]$, but

$$[e][r] = [r] \neq [f] = [rf][r].$$

Thus, D_8/J is *not* a group under our binary operation.

More generally, in an arbitrary quotient G/H it's possible that $[a] = [a']$ and $[b] = [b']$ but $[a][b] \neq [a'][b']$, i.e. that $[ab] \neq [a'b']$. If, however, the operation *is* well-defined, then G/H is an honest group; a success! This motivates distinguishing those nice subgroups H for which G/H is actually a group.

Definition. A subgroup $N \leq G$ is said to be a *normal subgroup* of G, denoted $N \trianglelefteq G$, iff G/N is a group with respect to the binary operation $[a][b] = [ab]$ (i.e. iff this operation is well-defined).

What can we say about normal subgroups? Turns out, there's an easy way to detect whether a given subgroup is normal. To see this, first recall that $[g] = gH.$ Rewriting our binary operation on G/H in this language, we are trying to define $(aH)(bH)$ as follows:

$$(aH)(bH) := abH.$$

Actually, it's odd to *define* this: either the above statement is true or it isn't! So, a subgroup $H \leq G$ is normal iff

$$aHbH = abH$$

for all $a, b \in G.$ It's easy to see that if $Hb = bH$, then the above must be true. It turns out that the converse also holds:

Proposition 2. *$H \trianglelefteq G$ if and only if $bH = Hb$ for all $b \in G$.*

This is commonly written in a different form: $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in G$.

Exercise 6. Prove that $4\mathbb{Z} \trianglelefteq \mathbb{Z}$ (both viewed as groups under addition), and determine $\mathbb{Z}/4\mathbb{Z}$.

DEPT OF MATHEMATICS & STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA, USA
E-mail address: leo.goldmakher@williams.edu