GROUPS AND SYMMETRY: LECTURE 18

LEO GOLDMAKHER

Recall that last time we discussed how to divide one group by another. This is similar to dividing one integer by another; sometimes the answer isn't so nice (e.g. $\frac{60}{7}$), but other times it is (e.g. $\frac{60}{6}$). Why would one want to do this? The hope is that one can decompose big mysterious groups into smaller, simpler groups; in other words, exactly the same reason why we decompose substances into molecules, or integers into products of smaller integers.

Intuitively, the idea went as follows: given $H \leq \Gamma$, we tried to tile Γ by (disjoint) copies of H:

$$\Gamma = \bigsqcup_g gH$$

over some set of g. We were able to do this, but it was a bit technical and tricky to specify exactly how to pick the g's which made the tiles gH disjoint. Instead, we took another approach: we defined

$$\Gamma/H := \{[a] : a \in \Gamma\},$$

where $[a] := \{g \in \Gamma : aH = gH\}$. Note that the set Γ/H is *not* a union of the sets $[a]$; Γ/H is a set, whose individual elements are the sets $[a]$. (Your body is made of cells, but cells are composed of even smaller pieces.) The advantage of this approach is that sets ignore repeated elements. On your homework, you will prove that for any $a, b \in \Gamma$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$. Along these lines, the following lemma is very useful.

Lemma 1. *Given $H \leq \Gamma$ and $x, y \in \Gamma$. The following are equivalent:*
(a) $xH = yH$
(b) $[x] = [y]$
(c) $x^{-1}y \in H$

Note that this lemma doesn't hold if H isn't a subgroup of Γ. This is part of the reason we only divide Γ by a subgroup, as opposed to by an arbitrary subset. (The other reason is that we're trying to break a group down into simpler *groups*, not just into sets.)

We worked out two example quotients.

(i) What is $\mathcal{G}_{\{\pm 1 \pm i\}}/\{\mathbb{1}, R_\pi\}$? First, we can predict the answer by writing down the elements of $\mathcal{G}_{\{\pm 1 \pm i\}}$ in the appropriate order, so that we can factor out $M := \{\mathbb{1}, R_\pi\}$:

$$\begin{aligned}\mathcal{G}_{\{\pm 1 \pm i\}} &= \{\mathbb{1}, R_{\pi/2}, R_\pi, R_{3\pi/2}, \rho, R_{\frac{\pi}{2}}\rho, R_\pi\rho, R_{\frac{3\pi}{2}}\rho\} \\ &= \{\underbrace{\mathbb{1}, R_\pi}_{M}, \underbrace{R_{\pi/2}, R_{3\pi/2}}_{R_{\pi/2}M}, \underbrace{\rho, R_\pi\rho}_{\rho M}, \underbrace{R_{\frac{\pi}{2}}\rho, R_{\frac{3\pi}{2}}\rho}_{R_{\frac{\pi}{2}}\rho M}\}.\end{aligned}$$

Date: November 11, 2013.

(Note that these calculation rely on the fact that $R_\pi \rho = \rho R_\pi$.) Factoring out M from each of these, we guess that

$$\mathcal{G}_{\{\pm 1 \pm i\}}/M = \{[\mathbb{1}], [R_{\pi/2}], [\rho], [R_{\frac{\pi}{2}}\rho]\}.$$

It is easy to check that this is indeed the case: these four sets are pairwise disjoint, and any other set $[g]$ is equal to one of these four.

(ii) What is $\mathcal{G}_{\{\pm 1 \pm i\}}/\{\mathbb{1}, R_{\pi/2}\rho\}$? With a bit of work, one shows that it is $\Big\{[\mathbb{1}], [R_{\pi/2}], [R_\pi], [R_{3\pi/2}]\Big\}$.

Now, the idea of all of this was to break a group down into simpler groups. This means we would like the set Γ/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? A natural guess is $[a][b] = [ab]$. It is easy to check that Γ/H satisfies all four group axioms with respect to this operation: closure (since $[ab] \in \Gamma/H$), associativity (since $([a][b])[c] = [ab][c] = [abc] = [a][bc] = [a]([b][c])$), identity, inverses. The thing which might throw you off a bit is that sometimes Γ/H might not look like a group. For example, (i) above doesn't look like it's closed, since $[R_{\pi/2}]^2 = [R_\pi]$, which doesn't look like any of the four elements of $\mathcal{G}_{\{\pm 1 \pm i\}}/M$ we listed. However, a bit more thought shows that $[R_\pi] = [\mathbb{1}]$, which *is* listed.

Thus, a quotient Γ/H might not look like a group and still be one. But there is something much worse which happens: Γ/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? As it turns out, example (ii) from above – which looks so much like a group! – isn't one. We'll talk about why on Friday.

WWW.MATH.TORONTO.EDU/LGOLDMAK/C01F13/
E-mail address: lgoldmak@math.toronto.edu