GROUPS AND SYMMETRY: LECTURE 19

LEO GOLDMAKHER

Recall that, given $H \leq \Gamma$, we defined

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

(read: 'Γ mod H') 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, which are composed of even smaller pieces.) We spent some time discussing this.

Last time, you worked out two examples of quotient groups.
(i) $\mathcal{G}_{\{\pm 1 \pm i\}}/\{\mathbb{1}, R_\pi\} = \Big\{[\mathbb{1}], [R_{\pi/2}], [\rho], [R_{\frac{\pi}{2}}\rho]\Big\}$.

(ii) $\mathcal{G}_{\{\pm 1 \pm i\}}/\{\mathbb{1}, R_{\pi/2}\rho\} = \Big\{[\mathbb{1}], [R_{\pi/2}], [R_\pi], [R_{3\pi/2}]\Big\}$.

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; we did this by defining a binary operation by

$$[a][b] := [ab].$$

It was a straightforward exercise to check that all four group axioms were satisfied. However, it turns out that example (ii) isn't a group! Why not? Dickson pointed out that the operation isn't always well-defined: in example (ii) above, we have $[\mathbb{1}] = [R_{\pi/2}\rho]$, but

$$[\mathbb{1}][R_{\pi/2}] \neq [R_{\pi/2}\rho][R_{\pi/2}].$$

Thus, $\mathcal{G}_{\{\pm 1 \pm i\}}/\{\mathbb{1}, R_{\pi/2}\rho\}$ is *not* a group under our binary operation.

More generally, in an arbitrary quotient Γ/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 Γ/H is an honest group; a success! This motivates distinguishing those nice subgroups H for which Γ/H is actually a group.

Definition. *A subgroup $N \leq \Gamma$ is said to be a* normal subgroup *of Γ, denoted $N \trianglelefteq \Gamma$, iff Γ/N is a group wrt 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 test whether a given subgroup is normal. To approach this, we first reconsidered the notion $[a]$. Dan suggested the following:

Proposition 1. *Given $H \leq \Gamma$ and $a \in \Gamma$. Then $[a] = aH$.*

(Prove this!) Writing our binary operation on Γ/H in this language, we are trying to define $(aH)(bH)$ as follows:

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

Date: November 15, 2013.

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

$$aHbH = abH$$

for all $a, b \in \Gamma$. Jamal and Eric pointed out that if $Hb = bH$, then the above is certainly true. It turns out that the converse is also true:

Proposition 2. *$H \trianglelefteq \Gamma$ iff $bH = Hb$ for all $b \in \Gamma$.*

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

One situation in which this condition for normality is automatically satisfied is if every pair of elements of Γ commutes, i.e. if for any $x, y \in \Gamma$ we have $xy = yx$. (Note that this isn't true in general. For example in $\mathcal{G}$ we have $T_2 R_\pi \neq R_\pi T_2$.) A group which has this special property is called *abelian*, in honor of the genius Norwegian mathematician Abel.

Thus, in an abelian group, every subgroup is normal. This means we can quotient out by any subgroup, and we'll get another group. Let's do a specific example. We know that $\mathbb{Z}$ (under addition!) is abelian, so $\mathbb{Z}/3\mathbb{Z}$ must be a group. Which group? By definition, we have

$$\mathbb{Z}/3\mathbb{Z} = \{[n] : n \in \mathbb{Z}\}.$$

From above, we know that $[n] = n + 3\mathbb{Z}$. Next, we observed that

$$\mathbb{Z} = \{\cdots \underbrace{-4}_{2+3\mathbb{Z}}, \underbrace{-3}_{3\mathbb{Z}}, \underbrace{-2}_{1+3\mathbb{Z}}, \underbrace{-1}_{2+3\mathbb{Z}}, \underbrace{0}_{3\mathbb{Z}}, \underbrace{1}_{1+3\mathbb{Z}}, \underbrace{2}_{2+3\mathbb{Z}}, \underbrace{3}_{3\mathbb{Z}}, \underbrace{4}_{1+3\mathbb{Z}}, \cdots\}$$

We deduced that $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$, and has the following addition table:

$+$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

This should look familiar from problem set 6!

More generally, given any positive integer n, we have

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\},$$

which is a group under the operation $[a] + [b] = [a + b]$. For example, in $\mathbb{Z}/7\mathbb{Z}$, we have

$$[4] + [5] = [9] = 9 + 7\mathbb{Z} = 2 + 7\mathbb{Z} = [2].$$

This is sometimes written as

$$4 + 5 \equiv 2 \pmod 7.$$

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