GROUPS AND SYMMETRY: LECTURE 15

LEO GOLDMAKHER

Last lecture we introduced the following notion:

Definition. *Given a group* Γ *and* $H \subseteq \Gamma$*, we say* H *is a* subgroup *of* Γ *iff* H *is a group under the same operation as* Γ*. In this case we write* $H \leq \Gamma$*.*

For example, $\mathcal{G}_{\{\pm 1 \pm i\}} \leq \mathcal{G}$, since $\mathcal{G}_{\{\pm 1 \pm i\}}$ is a subset of $\mathcal{G}$ and forms a group under composition. By contrast, $\{\pm 1\}$ is not a subgroup of $(\mathbb{Z}, +)$; it's a subset of $\mathbb{Z}$, and forms a group under multiplication, but does NOT form a group under addition (the binary operation of the bigger group).

Today we explored subgroups further. Recall that $\mathbb{Q}^\times$ is the group of all nonzero rationals under multiplication. What are some subgroups of $\mathbb{Q}^\times$? Pretty quickly, we came up with two trivial subgroups: $\{1\}$, and $\mathbb{Q}^\times$. A less trivial example is $\{\pm 1\}$. A nonexample is $\mathbb{Z}$ – it is neither a subset of $\mathbb{Q}^\times$ (it contains 0), nor is it a group under multiplication. A more interesting set of examples were suggested by Jay. His first suggestion was

$$\mathcal{J} := \left\{ \frac{a}{2^n} : a \in \mathbb{Z} - \{0\}, n \geq 1 \right\}.$$

This is almost a subgroup of $\mathbb{Q}^\times$; it's a subset which is closed, associative, and has an identity with respect to multiplication. However, not every element has an inverse. For example, $\frac{3}{4}$ has no inverse in $\mathcal{J}$. Note that it DOES have an inverse in $\mathbb{Q}^\times$, but for $\mathcal{J}$ to be a group the inverse would have to live in $\mathcal{J}$ itself.

Next, we modified the definition to

$$\mathcal{J}' := \left\{ \frac{1}{2^n} : n \geq 0 \right\}.$$

Once again, this satisfies almost all of the conditions for being a subgroup, but fails to have inverses in general; for example, $1/2$ has no inverse. Jay then suggested the set

$$\mathcal{J}'' := \{2^n : n \in \mathbb{Z}\}.$$

This is a subgroup of $\mathbb{Q}^\times$.

Next, we turned to the group $\mathbb{Z}$. (Note that we're not specifying the operation. When in doubt, assume the operation is the most obvious one. In the case of $\mathbb{Z}$, that means addition.) What are the subgroups of $\mathbb{Z}$? There are two trivial ones, $\{0\}$ and $\mathbb{Z}$ itself. Jay pointed out the more interesting example $2\mathbb{Z}$ of all even numbers; more generally, he observed that $n\mathbb{Z} \leq \mathbb{Z}$ for any integer n, where

$$n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}.$$

After verifying Jay's claim for $n = -3$, we tried to think of other subgroups of $\mathbb{Z}$. One suggestion was the set

$$2\mathbb{Z} + 3\mathbb{Z} := \{a + b : a \in 2\mathbb{Z}, b \in 3\mathbb{Z}\}.$$

Date: November 1, 2013.

This is easily verified to be a subgroup of $\mathbb{Z}$. Unfortunately, it's not a *new* subgroup: David pointed out that $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$! After a bit more thought, we guessed the following

Theorem 1. *$H \leq \mathbb{Z}$ iff $H = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.*

Building on an idea proposed by David, we eventually came up with the following proof.

Proof. As usual for 'if and only if' statements, we prove the two directions individually. The ($\Leftarrow$) direction we've already checked above, so it suffices to prove the forward direction ($\Rightarrow$).

We're given $H \leq \mathbb{Z}$. We're trying to show that $H = d\mathbb{Z}$ for some mysterious integer d. What is this d? After some discussion, Dickson proposed the following method of finding d. First, since H is a group, we must have $0 \in H$. If $H = \{0\}$, we're done! Otherwise, H must contain a positive element. (Why?) Set d to be the *least* positive element of H. We now claim $H = d\mathbb{Z}$.

As usual, we prove this in two steps: we separately prove $H \subseteq d\mathbb{Z}$ and $d\mathbb{Z} \subseteq H$. The latter follows easily from closure and existence of inverses (make sure you can write it down carefully!), so we focus on the former inclusion. Dan suggested the following argument: pick $x \in H$. Then we can write

$$\frac{x}{d} = q + \frac{r}{d}$$

where $q \in \mathbb{Z}$ and $0 \leq r < d$. (To test whether you understand this, find q and r in the case $x = -17$ and $d = 4$.) It follows that

$$r = x - qd.$$

The right hand side is an element of H by the group axioms (why?), whence $r \in H$. Since d is the least positive element in H and $0 \leq r < d$, we must have $r = 0$. It follows that

$$x = dq \in d\mathbb{Z}.$$

This demonstrates that $H \subseteq d\mathbb{Z}$, and concludes the proof of the theorem. □

This theorem immediately implies the following result.

Corollary 2. *Given $a, b \in \mathbb{Z}$, there exists $d \in \mathbb{Z}$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Proof. It is easy to verify that $a\mathbb{Z} + b\mathbb{Z} \leq \mathbb{Z}$. But every subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z}$ for some $d \in \mathbb{Z}$! □

Our proof of the theorem proceeded as follows: given a subgroup $H \leq \mathbb{Z}$, we found an integer d which 'generated' H. More generally, in an abstract group Γ and $g \in \Gamma$, we can always generate the following set:

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$$

This is a subgroup of Γ. We will discuss this further next lecture.

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