GROUPS AND SYMMETRY: LECTURE 16

LEO GOLDMAKHER

We started by briefly sketching the proof from last lecture of the following result:

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

Moreover, we found an appropriate value of d: the smallest positive element of H (unless $H = \{0\}$, in which case the theorem holds with $d = 0$). At the heart of our proof was the realization that H is the smallest subgroup of $\mathbb{Z}$ containing d. On the other hand, this subgroup is clearly $d\mathbb{Z}$.

This motivated the following question: given an arbitrary group Γ and some element $g \in \Gamma$, what is the smallest subgroup of Γ containing g? Jess pointed out that in addition to g, any such subgroup must contain the identity e and g^{-1} (to satisfy the group axioms). But it must also contain other elements, as Dan pointed out: by the closure axiom, the subgroup must contain $g^2 := g \cdot g$, which in turn forces it to contain $g^3 := g \cdot g^2$, etc. But then it must also contain the inverses of all these: $g^{-2} := (g^{-1})^2$, $g^{-3} := (g^{-1})^3$, etc. Thus we concluded that the smallest subgroup of Γ containing g is

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

where we are defining g^0 to be the identity of Γ. This is the 'smallest' subgroup of Γ containing g in the sense that it doesn't contain any unnecessary elements; it is common to refer to $\langle g \rangle$ as the subgroup of Γ generated by g.

More generally, given multiple elements $g_1, g_2, \ldots, g_n \in \Gamma$, we denote by $\langle g_1, g_2, \ldots, g_n \rangle$ the smallest subgroup of Γ containing all the g_i's; we call this the subgroup of Γ generated by the $g_1, g_2, \ldots, g_n$. We explored some examples.

(1) Given $d \in \mathbb{Z}$, we have $\langle d \rangle = d\mathbb{Z}$. In the proof of our theorem, we showed that any subgroup of $\mathbb{Z}$ is generated by its least positive element.

(2) Given $a, b \in \mathbb{Z}$, we have $\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z}$. Make sure you understand why!

(3) In the group $\mathcal{G}$ of plane isometries, we found that

$$\langle R_{\pi/2} \rangle = \{\mathbb{1}, R_{\pi/2}, R_\pi, R_{3\pi/2}\} = \{\pm\mathbb{1}, \pm R_{\pi/2}\}.$$

Thus, the subgroup generated by a single element can be finite. (Our first example shows that the subgroup generated by a single element can also be infinite.)

(4) Once again in $\mathcal{G}$, we found that $\langle R_{\pi/2}, \rho \rangle = \mathcal{G}_{\{\pm 1 \pm i\}}$, the group of symmetries of the square.

(5) In the group $\mathbb{C}^\times$ (the nonzero complex numbers under complex multiplication), the subgroup generated by i is

$$\langle i \rangle = \{1, i, i^2, i^3\} = \{\pm 1, \pm i\}.$$

Date: November 4, 2013.

(6) We've seen the group $SL_n(\mathbb{Q})$ before. It turns out that $SL_2(\mathbb{Z})$ is also a group! (Verify this.) Within this group, we generate the following subgroup:

$$\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle = \{I, M, M^2, M^3\} = \{\pm I, \pm M\}$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix, and $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Examples (3), (5), and (6) above are extremely similar, despite living inside of different groups. This observation will lead to some very powerful theorems in the upcoming weeks.

Having discussed these examples, we went back to our classification of the subgroups of $\mathbb{Z}$. By our theorem, we know that for any nonzero $a, b \in \mathbb{Z}$, we can write

$$\langle a, b \rangle = \langle d \rangle,$$

where d is the smallest positive element of $\langle a, b \rangle$. This is a nice result, in that it tells us how to find the generator d; all you have to do is determine the least positive element of $a\mathbb{Z} + b\mathbb{Z}$. In practice, this can be a painful process; for example, what is $\langle 17, 19 \rangle$? The following result makes answering such questions much easier.

Proposition 2. *Given a, b nonzero integers. Then*

$$\langle a, b \rangle = \big\langle \gcd(a, b) \big\rangle,$$

where $\gcd(a, b)$ is the greatest common divisor of a and b.

Proof. Let d be the least positive element of $\langle a, b \rangle$, so that $\langle d \rangle = \langle a, b \rangle$. Since $\langle a, b \rangle$ contains a and b, we see that

$$a, b \in \langle a, b \rangle = \langle d \rangle = d\mathbb{Z};$$

in other words, d is a common divisor of a and b.

Next, we show that d is the *largest* common divisor. Suppose d' is a common divisor of a and b, i.e. $a, b \in d'\mathbb{Z} = \langle d' \rangle$. By definition, $\langle a, b \rangle$ is the *smallest* subgroup containing a and b, whence

$$\langle d \rangle = \langle a, b \rangle \subseteq \langle d' \rangle.$$

It follows that $d \in \langle d' \rangle = d'\mathbb{Z}$, so d is a multiple of d'. In particular, $d \geq d'$. □

We finished with a definition. Given a group Γ and a subgroup $H \leq \Gamma$, we say H is *cyclic* iff H is generated by a single element (i.e. iff there exists $h \in \Gamma$ such that $H = \langle h \rangle$). For example, in $\mathbb{Z}$, we have that $\langle a, b \rangle$ is cyclic. More generally, our theorem asserts that *every* subgroup of $\mathbb{Z}$ is cyclic.

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