# GROUPS AND SYMMETRY: LECTURE 17

LEO GOLDMAKHER

Recall that

$$\mathcal{G}_{\{\pm1\pm i\}} = \{\underbrace{\mathbb{1}, R_{\pi/2}, R_\pi, R_{3\pi/2}}_{H}, \underbrace{\rho, R_{\pi/2}\rho, R_\pi\rho, R_{3\pi/2}\rho}_{H\rho}\}.$$

Thus we can "factor out $H$" and write

$$\mathcal{G}_{\{\pm1\pm i\}}/H = \{1, \rho\} =: K. \tag{1}$$

We could have also factored out $K$, by writing $\mathcal{G}_{\{\pm1\pm i\}}$ in a different order:

$$\mathcal{G}_{\{\pm1\pm i\}} = \{\underbrace{\mathbb{1}, \rho}_{K}, \underbrace{R_{\pi/2}, R_{\pi/2}\rho}_{R_{\pi/2}K}, \underbrace{R_\pi, R_\pi\rho}_{R_\pi K}, \underbrace{R_{3\pi/2}, R_{3\pi/2}\rho}_{R_{3\pi/2}K}\},$$

whence

$$\mathcal{G}_{\{\pm1\pm i\}}/K = H.$$

This is reassuring, given (1). Note that the process is reminiscent of factoring a polynomial: by writing the elements of the group in a certain order, we can see a common factor.

Next we considered a more complicated example: $\mathcal{G}/K$, where $K$ is as above. Jay suggested that we should have

$$\mathcal{G}/K = \{T_h R_\theta : h \in \mathbb{C}, \theta \in [0, 2\pi)\}.$$

We discussed this for some time.

Armed with some intuition, we tried to define this division rigorously. Given $H \leq \Gamma$, how do we define $\Gamma/H$? We want to tile $\Gamma$ by shifted copies of $H$. First, we noted that

$$\Gamma = \bigcup_{g \in \Gamma} gH \tag{2}$$

(with a proof suggested by Dinu). Although this is a nice covering of $\Gamma$ by copies of $H$, it isn't quite what we're looking for, because some of these copies of $H$ might overlap. (Think of a bathroom floor. What (2) does is the equivalent of pouring a bunch of ceramic tiles onto the floor until the whole floor is covered. But what we want a single layer of ceramic tiles, arranged to cover the entire floor without overlapping.) To see this more clearly, we looked at an example. We have

$$\begin{aligned}\mathcal{G}_{\{\pm1\pm i\}} &= \bigcup_{g \in \mathcal{G}_{\{\pm1\pm i\}}} gK \\ &= \mathbb{1}K \cup \rho K \cup R_{\pi/2}K \cup R_{\pi/2}\rho K \cup R_\pi K \cup R_\pi \rho K \cup R_{3\pi/2}K \cup R_{3\pi/2}\rho K.\end{aligned}$$

A lot of these are superfluous. For example, $\mathbb{1}K = \rho K$, so including them both in the union is pointless. Removing all these redundancies gives

$$\mathcal{G}_{\{\pm1\pm i\}} = \mathbb{1}K \cup R_{\pi/2}K \cup R_\pi K \cup R_{3\pi/2}K.$$

*Date*: November 8, 2013.

In fact, all of these are disjoint sets. We indicate this by using the *disjoint union* symbol:

$$\mathcal{G}_{\{\pm 1 \pm i\}} = \mathbb{1}K \sqcup R_{\pi/2}K \sqcup R_{\pi}K \sqcup R_{3\pi/2}K.$$

This is the same tiling as we found above.

This approach works quite generally. First, we cover $\Gamma$ using all possible tiles, as in (2). Then we remove all the excess tiles. Right away, there's a potential problem: some of the tiles might be overlapping (i.e. lying on top of two other tiles). It turns out this never actually happens.

**Lemma 1.** *Given any $a, b \in \Gamma$, either $aH = bH$ or $aH \cap bH = \emptyset$.*

Thus, in our covering (2) of $\Gamma$, any two tiles are either lying directly on top of one another, or else are entirely disjoint. Thus all we have to do is remove the redundant stacks. This can be done directly, but there's a cheat which makes life easier. We'll do the cheat first, then return to the question of doing this directly.

Given $a \in \Gamma$, define

$$[a] := \{g \in \Gamma : aH = gH\}.$$

As above, given any $a, b \in \Gamma$ we either have $[a] = [b]$ or $[a] \cap [b] = \emptyset$. We now define

$$\Gamma/H := \{[g] : g \in \Gamma\}.$$

(Note that we are treating each $[g]$ as an individual object, rather than as a set!) This eliminates all the redundant elements, since a set is blind to repeated elements (e.g. $\{1, 2, 2, 3\} = \{1, 2, 3\}$).

The above trick allows us to get around the redundancy problem in the earlier approach, but it's sort of a cheat – we rely on our notion of set, and the fact that it implicitly ignores redundancy. We can be more explicit if we employ the Axiom of Choice. In this context, AC tells us that there exists a set $\overline{\Gamma} \subseteq \Gamma$ which contains exactly one element of each $[g]$, i.e.

$$\left|\overline{\Gamma} \cap [g]\right| = 1 \qquad \forall g \in \Gamma.$$

This allows us to write $\Gamma$ as a disjoint union of tiles:

$$\Gamma = \bigsqcup_{g \in \overline{\Gamma}} gH.$$

Note that in some sense, $\Gamma/H$ and $\overline{\Gamma}$ are the same thing – they're just two different ways of keeping track of nonredundant tilings of $\Gamma$ by $H$. In particular, $|\overline{\Gamma}| = \#$ of distinct $[a]$'s $= |\Gamma/H|$.

Our work immediately gives us several nice consequences.

**Theorem 2** (Lagrange's Theorem)**.** *Given $\Gamma$ a finite group and $H \leq \Gamma$, we have*

$$|H| \Big| |\Gamma|,$$

*where the notation $d|n$ means $n$ is a multiple of $d$.*

*Proof.* We first observe that for any $g \in \Gamma$,

$$|gH| = |H|.$$

It follows that

$$|\Gamma| = \left| \bigsqcup_{g \in \overline{\Gamma}} gH \right| = \sum_{g \in \overline{\Gamma}} |gH| = \sum_{g \in \overline{\Gamma}} |H| = |\overline{\Gamma}| \cdot |H|.$$

The claim immediately follows. □

Note that, since $|\Gamma/H| = |\overline{\Gamma}|$, the above proof shows that

$$|\Gamma/H| = |\Gamma|/|H|.$$

Incidentally, we've been discussing the sizes of groups a lot. In words, one usually calls the number of elements in a group the *order* of the group. To see why we need a special word for this, try to rephrase the following corollary without using the word 'order'.

**Corollary 3.** *Every group of prime order is cyclic.*

*Proof.* Given a group $\Gamma$ of prime order, pick any $a \in \Gamma - \{e\}$. By Lagrange's theorem, the order of $\langle a \rangle$ must divide the order of $\Gamma$, whence we must have $|\langle a \rangle| = |\Gamma|$ or 1. Since $\langle a \rangle$ contains at least two elements ($a$ and $e$), we conclude that $|\langle a \rangle| = |\Gamma|$. But also $\langle a \rangle \subseteq \Gamma$! Thus $\langle a \rangle = \Gamma$. □

Actually, as Dan pointed out, we've proved something a bit stronger than what we claimed: a group of prime order is generated by *any* of its elements, aside from the identity.

Another nice application of Lagrange's theorem is the following, which you might look familiar if you've seen some number theory.

**Corollary 4.** *Given any finite group* $\Gamma$. *We have* $a^{|\Gamma|} = e$ *for every* $a \in \Gamma$.

*Proof.* Pick $a \in \Gamma$, and consider the subgroup $\langle a \rangle$ generated by $a$. Since $\Gamma$ is finite, $\langle a \rangle$ must also be finite. Let $n := |\langle a \rangle|$; it is an exercise to show that

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

and that $a^n = e$. By Lagrange's theorem, we know that the order of $\langle a \rangle$ divides the order of $\Gamma$, so $|\Gamma| = kn$ for some integer $k$. It follows that

$$a^{|\Gamma|} = a^{kn} = (a^n)^k = e^k = e.$$

□

Several times now we have dealt with the order of the subgroup generated by a given element $a$. Henceforth we will be lazy and say *the order of* $a$ rather than *the order of the subgroup generated by* $a$. In other words, the order of $a$ is defined to be $|\langle a \rangle|$.

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