GROUPS AND SYMMETRY: LECTURE 9

LEO GOLDMAKHER

Recall that given a set $S \subseteq \mathbb{C}$, we say that $\gamma \in \mathcal{G}$ is a *symmetry* of S iff $\gamma(S) = S$. We denote the set of all symmetries of S by $\mathcal{G}_S$. Last time, we considered the symmetries of the square $\{\pm 1 \pm i\}$. We found eight different symmetries, which we can write down in the following efficient way:

$$\{R_{\pi/2}^k \rho^j : j, k \in \mathbb{Z}\} \subseteq \mathcal{G}_{\{\pm 1 \pm i\}}.$$

Here we are using the notation f^n to denote $\underbrace{f \circ f \circ \cdots \circ f}_{n}$ if n is positive. Similarly, we define $f^{-n} := \underbrace{f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}}_{n}$. Finally, $f^0 := \mathbb{1}$.

At the end of last lecture, we struggled for some time (without success) to find a symmetry of $\{\pm 1 \pm i\}$ which wasn't one of these eight. This made you suspect that perhaps there aren't any other symmetries. As evidence for this, I gave the following heuristic argument (not a proof, just a thought experiment!). Suppose $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$. What is $\gamma(1+i)$? Well, there are four choices; it could be any element of $\{\pm 1 \pm i\}$. The key point is that, *once we've made this choice*, we have much less freedom about where to send the other three points. For example, say we know $\gamma(1+i)$. What could $\gamma(1-i)$ be? Since $1-i$ is an adjacent vertex to $1+i$, and since γ is an isometry, we see that $\gamma(1-i)$ must be adjacent to the vertex $\gamma(1+i)$. Thus, as soon as we choose where to send $1+i$, there are only two choices of where $1-i$ gets sent. Once we make this choice, we no longer have any freedom: the vertex $-1+i$, which is adjacent to $1+i$, must get sent to the unique vertex adjacent to $\gamma(1+i)$ which isn't $\gamma(1-i)$. Finally, $\gamma(-1-i)$ must be the vertex diagonally across from $\gamma(1+i)$. Thus, the action of γ on the points $\{\pm 1 \pm i\}$ are determined by where $1+i$ and $1-i$ get sent; since there are four choices for the first and (subsequently) two choices for the second, we see that there are $4 \times 2 = 8$ choices for γ. Since we've already found eight different elements of $\mathcal{G}_{\{\pm 1 \pm i\}}$, the above argument indicates that we've found all of the symmetries.

Of course, this isn't a proof. So, we started brainstorming. Formally, we're trying to prove:

Proposition 1. *If $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$, then $\gamma = R_{\pi/2}^k \rho^j$ for some $k, j \in \mathbb{Z}$.*

The first idea, proposed by Dan and developed by Dan and Eric, was as follows. Given $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$, we can write it in the form $\gamma = T_h R_\theta \rho^j$. We want to show that $\theta \in \frac{\pi}{2}\mathbb{Z}$, and that $h = 0$. We separate into two cases:

(1) $\theta \in \frac{\pi}{2}\mathbb{Z}$. This implies that $R_\theta \rho^j(\{\pm 1 \pm i\}) = \{\pm 1 \pm i\}$. But we also know that $\gamma(\{\pm 1 \pm i\}) = \{\pm 1 \pm i\}$. This forces $T_h(\{\pm 1 \pm i\}) = \{\pm 1 \pm i\}$, whence $h = 0$.

(2) $\theta \notin \frac{\pi}{2}\mathbb{Z}$. Then $R_\theta \rho^j(\{\pm 1 \pm i\}) \neq \{\pm 1 \pm i\}$, and by considering what γ does to each element of $\{\pm 1 \pm i\}$ one can find a contradiction.

This idea is direct, but a bit messy – one has to split into cases (and work out various details we didn't describe above). Kaidi suggested that we could instead look at distances to the origin: for

Date: October 4, 2013.

any $z \in \{\pm 1 \pm i\}$ we have $|z| = \sqrt{2}$, so $|\gamma(z)|$ should also be $\sqrt{2}$ for all $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$. If we write $\gamma = T_h R_\theta \rho^j$ as above, then we must have

$$|h + R_\theta \rho^j(z)| = \sqrt{2}$$

for all $z \in \{\pm 1 \pm i\}$. Now for any such z we also know that $|R_\theta \rho^j(z)| = \sqrt{2}$. We couldn't figure out how to make this argument work, but it certainly seems promising.

Kaidi's idea inspired a third approach, suggested by Quentin. Quentin's idea is to write points in complex polar coordinates:

$$\{\pm 1 \pm i\} = \{\sqrt{2} e^{i(\frac{\pi}{4} + \frac{\pi k}{2})} : k \in \mathbb{Z}\}.$$

Writing $\gamma = T_h R_\theta \rho^j$ as before, we see that

$$\gamma(1+i) = \gamma(\sqrt{2} e^{i\pi/4}) = h + \sqrt{2} e^{i(\theta \pm \pi/4)}.$$

If $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$, this would imply that

$$h + \sqrt{2} e^{i(\theta \pm \pi/4)} \in \{\sqrt{2} e^{i(\frac{\pi}{4} + \frac{\pi k}{2})} : k \in \mathbb{Z}\}.$$

From here one could try to play around algebraically and see where that leads.

Hui suggested yet another approach to the problem. Given $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$, write it as $R_\theta \rho^j T_h$. Then for any $z \in \{\pm 1 \pm i\}$ we have

$$\sqrt{2} = |\gamma(z)| = |R_\theta \rho^j T_h(z)| = |h + z|.$$

But if $h \neq 0$, there must exists some $z \in \{\pm 1 \pm i\}$ for which $|h + z| > \sqrt{2}$. Thus, h must be 0. It's then a straightforward exercise to prove that θ must be a multiple of $\pi/2$.

All of the above approaches have their merits. We ended lecture with a fifth approach which, while not the shortest, has a transparent strategy and is easy to generalize to sets other than $\{\pm 1 \pm i\}$. The key observation is:

Proposition 2. *If $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$, then $\gamma(0) = 0$.*

We'll prove this below. But first, let's take it on faith and see what we can deduce. In our proof of the decomposition lemma (that any isometry can be written in the form $T_h R_\theta \rho^j$) we saw that if $\gamma(0) = 0$, then $\gamma = R_\theta \rho^j$. Next, following Quentin's suggestion, we have

$$\gamma(1+i) = R_\theta \rho^j(\sqrt{2} e^{i\pi/4}) = \sqrt{2} e^{i(\theta \pm \pi/4)}$$

On the other hand, we know that $\gamma(1+i) \in \{\pm 1 \pm i\}$, whence

$$\sqrt{2} e^{i(\theta \pm \pi/4)} = \sqrt{2} e^{i(\frac{\pi}{4} + \frac{\pi k}{2})}$$

for some $k \in \mathbb{Z}$. Simplifying this, we conclude that

$$\theta \in \frac{\pi}{4} \pm \frac{\pi}{4} + \frac{\pi}{2}\mathbb{Z} + 2\pi\mathbb{Z} \subseteq \frac{\pi}{2}\mathbb{Z}.$$

We deduce that if $\gamma \in \mathcal{G}_{\{\pm 1 \pm i\}}$, then $\gamma = R_{\pi/2}^k \rho^j$, thus proving Proposition 1.

Thus, Proposition 1 follows easily from Proposition 2. Here's a proof strategy for Proposition 2. Let $\mathcal{L}_+$ denote the line segment connecting $-1-i$ to $1+i$, and let $\mathcal{L}_-$ denote the line segment connecting $-1+i$ to $1-i$. (In other words, $\mathcal{L}_\pm$ are the diagonals of the square.) Since $0 \in \mathcal{L}_+ \cap \mathcal{L}_-$, we see that

$$\gamma(0) \in \gamma(\mathcal{L}_+ \cap \mathcal{L}_-) = \gamma(\mathcal{L}_+) \cap \gamma(\mathcal{L}_-).$$

An easy argument will show that $\gamma(\mathcal{L}_+)$ is one of $\mathcal{L}_+$ or $\mathcal{L}_-$, and that $\gamma(\mathcal{L}_-)$ is the other. Therefore,

$$\gamma(0) \in \gamma(\mathcal{L}_+) \cap \gamma(\mathcal{L}_-) = \mathcal{L}_+ \cap \mathcal{L}_- = \{0\}.$$

This immediately implies that $\gamma(0) = 0$.

The following useful result will help us formalize the above argument.

Lemma 3. *Let $\overline{XY}$ denote the line segment between $X, Y \in \mathbb{C}$. Then for any $\phi \in \mathcal{G}$ and $X, Y \in \mathbb{C}$,*

$$\phi(\overline{XY}) = \overline{\phi(X)\phi(Y)}.$$

Proof. First, we express the line segment $\overline{XY}$ in a more precise way:

$$\overline{XY} = \{(1-t)X + tY : 0 \leq t \leq 1\}$$

Thus,

$$\phi(\overline{XY}) = \Big\{\phi\Big((1-t)X + tY\Big) : 0 \leq t \leq 1\Big\},$$

while

$$\overline{\phi(X)\phi(Y)} = \{(1-t)\phi(X) + t\phi(Y) : 0 \leq t \leq 1\}.$$

It therefore suffices to prove that

$$\phi\Big((1-t)X + tY\Big) = (1-t)\phi(X) + t\phi(Y) \tag{1}$$

for all $t \in [0, 1]$.

Recall from the decomposition lemma that we can write $\phi = T_h R_\theta \rho^j$. Moreover, we know that $R_\theta \rho^j$ is linear. It follows that

$$\begin{aligned}
\phi\Big((1-t)X + tY\Big) &= T_h R_\theta \rho^j \Big((1-t)X + tY\Big) \\
&= h + (1-t)R_\theta\rho^j(X) + tR_\theta\rho^j(Y) \\
&= (1-t)h + th + (1-t)R_\theta\rho^j(X) + tR_\theta\rho^j(Y) \\
&= (1-t)T_h R_\theta\rho^j(X) + tT_h R_\theta\rho^j(Y) \\
&= (1-t)\phi(X) + t\phi(Y).
\end{aligned}$$

This proves (1), and the claim follows. □

Next lecture, we will use this to prove Proposition 2.

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