GROUPS AND SYMMETRY: LECTURE 12

LEO GOLDMAKHER

Last time, we discussed the formal definition of a group. We'll review that later in the lecture. For now, here's a rough heuristic: a *group* is a set Γ, along with a nice binary operation (i.e. a way of combining any two elements of Γ to form a third), which we called $@$. What does it mean for a binary operation to be nice? Roughly, it means that you can use just that operation $@$ to get from any one element of Γ to any other element. We did a bunch of examples, some generated by me, others by you.

(1) $(\mathbb{Z}, +)$ is a group. For example, to get from 3 to 5, just add 2. More generally, to get from $a \in \mathbb{Z}$ to $b \in \mathbb{Z}$, just add the integer $b - a$.

(2) $(\mathbb{Z}, \times)$ is not a group; there's no way to get from 3 to 5 using multiplication by an integer.

(3) $(\mathbb{Q}, \times)$ is still not a group; now you can get from 3 to 5 (multiply by $\frac{5}{3}$), but you can't get from 0 to 1.

(4) $(\mathbb{Q}^\times, \times)$ is a group, where $\mathbb{Q}^\times := \mathbb{Q} - \{0\}$. To get from $a \in \mathbb{Q}$ to $b \in \mathbb{Q}$, just multiply by $\frac{b}{a}$, which is in $\mathbb{Q}$ since $a \neq 0$.

(5) $(\{1\}, \times)$ is a group; you can get from any element to any other by multiplying by 1.

(6) $\left(\left\{2, 3, \frac{2}{3}, \frac{3}{2}\right\}, \times\right)$ is not a group; $\times$ isn't a binary operation on the set, since for example $4 = 2 \times 2$ doesn't live in the set.

(7) $(\{\pm 1\}, \times)$ is a group; you can get from any element to any other by multiplying by 1 or -1.

(8) $(\{f : \mathbb{R} \to \mathbb{R} \text{ is a function}\}, +)$ is a group. What does it mean to add two functions? Exactly what you think: the function $f + g$ defined by $(f + g)(x) := f(x) + g(x)$. This is also a function from $\mathbb{R} \to \mathbb{R}$, so addition is really a binary operation on this set. Moreover, to get from any function $f : \mathbb{R} \to \mathbb{R}$ to any other function $g : \mathbb{R} \to \mathbb{R}$, simply add the function $g - f$, defined the way you think: $(g - f)(x) := g(x) - f(x)$.

(9) $(2\mathbb{Z}, \times)$ is not a group, where $2\mathbb{Z}$ is the set of all even numbers; there's no way to get from 0 to 2.

(10) $(2\mathbb{Z}, +)$ is a group: to get from the even number a to the even number b, add the even number $b - a$.

Date: October 21, 2013.

(11) $(\mathcal{G}, \circ)$, where $\mathcal{G}$ is the set of plane isometries, is a group. Here it was a bit harder to see how to get from one isometry to another, but Eric came up with a way: given $\phi, \psi \in \mathcal{G}$ we have

$$\begin{aligned}\psi &= \phi \circ (\phi^{-1} \circ \psi) \\ &= (\psi \circ \phi^{-1}) \circ \phi.\end{aligned}$$

Either way, this gives a way of getting from ϕ to ψ.

Next, we recalled the formal definition of a group:

Definition. *A* group *is a set* Γ *with a binary operation* $@$ *(i.e.* $@ : \Gamma \times \Gamma \to \Gamma$*) obeying the following 'group axioms'.*

(0) [Γ is closed under $@$] $x@y \in \Gamma$ *for all* $x, y \in \Gamma$ *(this verifies that* $@$ *is a binary operation)*

(1) [$@$ is associative] *The symbol* $x@y@z$ *is unambiguous. More precisely,* $(x@y)@z = x@(y@z)$ *for all* $x, y, z \in \Gamma$.

(2) [Γ has an identity with respect to $@$] *There exists an element* $e \in \Gamma$ *such that* $e@x = x = x@e$ *for all* $x \in \Gamma$.

(3) [Γ has inverses with respect to $@$] *Every element of* Γ *has an inverse in* Γ*, i.e. for every* $x \in \Gamma$ *there exists an element* $y \in \Gamma$ *such that* $x@y = e$*. (Usually,* y *is denoted* x^{-1}*.)*

We concluded lecture by verifying that $(\mathcal{G}, \circ)$ and $(\mathbb{Z}, +)$ are actually groups (by checking that they satisfy all the group axioms).

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