GROUPS AND SYMMETRY: LECTURE 14

LEO GOLDMAKHER

The first thing we did was agree on a new notation for groups. Recall that when we discussed the group $\mathcal{G}$ of all isometries, we at some point stopped writing $\circ$, instead writing expressions such as $T_h R_\theta \rho$. We now adopt the same lazy convention for groups: rather than writing $@$ as the binary operation of a group Γ, we'll simply write the operation as if it were multiplication. In this new notation, the group axioms become:

(0) Closure: $xy \in \Gamma$ for all $x, y \in \Gamma$;
(1) Associativity: $(xy)z = x(yz)$ for all $x, y, z \in \Gamma$;
(2) Identity: there exists $e \in \Gamma$ such that $ex = xe = x$ for every $x \in \Gamma$;
(3) Inverses: for each $x \in \Gamma$ there exists $y \in \Gamma$ such that $xy = e$.

Of course, this notation isn't always ideal. For example, in the group $(\mathbb{Z}, +)$ it would be quite confusing to represent the binary operation as multiplication! So sometimes, when discussing a specific group, we may sometimes write the binary notation explicitly. But for an 'abstract' group, we'll take the easy way and drop the binary operation. Note that this also makes it easier to talk about groups. Rather than writing $(\Gamma, @)$ we will just write Γ.

Last time we ended by discussing inverses. We started this lecture by proving the following result, which is unsurprising but reassuring.

Proposition 1. *Given a group Γ (with identity e), and suppose $x \in \Gamma$. Then there exists a unique $y \in \Gamma$ such that $xy = e$. Moreover, $yx = e$.*

Thus we can (and will!) denote the inverse of x as x^{-1}; note that we could not meaningfully use this notation if inverses weren't unique.

Proof. From the group axiom, we know that there exists $y \in \Gamma$ such that $xy = e$. Again from the group axiom, we know there exists $z \in \Gamma$ such that $yz = e$. But then

$$x = xe = x(yz) = (xy)z = ez = z,$$

whence $yx = yz = e$, which proves the second claim.

We now prove the uniqueness of y. Suppose y_1 and y_2 are both inverses of x, i.e. $xy_1 = e$ and $xy_2 = e$. By what we proved above, this implies $y_1 x = e$ and $y_2 x = e$. Using a similar trick as above, we deduce that

$$y_1 = y_1 x y_2 = y_2$$

as claimed. □

Given a group, it's often useful to discuss smaller groups living inside of it. For example, within the group $\mathcal{G}$ of symmetries, we might wish to study the group of symmetries of some set of points. This motivates 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 $H \leq \Gamma$.*

Date: October 28, 2013.

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).

Next lecture, we will explore subgroups further.

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