GROUPS AND SYMMETRY: LECTURE 11

LEO GOLDMAKHER

Recall that congruence is a natural example of ‘sameness’ among shapes; two congruent triangles are not the same, but we they have the same shape, so we consider them the same. Formally, we defined the binary relation $\cong$ by $A \cong B$ iff $\exists \phi \in \mathcal{G}$ such that $\phi(A) = B$. Next we verified that $\cong$ is an equivalence relation, i.e. it satisfies three properties:

(I) Reflexive: for all $A \subseteq \mathbb{R}^2$, we have $A \cong A$.
(II) Symmetric: if $A \cong B$, then $B \cong A$.
(III) Transitive: if $A \cong B$ and $B \cong C$, then $A \cong C$.

Further, recall that each of these holds because the set $\mathcal{G}$ of plane isometries satisfies some nice properties. More precisely, (I) holds because $\mathbb{1} \in \mathcal{G}$; (II) holds because $\phi^{-1} \in \mathcal{G}$ for every $\phi \in \mathcal{G}$; (III) holds because $\mathcal{G}$ is closed under composition (i.e. if $\phi, \psi \in \mathcal{G}$, then $\phi\psi \in \mathcal{G}$).

This is an example of a *geometric equivalence*, a geometric way of measuring similarity between different subsets of $\mathbb{R}^2$ (namely, by comparing their shape). Is there a natural geometric equivalence on $\mathcal{G}$ itself? In other words, is there a way of measuring similarity between different types of plane isometries? We quickly came up with one: types of motions. In particular, we already implicitly distinguish types of motions, by calling them *rotations* or *translations* or *reflections*. To formalize this, we need to come up with an equivalence relation $\approx$ on $\mathcal{G}$ such that any two rotations are equivalent, any two translations are equivalent, any two reflections are equivalent, etc, but which distinguishes these types from one another (i.e. translations and rotations shouldn’t be equivalent). There were many great suggestions – several of these are on the homework – but we saw that finding such an equivalence relation isn’t so easy. So, following Pólya’s dictum (“*If you can’t solve a problem, then there is an easier problem you can solve: find it.*”), we attacked a simpler problem: what if we just want to make all rotations by the same angle equivalent? We know from before that a rotation around C by angle α can be written $T_C R_\alpha T_C^{-1}$. A similar result we’d found was that any reflection can be written $\phi\rho\phi^{-1}$ for some $\phi \in \mathcal{G}$. Inspired by this, we defined the following binary comparison on $\mathcal{G}$:

$$f \sim g \quad \Longleftrightarrow \quad \exists \phi \in \mathcal{G} \text{ such that } \phi f \phi^{-1} = g.$$

As we saw above, any reflection is equivalent to ρ under this, and any rotation by α is equivalent to R_α. Moreover, we proved this is an equivalence relation:

(I) Reflexive: for all $f \in \mathcal{G}$, we have $f \sim f$.
(II) Symmetric: if $f \sim g$, then $g \sim f$.
(III) Transitive: if $f \sim g$ and $g \sim h$, then $f \sim h$.

You should make sure you can prove all of these, without referring to your lecture notes!

Analyzing our proofs of these, we realized that they implicitly depend on some properties of $\mathcal{G}$. (I) depends on the existence of the identity in $\mathcal{G}$. (II) follows from the existence of inverses in $\mathcal{G}$, i.e. $\phi^{-1} \in \mathcal{G}$ for any $\phi \in \mathcal{G}$; we also need $(\phi^{-1})^{-1} = \phi$ for all $\phi \in \mathcal{G}$. Finally, (III) is true because $(\phi\psi)^{-1} = \psi^{-1}\phi^{-1}$. More crucially, and much more subtly, (III) holds because composition is

Date: October 11, 2013.

associative: for any three isometries $\phi, \psi, \gamma \in \mathcal{G}$, the triple composition $\phi\psi\gamma$ is unambiguous. What does this mean? Well, in principle composition is a way of combining *two* things, not *three* things, so we cannot compose three different isometries simultaneously: we can compose two of them, then compose the result with the remaining one. Thus when we write $\phi\psi\gamma$ it could mean $(\phi\psi)\gamma$ or $\phi(\psi\gamma)$; associativity means that these are the same.

It might seem to you that associativity is esoteric. Certainly, it's true that most binary operations you've seen are associative. For example, addition: $3 + 4 + 7$ is entirely unambiguous. Multiplication is also associative: $3 \times 4 \times 7$ is unambiguous. But division is stranger. For example, what is $4 \div 2 \div 2$? Some of you thought the answer should be 1, others thought 4. The point is, it's not obvious – without explicitly writing parentheses – how to interpret $4 \div 2 \div 2$. So, $\div$ isn't associative.

From our two equivalence relations $\cong$ and $\sim$, we have the following list of important properties satisfied by $\mathcal{G}$:

(1) $\mathcal{G}$ has an identity (needed for reflexive property for $\cong$);
(2) every element of $\mathcal{G}$ has an inverse in $\mathcal{G}$ (needed for symmetric property of $\cong$);
(3) $\mathcal{G}$ is *closed* under composition (needed for transitive property of $\cong$);
(4) for all $\phi \in \mathcal{G}$, we have $(\phi^{-1})^{-1} = \phi$ (needed for symmetric property of $\sim$);
(5) $\mathcal{G}$ is *associative* (needed for transitive property of $\sim$); and
(6) for all $\phi, \psi \in \mathcal{G}$, we have $(\phi\psi)^{-1} = \psi^{-1}\phi^{-1}$ (needed for transitive property of $\sim$).

It is an exercise to show that properties (4) and (6) can both be derived from the definition of an inverse. By contrast, the remaining four properties – closure, associativity, existence of identity, and existence of inverses – are independent of one another. This inspires the following definition.

Definition. *A* group *is a set* Γ *with a binary operation* $@$ *(i.e.* $@ : \Gamma \times \Gamma \to \Gamma$*) such that*

(1) Γ *is associative under* $@$*;*
(2) Γ *has an identity under* $@$*, that is there exists an element* $e \in \Gamma$ *such that* $e@x = x = x@e$ *for all* $x \in \Gamma$*; and*
(3) *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}*.)*

Thus, a group is a set of objects (numbers, functions, etc.) with some nice way of combining two of these objects to get a third. Note that the four properties enjoyed by the set of isometries $\mathcal{G}$ are exactly what we use in this definition. (Where's closure?) Most of the rest of the semester will be spent discussing groups, many examples of which you've already seen.

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