GROUPS AND SYMMETRY: LECTURE 13

LEO GOLDMAKHER

We started by making one small but important change to our definition of a group. Here's the definition we had:

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 $@$
(1) $@$ is associative on Γ
(2) Γ has an identity with respect to $@$
(3) Γ has inverses with respect to $@$

The change we made was to our definition of identity: from now on, we say $e \in \Gamma$ is an *identity* of Γ with respect to $@$ iff for all $x \in \Gamma$, we have

$$e@x = x = x@e.$$

Last time, we only required the first equality. It's an easy exercise to verify that all of our examples from last lecture are still groups – in each case, the obvious 'left' identity also works as a 'right' identity.

We then discussed a few more examples of groups.
(12) $(V, +)$ is a group, for any vector space V. This should be familiar from linear algebra.

(13) Let $GL_n(\mathbb{Q})$ denote the set of all $n \times n$ matrices with rational entries and nonzero determinant. Then $(GL_n(\mathbb{Q}), \times)$ is a group, where $\times$ is the usual matrix multiplication. (GL stands for 'General Linear' group; recall that matrices represent linear maps, so $GL_n(\mathbb{Q})$ contains all linear maps which are invertible.)

(14) Let $SL_n(\mathbb{Q})$ denote all $M \in GL_n(\mathbb{Q})$ such that $det(M) = 1$. Then $(SL_n(\mathbb{Q}), \times)$ is a group. (This is called the *special linear group*.)

Our next two examples are more exotic, and take more preparation. Consider the following arrangement of numbers:

8	1	6
3	5	7
4	9	2

This arrangement has a special property: the sum of the entries in any row is 15 (e.g. $8+1+6 = 15$); the sum of the entries in any column is 15 (e.g. $8+3+4 = 15$); and even the sum of the entries in the two main diagonals is 15 (e.g. $8+5+2 = 15$). This is an example of a *magic square*: a square

Date: October 25, 2013.

arrangement of numbers such that every row, every column, and the two main diagonals each sums to the same value. Note that there are some trivial magic squares, for example

1	1	1
1	1	1
1	1	1

There's a natural notion of addition of magic squares: given any two 3×3 magic squares, define

a	b	c		a*	b*	c*		a+a*	b+b*	c+c*
d	e	f	+	d*	e*	f*	=	d+d*	e+e*	f+f*
g	h	i		g*	h*	i*		g+g*	h+h*	i+i*

A bit of thought shows that this is a binary operation on the space of 3×3 magic squares. This leads to our next example.

(15) Let $\mathcal{M}$ denote the set of all 3×3 magic squares. Then $(\mathcal{M}, +)$ is a group.

(16) Given a set A, let S_A denote the set of all *bijections* from A to itself. Then $(S_A, \circ)$ is a group, where $\circ$ is usual function composition.

We explored two special cases of this last example. First, let $A := \{1, 2, 3\}$. What are the elements of S_A? The first suggestion was the identity function: $\sigma_0 : A \to A$ defined by $\sigma_0(x) = x$ for all x. This is a bijection from A to itself, so we concluded that $\sigma_0 \in S_A$. The next suggestion was τ defined by $\tau(1) = 3$, $\tau(2) = 1$, $\tau(3) = 1$. This is a function from A to itself, but it's not a bijection! Hence, $\tau \notin S_A$. A third suggestion was $f : A \to A$ defined by $f(x) = |x - 4|$. This is easily seen to be a bijection from A to itself, so $f \in S_A$.

After these examples, one thing became very clear: we need to better notation for elements of S_A. To do this, we first discussed what the elements of S_A actually *do*: they permute the elements of A. For example, f above rearranges the ordered set $(1, 2, 3)$ into $(3, 2, 1)$. We represented this by

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

More generally, for any $\sigma \in S_A$, we describe σ by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$$

By thinking about this, we quickly realized that for this choice of A, we have $|S_A| = 6$.

Note that this notation works more generally than for the example $A = \{1, 2, 3\}$. For example, let $B := \{\text{apple, banana, charlie}\}$. Here's an example of an element of S_B:

$$\begin{pmatrix} \text{apple} & \text{banana} & \text{charlie} \\ \text{banana} & \text{charlie} & \text{apple} \end{pmatrix}$$

We quickly decided that, although the set B is quite different from the set A, the two groups S_A and S_B are very similar; if we replace every occurence of apple by 1, banana by 2, and charlie by 3, then every statement about S_B would be a statement about S_A.

We've now seen many examples of groups: sets of numbers, functions, geometric objects, even fruit mixed with a name. We now start proving things about groups. The power of the subject is

that any theorem we prove about an arbitrary groups *automatically* applies to every example of a group. Thus, any theorem about groups will simultaneously tell us something about the behavio(u)r of numbers, of words, of functions, of shapes, etc.

With this in mind, we started exploring properties of groups. The first question was about the identity property. Every example we've seen has an obvious identity. Are there ever multiple identities? The group axiom doesn't stipulate that there's a unique identity, just that there exists at least one. However, all of our examples convinced us that the following should be true:

Proposition 1. *Any group* $(\Gamma, @)$ *has a unique identity.*

It took us a few minutes to write down a proof of this. Our original proof was a bit complicated, but after writing it down we realized that it's possible to give a very short proof.

Proof. Suppose e_1 and e_2 are both identities of $(\Gamma, @)$. Then by definition of identity, we have

$$e_1 = e_1 @ e_2 = e_2. \qquad \square$$

From now on, we can (and will!) refer to *the* identity.

Next, we discussed inverses. Right away there are two properties we expect to be true, but don't know *a priori*.

(1) Every $x \in \Gamma$ has a unique inverse.

(2) If y is a left inverse of x (i.e. if $y@x = e$), the it is also a right inverse of x (i.e. $x@y = e$).

Dan pointed out that if (2) is true, then it allows us to say something about (1). We explored this at the very end of lecture, and will take this up anew on Monday.

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