GROUPS AND SYMMETRY: LECTURE 20

LEO GOLDMAKHER

We started by playing the *Game of 15*. The game is for two players (in class I played against Jay), and is played as follows. Jay and I take turns picking numbers from the list

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\};$$

whenever a player picks a number, it moves from A into his personal list. The first person to collect three numbers which sum to 15 is the winner.

For example, our first game went roughly like this:

(1) Jay picked 5.
(2) Leo picked 1.
(3) Jay picked 8.
(4) Leo picked 2. (Note that I was forced to pick this – otherwise Jay would have won in the next move.)
(5) Jay picked 3.
(6) Leo loses. Why? I must take 4, since otherwise Jay would win ($4 + 3 + 8 = 15$). But I also must take 7, since otherwise Jay would win ($7 + 3 + 5 = 15$). Since I can only take one of these, I lose the game!

After one game, people noted that this was reminiscent of tic-tac-toe. After a second game, Jay and Dinu (and possibly others) independently arrived at the conclusion that this game is like playing tic-tac-toe on the magic square

8	1	6
3	5	7
4	9	2

In fact, it isn't like playing tic-tac-toe on this board – the two games are identical, just played with different symbols. They are two different ways to view the same game.

We say these two games are *isomorphic*[1] (you have previously seen this term in linear algebra). Similarly, we will say that two groups are isomorphic if they are actually the same group, except that the elements are called by different names. For example, the groups $\{1, i, i^2, i^3\}$ and $\{\mathbb{1}, R_{\pi/2}, R_{\pi/2}^2, R_{\pi/2}^3\}$ are isomorphic: they have exactly the same multiplication table, once you relabel 1 as $\mathbb{1}$ and i as $R_{\pi/2}$ everywhere in the table. Of course, as *sets* these two are quite different. But as *groups* they are indistinguishable; in each one, the elements are related to the other elements in precisely the same way.

We will give a more precise definition of isomorphism next lecture. For now, we explored the idea by creating all possible multiplication tables of a group Γ. What does this mean? Consider an arbitrary group of order 3; let's say its elements are $\{e, a, b\}$ where e is the identity of the group. What is the multiplication table of this group? Right away from the definition of identity, we have the following:

Date: November 18, 2013.

[1] $\iota\sigma o\zeta$ means 'equal', $\mu o\rho\varphi\eta$ means 'shape'.

$\cdot$	e	a	b
e	e	a	b
a	a		
b	b		

To keep filling in the above, we need to decide what a^2 is. Could it be a? No, because if $a^2 = a$ then $a = e$, which is not the case (our group has order 3, so all three elements are distinct). We next observed there was another way to see that $a^2 \neq a$. From problem 7.1(b), we know that $g\Gamma = \Gamma$ for any group Γ and any $g \in \Gamma$; this implies that all the elements of the group must appear in any row of the multiplication table. Put another way, *no element appears twice in any row of the multiplication table*. I called this the Sudoku property. Similarly, one can prove $\Gamma g = \Gamma$ for any $g \in \Gamma$, whence no element appears twice in the same column. These observations demonstrate that there is only one way to fill in the rest of the multiplication table (make sure you understand why!):

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We conclude that every group of order 3 has the same operation table. (Compare this with the addition table for $\mathbb{Z}/3\mathbb{Z}$ from the end of the previous lecture.) In other words, there is only one group of order 3, up to isomorphism (i.e. up to renaming the elements of the group).

A group is completely described (up to isomorphism) by its multiplication table. In practice, however, it's a pain to write the whole table out. Is it possible to describe a group in an easier way? Consider the multiplication table above (for the abstract group of order 3). Note that $b = a^2$. It follows that the group is cyclic, generated by a; we write $\langle a \rangle$. The problem with this notation is that, if I just wrote that down without telling you anything else about the group, you'd be hard pressed to know which group I was trying to generate. Instead, we write down $\langle a : a^3 = e \rangle$; in other words, the group generated by a, subject to the condition that $a^3 = e$. Now, even if you knew nothing else about the group, you could completely reconstruct its multiplication table. This way of describing a group – in terms of its generators and relations between them – is called a *group presentation*. We'll see a more complicated example below, but for now observe that we could have listed more relations for the group above (e.g. $a^4 = a$). However, any additional relation is superfluous, since the one relation we listed completely determines the multiplication table already. In general, when writing a group presentation, you should try to list the smallest possible number of relations.

The above shows that there's only one group of order 3 (up to isomorphism), and that it's cyclic. This isn't terribly surprising in hindsight, since we already know that any group of prime order is cyclic, and is in fact generated by any of its non-identity elements.

Next, we turned to groups of order 4. Denote the elements by $\{e, a, b, c\}$, where e is the identity of the group. As before, by definition of the identity we can write

$\cdot$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

What about a^2? By the Sudoku principle, it can't be a (since there's already an a in that row), but it could be any of e, b or c. Now, e and b are legitimately two different possibilities, but b and c are not – we haven't assumed anything them, except that they were two different non-identity elements. Thus, at this point in our process, we can switch the names of b and c with impunity. We therefore really only have two cases to consider:

Case (I)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			
c	c			

Case (II)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b		
b	b			
c	c			

Case (II) is the simpler of these: the Sudoku principle forces us to complete as below (make sure you can do this on your own!). Applying the Sudoku principle to Case (I), however, only gets us so far:

Case (I)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

Case (II)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

To continue filling in Case (I), we once again must make a choice: should $b^2 = e$ or a? Either is possible, so we have two cases to consider:

Case (I.a)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	
c	c	b		

Case (I.b)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	
c	c	b		

The Sudoku principle now forces us to complete both of these cases as follows:

Case (I.a)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Case (I.b)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

To summarize, there are only three cases to consider. Case (II) is easily seen to be cyclic, generated by a; its group presentation is

$$\text{Case (II)} \qquad \langle a : a^4 = e \rangle$$

Case (I.b) is not too difficult either:

$$\text{Case (I.b)} \qquad \langle b : b^4 = e \rangle$$

Right away, we conclude that the groups defined by these two cases are isomorphic: if we switch the roles of a and b, their multiplication tables become indistinguishable. They are both *the* cyclic group of order 4. (I've highlighted the definite article to point out that there can only be one such group up to isomorphism. Make sure you understand this point.)

The final situation, Case (I.a), is more interesting. The group cannot be generated by any of its elements, since the square of each element is e. Thus, we need at least two generators. However, we don't need all three non-identity elements, since a and b generate c. Now, which relations do we need in order to be able to generate the multiplication table from scratch? We need to know that both $a^2 = e$ and $b^2 = e$ (knowing one of these isn't enough: for example, if we only knew that $a^2 = e$, we wouldn't be able to say anything about the element b^3). Are these two relations enough? Not quite. Try writing down a multiplication table based on just these two relations to see what goes wrong. We can get away with just one more relation, however:

$$\text{Case (I.a)} \qquad \langle a, b : a^2 = e, b^2 = e, ab = ba \rangle$$

For example, what is $(ab)^2$ in the group determined by the above presentation? We have

$$(ab)^2 = abab = a(ba)b = a(ab)b = a^2b^2 = e.$$

A better exercise is to prove that the every element of the above group can be written uniquely in the form $a^j b^k$, where $j, k \in \{0, 1\}$. (Even things like $a^{153}b^4a^7b^{-2}$ can be simplified to this form.) We deduce that the group defined by the above presentation must have four elements – which is exactly what we wanted!

We concluded that there are exactly two groups of order 4 (up to isomorphism); the cyclic group of order 4, and the second weirder one in which every element squares to e. This second group is called the Klein V group (named after Felix Klein, one of the innovators of using group theory to study geometry). The V is short for *vier*, which is the German word for 'four'.

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