Math 31 Lesson Plan

Day 5: Intro to Groups

Elizabeth Gillaspy

September 28, 2011

Supplies needed:

- Sign in sheet

Goals for students: Students will:

- Improve the clarity of their proof-writing.
- Gain confidence in their proof-writing abilities.
- Understand the proofs of the selected propositions (which we had mentioned in class but hadn't discussed the proofs)
- Feel more comfortable with the concept of a group
- Feel more comfortable with the notation used for matrix groups and $\mathbb{Z}_n$.

[**Lecture Notes: Write everything in blue, and every equation, on the board. [Square brackets] indicate anticipated student responses. *Italics* are instructions to myself.**]

pass around sign-in sheet

I'll return your quizzes on Friday – or you can come get them in office hours – everyone got 100%.

Please come meet with me this week, so that I can figure out the groups for the presentations!

Today we're going to finish up yesterday's activity about proof-writing. Then we're going to discuss your questions about groups from the reading, and tie that material back to D_4, the symmetry group of the square. At the end, if there's time, we'll start on Section 3, Fundamental Theorems about Groups.

Please get back into your groups from yesterday.

Is there one person from each group who has a copy of the lists we had on the board yesterday? *If not, ask for dictation and I'll write them on the board*

Once you've figured out the problem you were working on, try to write up a proof following the guidelines we discussed for writing good proofs. As you write (and read), think about:

- Which of the characteristics of a good proof does this proof exhibit?
- Are there other characteristics that you want to add to the list?

Have groups switch papers, and read & comment on each other's proofs, when finished. At end, brief class discussion about characteristics to add to lists. Does everyone understand the proofs of both Proposition A and Proposition B? 12:55

I wanted to make a couple of general comments. First, two points about proofs of statements about sets:

1. To show two sets A and B are equal, what do you have to do? [Show $A \subseteq B$ and $B \subseteq A$.]
2. To prove a statement about a set, first prove it for an arbitrary element of the set.

Who can tell me why this will prove the statement in general?

Another general comment: Just because Saracino says something is obvious doesn't mean it's true! Often, Saracino doesn't check whether something is a binary operation, or whether it's associative. This is another way of encouraging you to be an active reader and check the statement yourself! As we said when talking about reading math, you need to make sure that you're convinced of the truth of each sentence before moving on.

OK, enough generalities. Let's start talking about Groups!

A lot of you asked about why groups are useful and why they're defined the way they are. For the second question: As happens with a lot of mathematical concepts, mathematicians spent a lot of time muddling around trying to come up with the right definition, the right way to understand or generalize the problem they were seeing, and then once they found the right definition, they just stuck with it. Math is, unfortunately, not usually taught from the historical perspective, so you don't often know why we have a certain definition, other than "It works pretty well this way." I don't know why we require associativity and not commutativity for groups, except that every type of multiplication we know of is associative, but (for example) matrix multiplication and function composition are not usually commutative, so that seems like a more sensible requirement to drop.

As to why groups are useful, you could read pp. 36-37 in Gallian. This talks more about the symmetry groups, like D_4, and their applications to chemistry and design. And of course we'll see more applications later in the term, with presentations.

Speaking of the symmetry groups, who can tell me Why is D_4 a group? *Think-Pair-Share?*

- We checked that the operation is binary on Monday.
- To check that the operation is associative, we could either check that $(a*b)*c = a*(b*c)$ for all $a, b, c \in D_4$ – or we could observe that function composition is associative, and that's the group operation in D_4.
- We have an identity element, 0.
- Every element has an inverse.

Notice that there's only one identity element in D_4. How many inverses does each element have? [one] This is true in more generality; you'll prove this at the end of class if there's time, or you'll read the proofs in the text if there's not. 1:15

Let's talk about another example. This one comes from linear algebra: The general linear group $GL(2, \mathbb{R})$. Who can tell me what this is in words? [The group of all 2×2 invertible matrices with real entries.] In symbols,

$$GL(2, \mathbb{R}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \}.$$

Why did I say $ad - bc \neq 0$? [$ad - bc$ is the determinant of the matrix, and that's a condition for invertibility.]

What group operation do we want to use here? [multiplication]

What do we have to check in order to see that $GL(2, \mathbb{R})$ is actually a group?

- Matrix multiplication is a binary operation on $GL(2, \mathbb{R})$
- Matrix multiplication is associative
- $GL(2, \mathbb{R})$ has an identity
- Every element of $GL(2, \mathbb{R})$ has an inverse

Who wants me to check what? *Don't check associativity; it's a long messy calculation.*

To show that matrix mult is binary, here's a different approach than Saracino's. Suppose $A, B \in GL(2, \mathbb{R})$. What do we want to show? [We want to show that $AB \in GL(2, \mathbb{R})$.] What do we know about A and B? [We know that $\det A \neq 0$ and $\det B \neq 0$.] So, now what? Since $\det AB = \det A \det B$, it follows that $\det AB \neq 0$, so $AB \in GL(2, \mathbb{R})$ as claimed. □ *Comment on box at end of proof*

Next example: $(\mathbb{Z}_n, \oplus)$. I'd like to talk about these groups via a specific example, $\mathbb{Z}_8$. Then we'll talk a little about the different notation you can use for congruence mod n. At the end, if there's time, I'll let you choose between reviewing the proof of the division algorithm, and proving uniqueness of identities and inverses.

Cayley table of $(\mathbb{Z}_8, \oplus)$. In order to draw a Cayley table, we have to have at least a binary operation, so that everything in the diagram is part of the same set. How can we make addition on $\mathbb{Z}_n$ into a binary operation? [By taking remainders modulo n. Let's work through this in the case of $\mathbb{Z}_8$. Don't worry, this is much easier than D_4!

Fill out Cayley table. I know the textbook denotes elements in $\mathbb{Z}_n$ by a bar over the top. You can do that. I usually just write the number, as long as it's clear from context that I'm thinking about the number as an element of $\mathbb{Z}_n$, not $\mathbb{Z}$ or $\mathbb{N}$. You can also write an element in $\mathbb{Z}_n$ as [k]. If you've seen equivalence relations before, this will be familiar – if not, no worries!

So – Can we tell from the Cayley table whether $(\mathbb{Z}_8, \oplus)$ is a group? What do we have to check?

- Binary?
- Associative?
- Identity?
- Inverses?

We can tell binary from the table – every element in the table also shows up in the top row, so it's definitely an operation that takes pairs of elements to some other element in the set.

Associativity follows from the associativity of addition in $\mathbb{Z}$. Since $(a+b)+c = a+(b+c)$ in $\mathbb{Z}$, let's give them both a name: k. Since $[(a+b)+c] \in \mathbb{Z}_n$ is the remainder of $(a+b)+c = k \bmod n$, and $[a+(b+c)] \in \mathbb{Z}_n$ is also the remainder of $k \bmod n$, it follows that $[a+(b+c)] = [a+(b+c)]$. In other words, addition is associative in $\mathbb{Z}_n$.

OK, any questions about $\mathbb{Z}_n$?

Who wants to go over the Division Algorithm? *if lots, get someone to tell me the statement; have the class help me prove it.*

Why is the Division Algorithm useful in this section? [It tells us that the remainder mod n is well defined – that is, for each $a \in \mathbb{Z}$, there's exactly one number in $\mathbb{Z}_n$ that is the remainder of a after dividing by n.]

LEMMA 2.1: THE DIVISION ALGORITHM *If $a, n \in Z$ and $n > 0$, then there exist unique integers q, r with $0 \leq r < n$ such that $a = qn + r$.*

Proof: For existence, let q be the largest integer such that $qn \leq a$. Then define $r = a - qn$. Clearly $0 \leq r$, so we need to show that $r < n$. Let's use proof by contradiction: Suppose $r \geq n$ – then $a - qn \geq n \Rightarrow a \geq (q+1)n$, which contradicts our choice of q. Therefore, we must have $r < n$ as desired.

For uniqueness, suppose $a = q_1 n + r_1 = q_2 n + r_2$. Then $r_2 - r_1 = (q_1 - q_2)n$, so $r_2 - r_1$ is a multiple of n. But since $0 \leq r_1, r_2 \leq n - 1$, the biggest $r_2 - r_1$ can be is $n - 1$; the smallest it can be is $-(n - 1)$. The combination of these conditions tells us that $r_2 - r_1 = 0$. Therefore $r_2 = r_1$; subtracting and dividing by n shows us that we also have $q_2 = q_1$. Thus there is only one way to write $a = qn + r$. $\square$

THEOREM 3.1: In a group $(G, *)$, there is only one identity element.

THEOREM 3.2: If x is an element of a group $(G, *)$, then there is only one inverse $y \in G$ for x.

The easiest way to prove either of these is proof by contradiction.

I'd like half the room to work on proving Theorem 3.1, and half to work on Theorem 3.2. You can work together if you'd like; when you're done, I'll ask you to present your proof to the class. No peeking in the textbook!

- Read Section 3. Post a comment by Thursday at 10 PM.
- Homework 1!
- Talk to me

homework