Math 31 Lesson Plan

Day 6: Fundamental Theorems

Elizabeth Gillaspy

September 30, 2011

Goals for students: Students will:

- Improve their fluency with the concept of a group
- Gain more familiarity with basic groups

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

- *Return quizzes.*
- *Collect HW*
- *Pass around sign-in sheet.*
- *Remind them to come talk to me; say I'll have groups figured out by Monday.*

I want to start today by talking about different notation for the group operations, especially since that came up on the homework as well. Then, since there was a lot of confusion about Theorem 3.7, I'm going to go through a different proof of it. And at the end we're going to play Group Quiz Bowl!

I also want your opinion about topic for x-hour next week. We could spend more time on proof by induction; we could spend more time on proof-writing tips in general; if you still have unanswered questions from Sections 0-4 we could go back to those. For example, I know some people were confused about the Fundamental Theorem of Arithmetic, Division Algorithm.

I'd like you to think about it, and if you have a suggestion for a topic for x-hour (or if you'd like to cancel it next week!) email me your vote this weekend.

As you noticed on the homework, I (and many people) get tired of writing things like $(a*b)^{-1}*(a*b)^{-1}$, and so we simplify it to $(ab)^{-2}$. You can check, if you want, that

$$(a*b)^{-1}*(a*b)^{-1} = \left((a*b)^2\right)^{-1} = (a*b*a*b)^{-1},$$

so that the notation $(ab)^{-2}$ is unambiguous.

Anyway: For an arbitrary group, the operation is usually written as multiplication. We do this because, as we talked about on Wednesday, groups are an attempt to generalize multiplication (and this is why we require associativity for groups, but not commutativity).

However, If we're working with a specific group, and the operation is familiar from our life before Math 31, we'll use the familiar notation for the operation. For example, in $(\mathbb{Z}, +)$, what's the identity element? [0] So therefore, what's the inverse of an element $x \in \mathbb{Z}$? $[-x]$. So, when we're writing about this group, we use $-x$ rather than x^{-1} to denote the inverse. This is also why we use $\oplus$ for the groups $\mathbb{Z}_n$; these groups are closely related to $(\mathbb{Z}, +)$, and we want our notation for the operation to remind us of that.

We'll spend some more time talking about different notation for different groups next week, but for now, are there any questions? 1:45

OK, let's talk about Theorem 3.7. I know some of you asked "What's the point of this theorem?" *ask for volunteers to answer this* Basically, Theorem 3.7 means that to show $(G, *)$ is a group, we only have to check that we have a left identity, and that every element has a left inverse.

Some of you asked why we didn't define a group this way in the first place. Does anyone have any ideas? [We want the identity and inverses to always work on both sides, but the Example on page 30 shows that a left identity need not be a two-sided identity in general.] So we started by requiring two-sided identities and inverses, since that's what we needed, and then we showed that we can be less strict with our requirements.

This happens a lot in math – you make a bunch of assumptions, and then you get to the end of a theorem and you realize that there's a tidier way to prove it that doesn't require assuming so much. I know some of you had this experience with the starred problem for this week's homework assignment.

I'm actually going to prove the analogue of Theorem 3.7 for a left identity and left inverses, so that you have both results available to you.

EG's Theorem 3.7 *Let G be a set and let $*$ be an associative binary operation on G. Suppose that:*

- *there exists an element $e \in G$ such that $e * x = x$ for all $x \in G$; and*
- *for every element $x \in G$, there exists $y \in G$ such that $y * x = e$.*

Then G is a group.

Proof: What do we have to show? [We must show that $x * e = x$ for every $x \in G$, and also that $x * y = e$.] For the first assertion, fix $x \in G$ and let y be a left inverse for x. Observe that

$$y * x = e = e * e = (y * x) * e.$$

Now, multiply both sides of the equation by a left inverse for y: Call it z.

$$\text{LHS: } z * y * x = e * x = x; \text{RHS: } z * y * x * e = e * x * e = x * e.$$

For the second assertion, we know that y has a left inverse – Call it z. We want to show that $z = x$. Is that clear to everyone? *The idea is that we need to show that our given left inverse for x, which is y, is also a right inverse – but that's equivalent to saying that x is a left inverse for y.* Now,

$$z * (y * x) = (z * y) * x = e * x = x,$$

but associativity also tells us that

$$z * (y * x) = z * e = z$$

by the first assertion. Therefore $x = z$ as claimed. $\square$.

Questions?

Remember, In an arbitrary group, you can't assume that the operation is your usual multiplication! The operation could be symmetric difference, or matrix multiplication, or something even crazier. That's why in this section we were so careful to show that (many of) the properties we associate with multiplication still hold in any group – the uniqueness of identities and inverses, the cancellation laws.

Now, in the future, thanks to these kind of messy technical results, future proofs should be tidier.

Quiz Bowl: *divide class into two teams*

Race to answer correctly: If Team A answers correctly, then Team B has to explain why.

That is, I'll put on board a set with a binary operation – eg, $(\mathbb{Z}, -)$. If Team A is the first to say "$(\mathbb{Z}, -)$ is not a group," then Team B has to come up with a reason why.

Once a person from Team A has answered, they can't talk again for the next 2 rounds – this is to give everyone a chance to participate.

The sets we used were:

- $(\mathbb{R}, -)$ [no; not associative]
- $(\mathbb{Q}, \times)$ [no; 0 has no inverse]
- $(SL(2, \mathbb{R})$, matrix addition) [no; the identity is the 0 matrix, which is not in $SL(2, \mathbb{R})$
- $(3\mathbb{Z}, +)$ [yes]
- $(\mathbb{Q}^\times, \times)$ [yes]
- $(\{1, -1\}, \times)$ [yes]

- $(\mathbb{R}\backslash 0, a * b = |ab|)$ [no; no identity element]
- $(SL(2,\mathbb{R})$, matrix multiplication) [yes]
- ({continuous functions f on the real line such that $f(x) \neq 0$ for all $x \in \mathbb{R}$}, $f * g(x) = f(x)g(x)$) [yes]