Math 31 Lesson Plan

Day 9: Order; Cyclic Groups

Elizabeth Gillaspy

October 5, 2011

Supplies needed:

- Worksheets
- Colored chalk

Goals for students: Students will:

- Recognize that they are already familiar with examples of cyclic groups
- Become more precise and careful when making, reading and proving statements

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

Introduce Rosa

Today we're going to spend a little time reviewing the concept of the order of an element. I'll also try to clear up your questions from the reading about cyclic groups, and then I'd like you to work in groups on some more exercises dealing with examples of cyclic groups.

Check with Steven if he wants to discuss his question from Monday, about the $-m$ in the proof that $x^{mn} = (x^m)^n = (x^n)^m$.

Order of an element: *Ask students for definition; write on board* [The order $o(x)$ of an element x in a group G is the smallest integer n such that $x^n = e$.

- We talked on Monday about how we can use order to tell two groups apart. Can anyone summarize that discussion for me?
- Order is always a positive integer, or ∞. We define $x^0 = e$ for any x.
- Ask students to give some examples of elements of finite order, both in finite and infinite groups. 12:40
- What does it mean for an element to have infinite order?

I'd like you to divide into groups of 3 or so. As a group, decide if you're A or B; work on proving the corresponding statement. If you finish early, start trying to prove the other one! Then I'll ask a volunteer to prove each statement at the board.

A Prove that every element of a finite group must have finite order.

B Prove that $o(x) = o(x^{-1})$ (Theorem 4.4 (i)) 1:00

A lot of people had questions about Theorem 4.4 (iii), so we're going to go over the proof of that. As far as why it's useful, some problems where you need this will come up on the homework! In general, this is useful because it helps us to calculate the order, which can tell us more about a group.

Theorem 4.4 (iii) *If $o(x) = n$ and $(m, n) = d$, then $o(x^m) = n/d$.*

Proof: We want to show two things; any idea what? [first, that $(x^m)^{n/d} = e$, and second, that if $(x^m)^k = e$ then $k \geq n/d$.] How would we prove the first statement? [For the first statement, since $d = (m, n)$ divides m, we can rewrite:]

$$(x^m)^{n/d} = (x^{m/d})^n = (x^n)^{m/d} = e^{m/d} = e.$$

For the second statement, use Theorem 4.4 (ii) – If $(x^m)^k = e$, then we must have $n|mk$. Observe that d divides both sides evenly; therefore, we know that $n/d|(m/d)k$. Since $(m, n) = d$, it follows that $(m/d, n/d) = 1$. Why? [If $(m/d, n/d)$ had a larger divisor, say j, then jd would divide both m and n, contradicting the definition of $(m, n) = d$.] Therefore, by Theorem 4.3, we must have $n/d|k$, and so $n/d \leq k$ as claimed. □ 1:10

Questions?

Cyclic groups: *Ask students for definition; write on board.* [The cyclic group generated by x is written $< x >$, and it consists of all integer powers of x.] The operation we want to use on x is generally clear from context, but if it's not, you can specify by writing $< x, * >$.

- What examples do we know of cyclic groups? [$\mathbb{Z}, (\mathbb{Z}_n, \oplus)$] *Explain why these are cyclic*
- What's the identity in an infinite cyclic group?
- A cyclic group is necessarily abelian. Are all abelian groups cyclic? *discuss V_4 via $P(\{a, b\}, \Delta)$ and also via Cayley table*

- What's the identity in $P(\{a, b\}, \Delta)$? [emptyset]
- Observe that everything squares to $\emptyset$.
- Fill out Cayley table.

- Must every element of $< x >$ be a generator? *discuss in pairs*

Worksheet, if time The worksheet is to give you more practice with cyclic groups, and order, before doing the homework. These problems are all taken from the textbook, and many of them have the answers in the back, too. But you can also come ask me about the worksheet in office hours.