Math 31 Lesson Plan

Day 7: Order and Euclidean Algorithm

Elizabeth Gillaspy

October 3, 2011

Supplies needed:

- Quizzes
- Starred problems

Goals for students: Students will:

- Solidify their understanding of the Euclidean algorithm
- Become (more) able to use multiplicative notation without automatically assuming the group consists of real numbers.

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

- *Quizzes*
- *Return starred problems*
- *Reminder – Name on starred problem!*
- *No texting in class!*
- *Announce topic for Tuesday (Fund Thm of Arith?)*
- *Announce reading for Weds*

Today we're going to discuss some of the questions you had about notation and about the order of an element. We'll also spend a lot of time reviewing the Euclidean algorithm; it can be pretty confusing the first time you see it! Hopefully a few more examples will help clear things up.

Notation:

- Be careful: multiplicative notation doesn't mean you're actually multiplying numbers! Even though the notation is familiar, you have to go back to the definitions and the theorems we've already proved. Can't assume that everything works the way it does in multiplying numbers till you've proved that!

  Of course, it turns out that things do work pretty much the way they do in multiplying real numbers; this is why we use multiplicative notation.
- Review definition of inverse
- Prove that $(x^{-1})^n = (x^n)^{-1}$

- Prove 4.2(i) ($x^{m+n} = x^m x^n$) if students want and there's time 12:50
- Prove 4.2(iii) ($x^{nm} = (x^n)^m = (x^m)^n$) in groups.

Order:

- Ask someone for the definition of order. Put it on the board.
- Order is *smallest* integer
- Order is always an integer because we can't take square roots (etc) in general
- Order can help us tell groups apart; $D_3, \mathbb{Z}_6$ from homework
- Ask for examples of elements of finite order in various groups – infinite (like matrices) and finite
- *in gps*
  - Prove that every element of a finite group must have finite order. 1:15
  - Prove that $o(x) = o(x^{-1})$ (Theorem 4.4 (i))

Euclidean algorithm:

- This is confusing! I had a really hard time with it the first time I studied it.
- These results from number theory about divisibility will be important for helping us to prove theorems about the possible orders of certain group elements. They will also come in handy when we get to the Fundamental Theorem of Finite Abelian Groups.

One of the important questions in group theory in general, and also in this class, is "How many different groups are there? Can we describe all of them?" In its full generality, this question is too big to answer in Math 31. But if we restrict ourselves to the case of finite abelian groups, we can answer it – and we will! We'll see that in order to describe all finite abelian groups with n elements, we need to understand the factorization of n; and in order to prove that we've found all possible groups with n elements, we'll need results like Theorem 4.2.

- Theorem 4.2, as stated, only applies to $\mathbb{Z}$ – but asking whether we can generalize it to make it apply to other groups is the sort of question that sparks a mathematical research project. That's a big part of what math research is all about; generalizing a cool result to work for more examples.
- Work a simple example of Euclidean algorithm – (60, 21)
  - Why is $(n, m) = (m, r)$?
  - The integers x, y such that $xn + ym = (n, m)$ can be negative!
- *in groups* Find (121, 44); (357, 240). Find integers x, y so that $121x + 44y = (121, 44)$, and integers z, w so that $357z + 240w = (357, 240)$.

Ask if they'd like to practice the Euclidean Algorithm more in x-hour tomorrow.

If time Theorem 4.4 (ii, iii)

- If $o(x) = n$ and $x^m = e$ then $n|m$.
- If $o(x) = n$ and $(m, n) = d$, then $o(x^m) = n/d$.

For first part, write $m = qn + r$. For second part, first show that $x^{mn/d} = e$; then observe that if $x^{mk} = e$, by part (ii) we must have $n|mk$. Hence n/d divides $k \cdot (m/d)$. Now, what's $(n/d, m/d)$? [1] Why?

Therefore, by Theorem 4.3, we must have $n/d|k$, and hence $n/d \leq k$. Thus n/d is the smallest integer k such that $x^{mk} = e$, so $n/d = o(x^m)$ as claimed. □