Math 31 Lesson Plan

Day 17: Sections 8 & 12

Elizabeth Gillaspy

October 19, 2011

Supplies needed:

- Colored chalk
- Quizzes/starred problems

Goals for students: Students will:

- See more examples of clear, coherent proofs
- Understand how to check whether a function is a homomorphism/monomorphism/epimorphism/isomo
- Believe that a permutation can't be both even and odd.

[**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, * probs*

Today's going to be a lecture-heavy day. First, I'm going to write on the board a proof of the fact about the order of a permutation that you guys figured out in your groups yesterday. Then we're going to talk about Section 12: Homomorphisms. At the end we'll talk about even and odd permutations and the alternating group.

CLAIM: *If $f \in S_n$ can be written as $f = f_1 \circ f_2 \circ \ldots \circ f_r$, where the f_i are disjoint cycles, then $o(f)$ is the lcm of the lengths of the f_i.*

Proof: Observe that the order of a cycle is the length ℓ of the cycle: If f_i^m is the identity, then we must have $f_i^m(x) = x$ for all $x \in \{1, 2, \ldots, n\}$. Since each successive application of the cycle f_i moves the element x one step to the right in the cycle, f_i^m will not act as the identity permutation for any $m < \ell$; but $f_i^\ell(x) = x$. Thus $\ell = o(f_i)$ as claimed.

Since each of the elements f_i affects distinct elements of $\{1, \ldots, n\}$,

$$f^m = f_1^m \circ f_2^m \circ \ldots \circ f_r^m.$$

(Alternatively, since the product of disjoint cycles is unaffected by the order of the cycles, we can group all the f_i's together.)

If f^m acts as the identity –that is, $f^m(x) = x$ for every $x \in \{1, 2, \ldots, n\}$, then we must have $f_i^m(x) = x$. Hence m must be a multiple of $o(f_i)$ for each i. Since the order of the cycle f_i is the length of the cycle, this tells us that the order of f – the smallest integer such that f^m is the identity permutation – must be the lcm of the lengths of the cycles, as claimed. $\square$

Section 12: Homomorphisms

Definition: Let $(G, \cdot), (H, *)$ be groups. A function $\phi : G \to H$ is a homomorphism if for all $a, b \in G$, we have $\phi(a \cdot b) = \phi(a) * \phi(b)$. We say that an onto homomorphism is an epimorphism and a 1-1 homomorphism is a monomorphism. A homomorphism that is 1-1 and onto is called an isomorphism.

Are the following maps homomorphisms? Onto? 1-1? Isomorphisms?

- $\phi : \mathbb{Z} \to \mathbb{Z}_n, \phi(m)$ is the remainder of m mod n
- $\phi : \mathbb{Z}_6 \to \mathbb{Z}_9, \phi(m)$ is the remainder of m mod 9
- G is the group of polynomials with real coefficients, $\phi : G \to G$ given by $\phi(p) = p'$
- $\phi : (\mathbb{R}^+, \cdot) \to (\mathbb{R}^+, \cdot), \phi(x) = \sqrt{x}$
- $\phi : (\mathbb{R}^+, \cdot \to (\mathbb{R}, +), \phi(x) = \sqrt{x}$

Define transposition/even/odd/A_n; emphasize that a product of transpositions need not be disjoint, and in fact usually won't be.

Theorem 8.4 A permutation can't be both even and odd.

In order to prove this, I want to introduce a new concept.

Definition: Let f be a permutation in S_n. An inversion in f is a pair of numbers i, j such that $i > j$ but j occurs to the left of i in the second line of the 2-line notation of f. We call this second line the 1-line notation of f.

Let's look at an example. How many inversions does the permutation $f = (1462)(35) \in S_6$ have?

First, we have to write the permutation in 2-line notation:

$$f = (1462)(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 6 & 3 & 2 \end{pmatrix}$$

Since 4 occurs to the left of 1, the pair $4, 1$ is an inversion. The pair $4, 3$ is also an inversion.

In this class, we're only interested in <u>how many</u> inversion there are, not which pairs (i, j) are inversions.

Since 4 occurs to the left of 1, 2, & 3; 5 occurs to the left of 2 & 3; 6 occurs to the left of 3 & 2; and 3 occurs to the left of 2, the permutation f has 8 inversions. We write inv((1462)(35)) = 8.

LEMMA: *If t is a transposition, and $f \in S_n$ is any permutation, then inv($t \circ f$) - inv(f) is an odd integer.*

Proof: Before we do the proof, let's see how this is working in the case of the example we looked at before: $f = 415632$ in 1-line notation. Let $t = (46)$. Then $t \circ f = 615432$ in 1-line notation. 6 occurs to the left of 1, 2, 3, 4, 5; 5 occurs to the left of 4, 3, 2; 4 occurs to the left of 3, 2; 3 occurs to the left of 2. Thus inv$(t \circ f) = 11 = 8 + 3$.

Back to the proof. Suppose t switches the integers i and j, and suppose $i < j$. There are two cases to consider: *Draw a picture!*

1. i occurs to the left of j in the 1-line notation of f;
2. i occurs to the right of j.

Observe that in Case 1, applying t makes i, j into an inversion when it wasn't before, and in Case 2, applying t makes i, j not an inversion, when it was one before. *Make a table: Case 1 vs Case 2. Put* +1 *in Case 1 column, -1 in Case 2 column.*

We also have to look at the effect of t on the other inversions in f. If k occurs to the left of both i&j, or to the right of both, does swapping i&j change the number of inversions that k is involved in? *Think-pair-share* [No]

So we only need to look at the case where k occurs between $i\&j$. If k occurs between i and j in the 1-line notation of f, and $k > j > i$, then when we apply t, do we change the number of inversions that k is involved in, in Case 1? In Case 2? *think-pair-share* [We don't change the number of inversions in either case, because if $k > j > i$, then k forms an inversion with whichever of i or j is to its right; it doesn't matter which one.]

If $i < k < j$, then applying t makes k, i and j, k into an inversion in Case 1. In Case 2, before applying t, both j, k and k, i would be inversions, but applying t makes them not inversions any more. Thus, in Case 1, we add two inversions and in Case 2 we subtract 2, for each k such that $i < k < j$ and k occurs between i and j in the 1-line notation of f. *add "+ even" to Case 1 column; "- even" to Case 2*

If $k < i < j$, does applying t change the number of inversions that k is involved in? *Think-pair-share* No!

Thus, the number of inversions changes by an odd number each time we multiply by a transposition. $\square$.

PROPOSITION *A permutation is even iff it has an even number of inversions.*

Proof: Notice that proving this Proposition will actually prove Theorem 8.4, because the number of inversions of a permutation can't be both even and odd. Since the 2-line notation for a permutation is unique, so is the 1-line notation, and since we can count the inversions based just on the 1-line notation, this tells us that the number of inversions is the same, no matter how we write the permutation as a product of transpositions.

To prove the Proposition, observe that by the Lemma, multiplying by a transposition will either increase or decrease the number of inversions by an odd number. Thus, if a permutation p can be written as the product of an even number of transpositions,

$$p = t_1 t_2 \dots t_r$$

for $r = 2k$ an even integer, then the number of inversions in p will be the sum of $2k$ odd integers. Since the sum of two odd integers is even, the number of inversions in p must be even.

To prove the other implication, we use proof by contrapositive. Suppose, therefore, that p is odd; we want to show that p has an odd number of inversions. But if p is odd, then p can be written as the product of an odd number of transpositions,

$$p = t_1 t_2 \dots t_r t_{r+1},$$

where $r = 2k$ is an even integer. Then, the transpositions $t_1, t_2, \dots, t_r$ contribute an even number of inversions to p, as above; and t_{r+1} changes the total number of inversions to be odd. Hence p has an odd number of inversions, as claimed. $\square$