Math 31 Lesson Plan

Day 22: Tying Up Loose Ends

Elizabeth Gillaspy

October 31, 2011

Supplies needed:

- Colored chalk

Other topics

- V_4 via $(P(\{1,2\}),\Delta)$ and Cayley table.
- D_n for general n; what's the center?
- Finding subgroups and the subgroup lattice?

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

Agenda: The plan for today is to just tidy up some loose ends. I didn't want to start on new material till after the midterm. And then tomorrow will be In-class office hours: I'll be here, in the classroom, and if you want to come work on the exam in a time and place when you can ask me questions, that's the time to do it. But tomorrow's x-hour is optional.

Today I want to talk more about Homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$, because I realized in office hours last week that I hadn't explained that very well. I also want to Prove Theorem 8.4 and Cayley's Theorem, since I think these are cool theorems and we didn't have time before the midterm. Then if we have time I'll talk about a connection between homomorphisms and cosets, which will lead into what we'll be doing the rest of the week.

Homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$.

Remember, when you add two numbers in $\mathbb{Z}_n$ you might get something that's bigger than n. What do you do then? In that case, you have to take the remainder mod n.

Therefore, in order to check that a map $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ is a homomorphism, what do we have to check? You have to check that

$$\phi(a + b \bmod n) = (\phi(a \bmod n) + \phi(b \bmod n)) \bmod m.$$

In words, this means you need to check that it doesn't matter whether you take mod m or mod n first.

Let's think about The identity map $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$; that is, the map that take any number in $\mathbb{Z}_n$ to the same number but in $\mathbb{Z}_m$. Can someone give me an example of two numbers m, n for which it doesn't matter whether we take mod m first or mod n?

How about an example where it does matter? *think-pair-share*

Any guesses as to a conjecture for the general rule? 12:45

If $m \not| n$ then the identity map $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ is NOT a homomorphism, because if $m \not| n$ then there will be elements in $\mathbb{Z}_n$ that add to zero mod n but they do not add to zero mod m.

Cayley's Theorem: *Every group $(G, *)$ is isomorphic to a subgroup of S_G, the symmetric group on the set G.*

Proof: Let $x \in G$. Define $f_x : G \to G$ by $f_x(y) = x * y$ for any $y \in G$. I claim that f_x is a bijection. *Have class check in pairs* If $f_x(y) = f_x(z)$, then $x * y = x * z$, and therefore $y = z$. So f_x is 1-1. To see that f_x is onto, let $z \in G$. Observe that $x^{-1} * z \in G$ as well, and $f_x(x^{-1}z) = x * x^{-1} * z = z$. Therefore f_x is onto.

Hence, f_x is a bijection on the set G and therefore it's an element of S_G. Is $f_x : G \to G$ a homomorphism, do you think? *check in pairs* Since $f_x(y * z) = x * y * z$ but $f_x(y) * f_x(z) = x * y * x * z$, we see that f_x is not a homomorphism. However, it is an element of S_G.

However, I claim that the map $\phi : G \to S_G$ given by $\phi(x) = f_x$ is a monomorphism. What do we have to check? To see this, we must check that ϕ is a 1-1 homomorphism. *check in pairs* First, we check that ϕ is a homomorphism; that is, $\phi(x * y) = f_x \circ f_y$. But, for any $z \in G$,

$$\phi(x * y)(z) = f_{x*y}(z) = x * y * z = x * (y * z) = f_x(y * z) = f_x(f_y(z)).$$

Thus ϕ is a homomorphism. Moreover, ϕ is 1-1: If $\phi(x) = \phi(y)$, then that means that $f_x(z) = f_y(z)$ for every $z \in G$. In particular, this holds for $e \in G$; so

$$f_x(e) = f_y(e) = x * e = y * e$$

and hence $y = x$.

Since $\phi : G \to S_G$ is a 1-1 homomorphism, $\phi : G \to \phi(G)$ is an isomorphism onto its range. Since $G \leq G$, Theorem 12.6 tells us that $\phi(G) \leq S_G$, and hence G is isomorphic to a subgroup of S_G as claimed. □ 1:05

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 how many 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. □.

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. □

Kernels and Cosets

Recall that if $\phi : G \to H$ is a homomorphism, then $\phi(e_G) = e_H$. But sometimes other things map to e_H.

EXAMPLE: Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$ be the identity map. Is ϕ a homomorphism? *think-pair-share* [Then ϕ is a homomorphism because $4|12$, so it doesn't matter whether we take the remainder mod 12 first or the remainder mod 4.] What elements map to the identity? *think-pair-share*

[Note that $\phi(0) = 0$, but there are two non-identity elements of $\mathbb{Z}_{12}$ that map to the identity via ϕ : 8&4.]

DEFINITION: The *kernel* of a homomorphism $\phi : G \to H$ is

$$\ker \phi = \{g \in G : \phi(g) = e_H\}.$$

CLAIM: The kernel of a homomorphism $\phi : G \to H$ is a subgroup of G. *Prove in groups*

In fact, PROPOSITION: Let G and H be groups, and let $\phi : G \to H$ be a homomorphism. The the <u>normalizer</u> $N(\ker \phi) = G$.

Who can remind me of the definition of the normalizer?

$$N(\ker \phi) = \{a \in G : aga^{-1} \in \ker \phi \ \forall\ g \in \ker \phi\}$$

So what do I have to show? **Proof:** If $a \in G$ is arbitrary, I want to show that $\phi(aga^{-1}) = e_H$ for any $g \in \ker \phi$. But,

$$\phi(aga^{-1}) = \phi(a)\phi(g)\phi(a)^{-1} = \phi(a)e_H\phi(a)^{-1} = e_H.$$

Therefore, $a \in N(\ker \phi)$, and since $a \in G$ was arbitrary, we have that $N(\ker \phi) = G$ as claimed. □