Math 31 Lesson Plan

Day 15: Review

Elizabeth Gillaspy

October 17, 2011

Supplies needed:

- Worksheets
- Colored chalk
- Quizzes!

Goals for students: Students will:

- improve their understanding of the applications and implications of important theorems from the textbook
- Solidify their understanding of order and subgroups

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

As they're taking quizzes, write the agenda on the board

- Quizzes
- D_4 homework problem;
- $\mathbb{Z}_{12} \times \mathbb{Z}_3 \times \mathbb{Z}_3$;
- Implications of theorems
- Worksheet;
- proofs of 5.5;
- Specific groups

If we don't answer the questions you posted in class today, please come see me in office hours!

With respect to the D_4 problem from Homework 3, some people pointed out that an ordered pair of elements is not a single element of D_4; but can you think of a way to take [for example] an element of $\langle 90\rangle \times \langle V\rangle$ – that is, a pair (r, f) where r is a rotation and f is a flip – and combine them to get an element of D_4? *Think-pair-share*

This problem was trying to get at the idea of isomorphism, which we will be learning next week. The idea is that even though D_4 can't be written as a product of some of its subgroups (why? [because they're all abelian and D_4 isn't]), some groups might be isomorphic to a direct product of some of their subgroups. In the D_4 case, the isomorphism would be the map you came up with just now, that takes a pair (r, f) to a single element of D_4 by composing the operations.

For general direct products, you can't mix up the operations this way; but since all the groups in this case are subgroups of the same big group, the operations are the same, so you can just multiply elements from the two factor groups.

Let's Find all the elements of order 6 in $\mathbb{Z}_{12} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

First, though, what do elements in this group look like? [Triples] Who can give me an example of an element in this group?

What's the order of this element? *Think-pair-share* Does anyone remember how this works in general? If $g = (g_1, g_2, g_3) \in G_1 \times G_2 \times G_3$, then what's $o(g)$? [$o(g) = lcm(ø(g_1), o(g_2), o(g_3)\ )$.]

So, if we want to find an element $g = (g_1, g_2, g_3)$ of order 6, what are our possibilities for $o(g_1), o(g_2), o(g_3)$? Grab a partner and figure this out.

Now that we know what our possible orders are, Which elements of $\mathbb{Z}_{12}$ have order

- 2
- 6

Think-pair-share Since $o(1) = 12$ in $\mathbb{Z}_{12}$, Theorem 4.4 tells us that $o(x) =$ what? Why is that? [$o(x) = x/(x, n)$, since $x = x \cdot 1$, which is the additive notation version of 1^x.]

So, What elements of $\mathbb{Z}_{12} \times \mathbb{Z}_3 \times \mathbb{Z}_3$ have order 6? *Think-pair-share; ask them to list on the board*

$$(6,1,1), (6,1,0), (6,0,1), (6,2,2), (6,2,1), (6,1,2), (6,2,0), (6,0,2);$$
$$(2,1,1), (2,1,0), (2,0,1), (2,2,2), (2,2,1), (2,1,2), (2,2,0), (2,0,2), (2,0,0)$$
$$(10,1,1), (10,1,0), (10,0,1), (10,2,2), (10,2,1), (10,1,2), (10,2,0), (10,0,2), (10,0,0)$$

How many cyclic subgroups of order 6 does $\mathbb{Z}_{12} \times \mathbb{Z}_3 \times \mathbb{Z}_3$ have? What would we have to do to find this out? *Think-pair-share* A cyclic subgroup of order 6 must have at least one element of order 6, to generate it. Does that mean that all the elements we have on the board generate different cyclic subgroups? [no] *find an example; eg,* $(2,2,2)\&(10,1,1)$. So, one way to find all the subgroups of order 6 would be to list, element by element, each cyclic group generated by an element of order 6, and check which ones are the same.

However, there's an easier way. If $o(x) = 6$, how many elements of order 6 are there in $\langle x \rangle$? *Think-pair-share* [Exactly two: x and $x^{-1} = x^5$] *make sure everyone understands why* Therefore, since we have 26 elements of order 6 in $\mathbb{Z}_{12} \times \mathbb{Z}_3 \times \mathbb{Z}_3$, there are 13 distinct cyclic subgroups of order 6 in $\mathbb{Z}_{12} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

I'm going to put some questions on the board, about implications of some of the big theorems from Sections 4 and 5. I'd like you to get into groups of 4 – and I want every group to have one person from the front row (and side, ie Ian and Tom, if needed). In your groups, please discuss these questions. When you think you've figured them out, pair up with another group and make sure you all agree.

For all of these, if they're true, try to come up with a logical argument or a proof. If not, try to come up with a counterexample!

1. Why doesn't Theorem 5.3 show that any finite subgroup is cyclic? Give an example of a finite, non-cyclic subgroup.
2. In a finite cyclic group, will elements of the same order generate the same subgroup? What about in non-cyclic groups?
3. If $a, b, c \in G$ are elements of a group $(G, *)$, and $a * b = b * c$, is it true that $a = c$?
4. If a, b, c are as above, and $a * b = c * b$, must $a = c$? What about if $a * b = a * c$; must we have $b = c$?

Ask for class vote: Prove Theorem 5.5(ii); Theorem 5.5(iii); or Worksheet 10/13.

Let's talk about Theorem 5.5.

Let $G = \langle x \rangle$ be a finite cyclic group of order n. Then:

1. *For any $m \in \mathbb{Z}^+$, G has a subgroup of size m if and only if $m|n$.*
2. *If $m|n$ then G has a unique subgroup of order m.*
3. *Two elements x^r, x^s of G generate the same subgroup of G iff $(r, n) = (s, n)$.*

Proof:

Proof of Part 3: We have to show both implications. *ask for a volunteer to explain what I mean by "implications." Write on board if needed.* First, assume $\langle x^r \rangle = \langle x^s \rangle$. This implies that

$$o(x^r) = |\langle x^r \rangle| = |\langle x^s \rangle| = o(x^s).$$

Therefore, by Theorem 4.4 (iii), $n/(n, r) = n/(n, s)$, which implies $(n, r) = (n, s)$.

On the other hand, if $(n, r) = (n, s)$, then by Theorem 4.4 (iii), we know that

$$o(x^r) = \frac{n}{(n, r)} = \frac{n}{(n, s)} = o(x^s).$$

Therefore, $|\langle x^r \rangle| = o(x^r) = o(x^s) = |\langle x^s \rangle|$, and so $\langle x^r \rangle = \langle x^s \rangle$ by Part 2. $\square$

Proof of Part 2: What proof technique should we use here? [contradiction] We use proof by contradiction. Suppose that $H, K \leq G$ are two subgroups of size m. Let $h \in \mathbb{Z}^+$ be the smallest positive integer such that $x^h \in H$; similarly, let $k \in \mathbb{Z}^+$ be the smallest positive integer such that $x^k \in K$. Why do we know that h, k exist? [Well-Ordering principle] What about the identity? we usually write $e = x^0$, and $0 \notin \mathbb{Z}^+$. *Think-pair-share if needed* [We can write $e = x^n$, so every element of G can be written as x^j for some $j \in \mathbb{Z}^+$.]

We would like to show that $h = k$. Can someone explain why this will tell us that $H = K$ as subgroups? *Think-pair-share* [Observe that $H = \langle x^h \rangle$ and $K = \langle x^k \rangle$, so proving that $h = k$ will show that $H = K$.]

Since $H = \langle x^h \rangle$, Theorems 4.4 and 4.6 tell us that $m = |H| = o(x^h) = n/(n, h)$. What else do we know? [By the same argument, $m = |K| = o(x^k) = n/(n, k)$.] Therefore, $(n, k) = (n, h)$.

I claim that $k|n$ and $h|n$. Can someone tell me why we would want this to be true? [If this is true, then $(n, k) = k$ and $(n, h) = h$, and so $k = h$ as desired.] Since $x^n = e$ must be in any subgroup, in particular we have $x^n \in \langle x^k \rangle$. Therefore, we must have $n = kq$ for some $q \in \mathbb{Z}^+$. The same argument tells us that $n = hq'$ for some $q' \in \mathbb{Z}^+$. Therefore, $(n, h) = h$ and $(n, k) = k$ as claimed, and so $H = K$. In words, G can only have one subgroup of any given order. □