Math 31 Lesson Plan

Day 11: Theorems about Subgroups

Elizabeth Gillaspy

October 10, 2011

Supplies needed:

- Colored chalk
- Quizzes!

Goals for students: Students will:

- Build mental connections between the concepts of subgroups, cyclic groups, and commutativity/center.
- Be able to visualize (via subgroup lattice) how subgroups fit together inside a larger group.
- Practice connecting theorems with examples.
- Improve the precision of their proof-writing.

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

Quizzes! Put D_4 Cayley table & subgroup lattice on board again while they're taking the quiz.

Are there any questions about order and cyclic groups before we get started?

Return to D_4 subgroup lattice.

Which of these groups are cyclic? How many generators do they have? *Think-pair-share if necessary* 12:50

Using colored chalk, relabel cyclic subgroups via their generators, two ways if possible. A cyclic group G can be written as $\langle a \rangle$ for <u>any</u> generator of G. Most cyclic groups will have multiple generators.

Who remembers what the center of a group is?

DEFINITION: The <u>center</u> of a group G is the set of all elements that commute with everything in the group. In symbols,

$$Z(G) = \{a \in G : ax = xa \;\forall\; x \in G\}.$$

Observe that $Z(G)$ is always non-empty; why? $e \in Z(G)$ always. If G is abelian, then $Z(G) = G$.

Example: What's $Z(D_4)$? *Think-pair-share* $Z(D_4) = \langle 180 \rangle$.

We'll come back to centers at the end of class if we have time, but first I wanted to go over a couple theorems from Section 5. Theorem 5.2 and Theorem 5.5.

If $G = \langle x \rangle$ is a cyclic group, then any subgroup of G is cyclic.

Proof: Let's suppose $H \leq G$. If $H = \{e\}$, is H a subgroup? [yes] Is it cyclic? [yes; generated by e.] then H is a cyclic subgroup with generator e. If $H \neq \{e\}$, then H has an element $g \neq e$. We can write $g = x^r$ for some $r \in \mathbb{Z}^+$. why? Let k be the smallest positive integer such that $x^k \in H$. How do we know that k exists? [Well-Ordering principle] I claim that $H = \langle x^k \rangle$. To see why, let $x^n \in H$ for some positive n. By the division algorithm, write $n = qk + r$ with $0 \leq r < k$. How do we know $n \geq k$? Therefore,

$$x^r = x^{n-qk} = x^n (x^{qk})^{-1} \in H.$$

But then, since k was the smallest positive integer such that $x^k \in H$, we must have $r = 0$. Therefore, if $x^n \in H$ for $n > 0$ we must have $n = qk$, and thus $x^n \in \langle x^k \rangle$.

If $x^n \in H$ for $n < 0$, observe that $(x^n)^{-1} = x^{-n}$ must also be in H. Moreover, $-n \in \mathbb{Z}^+$. Therefore, by the above argument, $x^{-n} = x^{qk}$ for some $q \in \mathbb{Z}$. In other words, $n = -qk \in k\mathbb{Z}$ also, so $x^n \in \langle x^k \rangle$. □

Questions?

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: I'm not going to go over the whole proof in class, for reasons of time, but let's see what the theorem says in the case of an example, so that we at least think the theorem might be true.

Example: $(\mathbb{Z}_6, \oplus)$. Work with a partner to figure out the lattice of subgroups for $(\mathbb{Z}_6, \oplus)$. You may want to look back at the Cayley table you drew for Homework 1. *ask for volunteer to put lattice of subgroups on board.*

- Notice that we only have subgroups of size $1, 2, 3, 6$
- Notice that the order of the generator tells us the order of the subgroup.
- What are the other generators for each of these subgroups?
- Here, every element of a proper subgroup generates it. However, the group $(\mathbb{Z}_{12}, \oplus)$ has subgroups that contain elements that don't generate the subgroup (this example is in the book).

Ask for class vote: Prove Part 2; Prove Part 3; group activity

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. $\square$

Count people off – 1, 2, 3. I would like everyone to find a partner that has the same number, and I would like you to work on proving the statement associated to your number. This time I don't need you to write it up neatly, but you need to be able to explain it to your classmates. *1s and 2s will need to form one group of 3 if everyone is in class.*

After 5 minutes or so, once people have figured out their proofs, I would like you to form meta-groups, with one pair labeled 1, 2, and 3. We should have 4 meta-groups. In your groups, I want you to discuss these proofs. Make sure everyone in the meta-group is convinced of all 3 proofs.

1. Show that $Z(G) \leq G$.
2. If $H \leq G$ and $K \leq H$, then $K \leq G$.
3. (Theorem 5.3) If H is a finite nonempty subset of a group G, and H is closed under multiplication, then $H \leq G$.

After all groups are convinced of all 3 proofs, if we want to spend more time on the activity,

- Assign each meta-group a number: 1 or 2.
- Have groups 1 write up the proof of Problem 1 and similarly for groups 2.
- Have the two groups 1 swap papers so they can see how the other group wrote it up; similarly for groups 2.