Math 31 Lesson Plan

Day 10: Subgroups

Elizabeth Gillaspy

October 7, 2011

Supplies needed:

- Homework
- Two envelopes; starred problem and regular homework
- D_4 Cayley table

Goals for students: Students will:

- Solidify their understanding of cyclic groups
- Have several examples of subgroups to think of.
- Be able to visualize (via subgroup lattice) how subgroups fit together inside a larger group.

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

- *D_4 Cayley table on board to start.*
- *Return & collect homework.*
- *Pass around sign-in sheet.*

If you have questions about the homework you just got back, please come and talk to me in office hours.

I want to thank all of you for reading Section 5. I gather that it's been a busy week for many of you, even without the amount of work we've had in this class. The reason I wanted to start talking about subgroups today is so that you would be able to at least start on the next homework assignment this weekend, if you were so inclined, and then hopefully you wouldn't have to leave it until the last minute next week.

So, to make up for this busy week, the beginning of next week will be a little more relaxed. Monday we'll spend some time catching up; so there will be no reading assignment this weekend. On Monday I'd like to talk more about subgroups and maybe spend some more time on order and cyclic groups, if you'd like. *ask for vote about reviewing order, cyclic groups.* We'll also talk more about proofs.

I would also like to remind you about our supplemental textbook, Gallian's "Contemporary Abstract Algebra." It's also on reserve in the library. If you get fed up with how abstract Saracino is, Gallian usually has more examples, so Gallian's explanations might make more sense to you. At any rate, it's a different perspective, which can help.

One more comment, which Ian reminded me of this morning: If $x * y = y * z$ in some group G, does that mean $x = z$? [No! For example, in the group $GL(2, \mathbb{R})$,] 12:40

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since Theorem 4.4 is really crucial to understanding cyclic groups, and subgroups of cyclic groups, I wanted to check how many people are comfortable with it. In particular, Theorem 4.4 (iii) is tricky. *Put statement on board; ask for vote about whether to go over proof.*

Theorem 4.4 (iii) *If* $o(x) = n$ *and* $(m, n) = d$, *then* $o(x^m) = n/d$.

Proof: We want to show two things; any idea what? [first, that $(x^m)^{n/d} = e$, and second, that if $(x^m)^k = e$ then $k \geq n/d$.] How would we prove the first statement? [For the first statement, since $d = (m, n)$ divides m, we can rewrite:]

$$(x^m)^{n/d} = (x^{m/d})^n = (x^n)^{m/d} = e^{m/d} = e.$$

For the second statement, use Theorem 4.4 (ii) – If $(x^m)^k = e$, then we must have $n|mk$. Observe that d divides both sides evenly; therefore, we know that $n/d|(m/d)k$. Since $(m, n) = d$, it follows that $(m/d, n/d) = 1$. Why? [If $(m/d, n/d)$ had a larger divisor, say j, then jd would divide both m and n, contradicting the definition of $(m, n) = d$.] Therefore, by Theorem 4.3, we must have $n/d|k$, and so $n/d \leq k$ as claimed. □ 12:50

Questions?

So. On to Subgroups.

DEFINITION: A subset H of a group $(G, *)$ is a subgroup of G if the elements of H form a group under $*$. We sometimes write $H \leq G$.

Let's look at some examples of subgroups: *Check that these are in fact subgroups.*

- $(\mathbb{R}^+, \cdot) \leq (\mathbb{R}\backslash\{0\}, \cdot)$
- $n\mathbb{Z} \leq \mathbb{Z}$ for any integer n

- If $a \in G$ is any element, then $\langle a \rangle \leq G$. *Discuss cyclic group notation!*
- If $H \leq G$ and $K \leq H$, then $K \leq G$. *Have them prove this in pairs.*
- *Draw lattice of subgroups for* D_4
- $Z(G) \leq G$ for any group G. *Find center of* $D_4 = \langle 180 \rangle$

A lot of people had questions about Theorem 5.2, so let's go through the proof of that.

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 $H =< x^k >$. 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 $x^n \in < x^k >$.

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 $x^n \in < x^k >$. □

Questions?

---

if time Cayley table for V_4

We'll talk about Theorem 5.5 on Monday, so I'd recommend that you go back and read it, now that (hopefully) Theorem 4.4 makes a little more sense. And I will post the next homework tomorrow.