Math 31 Lesson Plan

Day 20: Sections 9 & 10

Elizabeth Gillaspy

October 25, 2011

Supplies needed:

- Colored chalk

Goals for students: Students will:

- Feel comfortable with the notation, proof, and simple implications of Lagrange's Theorem.
- Understand how to check if that a relation is an equivalence relation.
- Understand the connection between equivalence relations and cosets.

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

A note about the midterm: Well, really, about this class in general. If you state something, you should prove it! Any time I (or the textbook) asks you a question, we're not just asking for the answer, we're asking for a proof. This is the difference between abstract algebra and calculus, or linear algebra even – No longer is a sort of hand-wavy justification good enough. The important thing isn't the answer to a calculation, it's the proof. So, when I ask you to justify your answers, I mean "please prove the statement you just made."

Today I want to start by going back to Lagrange's Theorem: If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. Grab a partner, or a group of 3, and look back at this theorem. Take a couple minutes to think about it and discuss in your groups; then I'll answer any questions your group-mates didn't clear up. *If some groups finish quickly, have them think about the proof that* $o(x) \mid |G|$. 1:10

As I promised, I want to use Lagrange's Theorem to prove Theorem 10.4 *Let G be a group of order n and let $x \in G$. Then $o(x)|n$.*

Proof: Consider $\langle x \rangle$. This is a subgroup of G for any $x \in G$, and therefore $|\langle x \rangle|$ must divide $|G|$. But $|\langle x \rangle| = o(x)$ by Corollary 4.6, and hence $o(x)|n = |G|$ as claimed. $\square$

A question of Notation: If $H \leq G$, then $|G|/|H|$ is an integer. We call this integer $[G : H]$, the <u>index</u> of H in G.

I want to spend the remaining half hour talking about Equivalence Relations. If there's extra time at the end then I'll take questions about the midterm material.

DEF: A relation R on a set X is called an *equivalence relation* if the following three properties are satisfied:

Reflexivity aRa for all $a \in X$

Symmetry If aRb then bRa

Transitivity If aRb and bRc then aRc.

Let's think of some Examples.

1. On $\mathbb{Z}$, define mR_1n if $n - m$ is even.
2. On $\mathbb{Q}$, define xR_2y if $y - x \in \mathbb{Z}$.
3. In a group G, if $H \leq G$, define aR_3b if $Ha = Hb$.

We need to check that these are equivalence relations: I'll do 1 and have them do 2 & 3 in groups.

(1): *Reflexivity* For any $n \in \mathbb{Z}$, $n - n = 0$ which is even. Thus R_1 is reflexive.

Symmetry If $n - m$ is even, $n - m \in 2\mathbb{Z}$, then $m - n = (-1)(n - m)$ because $2\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$ and hence is closed under inverses.

Transitivity If $n - m = 2i$ is even and $m - \ell = 2j$ is even, then $m = \ell + 2j$. Therefore,

$$2i = n - m = n - (\ell + 2j) = n - \ell - 2j,$$

and hence $n - \ell = 2i + 2j$ which is even. Therefore $nR_1\ell$ so R_1 is transitive, as claimed.

It can also be instructive to talk about a Non-example – in this case, a relation that is not an equivalence relation.

On $\mathbb{R}$, define aRb if $a - b \geq 0$.

Why isn't this an equivalence relation? *think-pair-share* [R is reflexive, but not symmetric: Suppose aRb, that is, $a - b \geq 0$. Then $b - a \leq 0$, and so bRa iff $b = a$. In particular, if $a = 7, b = 6$, then aRb but $b \not R a$.]

Let's talk some more about that last example, R_3. Recall that $Ha = Hb \Leftrightarrow b \in Ha$. In other words, $b = ha$ for some $h \in H$, and therefore $ba^{-1} \in H$. So another way to phrase R_3 is to say aR_3b iff $ba^{-1} \in H$.

If you have an equivalence relation R, you can define the equivalence classes of R.

Def: Given an equivalence relation R on a set X, we say that the <u>equivalence class of $x \in X$</u>, written $\overline{x}$, is the set of elements $y \in X$ such that xRy.

Example: The equivalence class of $a \in G$ under R_3 above is Ha. Can anyone explain why? [If aR_3b, then $Ha = Hb$ by definition. But, from yesterday, we know that $Ha = Hb$ iff $b \in Ha$, so aRb iff $b \in Ha$.]

Example: Consider R_2, the relation on $\mathbb{Q}$. For any $r \in \mathbb{Q}$, the equivalence class of r is the set

$$\overline{r} = \mathbb{Z} + r = \{n + r : r \in \mathbb{Z}\}.$$

Draw a picture! Indicate some different cosets

Notice that in these two examples, the equivalence classes partition the set X into disjoint sets. Is this true in general? [yes] Let's think about why.

Can an element be in more than one equivalence class? [no; transitivity]

Must an element be in at least one equivalence class? [yes; reflexivity]

If you have a partition of your set X – a division of X into disjoint subsets – then you can define an equivalence relation on X. *Draw a picture!*

Suppose $X = S_1 \cup S_2 \cup \ldots \cup S_n$, and $S_i \cap S_j = \emptyset$ if $i \neq j$. Then each $x \in X$ is in exactly one of the sets S_i. Suppose $x \in S_i$, and define xRy iff what? $[y \in S_i]$ In words, we say xRy iff x and y are in the same subset S_i.