Math 31 Lesson Plan

Last Day: Maximal Ideals and Fields from Rings

Elizabeth Gillaspy

November 21, 2011

Supplies needed:

- Colored chalk
- Homework
- Surveys

Goals for Students:

Students will:

- Gain a solid understanding of maximal ideals, and Theorem 18.10

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

Today we're goign to talk about maximal ideals and Theorem 18.10. These are the two ways we can get a field from an integral domain that I mentioned a week or more ago. Then, at the end, I have evaluations (of me/M31 and of the graders) for you to fill out, and starred problems to pass back. *Get volunteer to return evaluations to Stephanie*

DEF: If I is an ideal of a ring $(R, +, \cdot)$, then we say I is maximal if, whenever J is an ideal of R such that $I \subsetneq J$, then $J = R$. In other words, maximal ideals are the biggest possible proper ideals.

Note that this does not mean that a ring can have only one maximal ideal! Grab a partner. Think about

- What are the maximal ideals in $\mathbb{Z}$?
- Find a maximal ideal in $\mathbb{Z}[x]$.

So, what are the maximal ideals in $\mathbb{Z}$?

The maximal ideals in $\mathbb{Z}$ are the prime ideals: $p\mathbb{Z}$ for p a prime.

Proof: We know that the only ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Since 0 is contained in every ideal, we know that 0 is not maximal. Since $n\mathbb{Z} = (-n)\mathbb{Z}$, we can therefore consider only ideals of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}^+$.

If $n \in \mathbb{Z}^+$ is composite, say $n = ab$ for $1 < a, b < n$, then $a\mathbb{Z}$ contains $n\mathbb{Z}$, and $a\mathbb{Z} \neq \mathbb{Z}$ if $a \neq 1$. Therefore, $n\mathbb{Z}$ is not maximal if n is composite.

However, if p is prime, then $p\mathbb{Z}$ is maximal. To see this, suppose that J is an ideal that contains $p\mathbb{Z}$ but $J \neq p\mathbb{Z}$. We want to show that $J = \mathbb{Z}$.

To that end, pick $x \in J - p\mathbb{Z}$. Then $p \not| x$, and since p is prime, we have $(x,p) = 1$. Then, by the Euclidean Algorithm, we can find $a, b \in \mathbb{Z}$ such that $ax + bp = 1$. Since $x, p \in J$, it follows that $1 \in J$. But if $1 \in J$, what else is in J? [everything in $\mathbb{Z}$.] Since the unity is in the ideal J, it follows that every element of $\mathbb{Z}$ is in J. Therefore $J = \mathbb{Z}$, so what can we conclude? [and hence $p\mathbb{Z}$ is maximal.] □

Questions?

So, I said that maximal ideals are handy because they allow us to say something about the structure of the quotient ring. That "something" is

THEOREM 17.7 Let $(R, +, \cdot)$ be a commutative ring with unity, and let I be an ideal in R. Then I is prime iff R/I is a field.

The proof of this is in your book, on page 171. Please grab a partner, or a group of 3, and take a few minutes to figure out this proof. I'll come around to help.

If the proof makes sense to you, go ahead and think about what the maximal ideals look like in some of the other rings we've considered, like $(P(X), \Delta, \cap)$ and $M_2(\mathbb{C})$ and $\mathbb{H}$.

THEOREM 18.10: *If D is an integral domain, then there exists a field F that contains D as a subring.*

Proof: To prove this, we will construct the field of quotients or field of fractions of D. This is a field that contains D. To do this, we follow the same procedure we use to build $\mathbb{Q}$ from $\mathbb{Z}$.

2 columns: $\mathbb{Z}, \mathbb{Q}$ and gen'l case

Let $S = \{(a,b) : a, b \in D, b \neq 0_D\}$. We want to make S into a field where we can think of (a,b) as the fraction a/b. However, in the case of $\mathbb{Z}$ and $\mathbb{Q}$, we have lots of pairs (a,b)

corresponding to the same element $r \in \mathbb{Q}$:

$$1/2 = 2/4 = 5/10,$$

so we want to identify the pairs $(1,2),(2,4),(5,10)$.

In the general case, we define an equivalence relation on S:

$$(a,b)R(c,d) \Leftrightarrow ad = bc.$$

Note that in the case of $\mathbb{Q}$ and $\mathbb{Z}$, we have that

$$a/b = c/d \Leftrightarrow ad = bc,$$

so this is just the usual way to identify fractions that might not be written in lowest terms.

To see that R is an equivalence relation, what do we have to check? [Reflexivity, symmetry, transitivity] *Check in pairs that R is an equivalence relation*

Now, let $F = \{\overline{(a,b)} : (a,b) \in S\}$ be the set of equivalence classes of elements in S. Define

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,bd)}.$$

In the $\mathbb{Z}$ and $\mathbb{Q}$ case, recall that

$$a/b + c/d = \frac{ad+bc}{bd}.$$

Define

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)}.$$

Again, in $\mathbb{Q}$,

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

I claim that $(F,+,\cdot)$ is a field. To see this, what would we have to show?

- The operations $+,\cdot$ are binary and associative
- $(F,+)$ is an abelian group

- $(F \backslash e_+, \cdot)$ is an abelian group

To see that $+, \cdot$ are binary, we observe that if $b, d \neq e_+$, then since D is an integral domain, $bd \neq e_+$; why? [because D has no zero divisors.] Thus, the sum and product of two elements of F will still be an element of F.]

Your book checks associativity; it's a pain, so let's skip those.

To see that $(F, +)$ is an abelian group, what else do we have to check? [We need to find an identity element, inverses, and show that $\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}$.] Please grab a partner and check this.

discuss if necessary; then same drill for $(F \backslash e_+, \cdot)$.

So, now we see that F is a field. But I claimed that it contained D. What element in F would correspond to $d \in D$? *think-pair-share* $[(d, 1)]$

I claim that D is isomorphic to the subring of F given by $R = \{\overline{(a,1) : a \in D}\}$. To see this, we must first check that R is a subring of F, and then that there is an isomorphism $\phi : D \to R$. *check in pairs if time; homework if not.*

Thus, we have found a field F that has a subring isomorphic to our domain D. □

If time at end What have you learned in this course?