Math 31 Lesson Plan

Day 32: Ideals and Ring Homomorphisms, Take 2

Elizabeth Gillaspy

November 28, 2011

Supplies needed:

- Colored chalk
- Homework

Goals for Students:

Students will:

- Gain a solid understanding of prime and maximal ideals, and quotient rings

---

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

Return starred problems, homework.

- Office hours: Today after class (till 3:30); Tuesday 3-4; Weds usual; Friday 3-5.
- Exam: Kemeny 007
- Starred problem 4: Typo – should read "more than 2 elements"
- Principal ideals are only defined for commutative rings.

Today we're going to start by spending a lot of time with one example, so please get into groups (preferably with someone you haven't worked with before). Later we'll focus on prime and maximal ideals. Then on Wednesday I'll talk about ways to get fields from rings; Theorem 18.10 and Section 19, in particular.

EXAMPLE: Let X be the set $\{1, 2, 3, 4\}$. Consider the ring $R = (P(X), \Delta, \cap)$. Now, let $Y = \{1, 3\}$, and define $S = (P(Y), \Delta, \cap)$. Is S a subring of R? an ideal of R? *Check in groups* Let $Z = \{1\}$. Then $Z \cap S = S \cap Z \neq S$. *Again, check in groups*

Since S is an ideal in R, we can form the quotient ring R/S. What are the elements of the quotient ring? What familiar ring is R/S isomorphic to? *It's isomorphic to* $(P(\{2, 4\}), \Delta, \cap)$, *which is isomorphic to* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *since it's a four-element ring with all elements of additive* (Δ) *order 2.*

Show the isomorphism via Fund Thm

DEF: An ideal I in a ring R is prime if whenever $ab \in I$, then either $a \in I$ or $b \in I$.

DEF: An ideal I in a ring R is maximal if whenever J is an ideal that strictly contains I, $I \subsetneq J$, then $J = R$. Is S prime? Maximal? *The only prime ideal in R is R itself; there are no maximal ideals.*

Let's delve into prime and maximal ideals a little more.

The definition of a prime ideal comes from the case of $\mathbb{Z}$, because the prime ideals of $\mathbb{Z}$ are exactly the ones of the form $p\mathbb{Z}$ for p a prime (or zero).

To see this, we know that the ideals of $\mathbb{Z}$ are either $\{0\}$ or of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}^+$. The trivial ideal is prime; why? [$\mathbb{Z}$ is an integral domain, so if $ab = 0$ then at least one of a or b must be zero.]

If n is composite, then we can write $n = ab$ for $1 < a, b < n$, and so $a, b \notin n\mathbb{Z}$ but $ab \in n\mathbb{Z}$, so $n\mathbb{Z}$ is not a prime ideal.

If $n = p$ is prime, then whenever $ab \in p\mathbb{Z} = \{pk : k \in \mathbb{Z}\}$, we know that $p|ab$. By Euclid's Theorem, if $(p, a) = 1$ then $p|b$. But if $(p, a) \neq 1$, then $(p, a) = p$, so $p|a$. In other words, if $ab \in p\mathbb{Z}$ then either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$, and hence $p\mathbb{Z}$ is a prime ideal.

THEOREM 17.6: *Let R be a commutative ring with unity. Then an ideal I of R is prime iff R/I is an integral domain.*

Proof: We must prove two things: what?

1. If I is prime, then R/I is an integral domain.
2. If R/I is an integral domain, then I is prime.

Recall that an integral domain is a commutative ring with unity, with no nonzero zero divisors. So, to prove these statements, we have to know what the zero element is in R/I. What is it? *Think-pair-share* The zero element in R/I is the coset $I + 0 = I$. So, to show that R/I is an integral domain, what do we have to show? *think-pair-share* [We have to show that if

$(I+a)\cdot(I+b) = I+0 = I$, then either $I+a = I$ or $I+b = I$. We will have R/I a commutative ring with unity because R is.]

But $(I+a)\cdot(I+b) = I+ab$, so if I is prime and $I+ab = I$, then we know either $a \in I$ or $b \in I$. Hence, either $I+a = I$ or $I+b = I$. Therefore, if I is prime, then R/I is an integral domain.

Conversely, if R/I is an integral domain, that implies that whenever $(I+a)\cdot(I+b) = I$, then either $I+a$ or $I+b$ is the zero element — that is, I itself. In other words, if $I+ab = I$ then either $a \in I$ or $b \in I$, which is the definition of a prime ideal. Hence I is prime, and we have proved the second statement.

In other words, I is a prime ideal of a commutative ring R with unity iff R/I is an integral domain.

Why did we need commutativity? Why did we need unity? [These are requirements for a ring to be an integral domain.]

Let's go back to the $\mathbb{Z}/n\mathbb{Z}$ case. In this case, what do you think the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to? [$\mathbb{Z}_n$]

For now, let's just assume that's true, and apply Theorem 17.6. When does $\mathbb{Z}_n$ have zero divisors? *Think-pair-share if necessary* Precisely when n is composite.

Now let's talk about maximal ideals are the biggest possible proper ideals.

Note that this does not mean that a ring can have only one maximal ideal! In your groups, think about

- What are the maximal ideals in $\mathbb{Z}$?

- Find a maximal ideal in $M_2(\mathbb{Z})$.

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 maximal 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 you're comfortable with the proof, please try to come up with more examples of maximal ideals – in $\mathbb{Z}[x]$ for example.