Math 31 Lesson Plan

Day 30: Subrings, Ideals, and Quotients, Take 2

Elizabeth Gillaspy

November 18, 2011

Supplies needed:

- Colored chalk
- Quizzes
- 4 envelopes: evals, * probs, rubrics, homework

Goals for Students:

Students will:

- Feel comfortable with the concepts of ring homomorphism and quotient ring
- Begin to develop, via examples, an understanding of why maximal and prime ideals are useful.
- See good proofs modeled

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

Collect homework, rubrics; return quizzes. Ask re parents visiting.

Last time we mentioned quotient rings. Today I want to talk about those in more detail, which will be easiest to do if we first define ring homomorphisms, because then we can talk about some of the ring-theory versions of the Isomorphism Theorems from Section 13. So I'm going to jump ahead and do that; we'll come back to prime and maximal ideals on Monday if we don't get there today.

The Reading Assignment for Monday: Section 18. I'd also recommend that you reread the last half of Section 17, now that we've talked more about ideals in class.

Last time you found some ideals of $\mathbb{Z}[x]$: $\langle x \rangle, 2\mathbb{Z}[x], \{0\}, \mathbb{Z}[x]$. Am I missing any? Which ones of these are proper ideals? [all but $\mathbb{Z}[x]$] Which one is the trivial ideal? *Write these definitions on the board if people seem confused*

It turns out that all of these ideals are principal ideals.

Def: Let $(R, +, \cdot)$ be a commutative ring with unity and let $a \in R$. Then the *principal ideal generated by* a is written $\langle a \rangle$ or aR, and it's given by

$$\langle a \rangle = aR = \{a \cdot r : r \in R\}.$$

Your textbook likes the notation aR better; I like the notation $\langle a \rangle$ because then you don't get confused with cosets.

I claimed all the ideals above were principal; what are their generators? Please grab a partner and take a couple minutes to figure that out.

Def: Let I be an ideal of a ring $(R, +, \cdot)$. The *quotient ring* R/I consists of the set of

additive cosets of I, $\{I + r : r \in R\}$, with the operations given by

$$(I + r) + (I + s) = I + (r + s); \quad (I + r) \cdot (I + s) = I + r \cdot s.$$

Just as in the case of groups, it's really kind of a headache to work with quotient rings directly. Cosets are a mess! The nice thing is to be able to say that a quotient ring is isomorphic to some other, more familiar ring, and then we can work with that, rather than the cosets themselves.

So, to do that, we need to know what an isomorphism is in the case of rings. Which means we need to know what a homomorphism is.

DEF: Let R, S be rings and let $\phi : R \to S$ be a function. We say that ϕ is a ring homomorphism if for any $r_1, r_2 \in R$ we have

$$\phi(r_1 r_2) = \phi(r_1)\phi(r_2) \quad \text{and} \quad \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2).$$

In words, ϕ respects both of the ring operations.

We say that $\phi : R \to S$ is an isomorphism if ϕ is a 1-1 and onto homomorphism. Two rings R, S are isomorphic if there exists an isomorphism $\phi : R \to S$. Does this mean that every homomorphism $\phi : R \to S$ is an isomorphism? [no]

EXAMPLE: Define a ring homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}$. Please grab a partner and work on this.

after a few minutes, ask for volunteers to write their homomorphisms on the board

DEF: If $\phi : R \to S$ is a ring homomorphism, then the kernel of ϕ is

$$\ker \phi = \{r \in R : \phi(r) = 0_S\}.$$

In words, the kernel of a homomorphism is the set of things that maps to the additive identity of S.

So what are the kernels of some of the homomorphisms you wrote down? *Think-pair-share*

CLAIM: *If $\phi : R \to S$ is a ring homomorphism, then $\ker \phi$ is an ideal in R.*

Proof: To check that $\ker \phi$ is an ideal, we must check that

1. $(\ker \phi, +) \leq (R, +)$
2. If $q \in \ker \phi,\ r \in R$, then $qr \in \ker \phi$ and $rq \in \ker \phi$.

Why do these conditions tell us that $\ker \phi$ is an ideal? *think-pair-share* [Taking $r \in \ker \phi$ in (2), combined with (1), shows that $\ker \phi$ is a subring.]

Please grab a partner and check (1) and (2).

So, does everyone believe the Claim?

Since kernels are ideals, we can form the quotient $R/\ker \phi$. This is interesting because we have Fundamental Theorem of Ring Homomorphisms, just like we did for group homomorphisms:

THEOREM 18.5 If $\phi : R \to S$ is an onto ring homomorphism, then $R/\ker \phi \cong S$.

The proof is in your textbook; you'll read about it this weekend. For now, I want you to grab a partner and work on applying this question to the ring $\mathbb{Z}[x]$ and the ideals we found earlier: What familiar (or simpler) rings are the following quotients isomorphic to? Please write down the epimorphism ϕ that shows this isomorphism, and prove that it is an epimorphism!

- $\mathbb{Z}[x]/\langle x \rangle$
- $\mathbb{Z}[x]/\langle 2 \rangle$
- $\mathbb{Z}/n\mathbb{Z}$

But even without the concept of ring isomorphisms, we can still say some things about the quotient rings, if the ideals are nice enough.

DEF: An ideal I of a ring $(R, +, \cdot)$ is *prime* if whenever $a \cdot b \in I$, then either $a \in I$ or $b \in I$.

This definition 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.

In your groups, Please identify which of the ideals on the board are prime.

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? [$\mathbb{Z}_n$] We'll prove that later today.

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.

Another type of ideal that lets us say something about the structure of R/I are the maximal ideals.

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 $\mathbb{Z}[x]$. *Hint:* None of the ones on the board is maximal!

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.] $\square$

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 $\mathbb{H}$.