Math 31 Lesson Plan

Day 31: Ideals and Ring Homomorphisms

Elizabeth Gillaspy

November 21, 2011

Supplies needed:

- Colored chalk
- Quizzes

Goals for Students:

Students will:

- Gain a solid understanding of Section 18

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

- Principal ideals are only defined for commutative rings.
- Review of notation: what does nr mean for $r \in R$ an element of a ring? What about r^n?
- Reminder of definition of onto, 1-1: They don't have to do with the operation!

EXAMPLE: Let X be a set. Consider the ring $R = (P(X), \Delta, \cap)$. Then if $Y \subseteq X$, define $S = (P(Y), \Delta, \cap)$. Is S a subring of R? an ideal of R? *Check in pairs* Let $Z \subseteq Y$ be an element of both R and I. Then $Z \cap S = S \cap Z \neq S$. *Again, check in pairs*

Consider the case when $X = \{1, 2, 3, 4\}$ and $Y = \{1, 3\}$. 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?

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. $\square$

Today I want to talk about two particularly nice classes of ideals: prime and maximal ideals.

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.] □

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 $\mathbb{H}$.

Section 18

18.4(iv) [ideals & hms] also 18.4 (ii) and (iii) [inverse images]

18.8

18.10