Algebra Notes

Sept. 23: Ideals and the Chinese Remainder Theorem

Geoffrey Scott

Today, we continue our discussion of ideals. We'll learn ways that ideals in a ring can be combined to form new ideals, and we'll learn the first substantial theorem of the course, the Chinese remainder theorem. This concludes the part of the course on general ring theory. Next class, we'll begin studying the most important rings in this course: polynomial rings.

New Ideals from Old

If we have two ideals I, J in ring R, we can construct new ideals related to I and J.

Definition: Let I and J be ideals in R.

- $I + J := \{a + b \mid a \in I, b \in J\}$.
- IJ consists of all finite sums of elements of the form ab, where $a \in I$, $b \in J$.
- $I \cap J$ is the intersection of I and J.

Proposition: Let R be a ring. If I, J are ideals in R, then so are $I + J$, IJ, and $I \cap J$.

Proof: In each case, we must show that the subset under consideration is closed under addition, multiplication, and inverses (so that it is a subring), then prove that multiplying an element of the subset on the right or left by any $r \in R$ results in an element again in the subset. I will give a complete proof for the subset $I + J$; you can ask me if you have questions about the others.

Addition: Pick two elements of $I + J$; they can be expressed as $i_1 + j_1$ and $i_2 + j_2$, respectively, for some $i_1, i_2 \in I$ and $j_1, j_2 \in J$. Then their sum is $(i_1 + i_2) + (j_1 + j_2)$, which is again in $I + J$.

Multiplication: Using the same notation for elements of $I + J$ as above,

$$(i_1 + j_1)(i_2 + j_2) = i_1 i_2 + i_1 j_2 + j_1 i_2 + j_1 j_2.$$

Because $i_1 j_2$ and $j_1 i_2$ are both in I due to I being an ideal (in fact, they are in J also, but we won't need this), it follows that

$$\underbrace{i_1 i_2 + i_1 j_2 + j_1 i_2}_{\in I} + \underbrace{j_1 j_2}_{\in J}$$

so the product is indeed in $I + J$.

Additive inverses: For $i_1 + j_1 \in I + J$, then $-i_1 \in I$ and $-j_1 \in J$ (because I and J are themselves closed under additive inverses), so $-(i_1 + j_1) = -i_1 + (-j_1) \in I + J$.

Ideal condition: For $r \in R$,

$$r(i_1 + j_1) = ri_1 + rj_1,$$

and because $ri_1 \in I$ and $rj_1 \in J$ due to I and J satisfying the ideal condition, it follows that $r(i_1 + j_1) \in I + J$. The proof that $(i_1 + j_1)r \in I + J$ is analogous.

Question: Let $I = 4\mathbb{Z}$ and $J = 6\mathbb{Z}$, what are the ideals $I + J$, IJ, and $I \cap J$? Explain why $I \cup J$ is not an ideal.

Question: What are the containment relationships between $I, J, I + J$, and $I \cap J$?

There is also a way to construct an ideal out of any subset of elements of S.

> **Definition:** Let A be a subset of the ring R. The **ideal generated by** A is the smallest ideal of R containing A, and is written $\langle A \rangle$ (or (A)). An ideal which can be generated by a single element is called a **principal ideal**; an ideal which can be generated by a finite set is a **finitely generated ideal**.

Sometimes the definition of $\langle A \rangle$ is hard to work with; here are other ways to think about $\langle A \rangle$.

- $\langle A \rangle$ is the intersection of all ideals containing the subset A.
- If R is commutative, then $\langle A \rangle$ consists of all elements of R that can be written as

$$r_1 a_1 + ... + r_n a_n$$

where the r_i's and a_i's are elements of R and A, respectively.

Question 1: In the ring $\mathbb{Z}$, describe $\langle 5 \rangle$ and $\langle 6, 4 \rangle$.

Question 2: In the ring $\mathbb{Z}[x]$, describe $\langle x \rangle, \langle 5 \rangle$, and $\langle 5, x \rangle$.

Question 3: Find generating sets for the kernels of the following homomorphisms.

- $\mathbb{Z}[x] \to \mathbb{Z}$ given by $a_0 + a_1 x + a_2 x^2 + ... \mapsto a_0$.
- $\mathbb{Z}[x] \to (\mathbb{Z}/3\mathbb{Z})[x]$ given by $a_0 + a_1 x + a_2 x^2 + ... \mapsto [a_0] + [a_1]x + [a_2]x^2 + ...$
- $\mathbb{Z}[x] \to \mathbb{Z}/3\mathbb{Z}$ by $a_0 + a_1 x + a_2 x^2 + ... \mapsto [a_0]$.

Types of Ideals

On the first day of class, we learned words to describe rings that had certain nice properties.

1. In a *field* (commutative ring with identity where every nonzero element is a unit), we can divide by nonzero elements.
2. In an *integral domain* (commutative ring with identity having no zero divisors), we can't always divide but we have the next best thing, the cancellation property: If $a \neq 0$ and $ab = ac$, then $b = c$.

Last class, we constructed quotient rings R/I from ideals $I \subseteq R$. Now, we'll see that certain properties of the ideal translate into other properties of the quotient ring. Specifically, we can determine whether R/I will be a field or an integral domain just by studying I.

When will R/I be a field?

To answer this question, we first classify fields as the commutative rings with identity that have no nontrivial proper ideals, then prove that the ideals of a quotient ring are precisely the ideals containing I. This will motivate the definition of *maximal* ideal as an ideal which is not contained in any ideal except R and itself: it is precisely these *maximal* ideals of a commutative ring with identity whose quotient R/I is a field.

Proposition: A commutative ring with identity R is a field if and only if its only ideals are $\langle 0 \rangle$ and R.

Proof: Because every nonzero element of a field is a unit, and every ideal that contains a unit is the entire ring, it follows that the only ideals of a field are $\langle 0 \rangle$ and the entire field. Conversely, let R be a ring such that the only ideals are $\langle 0 \rangle$ and R. Then for every nonzero $x \in R$, the ideal $\langle x \rangle$ must be all of R. This means that $1 = rx$ for some $r \in R$, so x is invertible.

The next proposition describes the ideals of a quotient ring.

Proposition: Let $\varphi : R \to S$ be a ring homomorphism. If I is an ideal in S, then $\varphi^{-1}(I)$ is an ideal in R.

Proof: Let $a, b \in \varphi^{-1}(I)$. Using the definition of homomorphisms, $\varphi(a+b), \varphi(ab), \varphi(-a) \in I$, so $\varphi^{-1}(I)$ is a subring. Now let $r \in R$, $j \in \varphi^{-1}(I)$, and notice that $\varphi(rj) = \varphi(r)\varphi(j) \in I$ since I is an ideal and $\varphi(j) \in I$. A similar computation shows $\varphi(jr) \in I$, so $rj, jr \in \varphi^{-1}(I)$, proving that $\varphi^{-1}(I)$ is an ideal.

In the above proposition, because every ideal of S contains $0 \in S$, it follows that every ideal of R of the form $\varphi^{-1}(I)$ contains $\ker(\varphi)$.

Proposition: Let I be an ideal of a ring R, and let $\varphi : R \to R/I$ be the quotient map. The maps below are inverses (and hence define a bijection).

$$\left\{ \begin{array}{c} \text{Ideals in} \\ \text{R that contain I} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Ideals} \\ \text{in } R/I \end{array} \right\}$$
$$J \mapsto \varphi(J)$$
$$\varphi^{-1}(K) \mapsfrom K$$

Proof: First, we verify that $\varphi(J)$ is indeed an ideal in R/I.

- $\varphi(J)$ **is a subring:** This follows from the fact that φ is a homomorphism (check this!), and $\varphi(J)$ is the image of the homomorphism $\varphi\big|_J$, and we know that images of homomorphisms are subrings.
- $\varphi(J)$ **is an ideal:** Any element of $\varphi(J)$ can be written as $[j]$ for some $j \in J$, and let $[s] \in R/I$. Then $[j][s] = [js]$ and $[s][j] = [sj]$ are also inside $\varphi(J)$ (since $js, sj \in J$), so $\varphi(J)$ is an ideal.

So the map is well-defined. We also know (from the above proposition) that for any ideal $K \in R/I$, $\varphi^{-1}(K)$ is an ideal. To complete the proof it suffices to show that $\varphi(\varphi^{-1}(K)) = K$ for all ideals K in R/I, and $\varphi^{-1}(\varphi(J)) = J$ for all ideals J in R containing I (so that $K \mapsto \varphi^{-1}(K)$ and $J \mapsto \varphi(J)$ are inverse maps). The first claim follows from the fact that φ is surjective. To prove the second, notice that if $\varphi(a) = \varphi(j)$ for some $j \in J$, then $a - j \in I \subseteq J$, so $a \in J$. Therefore, if $\varphi(a) \in \text{im}(J)$, then $a \in J$. This proves that $\varphi^{-1}(\varphi(J)) = J$.

Combining this with the above, we see that a quotient ring R/I of a commutative ring with identity is a field precisely when there are no ideals "in between" I and R.

Definition: An ideal I of R is called **maximal** if there are no ideals J satisfying $I \subsetneq J \subsetneq R$

Corollary: Let I be an ideal in a commutative ring R with identity. Then R/I is a field if and only if I is maximal.

When will R/I be an integral domain?

Let R be a commutative ring with identity. In an integral domain, a product ab is zero only if a or b is zero. In a quotient ring R/I, the zero element is the coset I itself. Unsurprisingly, the condition that R/I is an integral domain translates into the condition that $ab \in I$ only if a or b is in I.

Definition: An ideal I of a commutative ring R is *prime* if $I \neq R$ and whenever $ab \in I$, then either $a \in I$ or $b \in I$.

Proposition: Let I be an ideal in a commutative ring R with identity. Then R/I is an integral domain if and only if I is prime.

Proof: In the ring R/I, then zero element is the coset $[0] = I$. In other words, $[a] = 0$ if and only if $a \in I$. After this observation, the proof is a matter of following the definitions:

$$\begin{aligned} R/I \text{ is an integral domain} &\iff [a][b] = 0 \text{ only if } [a] = 0 \text{ or } [b] = 0 \\ &\iff ab \in I \text{ only if } a \in I \text{ or } b \in I \\ &\iff I \text{ is a prime ideal} \end{aligned}$$

Chinese Remainder Theorem

Consider the following riddle (a version of which was allegedly first posed by Brahmagupta, a 7th century Indian mathematician):

> An old woman is carrying eggs to sell in the market when the eggs are crushed by a horse. The horseman wants to know how many eggs she had so that he can repay her, but she only knows the following: when she arranged them into groups of 2 or 3 or 4 or 5 or 6, there was always precisely one left over. But when she arranged them into groups of 7, there were none left over. What is the smallest number of eggs she might've had?

One way to express this problem mathematically is the following:

> Consider the homomorphism
>
> $$\mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7$$
>
> given by the product of the quotient homomorphisms $\mathbb{Z} \to \mathbb{Z}_i$. What is the smallest number in the preimage of $([1], [1], [1], [1], [1], [0])$?

The topic of this section, the chinese remainder theorem, does *not* answer this riddle, but it tells us important information about the kernel and image of the homomorphism. In fact, it does it in the more general setting of *any* product of quotient homomorphisms from *any* commutative ring with unity R

$$R \to \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_n}$$

not just the case when $R = \mathbb{Z}$. Here's why we might care about the kernel and image of this map using the egg riddle as motivation.

1. There is no way to determine the *exact* number of eggs the woman was carrying because there are infinitely many elements in the preimage. For example, the number $2 * 3 * 4 * 5 * 6 * 7 = 5040$ is in the kernel of this homomorphism, so if you find any element in the preimage, you can add 5040 to get another element in the preimage. But is $\langle 5040 \rangle$ the entire kernel? The chinese remainder theorem will tell us exactly what the kernel is (in our case, $\langle 420 \rangle$), which answers the question "Up to what additive factor can you determine an element of $\mathbb{Z}$ just by knowing its image in $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6$, and $\mathbb{Z}_7$?"

2. The old woman had redundant information: if you group eggs into groups of four and have one left over, then you already know that if you group the eggs into groups of two, you'll have one left over. The old woman wasted time in making the groups of two. This inefficiency in the woman's choice of grouping sizes is reflected in the fact that the homomorphism is not surjective. For example $([1], [0], [0], [0], [0], [0])$ is not in the image. If the woman wanted to be efficient and guarantee that none of her information is redundant, she should have chosen her "egg grouping sizes" to be pairwise coprime. In the more general ring-theory context, the condition of being coprime translates into the condition that the ideals I_k are pairwise *comaximal*.

Definition: Ideals I and J in a ring R are *comaximal* if $I + J = R$. A set of ideals $I_1, \ldots, I_n$ is *pairwise comaximal* if every pair of ideals from the set is comaximal.

In other words, the chinese remainder theorem will answer the following riddle.

> An old woman is carrying an element of a commutative ring to sell in the market when the ring element gets crushed by a horse. The woman forgets exactly which ring element it was, but knows which coset it belongs to modulo the pairwise comaximal ideals $I_1, I_2, \ldots, I_k$. Exactly how much information does this determine about the original ring element?

Theorem (Chinese Remainder Theorem): Let $I_1, \ldots, I_n$ be ideals in a commutative ring R with identity, and consider the homomorphism

$$\begin{aligned} R &\to \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_n} \\ r &\mapsto ([r], [r], \ldots, [r]) \end{aligned}$$

(the first bracket signifies a coset of I_1, the second is a coset of I_2, etc.)

1. The kernel equals $I_1 \cap I_2 \cap \cdots \cap I_n$
2. If the ideals are pairwise comaximal (i.e., I_j and I_ℓ are comaximal when $j \neq \ell$), then the map is surjective and

$$I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \ldots I_n$$

so the first isomorphism theorem gives

$$\frac{R}{I_1 I_2 \ldots I_n} \cong \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_n}.$$

Proof: To prove the first claim, observe that $r \in R$ is in the kernel precisely when r is a representative of the zero coset with respect to each ideal. But this is just another way of saying that r is contained in each ideal, so the kernel is $I_1 \cap \cdots \cap I_n$.

We prove the second claim only in the $n = 2$ case (the full proof has an extra inductive step which is not very educational).

Case $n = 2$: Let I, J be two comaximal ideals. To show that the homomorphism is surjective, pick $i \in I$ and $j \in J$ satisfying $i + j = 1$ (this is possible by the comaximality condition). If we reduce both sides of this equation modulo i, we see that $[j] = [1]$ modulo i, and also by reducing modulo j, we see that $[i] = [1]$ modulo j. This shows that

$$\begin{aligned} R &\to R/I \times R/J \\ j &\mapsto ([1], [0]) \\ i &\mapsto ([0], [1]) \end{aligned}$$

So in particular, any element $([r_i], [r_j]) \in R/I \times R/J$ is the image of $r_i j + r_j i$. This proves surjectivity.

To show that $I \cap J = IJ$, notice that because everything in IJ is both in I and also in J, the inclusion $I \cap J \supseteq IJ$ is clear. To see the opposite inclusion, let $r \in I \cap J$. Then $r = r1 = r(i + j) = ir + rj$. Because $r \in J$, it follows that $ir \in IJ$. And because $r \in I$, it follows that $rj \in IJ$. Therefore, $ir + rj = r \in IJ$.