Math 4527 (Number Theory 2)

Lecture #21 of 38 $\sim$ March 10, 2021

Ideals and Quotient Rings

- Quotient Rings
- Maximal Ideals and Their Properties

This material represents §8.1.2-8.1.3 from the course notes.

Recall, I

Last time we introduced ideals:

Definition

If R is a commutative ring with 1, a subset I is called a (two-sided) ideal of R if it contains 0, is closed under subtraction, and is closed under arbitrary multiplication by elements of R.

Explicitly, I is an ideal if I contains 0 and for any $x, y \in I$ and any $r \in R$, the elements $x - y$ and rx are in I.

Recall, II

We also said some things about generation of ideals:

Definition

Suppose R is a commutative ring with 1 and A is a subset of R. We define the ideal generated by A, denoted (A), to be the intersection of all ideals of R containing A. This ideal is the smallest ideal of R containing A.

Definition

If R is a ring with 1, we say an ideal I is finitely generated if I is generated by a finite set, and we say I is principal if I is generated by a single element. Thus, a finitely generated ideal has the form $I = (a_1, a_2, \ldots, a_n)$, while a principal ideal has the form $I = (a)$.

More With Ideals, I

As we noted in both of the examples, we always have $(1) = R$. We can generalize this statement somewhat:

Proposition (Ideals and Units)

If I is an ideal of the ring R with 1, then $I = R$ if and only if I contains a unit.

Proof:

- If $I = R$ then certainly I contains a unit (namely, 1).
- Conversely, if $u \in I$ is a unit with $ur = 1$, then since I is an ideal we have $1 = ur \in I$.
- Then for any $s \in R$, the element $s = 1s$ is also in I, and so $I = R$.

More With Ideals, II

Since every nonzero element in a field is a unit, the only nonzero ideal of a field F is F itself. The converse is also true:

Corollary (Ideals of Fields)

A commutative ring R with 1 is a field if and only if the only ideals of R are 0 and R.

Proof:

- If F is a field and $I \neq (0)$, then I contains some nonzero r. Since F is a field, r is a unit, so $I = R$ by the proposition.
- Conversely, if the only ideals of R are 0 and R, let $r \in R$ be any nonzero element. Then (r) contains $r \neq 0$ so it cannot be the zero ideal, so we must have $(r) = R$.
- By the previous proposition, this means (r) contains 1: then $rs = 1$ for some $s \in R$, so r is a unit. Hence every nonzero element of R is a unit, so R is a field as claimed.

Quotient Rings, I

Now we can get back to constructing quotient rings:

Definition

If I is an ideal of the ring R, then we say a is congruent to b modulo I, written $a \equiv b \pmod{I}$, if $a - b \in I$.

Proposition (Ideal Congruences)

Let I be an ideal of R and $a, b, c, d \in R$. The following are true:

1. $a \equiv a \pmod{I}$.
2. $a \equiv b \pmod{I}$ if and only if $b \equiv a \pmod{I}$.
3. If $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.
4. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $a + c \equiv b + d \pmod{I}$.
5. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $ac \equiv bd \pmod{I}$.

Quotient Rings, II

Proofs:

1. $a \equiv a \pmod{I}$.
   - Since $a - a = 0 \in I$, the statement is immediate.
2. $a \equiv b \pmod{I}$ if and only if $b \equiv a \pmod{I}$.
   - If $a - b \in I$ then $-(a - b) = b - a \in I$ since I is closed under additive inverses, and conversely if $b - a \in I$ then so is $-(b - a) = a - b$.
3. If $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.
   - We are given $a - b \in I$ and $b - c \in I$, so since I is closed under addition, we see $(a - b) + (b - c) = a - c \in I$.

Quotient Rings, III

Proofs (continued):

4. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $a + c \equiv b + d \pmod{I}$.
   - We are given $a - b \in I$ and $c - d \in I$, so since I is closed under addition, $(a - b) + (c - d) = (a + c) - (b + d) \in I$.
5. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $ac \equiv bd \pmod{I}$.
   - We are given $a - b \in I$ and $c - d \in I$.
   - Then since I is closed under arbitrary left and right multiplication, $(a - b)c$ and $b(c - d)$ are also in I.
   - Hence $ac - bd = (a - b)c + b(c - d)$ is also in I since I is closed under addition.

Quotient Rings, IV

Now we can define residue classes:

Definition

If I is an ideal of the ring R, then for any $a \in R$ we define the residue class of a modulo I to be the set $\overline{a} = a + I = \{a + x : x \in I\}$. This set is the left coset of I (under the addition operation of R) represented by a.

- We will use the notation $\overline{a}$ and $a + I$ interchangeably. (The latter is intended to evoke the idea of "adding" a to the set I.)
- It follows from properties of cosets that two residue classes are either disjoint or identical and that they partition R: $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{I}$ if and only if $a - b \in I$.

Quotient Rings, V

All that remains is to verify that the residue classes form a ring.

Theorem (Quotient Rings)

Let I be an ideal of the ring R. Then the collection of residue classes modulo I forms a ring, denoted R/I (read as "R mod I"), under the operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$. (This ring is called the quotient ring of R by I.) If R is commutative then so is R/I, and likewise if R has a 1 then so does R/I.

The notation R/I is intended to emphasize the idea that I represents a single element (namely, $\overline{0}$) in the quotient ring R/I, and the other elements in R/I are "translates" of I. In this way, R/I is the ring obtained from R by "collapsing" or "dividing out" by I, whence the name "quotient ring".

Quotient Rings, VI

Proof:

- The proof is essentially bookkeeping, and the only real content is to show that the operations are well-defined: that is, if we choose different elements $a' \in \bar{a}$ and $b' \in \bar{b}$, the residue class of $a' + b'$ is the same as that of $a + b$, and similarly for the product.
- To see this, if $a' \in \bar{a}$ then $a' \equiv a \pmod{I}$, and similarly if $b' \in \bar{b}$ then $b' \equiv b \pmod{I}$.
- Then $a' + b' \equiv a + b \pmod{I}$, so $\overline{a' + b'} = \overline{a + b}$. Likewise, $a'b' \equiv ab \pmod{I}$, so $\overline{a'b'} = \overline{ab}$.
- Thus, the operations are well-defined.

Quotient Rings, VII

Proof (continued):

- Now we just observe that the ring axioms are essentially inherited from R.
- For the ring axioms, we observe that associativity, commutativity, and the distributive laws follow immediately from the corresponding properties in R: the additive identity in R/I is $\overline{0}$, the multiplicative identity is $\overline{1}$, and the additive inverse of $\overline{a}$ is $\overline{-a}$.
- For example, we have $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$.

Quotient Rings, VIII

We will also occasionally want to mention structure-preserving maps from one ring to another, which are called homomorphisms:

Definition

A function $\varphi : R \to S$ is a ring homomorphism if $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$ for all elements r_1 and r_2 in R. A homomorphism $\varphi : R \to S$ that is a bijection is called a ring isomorphism.

Examples:

1. The map $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $\varphi(a) = \overline{a}$ is a ring homomorphism.
2. If R is any ring, the map $\varphi : R \to R \times R$ given by $\varphi(r) = (r, r)$ is a ring homomorphism.
3. The map $\varphi : \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ given by $\varphi(a) = (a \bmod 2, a \bmod 3)$ is a ring isomorphism.

Quotient Rings, IX

Here are some examples of quotient rings.

Examples:

1. If R is any ring, the quotient ring of R by the zero ideal, namely $R/0$, is (isomorphic to) R itself, while the quotient ring of R by itself, namely R/R, is (isomorphic to) the trivial ring $\{0\}$.
2. If $R = \mathbb{Z}$, then the quotient $\mathbb{Z}/m\mathbb{Z}$ is simply the ring of residue classes modulo m, with which we are already quite familiar.

Quotient Rings, X

Examples:

3. In $R = \mathbb{Z}[x]$, with $I = (x, 2)$ describe the structure of the quotient ring R/I.
   - Notice that I consists of the polynomials in R whose constant term is even.
   - We can therefore see that there are two residue classes modulo I, namely, the polynomials congruent to 0 and the polynomials congruent to 1.
   - Explicitly, the two residue classes are $0 + I$ (the polynomials with even constant term) and $1 + I$ (the polynomials with odd constant term).
   - The quotient ring R/I therefore has two elements, and it is easy to see that the resulting ring structure is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Quotient Rings, X

Examples:

4. In $R = \mathbb{Z}[x]$, with $I = (x^2 + 1)$ describe the structure of the quotient ring R/I.
   - From the division algorithm for polynomials, the residue classes in R/I are represented uniquely in the form $\overline{a + bx}$ where $a, b \in \mathbb{Z}$ (simply divide a polynomial by $x^2 + 1$ and consider the remainder).
   - In R/I, we have $\overline{x}^2 + \overline{1} = \overline{0}$, which is to say, $\overline{x}^2 = -\overline{1}$.
   - The operations in R/I are given by $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$ and $\overline{a + bx} \cdot \overline{c + dx} = \overline{(ac - bd) + (ad + bc)x}$, via the distributive law and the fact that $\overline{x}^2 = -\overline{1}$.
   - In this case, the quotient ring is isomorphic to the ring of Gaussian integers $\mathbb{Z}[i]$, with the isomorphism $\varphi : R/I \to \mathbb{Z}[i]$ given by $\varphi(\overline{a + bx}) = a + bi$.

Quotient Rings, XI

Examples:

5. In $R = \mathbb{Z}/8\mathbb{Z}$, with $I = (4) = \{0, 4\}$, describe the structure of the quotient ring R/I.

   - Each residue class has 2 elements, so since R has 8 elements, there are four residue classes. They are
     $\overline{0} = 0 + I = \{0, 4\}$,
     $\overline{1} = 1 + I = \{1, 5\}$,
     $\overline{2} = 2 + I = \{2, 6\}$, and
     $\overline{3} = 3 + I = \{3, 7\}$.
   - Notice, for example, that in the quotient ring R/I, we have $\overline{1} + \overline{3} = \overline{0}$, $\overline{2} \cdot \overline{2} = \overline{0}$, and $\overline{2} \cdot \overline{3} = \overline{2}$.
   - In fact, we can see that the ring structure of R/I is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ (the labelings of the elements are even the same).

Quotient Rings, XII

Just as with group homomorphisms, the kernel and image of a ring homomorphism play important roles:

Definition

If $\varphi : R \to S$ is a ring homomorphism, the kernel of φ, denoted $\ker \varphi$, is the set of elements in R mapped to 0_S by φ. In other words, $\ker \varphi = \{r \in R : \varphi(r) = 0\}$.

The kernel measures how close φ is to being the zero map: if the kernel is large, then φ sends many elements to zero, while if the kernel is small, φ sends fewer elements to zero.

- Example: The kernel of the reduction homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $\varphi(a) = \overline{a}$ is $m\mathbb{Z}$.

The kernel of any homomorphism $\varphi : R \to S$ is an ideal of R. In fact, kernels of homomorphisms and ideals are the same objects.

Quotient Rings, XIII

We also have the image:

Definition

If $\varphi : R \to S$ is a ring homomorphism, the image of φ, denoted $\operatorname{im} \varphi$, is the set of elements in S of the form $\varphi(r)$ for some $r \in R$.

- In the context of general functions, the image is often called the range of φ.
- Intuitively, the image measures how close φ is to being surjective: indeed (by definition) φ is surjective if and only if $\operatorname{im} \varphi = S$.

Quotient Rings, XV

One of the fundamental results about quotient rings is a relationship between homomorphisms and quotients. The statement is identical to the corresponding result for groups:

Theorem (First Isomorphism Theorem)

If $\varphi : R \to S$ is a homomorphism of rings, then $R/\ker\varphi$ is isomorphic to $\operatorname{im}\varphi$.

- By definition φ is a surjective homomorphism $\varphi : R \to \operatorname{im}\varphi$.
- The idea of the first isomorphism theorem is that if we want to turn φ into an isomorphism, we must "collapse" its kernel to a single element: this is precisely what the quotient ring $R/\ker\varphi$ represents.

Quotient Rings, XVI

Proof:

- Let $I = \ker \varphi$. We use φ to construct a map $\psi : R/I \to \operatorname{im} \varphi$, and then show that it is injective and surjective.
- The map is defined as follows: for any residue class $\overline{r} \in R/I$, we define $\psi(\overline{r}) = \varphi(r)$.
- We must verify that this map ψ is well-defined, so suppose that r' is some other representative of the residue class $\overline{r}$: then $r' - r \in I$, so $\varphi(r' - r) = 0$ and thus $\varphi(r') = \varphi(r)$.
- Thus, $\psi(\overline{r'}) = \varphi(r') = \varphi(r) = \psi(\overline{r})$, so the map ψ is well-defined.

Quotient Rings, XVII

Proof (continutuateatedly):

- It is then easy to see ψ is a homomorphism, since $\psi(\overline{r} + \overline{s}) = \varphi(r + s) = \varphi(r) + \varphi(s) = \psi(\overline{r}) + \psi(\overline{s})$ and likewise $\psi(\overline{r} \cdot \overline{s}) = \varphi(r \cdot s) = \varphi(r) \cdot \varphi(s) = \psi(\overline{r}) \cdot \psi(\overline{s})$.
- Next, we see that $\psi(\overline{r}) = 0$ precisely when $\varphi(r) = 0$, which is to say $r \in \ker(\varphi)$, so that $\overline{r} = \overline{0}$. Thus, the only element in $\ker \psi$ is $\overline{0}$, so ψ is injective.
- Finally, if s is any element of $\operatorname{im} \varphi$, then by definition there is some $r \in R$ with $\varphi(r) = s$: then $\psi(\overline{r}) = s$, meaning that ψ is surjective.
- Since ψ is a homomorphism that is both injective and surjective, it is an isomorphism.

Quotient Rings, XVIII

The main utility of the first isomorphism theorem is that we can use it to construct isomorphisms of rings.

- In order to show that R/I is isomorphic to a ring S, we search for a surjective homomorphism $\varphi : R \to S$ whose kernel is I.
- The idea above is quite simple, but it is surprisingly powerful.
- Now, our course is not entirely about ring theory, but it is not entirely *not* about ring theory either, so it is very worthwhile to become at least moderately comfortable with recognizing when the first isomorphism theorem might be of use.

Quotient Rings, XIX

Example: Show that $\mathbb{Z}/12\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

- We seek a surjective homomorphism $\varphi : \mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ whose kernel is $12\mathbb{Z}$.
- Once this idea is suggested, it is not hard to come up with a candidate, namely, $\varphi(a) = (a \bmod 3, a \bmod 4)$.
- It is easy to verify that map is a homomorphism (since the individual maps of reduction mod 3 and reduction mod 4 are homomorphisms) and it is likewise fairly easy to see that the map is surjective by checking that the images of 0, 1, ... , 11 represent all of the elements in $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.
- Finally, the kernel of the map consists of all integers a with $\varphi(a) = (0, 0)$, which is not hard to see is precisely $12\mathbb{Z}$.
- Therefore, by the first isomorphism theorem applied to φ, we conclude that $\mathbb{Z}/12\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

Maximal Ideals, I

An important class of ideals are those that are "maximal" under inclusion (i.e., which are not contained in any other ideal except the full ring):

Definition

If R is a ring, a maximal ideal of R is an ideal $M \neq R$ with the property that the only ideals of R containing M are M and R.

Examples:

1. If F is a field, then since the only ideals of F are 0 and F, the zero ideal is a maximal ideal of F.
2. In $\mathbb{Z}$, the ideal $m\mathbb{Z}$ is contained in $n\mathbb{Z}$ precisely when n divides m. Accordingly, the maximal ideals of $\mathbb{Z}$ are precisely the ideals of the form $p\mathbb{Z}$, where p is a prime.
3. The ideal (x) is not a maximal ideal of $\mathbb{Z}[x]$ because it is contained in the proper ideal $(2, x)$.

Maximal Ideals, II

A commutative ring with 1 must have maximal ideals:

Theorem (Existence of Maximal Ideals)

If R is a commutative ring with 1, then any proper ideal of R is contained in a maximal ideal.

Like a number of other general existence theorems (e.g., the proof that every vector space has a basis), this proof requires the (in)famous axiom of choice from set theory.

- The version of the axiom of choice typically used in algebra is known as Zorn's lemma: if S is a nonempty partially ordered set with the property that every chain in S has an upper bound, then S contains a maximal element.
- Since the goal of this course is not to dwell too much on foundational minutia, I will skip this proof (though if you want to see the details, they're in the notes).

Maximal Ideals, III

It might initially appear to be difficult to detect whether a particular ideal is maximal. However, by using quotient rings, we can do this quite easily:

Proposition (Maximal Ideals and Quotients)

If R is a commutative ring with 1, then the ideal M is maximal if and only if R/M is a field.

I will remark that this result is *not* true if we drop either of the assumptions on R (i.e., that it is commutative and has a 1).

- The standard noncommutative counterexample is to take $R = M_{2\times 2}(F)$, the 2×2 matrices over a field F. One can show that the only ideals of this ring are (0) and R, so (0) is maximal. But clearly $R/(0) \cong R$ is not a field.
- A counterexample for a ring R that does not have a 1 is $I = 4\mathbb{Z}$ inside $R = 2\mathbb{Z}$: I is maximal but R/I is not a field.

Maximal Ideals, IV

Proof:

- It can be verified that there is a correspondence between ideals of R containing I and the ideals of R/I: if J is an ideal of R, then $\tilde{J} = \{j + I : j \in J\}$ is easily seen to be an ideal of R/I. Conversely, if we have any ideal $J/I = \{j + I : j \in J\}$ of R/I, it is straightforward to check that the collection of all elements $j \in R$ such that $j + I \in \tilde{J}$ is an ideal of R.
- This means the ideals of R/M are in bijection with the ideals of R containing M: therefore, M is maximal precisely when the only ideals of R/M are 0 and R/M.
- Furthermore, if R is commutative with 1, then R/M is also a commutative ring with 1, so R/M is a field if and only if the only ideals of R/M are 0 and R/M. Putting these two statements together yields the proposition.

Maximal Ideals, V

Using that characterization, we can write down the maximal ideals of $\mathbb{Z}$ and of $F[x]$:

Corollary

The maximal ideals of $\mathbb{Z}$ are precisely the ideals (p) where p is prime, and the maximal ideals of $F[x]$ are precisely the principal ideals (p) where p is irreducible.

Proof:

- As noted earlier, every ideal of $\mathbb{Z}$ is principal.
- Also, $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if p is prime. Thus, (m) is maximal if and only if m is prime.
- The statement for $F[x]$ is similar: every ideal is principal, and the quotient ring $F[x]/(p)$ is a field if and only if p is irreducible.

Maximal Ideals, VI

Example: Determine whether the ideals $I = (2, x)$ and $J = (x^2 + 1)$ are maximal ideals of $R = \mathbb{Z}[x]$.

Maximal Ideals, VI

Example: Determine whether the ideals $I = (2, x)$ and $J = (x^2 + 1)$ are maximal ideals of $R = \mathbb{Z}[x]$.

- We simply look at the quotient rings R/I and R/J and decide whether they are fields.
- Conveniently, we did both of these earlier in the lecture: $R/(2, x)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is a field, while $R/(x^2 + 1)$ is isomorphic to $\mathbb{Z}[i]$, which is not a field.
- Thus, I is a maximal ideal of R, but J is not.
- If you like, you can try to find a proper ideal of R that properly contains J.

Maximal Ideals, VII

Example: Determine whether the ideal $I = (3)$ is maximal in $R = \mathbb{Z}[\sqrt{3}]$.

Maximal Ideals, VII

Example: Determine whether the ideal $I = (3)$ is maximal in $R = \mathbb{Z}[\sqrt{3}]$.

- In the quotient ring R/I, the residue class $\sqrt{3} + I$ is nonzero, but has the property that $(\sqrt{3} + I)^2 = 3 + I = 0 + I$ is equal to zero.
- Thus, the quotient ring R/I has zero divisors hence is not a field, meaning that I is not a maximal ideal of R.
- Another approach is to observe that I is properly contained in the ideal $M = (\sqrt{3})$, which is proper because $\sqrt{3}$ is not a unit in R. (In fact, this is really the same observation as the one made above.)

Summary

We discussed some additional properties of quotient rings.

We defined maximal ideals and identified some of their properties.

Next lecture: Prime ideals, arithmetic in domains, quadratic integer rings.