Introduction to Ring Theory

Sachi Hashimoto
Mathcamp
Summer 2015

1 Day 1

1.1 What are we talking about?

Broadly speaking, a ring is a set of objects which we can do two things with: add and multiply. In many ways it will look like our familiar notions of addition and multiplication, but sometimes it won't. We have to decide what properties of addition and multiplication we are going to require to be true, and which ones we can do without. Before we give these properties, let's go through a few familiar examples.

Example 1. Our basic example of a ring will be the integers, which we will write as $\mathbb{Z}$. As a set, this is just the numbers $\{0, 1, -1, 2, -2, \dots\}$ and addition and multiplication work "as usual".

Example 2. Another key example that will come up again and again are the polynomials, which I will denote as $\mathbb{Z}[x]$. Here, my objects are polynomials $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where the coefficients a_i are integers. We could also take polynomials whose coefficients are in $\mathbb{R}$ or $\mathbb{Q}$ or $\mathbb{C}$, in which case we would write our ring as $\mathbb{R}[x]$ or $\mathbb{Q}[x]$ or $\mathbb{C}[x]$. Polynomials come equipped with a usual notion of how to multiply them and how to add them.

These two basic examples in some sense represent all of the examples we will talk about in this class. Roughly speaking, we usually think of rings as either 'functions' or 'numbers'. (Actually, we could generalize even further, and think of numbers as constant functions, but this is quite silly, and it's better to just think of numbers like $\mathbb{Z}$ or $\mathbb{Q}$.) Let's look at three more examples.

Example 3. The functions $f : \mathbb{R} \to \mathbb{R}$ form a ring which we will (nonstandardly) name $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$. When we add two functions f and g, we get a new function $(f + g) : \mathbb{R} \to \mathbb{R}$ which takes $r \in \mathbb{R}$ to $f(r) + g(r)$. When we multiply two functions, f and g, we produce a new function $(f \cdot g) : \mathbb{R} \to \mathbb{R}$ where $(f \cdot g)(r) = f(r)g(r)$. We call this pointwise addition and pointwise multiplication, because the rule to add or multiply two functions is to add or multiply them at each point.

Example 4. The Gaussian integers are the subset of the complex numbers consisting of all complex numbers $\mathbb{C}$ with integer coefficients $\{a + bi | a, b \in \mathbb{Z}\}$. We write them as $\mathbb{Z}[i]$. The usual addition and multiplication of complex numbers apply.

Example 5. Modular arithmetic, $\mathbb{Z}/n\mathbb{Z}$, is a ring with the usual addition and multiplication.

Example 6. The two by two matrices with entries in the real numbers $\mathbb{R}$ form a ring, under matrix multiplication and addition.

1.2 Laying Down the Rules

Now that we've seen a bunch of examples, let's nail down a definition of ring.

Definition. A *ring*, R, is a set of objects along with two binary operations, $\cdot$ multiplication and $+$ addition, with the following properties:

1. Closure: if $a, b \in R$ then $a + b$ and $a \cdot b$ are in R.
2. Associativity: if $a, b, c \in R$ then $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Zero: there is an element $0 \in R$ such that for all $a \in R$, $a + 0 = 0 + a = a$.
4. One: there is an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.
5. Commutativity of Addition: if $a, b \in R$ then $a + b = b + a$.
6. Additive Inverses: for every $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.
7. Distributivity: for any $a, b, c \in R$ we have that $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.

One thing that might seem funny about these examples is that while we require addition to be commutative and have inverses, we don't require multiplication to be commutative or have inverses. We want to be able to work with rings that have a looser multiplicative structure: for example, we want our rings to model sets of functions, and one thing we notice about functions is that they don't always commute. The two by two matrices over $\mathbb{R}$ are are good simple example of a noncommutative ring. Also, in the case of rings of numbers, like our example $\mathbb{Z}$, many numbers don't have multiplicative inverses. The only integers which have multiplicative inverses are 1 and -1.

Remark. In this class, we will only work with commutative rings (rings where multiplication is commutative), but for the purpose of proving things in more generality, all of the proofs we do today will work whether or not we require our rings to be commutative.

1.3 Basic Properties of Rings

From the definition, we can deduce a few basic propositions. The goal in proving these is to say some facts about rings, but also to give you an example for how basic proofs in ring theory go.

Proposition 1. *The multiplicative identity* 1 *is unique.*

Proof. Suppose R is a ring with two multiplicative identities, 1 and $1'$. Then both of them satisfy the property that for all $r \in R$, $1r = r1 = r$ and $1'r = r1' = r$.

In particular, we can let $r = 1'$ in the first equation and then we get the identity $11' = 1'1 = 1'$ but in the second equation letting $r = 1$ we get $1'1 = 11' = 1$. This proves that $1 = 1'$. □

Proposition 2. *For any* $r \in R$, $0r = r0 = 0$.

Proof. We know that $0 + 0 = 0$ since 0 is the additive identity. So $r0 = r(0 + 0) = r0 + r0$. Adding $-(r0)$ to both sides (the additive inverse of $r0$, whatever it is!) we get that $0 = r0$. To get $0r = 0$ do the same thing with the other distributive equation. □

Proposition 3. *For any* $a, b \in R$ *we have* $(-a)b = a(-b) = -(ab)$.

Proof. First consider $(-a)b$. Then we know that $-a$ is the element such that $a + (-a) = 0$. So using distributivity we get that $(a + (-a))b = ab + (-a)b$ and also $(a + (-a))b = 0b = 0$ by the previous proposition. Therefore $ab + (-a)b = 0$. Let's add $-(ab)$ to both sides: we get $ab + (-a)b + (-(ab)) = -(ab)$ and we can commute the things on the left side to get $0 + (-a)b = -(ab)$ and so $(-a)b = -(ab)$. You will show on the homework that $a(-b) = -(ab)$ to complete the proof.

□

We're not going to be this explicit about associativity, zero, commutativity, and so on in the future, because it does get a little tedious. However, it's good to have a grounding in the basics.

2 Homework Day 1

2.1 The Basics

1. Prove that the additive identity 0 is unique. That is, if 0 and $0'$ are two elements of a ring R such that for all $r \in R$, $r+0 = 0+r = r$ and $0'+r = r+0' = r$ then $0 = 0'$.

2. Emulating the proof in class, show that $a(-b) = -(ab)$.

3. Convince yourself that each of the examples we talked about in class are actually rings. That is, go through the definition of ring, and verify any property that you aren't sure you believe. (For example: what is the identity in the ring of functions from $\mathbb{R}$ to $\mathbb{R}$?)

4. Show that additive identities are unique: that is, show that if $a+b = 0$ then $b = -a$.

5. Show that $(-1)(-1) = 1$.

2.2 Getting your hands dirty

1. Convince yourself that $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}$ is a ring. Most of the properties should be easy, but the closure under multiplication will require some justification.

2. Which elements in $\mathbb{Z}[x]$ have multiplicative inverses? What about $\mathbb{Q}[x]$? What about $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$?

3. Let X be a set and let $P(X)$ be the power set of X, that is, the set of all subsets of X. (For example, if $X = \{a, b, c\}$ then $P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$). Show that we can make $P(X)$ into a ring where if $Y, Z \in P(X)$ then $Y + Z = (Y - Z) \cup (Z - Y)$ and $Y \cdot Z = Y \cap Z$. What is the identity? What is $Y \cdot Y$ for any $Y \in P(X)$?

2.3 To ponder

1. Consider the power series ring $\mathbb{Q}[[x]]$ that consists of elements of the form $\sum_{n=0}^{\infty} a_n x^n$. What elements have multiplicative inverses? What is the inverse of the power series $1 + x$? Note that $\mathbb{Q}[x]$, the polynomials in x with rational coefficients, sits inside $\mathbb{Q}[[x]]$ and $1 + x \in \mathbb{Q}[x]$ but $1 + x$ is not a unit in $\mathbb{Q}[x]$. Deduce that if S is a subring of R then all of the units of S are units of R but not all of the units of R contained in S are also units of S.

3 Day 2

Consider the rings $\mathbb{Z}[x] = \{a_n x^n + \cdots + a_1 x + a_0 | a_i \in \mathbb{Z}\}$ and $\mathbb{Z}[y^2] = \{b_{2n} y^{2n} + b_{2n-2} y^{2n-2} + \cdots + b_2 y^2 + b_0 | b_{2i} \in \mathbb{Z}\}$. These two rings act and seem very much the same. In fact, we can make a one to one correspondence of objects in $\mathbb{Z}[x]$ with objects in $\mathbb{Z}[y^2]$ just by taking replacing each x with y^2, or vice verse. How do we quantify this notion of sameness? How can we in general talk about rings being the same?

Definition. We say two rings R and S are *isomorphic* if there is a bijective function $f : R \to S$ such that $f(a +_R b) = f(a) +_S f(b)$, $f(a \cdot_R b) = f(a) \cdot_S f(b)$, and $f(1_R) = 1_S$.

More generally, we can make analogies between rings by considering other functions from one ring to another.

Definition. A *ring homomorphism* from R to S is a map $f : R \to S$ such that $f(a +_R b) = f(a) +_S f(b)$, $f(a \cdot_R b) = f(a) \cdot_S f(b)$, and $f(1_R) = 1_S$.

Here, we're just relaxing the idea that it has to be a bijection. If our function is injective, then f gives us a way to situate R in S as a smaller ring, and if our function is surjective, we will see that f gives a way of grouping elements of R into "symmetry classes" so that S is R mod some symmetries. In math, we often look at homomorphisms to tell us more about the structure of a ring, rather than looking at the individual ring itself.

Example 7. Consider the map $f : \mathbb{Z}[x] \to \mathbb{Z}$ given by $p(x) \mapsto p(0)$. This just plucks out the constant term of the polynomial $p(x)$. This map is surjective but not injective. All the polynomials with no constant term get sent to 0.

Notice that if p and q are polynomials that get sent to 0 under f then $p + q$ and rp get sent to zero for any $r \in \mathbb{Z}[x]$.

Example 8. More generally, if we have a ring of functions like $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$, we can create a ring homomorphism which is evaluation of the functions at a point. For example, the ring of functions from $\mathbb{R} \to \mathbb{R}$ has a homomorphism $f_p : \mathrm{Fun}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ for each point $p \in \mathbb{R}$, sending $\phi : \mathbb{R} \to \mathbb{R}$ to $\phi(p)$. We can check that if $\phi : \mathbb{R} \to \mathbb{R}$ and $\psi : \mathbb{R} \to \mathbb{R}$ are elements of $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$, then $f_p(\phi + \psi) = (\phi + \psi)(p) = \phi(p) + \psi(p) = f_p(\phi) + f_p(\psi)$. Also $f_p(\phi \cdot \psi) = (\phi \cdot \psi)(p) = \phi(p)\psi(p) = f_p(\phi) f_p(\psi)$. Finally since the constant function $c_1 : \mathbb{R} \to \mathbb{R}$ is the multiplicative identity in $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$ we check $f_p(c_1) = c_1(p) = 1$.

Example 9. The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $a \mapsto a \mod n$.

Example 10. The map $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ given by $\sqrt{2} \mapsto -\sqrt{2}$ is an isomorphism.

Example 11. There are injective maps $\mathbb{Z} \to \mathbb{Z}[x]$ and $\mathbb{Z} \to \mathbb{Q}$ realizing $\mathbb{Z}$ as a smaller ring inside these rings.

Definition. More formally: a *subring* of a ring is a subset of a ring which is also a ring.

Definition. The *image* of a ring homomorphism $f : R \to S$ is the set of elements $s \in S$ such that there exists $r \in R$ with $f(r) = s$.

Definition. The *kernel* of a ring homomorphism $f : R \to S$ is the set of elements $r \in R$ such that $f(r) = 0$.

Let's go back and take a look at the image and kernel of the previous examples.

Notice that we can characterize being injective as having the kernel equal to 0, and surjective as having image equal to the target.

Proposition 4. *The kernel of a ring homomorphism $f : R \to S$ has the following properties:*

1. *If $r \in \ker(f)$ then for all $c \in R$, $cr \in \ker(f)$.*
2. *If $r, s \in \ker(f)$ then so is $r + s$.*
3. *$0 \in \ker(f)$.*

Proof. We'll start with $0 \in ker(f)$. Note that $f(0) = f(0+0) = f(0)+f(0)$, so subtracting $f(0)$ from both sides in S we see that $0 = f(0)$.

Then, consider $r \in \ker(f)$ and suppose c is any element of R. Then $f(cr) = f(c)f(r)$ because f is a homomorphism, and $f(r) = 0$ because r is in the kernel of f. Thus $f(cr) = f(c)f(r) = f(c)0 = 0$.

If $r, s \in \ker(f)$ then $f(r + s) = f(r) + f(s) = 0 + 0 = 0$ so $r + s \in \ker(f)$.

□

Definition. We call any subset I of a ring R satisfying:

1. If $r \in I$ then for all $c \in R$, $cr \in I$.
2. If $r, s \in I$ then so is $r + s$.
3. $0 \in I$.

an *ideal* of R.

Example 12. The subset $I = 2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. More generally, $a\mathbb{Z} = \{an | n \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. In fact, these are the kernels of $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. We write these as (n), where this notation denotes the ideal generated by n.

Example 13. The subset $\{0\}$ in R is always an ideal. So is R.

Example 14. Let $p \in \mathbb{R}$ and consider $M_p = \{f \in \text{Fun}(\mathbb{R}, \mathbb{R}) | f(p) = 0\}$. Then M_p is an ideal of $\mathbb{R}$ and there are no other ideals other than $\text{Fun}(\mathbb{R}, \mathbb{R})$ containing M_p.

Definition. We say $M \subset R$ is a *maximal ideal* of R if it is not contained in any proper ideals of R.

Example 15. The ideal (x) in $\mathbb{Z}[x]$ is all polynomials divisible by x. Similarly, for any element $p(x)$ we can create the ideal generated by $p(x)$ which will consist of all multiples of $p(x)$ and be denoted $(p(x))$. Another way of thinking of this notation is that $(a, b, c) \subset R$ is the smallest ideal containing the elements a, b, c. So it must contain all multiples as well as differences and sums.

4 Homework Day 2

4.1 The Basics

1. Let R be a commutative ring. A *field* is a commutative ring where every nonzero element has a multiplicative inverse. Show that $\{0\}$ is a maximal ideal of R if and only if R is a field. Hint: An ideal is a proper ideal if and only if it does not contain 1. Consider the ideals (a) for $a \in R$.

2. Which of the following are ideals of $\mathbb{Z}[x]$:

   (a) The set of all polynomials whose constant term is a multiple of 3.

   (b) The set of all polynomials whose x^2 term is a multiple of 3.

   (c) The set of all polynomials with no constant, x or x^2 term.

   (d) The set of polynomials whose coefficients sum to zero.

3. Show that if $I, J \subset R$ are ideals then so is $I \cap J$.

4. Show that if $\phi : R \to S$ is a ring homomorphism and J is an ideal of S then $\phi^{-1}(J) = \{r \in R | \phi(r) \in J\}$ is an ideal. If I is an ideal of R, is $\phi(I)$ necessarily an ideal of S?

5. Let I be an ideal of R. Suppose $r \in R$. Define $r + I = \{r + a | a \in I\}$. Show that $r + I = s + I$ as sets if and only if $r - s \in I$. (Hint, for one direction show that $r \in r + I$ and therefore $r \in s + I$ and use this to write an equation $r = s + a$ for $a \in I$.) Let $R = \mathbb{Z}$ and $I = 5\mathbb{Z}$. What is the set $m + 5\mathbb{Z}$ for $m = 1, 2, 5, 7$?

4.2 Getting your hands dirty

1. Show that $M_p \subset \text{Fun}(\mathbb{R}, \mathbb{R})$ defined as $M_p = \{f : \mathbb{R} \to \mathbb{R} | f(p) = 0\}$ is a maximal ideal of $\text{Fun}(\mathbb{R}, \mathbb{R})$ for each $p \in \mathbb{R}$.

2. Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. Describe the kernel and image.

3. What is the ideal $(4, 6)$ generated by the elements 4 and 6 in $\mathbb{Z}$? What about $(2, 3)$? What about (m, n)?

4.3 To ponder

1. Show that if $I_1 \subset I_2 \subset \ldots$ are ideals of a ring R then so is $\cup_{n=1}^{\infty} I_n$. Come up with an example of an inclusion of ideals $I_1 \subset I_2 \subset I_3 \subset \ldots$ such that $I_n \neq I_{n+1}$ for all n. (You will need to think of rings that we haven't talked about yet.)

2. Let R be a commutative ring. Then we denote $\mathfrak{N}(R)$ to be the nilradical of R, where $\mathfrak{N}(R) = \{r \in R | r^n = 0, \text{for some } n \in \mathbb{N}\}$ is the set of all nilpotent elements. Show that $\mathfrak{N}(R)$ is an ideal.

5 Day 3

Yesterday, we defined ideals and talked about how they arose from the kernel of ring homomorphisms. Today, we will talk about how, given an ideal I of R we can find a ring S and a ring homomorphism $\phi : R \to S$ where $I = \ker(\phi)$. To do this, we will construct S as a quotient ring R/I.

On the homework, for $r \in R$ and I an ideal of R, we constructed the set $r + I = \{r + a | a \in I\}$. For example, if $R = \mathbb{Z}$ and $I = 5\mathbb{Z}$ we computed that we have $0 + 5\mathbb{Z}$, $1 + 5\mathbb{Z}$, $2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$, and $4 + 5\mathbb{Z}$. If n is any other number then $n + 5\mathbb{Z} = (n \mod 5) + 5\mathbb{Z}$. For example, $7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$.

Recall from the homework that we have the following proposition:

Proposition 5. *The sets $r + I$ and $s + I$ are equal if and only if $r - s \in I$.*

Proof. We showed this by noting that if $r - s \in I$ then $r + I = r - s + s + I = \{r - s + s + a | a \in I\} = \{s + a | a \in I\}$ since $r - s + a \in I$ because I is closed under addition. Conversely, if the two sets are equal then $0 \in I$ implies $r \in r + I$ so $r \in s + I$ so $r = s + a$ for some $a \in I$ and so $r - s = a \in I$.

□

We would like to construct $S = R/I$ to be the set of $r + I$ for $r \in R$. In our example, $S = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$. For ease of notation, we often write $r + I$ as $[r]$, for example $S = \{[0], [1], [2], [3], [4]\}$ but we could just as easily say that $S = \{[5], [6], [7], [8], [9]\}$.

There is a natural way to define addition and multiplication on R/I. If $[r]$ and $[s]$ are in R/I then $[r] + [s] = [r + s]$ and $[r][s] = [rs]$. One thing we have to do when working with quotient rings is to check that if we defined something in terms of r and s that this operation is well defined, meaning that no matter which name we give to $[r]$ and $[s]$ we get the same answer for $[r] + [s]$.

For example, is $[0] + [6]$ the same as $[0] + [1]$? In our definition the first would be $[6]$ whereas the second would be $[1]$, but we know that $[6] = [1]$.

Proposition 6. *Addition and multiplication defined in this way on R/I are well defined.*

Proof. Suppose r, r' are two elements of $[r] = [r']$ and s, s' are both elements of $[s] = [s']$. Then we want to show that $[r + s] = [r' + s']$ On the homework, we showed that $r - r' \in I$ and $s - s' \in I$. Let's call these a and b. Then $(r + s) - (r' + s') = a + b \in I$ since I is closed under addition. Therefore by the some homework problem, we see that $[r + s] = [r' + s']$.

Now consider $[rs]$ and $[r's']$. We would like to show that $rs - r's' \in I$. Let's replace r' with $r - a$ and s' with $s - b$. Then $rs - r's' = rs - (r - a)(s - b) = rs - rs + as + bs + ab = as + bs + ab \in I$, since anything times a or b is in I, as $a, b \in I$. Therefore $[rs] = [r's']$.

□

This proposition showed us that it doesn't matter what name we give for these sets $r + I$, the operations on R/I are well defined. In fact, these operations turn R/I into a ring (if you don't believe it, take some time on the homework to test out each of the ring axioms.)

Note that there is a nice way to take elements of R to elements of R/I, by taking r to $r + I$.

Proposition 7. *The map $\phi : R \to R/I$ given by $r \mapsto r + I$ is a surjective ring homomorphism with kernel I.*

Proof. Clearly this map is surjective. Note that we actually defined R/I to make this into a ring homomorphism: suppose $r, s \in R$. Then $\phi(r + s) = [r + s] = [r] + [s] = \phi(r) + \phi(s)$ and similarly $\phi(rs) = [rs] = [r][s] = \phi(r)\phi(s)$. Check for yourself that $\phi(1) = [1]$ is the identity in R/I.

What's the kernel of ϕ? It's the set of $r \in R$ such that $[r] = [0]$, i.e. the set of $r \in R$ such that $r - 0 \in I$ or $r \in I$.

□

What's neat is that there is a sort of converse to this idea:

Proposition 8 (First Isomorphism Theorem)**.** *Suppose $\phi : R \to S$ is any ring homomorphism. Then $R/\ker(\phi)$ is isomorphic to $\phi(R)$ as rings.*

Proof. You!

□

Thus, every ideal is the kernel of a homomorphism and every kernel is an ideal, and we know exactly how that correspondence works.

Example 16. Let's use the quotient ring construction in one particular case, $\mathbb{Z}[x]/(x^2-2)$. Suppose $p(x)$ is any polynomial in $\mathbb{Z}[x]$. We can use polynomial long division (since $x^2 - 2$ has leading coefficient 1) to write $p(x) = r(x)+(x^2-2)q(x)$ for some polynomials $q(x), r(x)$ in $\mathbb{Z}[x]$ with the degree of $r(x)$ less than 2. Then we can see that $[p(x)] = [r(x)]$ since $p(x) - r(x) \in (x^2 - 2)$ is a multiple of $(x^2 - 2)$. Conversely, for any two polynomials $p(x)$ and $r(x)$ with degree less than 2, then $[p(x)] \neq [r(x)]$ because $p(x) - r(x)$ has degree less than 2, and cannot be in the ideal $(x^2 - 2)$ unless $p(x) - r(x) = 0$, as 0 is the only element of $(x^2 - 2)$ of degree less than 2. Therefore $p(x) = r(x)$.

So we can find equivalence class representatives by taking all of the elements of $\mathbb{Z}[x]$ less than degree 2: $\mathbb{Z}[x]/(x^2 - 2) = \{[a + bx] | a, b \in \mathbb{Z}\}$.

Let's do a few computations: $[x][x] = [x^2]$ and we can write $x^2 = 2 + x^2 - 2$ using division. Therefore $[x]^2 = [2]$.

This ring is actually the same as the ring $\mathbb{Z}[\sqrt{2}]$ because x acts as a root of the polynomial $x^2 - 2$. In general, taking polynomial rings mod an ideal is a nice way to construct new rings when we want to force x to act a certain way.

6 Homework Day 3

6.1 The Basics

1. Prove the proposition from class: if $\phi : R \to S$ is a homomorphism of rings then $R/\ker(\phi)$ is isomorphic to $\phi(R)$.

2. Show that if $I \subset R$ is an ideal of R and $1 \in R$ is the multiplicative identity then $[1]$ is the identity in R/I and $[0]$ is the additive identity. Find the additive inverse of $[a]$ for $a \in R$ and verify that this works for the toy example $\mathbb{Z}/5\mathbb{Z}$.

3. Describe the elements of $\mathbb{Z}[x]/(x)$. What ring homomorphism that we have discussed does this correspond to? What about $\mathbb{Z}[x]/(x-3)$?

4. Suppose R is a commutative ring and $M \subset R$ is a maximal ideal. Show that R/M is a field. Hint: on an earlier homework, you showed that $\{0\}$ is a maximal ideal of S if and only if S is a field. Combine this with another result from a previous homework that if $I \subset S$ is an ideal and $\phi : R \to S$ a ring homomorphism then $\phi^{-1}(I)$ is an ideal of R.

5. A prime ideal $P \subset R$ is an ideal of R such that if $a \cdot b \in P$ then $a \in P$ or $b \in P$ (or both!). Show that $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime. A domain is a ring S where for any $a, b, \in S$, $ab = 0$ implies $a = 0$ or $b = 0$. Show that R/P is a domain if and only if P is prime.

6.2 Getting your hands dirty

1. The ring $\mathbb{Z}[x]/(x^2+1)$ is a familiar ring. What ring is that?

2. Write out the multiplication table for $(\mathbb{Z}/3\mathbb{Z})[x]/(x^2+1)$. How many elements does this have? Note that this satisfies the field axioms, and is an example of a "finite field".

3. Suppose I want to construct a ring such that there is some element which is not zero but whose square is zero. What quotient of $\mathbb{Z}[x]$ would I take?

6.3 To ponder

1. What is the map $\mathrm{Fun}(\mathbb{R}, \mathbb{R}) \to \mathrm{Fun}(\mathbb{R}, \mathbb{R})/M_p$ where M_p is defined as before as the maximal ideal of functions $f : \mathbb{R} \to \mathbb{R}$ which are zero at p?

7 Day 4

7.1 Generating Ideals

Up until now, we've been playing a little fast and loose with the notation that we have been using for ideals. We have been writing ideals using their generators: for example, the ideal $\{2n|n \in \mathbb{Z}\} \subset \mathbb{Z}$ we write as (2), because it's in some sense the ideal generated by the element $2 \in \mathbb{Z}$. How does that work? Well, it's the smallest ideal that could possibly contain the element 2, because in order for an ideal of $\mathbb{Z}$ to contain 2, it would need to contain every $\mathbb{Z}$-multiple of 2, and in turn, the set of multiples is closed under addition and multiplication.

What about the ideal $(4, 6)$ in $\mathbb{Z}$, generated by the two elements 4 and 6? This means we want to find the smallest ideal containing 4 and 6. Certainly that ring should contain $\{4n|n \in \mathbb{Z}\}$ and $\{6n|n \in \mathbb{Z}\}$. But it also has to contain other elements, like 2, since we can write $2 = 6 - 4$, and thus if 6 and 4 are in my ideal, then so is 2. But then it must also contain all multiples of 2, that is, (2). However, no sum or product or sum of products of 4 and 6 will ever contain an odd number, so we can conclude $(4, 6) = (2)$. In this case, we started with an ideal generated by two elements, and did some work to show that it actually was generated by one element.

Warning! Not every ideal in every ring can be generated by the multiples of just one element of the ring. This is a little tricky, because in some rings like $\mathbb{Z}$ and $\mathbb{R}[x]$, it is true that every ideal is generated by one element, but it is easy to construct a ring in which this doesn't hold.

Example 17. Consider the ring $\mathbb{R}[x, y]$ polynomials in two variables with coefficients in $\mathbb{R}$. The ideal (x, y) is not generated by one element.

First of all, what is this ideal? It should be sums of multiples of x and y. But that's everything that you can write without a constant term. So $(x, y) = \{f(x, y)|f(0, 0) = 0\}$. Suppose that we did have a way of writing $(x, y) = (g)$ for some $g \in \mathbb{R}[x, y]$. Then $x \in (g)$ and $y \in (g)$ so we would have to have that both x and y were multiples of g. That would be impossible, unless g were an element of $\mathbb{R}$, but we know that (x, y) does not contain any element of $\mathbb{R}$ other than 0.

There are plenty more examples exactly like this: we could create ideals like $(x-2, y-3)$ and $(x - 1, y - 5)$ that are not generated by one element for exactly the same reason.

One more thing to note about generating ideals is that if you have two elements that differ by a unit (an invertible element of your ring) then they generate the same ideal. So, for example $(-2) = (2)$ in $\mathbb{Z}$ because -1 is a unit, with inverse -1. Or, in $\mathbb{R}[x]$, $(3x) = (x)$, since 3 is a unit with inverse $1/3$. In general, if R is a ring, $a \in R$ and $u \in R$ a unit, then $(ua) = (a)$ because $u^{-1}(ua) \in (ua)$ and so $a \in (ua)$, but clearly also $ua \in a$.

7.2 Maximal and Prime Ideals

Let's switch gears to talk about maximal and prime ideals. Recall from the last homework:

Definition. A *maximal ideal* M of R is an ideal which is not contained in any proper ideal.

Definition. A *prime* ideal P of R is an ideal such that whenever $ab \in P$, with $a, b \in R$, then $a \in P$ or $b \in P$ (or both.)

Example 18. Consider the ring $\mathbb{R}[x]$. What are the maximal ideals in this ring? Suppose we have an ideal generated by one element, $f(x) \in \mathbb{R}[x]$. Then $(f(x))$ is the ideal of all multiples of $f(x)$, that is, anything we can write as $m(x)f(x)$ for some $m(x) \in \mathbb{R}[x]$. When is this contained in another ideal? If $f(x)$ factors, say $f(x) = a(x)b(x)$ then the ideal $(a(x))$ contains $f(x)$, because $f(x)$ is a multiple of $a(x)$. That is, if $m(x)f(x)$ is an element of $(f(x))$, we can rewrite it as $m(x)a(x)b(x)$, to make it more obvious that $m(x)f(x) \in (a(x))$. This shows that $(f(x)) \subset (a(x))$ and therefore is not maximal. This both very easily generalizes to a proof that all maximal ideals are prime, and also suggests that if our ideal $(f(x))$ is going to be maximal, then $f(x)$ can't factor.

Example 19. What about the ring $\mathbb{C}[x]$? If you're familiar with the fundamental theorem of algebra, you might know that every polynomial factors if you're allowed to have coefficients over the complex numbers, so that if $f(x)$ is a degree n polynomial, we can write it as $A(x - r_1)(x - r_2)\dots(x - r_n)$ for $A, r_i \in \mathbb{C}$, like $3x^2 + 5 = 3(x + i5/\sqrt{3})(x - i5/\sqrt{3})$. Thus the only things that generate maximal ideals are polynomials of degree 1, which can't factor anymore. (Elements of $\mathbb{C}$ will generate the whole ring.)

The maximal ideals of $\mathbb{C}[x]$ are of the form $(x - a)$ for $a \in \mathbb{C}$ (since if we have a degree one polynomial like $(bx - c)$ we can divide by b and get $(x - c/b)$ which makes the same ideal.) So we get a bijection between maximal ideals of $\mathbb{C}[x]$ and points of the complex plane.

This is actually a very deep observation, and the connection between points and maximal ideals, as well as rings and functions, form the basis of modern algebraic geometry and radically transformed the ways that we do geometry around the end of the 1800s and into the beginning of the 1900s. For the remainder of the class, we will explore a little bit of this connection between ring theory and geometry, as a means to show one reason why mathematicians have developed a theory of rings.

7.3 Coordinate Rings

We've seen how rings can be interpreted as functions, and we can use this notion to develop a correspondence between rings and geometric objects. Some basic geometric objects that we are interested in studying are curves: things like the parabola, the ellipse, the hyperbola, the line, and more exotic things like cubic curves, and higher degree curves. For our purposes we will define a curve as follows.

Definition. A curve is the set of points in $\mathbb{R}^2$ satisfying the equation $f(x,y) = 0$ for some polynomial $f(x,y) \in \mathbb{R}[x,y]$.

Let's start with the hyperbola. The equation for the standard hyperbola is $y = 1/x$ or, to avoid dividing by x, we can write it as $xy - 1 = 0$. Already we have a familiar object living in a ring like $\mathbb{R}[x,y]$. What happens when we evaluate functions in $\mathbb{R}[x,y]$ on points of $xy - 1$? Consider the function $x + 2y + 4 \in \mathbb{R}[x,y]$. Then this takes a point $(2, 1/2)$ on the hyperbola, and adds two times the y-coordinate plus 4 to the x-coordinate to get $2 + 2/2 + 4 = 7$. Let's also consider the function $x + 2y + xy + 3$ and apply these to some points:

Hyperbola Point	$x + 2y + 4$	$x + 2y + xy + 3$
$(2, 1/2)$	7	7
$(3, 1/3)$	$7.\overline{6}$	$7.\overline{6}$
$(1/2, 2)$	8.5	8.5
$(-1, -1)$	1	1

Why are these two different functions giving us the same values when we apply them to points on the hyperbola? We can write $x+2y+xy+3 = x+2y+4+(xy-1)$. For every point on the hyperbola, $xy - 1 = 0$ so these have to be the same. So, when two functions in $\mathbb{R}[x,y]$ differ by a multiple of $(xy - 1)$ we can see that they will give the same values on the the hyperobola.

Therefore, if we only care about functions on our hyperbola, taking the curve to $\mathbb{R}$, then the functions are $\mathbb{R}[x,y]/(xy - 1)$, the equivalence classes of functions, up to adding a multiple of $(xy - 1)$, which we know doesn't change the value of the function. Suppose $f(x,y)$ is the equation for a curve. Then we would like the functions on $f(x,y)$ correspond to the ring $\mathbb{R}[x,y]/(f(x,y))$.

This is almost right, but there is a slight problem. What if we consider the curve $x^2 = 0$, which looks like just a copy of the y-axis? If we evaluate functions on the points of this curve, then the functions $x + y$ and $x^2 + y$ take on the same values (namely, just y) since $x^2 = 0$ implies $x = 0$, but in the ring $\mathbb{R}[x,y]/(x^2)$ these are two different equivalence classes. So, instead of taking the ideal (x^2) we should have taken the ideal (x), which really represents all of the functions which are zero on the points where $x^2 = 0$. In general, we will need to take $\sqrt{(f(x,y))}$ the radical of the ideal $f(x,y)$, to make sure we include all functions which are zero on the points of $f(x,y) = 0$.

Definition. We say an ideal $I \subset R$ is *radical* if whenever $a^n \in I$ for $n \in \mathbb{N}$, then $a \in I$. If I is an ideal, then the *radical of* I, denoted $\sqrt{I}$, is the smallest radical ideal containing I, which is the set $\{r | r \in R \text{ and } r^n \in I \text{ for some } n \in \mathbb{N}\}$.

With this we can define the coordinate ring.

Definition. Let $f(x,y) \in \mathbb{R}[x,y]$ and consider the curve $f(x,y) = 0$. Then the functions on this curve to $\mathbb{R}$ form a ring, called the *coordinate ring*, which is $\mathbb{R}[x,y]/\sqrt{(f(x,y))}$.

8 Homework Day 4

8.1 The Basics

1. Show that if $I \subset R$ is an ideal than what we defined as the radical of I, $\sqrt{I} = \{r | r \in R \text{ and } r^n \in I \text{ for some } n \in \mathbb{N}\}$, is actually an ideal of R containing I.

2. Exhibit an isomorphism between the coordinate ring of the parabola $y = x^2$ and the coordinate ring of the x-axis.

3. What are the maximal ideals of $\mathbb{Z}$?

4. For the sake of not giving you a very complicated definition, our notion of curve is a little sillier than most. For example, we allow a "curve" which consists of the points in the x or y-axis, i.e. $\{(x, y) | x = 0 \text{ or } y = 0\}$. What is the equation of this curve? Can you think of a curve that only has two points in it?

   (To avoid this non-intuitive definition, some people define curve to be the set of pairs of complex numbers satisfying a polynomial which doesn't factor, or the zeroes in $\mathbb{R}^2$ of a polynomial which doesn't factor and has infinitely many points in $\mathbb{R}^2$. Both of these will lead to more familiar shapes.)

5. If you missed this problem on the previous homework, use your improved understanding of generators and ideals to compute the elements of the ideal $(8, 6) \subset \mathbb{Z}$ and write it as an ideal with one generator. Do this also with $(10, 15)$ and predict the answer with (m, n).

8.2 Getting your hands dirty

Catch up on any past homework problems (especially from yesterday) that you haven't done, or just take some time to think about the ideas from class.

8.3 To ponder

1. Some ideals aren't finitely generated, for example, the ring of polynomials $\mathbb{R}[x_1, x_2, x_3, \dots]$ in infinitely many variables $x_i, i \in \mathbb{N}$ has the ideal $(x_1, x_2, x_3, \dots)$ which is not finitely generated. A ring in which every ideal is finitely generated is called *Noetherian*. Show that if R is a Noetherian ring then any chain of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ must be finite.

9 Day 5

Yesterday, we left off by defining the coordinate ring of a curve, which we said was the ring of distinct polynomial functions on the curve $\mathbb{R}[x,y]/\sqrt{(f(x,y)}$ where we are thinking of $\sqrt{(f(x,y)}$ as the ideal of functions which are zero on the curve $f(x,y)=0$.

So, we have found a way to associate a ring to a curve, but this would be more useful if we knew the ring encoded other information about the curve. It's hopeless to think that the ring completely defines the curve and vice verse: on the homework, we saw that even though the parabola and the x-axis are different curves, they have isomorphic coordinate rings.

In fact, we can make ring-like objects which completely encapsulate the geometric information about the curves we care about. This was a major innovation of 20th century algebraic geometry pioneered by Grothendieck. He showed that something called "locally ringed spaces" can be assigned to geometric objects which contain almost all of the data that we care about. The basic idea that for any geometric object, like a curve, or a hypersurface, or something which we have glued together which is locally the zero-set of polynomials in n-dimensions, we can assign a topology, or notion of closeness/far awayness, and to every neighborhood of the space we can assign a ring which consists of the functions of the geometric object on that neighborhood. At each point, we assign a special kind of ring, called a local ring, which only has one maximal ideal, corresponding to the functions that are zero at that point.

Today, though, we're going to try to show the correspondence between algebra and geometry in the two most important properties of a curve: points on the curve (which will correspond to maximal ideals) and maps between curves (which will correspond to maps between rings.)

9.1 Points and Maximal ideals

Let's start with something simple though. One basic thing we might hope to do is encode the information of what points are on the curve. Let's consider the hyperbola $xy-1=0$ and the point $(2,1/2)$. Earlier this week, we talked about the evaluation homomorphism for rings of functions. In this case it takes a function $g(x,y)\in\mathbb{R}[x,y]/(xy-1)$ and evaluates it at a the point $(2,1/2)$. This gives us a map $\phi_{(2,1/2)}:\mathbb{R}[x,y]/(xy-1)\to\mathbb{R}$. But we can turn that data of the map $\phi_{(2,1/2)}$ into something more intrinsic to our coordinate ring: the kernel, which is an ideal of the coordinate ring.

What is the kernel in this case? Let's call it $M_{(2,1/2)}$. It's any function $g(x,y)$ such that $g(2,1/2)=0$. Let's figure out what functions are in this ideal. First of all, any polynomial which is divisible by $x-2$ must be in here, and similarly $y-1/2$. So our ideal $M_{(2,1/2)}\supseteq(x-2,y-1/2)$. But let's think about what happens when we take the quotient $\mathbb{R}[x,y]\mapsto\mathbb{R}[x,y]/(x-2,y-1/2)$. This is like setting $x=2$ and $y=1/2$, so it's exactly the evaluation homomorphism.

Note that $(x-2)(y-1/2) = xy+1-1/2x-2y$, and $xy+1-1/2x-2y+1/2(x-2) = xy-2y$ and finally $xy-2y+2(y-1/2) = xy-1$ so the ideal $(xy-1) \subset (x-2, y-1/2)$. But, we should have predicted that because $(xy-1)$ is the ideal of polynomial functions which are zero on the whole curve $xy-1$, while $(x-2, y-1/2)$ is the ideal of functions which are zero on the point $(2, 1/2)$, and since $(2, 1/2)$ is a point on the curve $xy-1$, any function in the first ideal must be in the second. However, it's nice to see this algebraically.

So we have a series of maps where we take

$$\mathbb{R}[x,y] \to \mathbb{R}[x,y]/(xy-1) \to \mathbb{R}[x,y]/(x-2, y-1/2)$$

first, sending all the functions which are zero on $xy-1$ to zero, then sending all functions which are zero on the point $(2, 1/2)$ to zero. We had to check that this made sense, that the first ideal was contained in the second, so that it makes sense to take successive quotients.

In general, if (a, b) is a point on our curve $f(x, y) = 0$, we can look at the maximal ideal $M_{(a,b)} = (x-a, x-b)$ in the coordinate ring $\mathbb{R}[x,y]/\sqrt{(f(x,y))}$ and we get a way of turning points of our curve into maximal ideals. (Note that this correspondence isn't exact: in general, there will be some maximal ideals of $\mathbb{R}[x,y]/\sqrt{(f(x,y))}$ which do not correspond to points, and this comes from the fact that we are working over $\mathbb{R}^2$ and that means we're missing some points that we can't see because they lie in $\mathbb{C}^2$. In the case where we look at $\mathbb{C}$ instead of $\mathbb{R}$, we get an exact correspondence between maximal ideals and points.)

9.2 Functions between curves

Suppose we have a map from one curve to another. Is there a way we can turn this into a map between the rings? Let's take, for example, the map π from the hyperbola to the x-axis, where we project down, taking $(a, b) \mapsto (a, 0)$. This seems like a nice map which respects the geometric properties of the two curves: points that are near each other on the hyperbola go to points that are near each other on the x-axis. We would like such a map to induce a map on the coordinate rings.

First, what are the coordinate rings? The coordinate ring for the hyperbola is $\mathbb{R}[x,y]/(xy-1)$ and the coordinate ring for the x-axis is $\mathbb{R}[x,y]/(y)$ (because the x-axis is cut out by the equation $y = 0$, as unfortunate a name as that is.)

Now, the slightly strange thing about the correspondence we're about to exhibit is that the map is going to go backwards: that is, we have a geometric map from the hyperbola to the x-axis, but our map of rings is going to go from the coordinate ring of the x-axis to the coordinate ring of the hyperbola. Why? Well, let's think about what these rings represent: functions from the curve to $\mathbb{R}$. If I have a function g from the x-axis to $\mathbb{R}$, how can I construct a function from the hyperbola to $\mathbb{R}$? Well, for any point on the hyperbola, I can simply map it to the x-axis using π, and then use g to map it to $\mathbb{R}$. So g in $\mathbb{R}[x,y]/(y)$ corresponds to $g \circ \pi \in \mathbb{R}[x,y]/(xy-1)$.

Remark. We're sweeping a lot under the rug here! How do we know that $g \circ \pi$ is even a polynomial? Well, π takes (a, b) to $(a, 0)$ and then g is a polynomial in x and y. So when we compose, g we plug $(a, 0)$ into g instead of (a, b), so it is the same as taking g and letting $y = 0$ everywhere.

Definition. Suppose that $\pi : C \to C'$ is any "nice" map of curves, $C : f(x, y) = 0$ and $C' : f'(x, y) = 0$. Then we get a ring homomorphism $\pi^* : \mathbb{R}[x, y]/\sqrt{(f'(x, y))} \to \mathbb{R}[x, y]/\sqrt{(f(x, y)}$ which is given by $\pi^*(g) = g \circ \pi$ precomposing with π.

Let's do an example using our hyperbola projecting to the x-axis map. Consider the function $g(x, y) \in \mathbb{R}[x, y]/(y)$ which is $g(x, y) = 2x + y - 1$. Where does this go under the map π? Well we just precompose with π: so $g \circ \pi(x, y) = g(x, 0) = 2x - 1$. Now if $(2, 1/2)$ is a point on the hyperbola, it goes to $4 - 1 = 3$, or, instead, if we first mapped it to the x-axis point $(2, 0)$, then we could apply g to get $4 + 0 - 1 = 3$.

Where do the functions x and y in $\mathbb{R}[x, y]/(y)$ go? Well, $x \mapsto x$ and $y \mapsto 0$ according to our calculations. So if we want to describe the image of the map π^* we can see that $\pi^* : \mathbb{R}[x, y]/(y) \to \mathbb{R}[x, y]/(xy - 1)$ has image which is just all polynomials which are only in x.